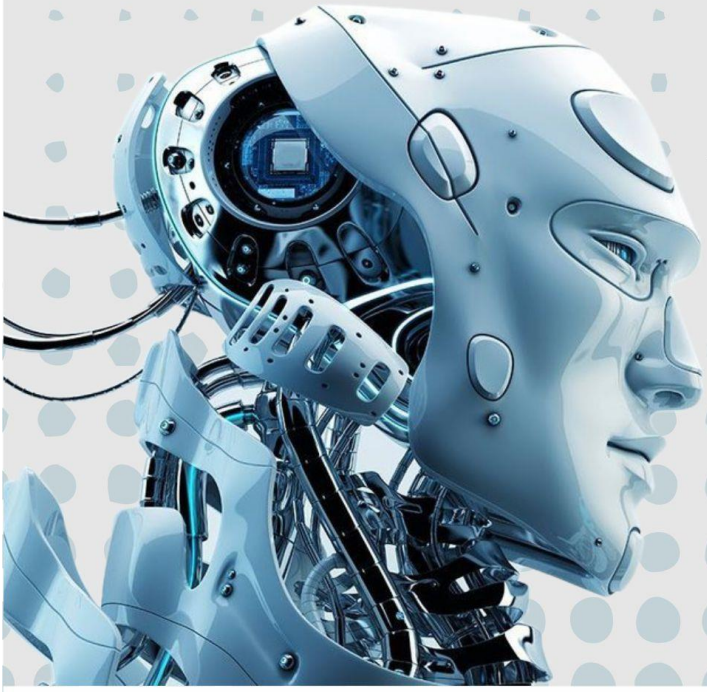
Проблемы борьбы с преступностью в условиях цифровизации: теория и практика



Сборник статей
XVIII Международной
научно-практической
конференции

«Уголовно-процессуальные
и криминалистические
чтения на Алтае»

Выпуск XVI

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: ТЕОРИЯ И ПРАКТИКА

Сборник статей XVIII Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае»

Выпуск XVI

Барнаул
Издательство
Алтайского государственного
университета
2020

УДК 343:004(08)
ББК 67.51с51я431
П 781

Ответственные редакторы:
С.И. Давыдов, *доктор юридических наук, заведующий кафедрой уголовного процесса и криминалистики*
В.В. Поляков, *кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики*

П 781 **Проблемы борьбы с преступностью в условиях цифровизации: теория и практика** : сборник статей XVIII Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае». — Вып. XVI / Министерство науки и высшего образования РФ, Алтайский государственный университет ; отв. ред. С.И. Давыдов, В.В. Поляков. — Барнаул: Изд-во Алт. ун-та, 2020. — 276 с.

ISBN 978-5-7904-2506-6.

В сборник включены статьи участников тематической XVIII Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае», посвященной особенностям противодействия преступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами в условиях цифровизации общества. Авторами публикаций являются ученые, преподаватели, сотрудники правоохранительных органов, аспиранты из России (более чем 20 городов — Барнаул, Владимир, Волгоград, Воронеж, Калининград, Кемерово, Красноярск, Москва, Омск, Орел, Санкт-Петербург, Саратов, Челябинск и др.), а также ученые из Украины, Белоруссии, Сербии.

Предназначено для ученых, преподавателей, сотрудников правоохранительных органов, аспирантов и студентов учебных заведений юридического профиля.

УДК 343:004(08)
ББК 67.51с51я431

ISBN 978-5-7904-2506-6

© Оформление. Издательство Алтайского государственного университета, 2020
© Коллектив авторов, 2020

СОДЕРЖАНИЕ

ПЛЕНАРНЫЕ ДОКЛАДЫ 9

Давыдов С.И., *д.ю.н., заведующий кафедрой уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул,* ***Моляров Е.А.,*** *адъюнкт Барнаульского юридического института МВД России, г. Барнаул,* ***Шмидт А.А.,*** *к.ю.н., начальник кафедры оперативно-разыскной деятельности ОВД Барнаульского юридического института МВД России, г. Барнаул*

О проведении оперативно-розыскного мероприятия «отождествление личности» с использованием сети Интернет 9

Зуев С.В., *д.ю.н., заведующий кафедрой правоохранительной деятельности и национальной безопасности Южно-Уральского государственного университета, г. Челябинск*

Цифровая уголовно-процессуальная политика 11

Комаров И.М., *д.ю.н., заведующий кафедрой криминалистики МГУ им. М.В. Ломоносова, г. Москва*

Некоторые проблемные вопросы «цифровизации» в криминалистике 18

Козлов В.Е., *к.ю.н., Академия МВД Республики Беларусь, г. Минск*

Об отдельных аспектах криминалистического и оперативно-технического обеспечения противодействия преступлениям, совершаемым с использованием средств компьютерной техники 20

Кучин О.С., *д.ю.н., профессор кафедры судебных экспертиз и криминалистики Российского государственного университета правосудия, г. Москва*

О некоторых тенденциях развития мировой криминалистики 26

Мещеряков В.А., *д.ю.н., Воронежский государственный университет, г. Воронеж,* ***Цурлуй О.Ю.,*** *к.ю.н., Центральный филиал Российского государственного университета правосудия, г. Воронеж*

Некоторые вопросы фиксации и изъятия компьютерной информации с цифровых носителей при производстве отдельных следственных действий 30

Милич И.Д., *ассистент кафедры уголовного права Юридического факультета Государственного университета в г. Нови-Сад, Республика Сербия, г. Нови-Сад*

Пришло ли время для нового уголовного наказания в Республике Сербия — запрета доступа в Интернет? 37

Поляков В.В., *к.ю.н., доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул,*

Алгоритмизация разрешения криминалистических ситуаций при расследовании высокотехнологичных преступлений 41

Федюнин А.Е., *д.ю.н., профессор кафедры уголовного процесса Саратовской государственной юридической академии, г. Саратов,* ***Н.М. Перетятько,*** *к.ю.н., доцент кафедры уголовного процесса Саратовской государственной юридической академии, г. Саратов,* ***Алферов В.Ю.,*** *к.ю.н., доцент кафедры правосудия и правоохранительной деятельности Саратовского социально-экономического института (филиал) РЭУ им. Г.В. Плеханова, г. Саратов*

Вопросы правового регулирования оперативно-розыскного мероприятия (наблюдение) с использованием информационно-телекоммуникационных технологий при раскрытии и расследовании преступлений 45

РАЗДЕЛ 1. ПРОБЛЕМЫ КВАЛИФИКАЦИИ, КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ 51

Ермаков М.Г., *к.ю.н., старший преподаватель кафедры криминалистики Омской академии МВД России, г. Омск*

«Телефонное» мошенничество 51

Иващенко М.А., *младший научный сотрудник Научно-исследовательского института Московской академии Следственного комитета РФ, аспирант Московской академии Следственного комитета РФ, г. Москва*

Проблемы квалификации экстремистских преступлений, совершенных в сети Интернет 55

Кучина Я.О., *к.ю.н., LL.M., докторант Университета Макао (Макао, САР КНР), профессор РАЕ*
Некоторые особенности объекта преступления в ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» 60
Мазуров В.А.*, к.ю.н., доцент кафедры уголовного права и криминологии Алтайского государственного университета, г. Барнаул,* ***Стародубцева М.А.,*** *преподаватель Алтайского государственного университета, г. Барнаул*
О некоторых аспектах международного сотрудничества в сфере противодействия кибертерроризму..... 63
Савчук Т.А.*, к.ю.н., доцент кафедры правового обеспечения правоохранительной деятельности Академии управления при Президенте Республики Беларусь, г. Минск,* ***Городецкая М.А.,*** *магистр юридических наук, старший преподаватель кафедры правового обеспечения правоохранительной деятельности Академии управления при Президенте Республики Беларусь, г. Минск*
Обзор национальной ситуации по противодействию киберпреступности в Республике Беларусь 68
Симонова С.С., *к.ю.н., доцент кафедры уголовного права, уголовного процесса и криминалистики Волгоградского института управления (филиал РАНХиГС), г. Волгоград*
Криминологическая характеристика и особенности предупреждения преступлений, совершаемых с применением информационных технологий в период Covid-19 74
Поляков В.В., *к.ю.н., доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул,* ***Толстошеев С.Н.,*** *начальник отдела «К» ГУВД МВД России по Алтайскому краю, г. Барнаул*
Некоторые проблемы теории и практики расследования преступлений, предусмотренных статьей 273 УК РФ..... 78

РАЗДЕЛ 2. КРИМИНАЛИСТИЧЕСКОЕ И ОПЕРАТИВНО-РОЗЫСКНОЕ ОБЕСПЕЧЕНИЕ УГОЛОВНОГО СУДОПРОИЗВОДСТВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ 82
Драпезо Р.Г., *старший преподаватель кафедры уголовного процесса и криминалистики Кемеровского государственного университета, г. Кемерово*
Оперативно-разыскная характеристика «наемного факела» в сети Интернет с некоторыми элементами тактики 82
Емельяненко Д.В., *аспирант кафедры уголовного процесса и криминалистики Алтайского государственного университета, директор АНО «Сибирский центр судебной экспертизы и криминалистики», г. Барнаул*
Проблемы соблюдения тайны коммуникации при назначении судебной компьютерно-технической экспертизы 88
Ерина К.А., *преподаватель кафедры уголовно-процессуального права и криминалистики юридического факультета ВЮИ ФСИН России, г. Владимир*
Использование информационных технологий в целях получения показаний при расследовании преступлений 92
Иванова И.Г., *к.ю.н., доцент кафедры уголовного процесса и криминалистики Юридического института Сибирского федерального университета, г. Красноярск*
Некоторые проблемы назначения и производства судебной компьютерно-технической экспертизы мобильных телефонов..... 95
Ищенко П.П., *к.ю.н., старший преподаватель кафедры организации судебной и прокурорско-следственной деятельности Московского государственного юридического университета им. О.Е. Кутафина, г. Москва*
Хватит ли «интеллектуальным агентам» искусственного интеллекта, чтобы заменить следователя? 98
Калюжный А.Н., *к.ю.н., сотрудник Академии Федеральной службы охраны Российской Федерации, г. Орел*
Тактические особенности производства осмотра данных, обнаруженных на электронных носителях по делам о посягательствах на свободу личности..... 103

Кондратьев В.М., *адъюнкт кафедры оперативно-разыскной деятельности в ОВД Санкт-Петербургского университета МВД России, г. Санкт-Петербург, заместитель начальника Управления по контролю за оборотом наркотиков ГУ МВД России по Кемеровской области, г. Кемерово*

Некоторые особенности оперативно-розыскного выявления, пресечения и раскрытия незаконного сбыта наркотических средств, совершаемого с использованием информационно-телекоммуникационных технологий 107

Королева Е.А.*, аспирант кафедры криминалистики Московской академии Следственного комитета РФ, старший следователь отдела по расследованию особо важных дел следственного управления по Западному административному округу Главного следственного управления Следственного комитета РФ в г. Москве, г. Москва*

Особенности расследования половых преступлений, совершенных несовершеннолетними с использованием цифровых технологий 113

Космодемьянская Е.Е., *к.ю.н., доцент кафедры криминалистики Сибирского юридического института МВД России, доцент кафедры уголовного процесса и криминалистики Юридического института СФУ, г. Красноярск,* ***Межинский Е.А.,*** *слушатель Сибирского юридического института МВД России, г. Красноярск*

Возможности использования информационно-телекоммуникационных технологий в раскрытии и расследовании корыстно-насильственных преступлений, совершенных в условиях неочевидности 117

Кузнецов А.А., *к.ю.н., профессор кафедры криминалистики Омской академии МВД России, г. Омск,* ***Макаров Р.А.,*** *начальник отдела по расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий следственного управления Управления Министерства внутренних дел Российской Федерации по городу Кургану, г. Курган*

Основные элементы криминалистической характеристики хищений, совершенных дистанционно с использованием средств сотовой связи 123

Курин А.А., *к.т.н., доцент кафедры криминалистики Волгоградской академии МВД России, г. Волгоград*

Криминалистическая регистрация как интегрирующее звено в системе информационного обеспечения раскрытия и расследования преступлений 128

Лютынский А.М., *к.ю.н., доцент кафедры уголовного процесса и криминалистики Северо-Западного института Университета им. О.Е. Кутафина (МГЮА), г. Вологда,* ***Селякова А.В.,*** *помощник прокурора г. Вологды, г. Вологда*

Особенности доказывания некоторых обстоятельств присвоения в сфере ЖКХ в контексте цифровизации 134

Машлякевич В.А., *старший преподаватель Барнаульского юридического института МВД России, г. Барнаул*

Некоторые вопросы взаимодействия следователей с оперативными подразделениями на этапе предварительной проверки материалов по делам о мошенничествах, совершаемых с использованием средств телефонной связи 137

Менжега М.М., *к.ю.н., доцент кафедры криминалистики Саратовской государственной юридической академии, г. Саратов,* ***Хижняк Д.С.,*** *д.ю.н., доцент, профессор кафедры криминалистики Саратовской государственной юридической академии, г. Саратов*

К вопросу о криминалистической классификации транснациональных киберпреступлений 141

Лавнов М.А., *к.ю.н., доцент кафедры уголовного процесса Саратовской государственной юридической академии, г. Саратов,* ***Овчинникова Н.О.,*** *к.ю.н., доцент кафедры уголовного процесса Саратовской государственной юридической академии, г. Саратов*

Уголовно-процессуальное доказывание по делам о киберпреступлениях 143

Лазарева Л.В., *д.ю.н., профессор кафедры уголовно-процессуального права и криминалистики Владимирского юридического института ФСИН России, г. Владимир*

О доказывании преступлений в сфере информационных технологий с использованием специальных знаний 149

Меркулова М.В., *к.ю.н., старший преподаватель кафедры криминалистики Московского университета МВД России имени В.Я. Кикотя, г. Москва*

О некоторых проблемах осмотра персонального компьютера 153

Моляров Е.А., *адъюнкт кафедры оперативно-розыскной деятельности ОВД Барнаульского юридического института МВД России, г. Барнаул*

Особенности отождествления личности в оперативно-розыскной деятельности с использованием информационно-поисковых систем 156

Неупокоева И.А., *к.ю.н, доцент кафедры криминалистики Омской академии МВД России, г. Омск*

Современный подход к криминалистической характеристике незаконного сбыта наркотических средств и психотропных веществ через сеть Интернет 158

Поддубный И.В., *адъюнкт кафедры ОРД ОВД Орловского юридического института МВД России имени В.В. Лукьянова, г. Орел*

Некоторые аспекты проведения оперативно-розыскного мероприятия «опрос» при раскрытии дистанционных хищений с банковских карт 162

Псарева Б.В., *к.ю.н., доцент кафедры ГМУ и права Рубцовского института (филиал) Алтайского государственного университета, г. Рубцовск,* ***Пирова С.А.,*** *студентка Рубцовского института (филиал) Алтайского государственного университета, г. Рубцовск*

Юристы-боты и правовая помощь 165

Репин М.Е., *судебный пристав специализированного отдела оперативного дежурства Управления ФССП России по Нижегородской области, г. Нижний Новгород*

Уголовно-процессуальные проблемы доказывания отдельных видов преступной деятельности в сфере информационных технологий 170

Ряполова Я.П., *к.ю.н., доцент кафедры уголовного процесса и криминалистики Юго-Западного государственного университета, г. Курск*

Правовой режим использования технических средств и технологий в доказательственной деятельности на этапе возбуждения уголовного дела 176

Смирнов А.А., *аспирант кафедры криминалистики Московской академии СК РФ, руководитель отдела криминалистики СУ СК РФ по Липецкой области, полковник юстиции, г. Липецк*

Аспекты генезиса криминалистических знаний об информационных технологиях при совершении преступлений 180

Соколов А.Б., *к.ю.н., доцент кафедры криминалистики Омской академии МВД России, г. Омск*

Понятие и структура криминалистической характеристики неправомерного доступа к компьютерной информации 184

Сысенко А.Р., *к.ю.н., доцент кафедры криминалистики Омской академии МВД России, г. Омск,* ***Герасименко Н.И.,*** *к.ю.н., старший преподаватель кафедры криминалистики Омской академии МВД России, г. Омск*

Особенности подготовительного этапа осмотра информационной среды в сети Интернет 188

Цахуев А.В., *старший преподаватель кафедры уголовного процесса и криминалистики Юридического института Дагестанского государственного университета, эксперт отдела криминалистики следственного управления Следственного комитета Российской Федерации по Республике Дагестан, г. Махачкала*

Особенности доказывания приготовления к участию в незаконных вооруженных формированиях и международных террористических организациях за пределами Российской Федерации 190

Ширяев А.В., *аспирант кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*

Классификация следов мошенничества в сфере компьютерной информации 193

Шишов В.В., *к.ю.н., преподаватель кафедры уголовного процесса Московского университета МВД России им. В.Я. Кикотя, г. Москва*

О необходимости совершенствования использования технологий удаленной биометрической идентификации личности сотрудниками органов внутренних дел 198

Яковец Е.Н., *д.ю.н., заслуженный юрист РФ, в/ч 2462, ведущий научный сотрудник, г. Москва*

Использование информационных технологий на государственной границе Российской Федерации 200

РАЗДЕЛ 3. УГОЛОВНО-ПРОЦЕССУАЛЬНАЯ ДЕЯТЕЛЬНОСТЬ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ 207

Климова Я.А., *к.ю.н., старший преподаватель кафедры административной деятельности и охраны общественного порядка Волгоградской академии МВД России, г. Волгоград*

Особенности осуществления прокурором надзора за расследованием уголовных дел в сфере компьютерных преступлений 207

Латынская Ю.С., *помощник мирового судьи Вологодской области по судебному участку № 59, г. Харовск*

Возбуждение уголовного дела частного обвинения в контексте цифровизации 209

Попова И.П., *к.ю.н., доцент кафедры уголовного процесса Восточно-Сибирского института МВД России, председатель Усть-Илимского городского суда Иркутской области в почетной отставке, г. Иркутск*

К вопросу доказывания в уголовном судопроизводстве в аспекте цифровизации и использования информационных технологий 212

Смолин А.В., *преподаватель кафедры криминалистики Нижегородской академии МВД России, г. Нижний Новгород*

Уголовно-процессуальная природа электронного доказательства 215

Соколов А.С., *старший преподаватель кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул,* ***Поволотцкий А.Ю.,*** *преподаватель кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул,* ***Мухортов Р.А.,*** *магистрант Алтайского государственного университета, г. Барнаул*

Особенности расследования преступлений в сфере компьютерной информации, совершенных с участием несовершеннолетних 219

Умнягина Ю.А., *адъюнкт Нижегородской академии МВД России, г. Н. Новгород*

Проблемы соблюдения прав участников уголовного судопроизводства при получении сведений с электронных носителей информации 222

РАЗДЕЛ 4. ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ 226

Баев М.О., *д.ю.н., заведующий кафедрой криминалистики Воронежского государственного университета, г. Воронеж*

К вопросу о видах риска в деятельности защитника по уголовном делам 226

Власова С.В., *к.ю.н., профессор кафедры уголовного процесса Нижегородской академии МВД России, г. Нижний Новгород*

К вопросу о модернизации полномочий прокурора в контексте обвинительной власти 230

Грачёва О.А., *к.ю.н., доцент кафедры прокурорского надзора и криминологии Саратовской государственной юридической академии, г. Саратов*

К вопросу об унификации поводов к проведению прокурором проверки в досудебном производстве по уголовным делам 234

Ильин Н.Н., *к.ю.н., заведующий кафедрой судебно-экспертной и оперативно-разыскной деятельности Московской академии Следственного комитета Российской Федерации, г. Москва*

Использование специальных знаний при работе с электронным оборудованием транспортных средств 236

Корж В.П., *д.ю.н., профессор кафедры уголовного процесса, криминалистики и экспертологии Харьковского национального университета внутренних дел МВД Украины, почетный работник прокуратуры Украины, г. Харьков*

Коррупционные технологии организованной преступной деятельности в сфере экономики..... 239

Куркова Н.А., *к.ю.н, доцент кафедры уголовного процесса, криминалистики и правовой информатики Балтийского федерального университета им. И. Канта, г. Калининград,* ***Макарова О.А.,*** *к.ю.н., доцент кафедры уголовного процесса, криминалистики и правовой информатики Балтийского федерального университета им. И. Канта, г. Калининград*

Проблема оценки показаний свидетелей в судебном следствии 243

Лифанова Л.Г., *к.ю.н., доцент, профессор кафедры криминалистики Ставропольского филиала Краснодарского университета МВД России, г. Ставрополь*

Отдельные проблемы производства следственных действий с участием несовершеннолетних на первоначальном этапе расследования..... 248

Маркелов А.Г., *к.ю.н., доцент кафедры уголовно-правовых дисциплин Чувашского государственного университета им. И.Н. Ульянова, г. Чебоксары*

Качественное уголовное судопроизводство в особом (компромиссном) порядке принятия судебного решения при согласии лица с предъявленным ему обвинением 252

Марфицин П.Г., *д.ю.н., профессор кафедры уголовного права и процесса ННГУ им. Н.И. Лобачевского, г. Н. Новгород*

УПК РФ об иных процессуальных действиях 256

Мешков В.М., *д.ю.н., профессор кафедры криминалистики Калининградского филиала Санкт-Петербургского университета МВД России, заслуженный юрист России, г. Калиниград*

Проблемы допустимости использования сведений, полученных оперативно-розыскным путем, в доказывании по уголовному делу..... 259

Мигунов О.С., *старший преподаватель кафедры криминалистики Барнаульского юридического института МВД России, г. Барнаул*

К вопросу об использовании криминалистических учетов при расследовании преступлений, связанных с применением огнестрельного оружия ограниченного поражения 264

Мунгалов Е.А., *к.б.н., старший преподаватель кафедры криминалистики Барнаульского юридического института МВД России, г. Барнаул*

Об опыте проведения сравнительных исследований единичных волокон и перчаток, изъятых с места происшествия 267

Сильнов М.А., *доцент кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации, г. Москва*

К вопросу о цели уголовно-процессуального доказывания 269

ПЛЕНАРНЫЕ ДОКЛАДЫ

С.И. Давыдов, *д.ю.н., заведующий кафедрой уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*
Е.А. Моляров, *адъюнкт Барнаульского юридического института МВД России, г. Барнаул*
А.А. Шмидт, *к.ю.н., начальник кафедры оперативно-разыскной деятельности ОВД Барнаульского юридического института МВД России, г. Барнаул*

О ПРОВЕДЕНИИ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ОТОЖДЕСТВЛЕНИЕ ЛИЧНОСТИ» С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Современный период активного развития информационных технологий и цифровой трансформации характеризуется появлением новых возможностей и для правоохранительных органов в сфере борьбы с преступностью. Изучение деятельности оперативных подразделений показало, что при проведении отдельных оперативно-розыскных[1] мероприятий (далее — ОРМ), включая «отождествление личности», все чаще используются биометрические технологии, электронные банки данных, интернет-технологии, технологии видеоидентификации и т.д. При этом изучение научной и учебной литературы показало, что вопросы проведения отождествления личности с применением таких технологий на сегодняшний день освещены достаточно слабо. Целенаправленных научных исследований, посвященных особенностям проведения указанного ОРМ с использованием сети Интернет, пока не проводилось.

В действующем Федеральном законе «Об оперативно-розыскной деятельности», принятом в Российской Федерации в 1995 г., понятие отождествления личности как оперативно-розыскного мероприятия не содержится. Вместе с тем Модельный закон Содружества Независимых Государств об оперативно-розыскной деятельности (2007) определяет отождествление личности как установление и идентификацию лица по индивидуализирующим статическим и динамическим неизменяемым признакам, а равно и при помощи других способов, позволяющих с достаточной степенью вероятности опознать личность.

Отметим, что Конституционный Суд РФ в своем Определении от 15 апреля 2008 г. № 312-О-О отнес отождествление личности к мерам проверочного характера с целью установления лиц, причастных к преступной деятельности, путем непроцессуального опознания по идентифицирующим признакам.

Как показывает практика, все чаще отождествление личности проводится с использованием сети Интернет. Тем более что развитие глобальных компьютерных сетей связано с их интеграцией с иными коммуникационными и информационными сетями, в том числе с сетями сотовой связи.

Необходимо учитывать, что в зависимости от публичности в Интернете выделяют два вида пространства, отличных по своей форме: публичное и приватное. Публичное интернет-

[1] Написание слова «оперативно-розыскной» здесь и далее — в авторской редакции. В соответствии с современными правилами русского языка — «оперативно-разыскной». См.: Правила русской орфографии и пунктуации. Полный академический справочник / под ред. В.В. Лопатина. М., 2006; С. 53 (§40); URL: http://gramota.ru/class/istiny/istiny_2_razysknoj/. В документах, названиях подразделений, цитатах и т.п. сохранена орфография первоисточника. – Прим. ред.

пространство представляет собой часть виртуального пространства, к которому любой его пользователь имеет свободный доступ. В приватном интернет-пространстве осуществляются непубличные коммуникации, которые содержат информацию, не имеющую публичного статуса.

Как установлено, оперативными сотрудниками при проведении отождествления личности активно используется публичное пространство Интернета. Оно выступает, во-первых, как ресурс, позволяющий получить (добыть) необходимую для обеспечения отождествления личности идентификационную информацию об опознаваемых объектах и, во-вторых, как средство (инструмент) отождествления личности.

Рассматривая первый аспект использования Интернета, акцентируем внимание на наличие в его среде социальных сетей, то есть интерактивных многопользовательских веб-сайтов, в рамках которых пользователи имеют возможность создавать связи с другими пользователями (социальные связи). Примерами социальных интернет-сетей являются «ВКонтакте», «Одноклассники», «Twitter», «Facebook», «Instagram», «YouTube» и т.д. Одной из функций таких сетей является идентификационная, которая реализуется при создании индивидуального профиля пользователя. В его рамках участник сети наполняет свою учетную запись идентификационной информацией, включая фотографии с собственным изображением, видеозаписи, свои фамилию, имя, отчество, дату рождения, семейный статус, место работы и учебы, интересы и другие сведения. В оперативно-розыскной практике такая информация добывается и используется при проведении отождествления личности в отношении пользователя социальной сети.

Использование сотрудниками оперативных подразделений публичного интернет-пространства как средства (инструмента) идентификации личности предполагает применение специализированных общедоступных онлайн-сервисов поиска и отождествления лиц по фотоизображениям, опубликованным в социальных сетях, например, FindClone. В ходе проведенного нами анкетирования выявлено, что именно такой способ отождествления личности активно применяется в оперативно-розыскной практике. Реализация такого способа предполагает загрузку на веб-странице или в компьютерной программе соответствующего онлайн-сервиса фотоизображения лица, имеющегося у субъекта проведения оперативно-розыскного мероприятия. После чего активируется поиск и отождествление интересующего лица по фотографиям, размещенным в социальных сетях. По результатам поиска отображаются фотографии со ссылками на аккаунты в социальных сетях, на которых присутствует вероятный искомый объект. Найденные аккаунты изучаются на предмет наличия информации, которая может способствовать установлению личности объекта поиска (ФИО, дата и место рождения, место проживания и другие сведения). Важно отметить, что обозначенный способ не гарантирует получение полной и достоверной информации об отождествляемом лице. Полученные по результатам такого поиска данные требуют дополнительной проверки.

В качестве примера отождествления личности с использованием публичного интернет-пространства приведем уголовное дело, возбужденное по факту совершения преступлений, предусмотренных п. «г» ч. 4 ст. 228.1, ч. 3 ст. 30 и п. «г» ч. 4 ст. 228.1, ч. 2 ст. 228, ч. 1 ст. 222 УК РФ (Челябинская область). Из материалов дела следует, что оперуполномоченным ОУР ЛОП на ст. Златоуст в ходе оперативной работы с гр-н Н., в отношении которого осуществлялось уголовное преследование по факту совершения им преступления, предусмотренного ч. 2 ст. 228 УК РФ, выразившегося в незаконном приобретении и хранении без цели сбыта наркотических средств в крупном размере, была получена оперативная информация о том, что он (гр-н Н.) приобрел наркотическое средство под условным наименованием «спайс» у мужчины по имени Ф. В ходе дальнейшей оперативной работы была установлена личность гр-на Ф., из социальной интернет-сети «ВКонтакте» получено его фото. Данное фото предъявлено гр-ну

Н. для отождествления личности, по результатам которого гр-н Ф. был опознан как лицо, которое ранее сбыло опознающему наркотическое средство. В дальнейшем оперативными сотрудниками проведен комплекс ОРМ, гр-н Ф. изобличен в совершении преступления. Немало примеров о проведении отождествления личности с использованием сети Интернет можно обнаружить и в других регионах.

Очевидно, что условием подготовки и проведения отождествления личности с использованием публичного пространства сети Интернет является наличие современной компьютерной техники с доступом в Интернет, а также специфического программного обеспечения и сервисов, которые позволяют осуществлять поиск и отождествление лиц по их фотоизображениям, опубликованным в социальных интернет-сетях. Однако проведенное исследование показывает, что сотрудники оперативных подразделений ОВД зачастую не имеют ни служебного компьютера с доступом в Интернет, ни возможности использования вышеуказанных программных средств и сервисов. Заметим, что позволяющий идентифицировать граждан по их изображениям в социальных сетях FindClone, наиболее часто используемый оперативными сотрудниками в служебной деятельности, является общедоступным условно бесплатным сервисом. Бесплатная версия этого сервиса имеет существенные ограничения по количеству возможных поисков лиц по их изображениям. Кроме того, не гарантирована постоянная работа подобных публичных сервисов, в любой момент они могут оказаться недоступными.

Приведенные обстоятельства вызывают существенные трудности у оперативных сотрудников при использовании Интернета и как источника идентификационной информации, и как средства (инструмента) отождествления личности. Это подтверждается и результатами анкетирования сотрудников оперативных подразделений, проведенного В.И. Шаровым. Так, 64% респондентов указали, что причиной неудовлетворительных результатов использования Интернета для поиска и обнаружения оперативно-значимой информации является отсутствие доступа к нужным веб-сайтам и базам данных, 14% респондентов в качестве причины отметили отсутствие специального программного обеспечения.

Следует признать и недостаточный уровень профессиональных компетенций у оперативных сотрудников в сфере использования Интернета для получения оперативно значимой информации — 23% опрошенных в качестве причины неудовлетворительных результатов использования Интернета указали отсутствие методики поиска информации в этой глобальной компьютерной сети, с чем трудно не согласится.

Таким образом, мы приходим к следующим выводам. Во-первых, имеется потребность в более глубоких научных исследованиях и разработке рекомендаций по проведению ОРМ, в том числе отождествления личности, в условиях развития информационных технологий. Во-вторых, необходимы меры по обеспечению оперативно-розыскных подразделений собственными программными и аппаратными средствами, позволяющими осуществлять поиск и идентификацию лиц по их изображению в публичной сети Интернет.

С.В. Зуев, *д.ю.н., заведующий кафедрой правоохранительной деятельности и национальной безопасности Южно-Уральского государственного университета, г. Челябинск*

ЦИФРОВАЯ УГОЛОВНО-ПРОЦЕССУАЛЬНАЯ ПОЛИТИКА

Политика — искусство управлять. Именно таким слоганом можно коротко обозначить суть этого явления. Если обратиться к этимологии слова, то в переводе с греческого политика — это искусство управлять государством, что подразумевает участие в государственных

делах, определение направлений его функционирования, а также форм, задач и содержание этой деятельности. При этом преследуется цель — сохранение и (или) создание наиболее приемлемых для определенных слоев общества или классов условий и способов осуществления государственной власти.

Платон в диалоге «Политик» (Πολιτικός, 370–360 до новой эры) приводит взгляд Сократа на политику как на «искусство управления людьми».

Уголовно-процессуальная политика является «самостоятельным направлением государственной социальной политики, которая должна рассматриваться ввиду своего производного характера как самостоятельный элемент уголовной государственной политики, выступающей во взаимосвязи с политикой уголовно-правовой и уголовно-исполнительной» [9, с. 63].

Условно уголовно-процессуальную политику можно разделить на внутреннюю и внешнюю. Внутренняя политика направлена на реализацию национального законодательства, внешняя — на исполнение международных правовых актов и сотрудничество с другими странами.

По мнению И.Г. Смирновой, при первом поверхностном рассмотрении можно констатировать, что уголовно-процессуальная политика современного этапа — это политика, опирающаяся на идеи, провозглашенные в ст. 2 Конституции РФ (личность, ее права и свободы — высшая ценность в государстве). Кроме того, указанная деятельность носит внешнеполитический, международный характер и требует дополнительного урегулирования путем заключения международных договоров и соглашений.

В Руководящих принципах отношений между Советом Европы и Европейским Союзом от 16-17 мая 2005 г. указано, что Совет Европы и Европейский Союз основывают свои взаимоотношения на соблюдении прав человека, которые составляют основу стабильности и безопасности. Нельзя забывать и положения Концепции национальной безопасности РФ от 10 января 2000 г., где во втором разделе «Национальные интересы России» подчеркивается, что интересы личности заключаются в обеспечении личной безопасности. Действительно, гражданин и общество не столько жаждут борьбы с опасностью, сколько защиты, т.е. безопасности. Таким образом, уголовно-процессуальная политика должна ориентироваться на предназначение уголовного судопроизводства защищать права личности, общества и государства не только от преступных посягательств, но и от их последствий, обеспечивать баланс законных интересов и безопасность [9, с. 65].

В документе под названием «Уголовная политика: дорожная карта (2017–2025 гг.)», разработанном под эгидой Центра стратегических разработок, указывается, что уголовная политика в России, направлена на то, как отвечать на новые виды общественно опасных деяний, возникающие при переходе к новому технологическому укладу. В рамках вызовов XXI века внимание следует сконцентрировать на следующих направлениях: 1) транснациональная преступность и меры противодействия ей (развитие механизмов процессуального сотрудничества, унификация при необходимости уголовного законодательства, разработка международных документов в этой сфере); 2) преступления, связанные с новыми технологиями (описание новых преступных деяний, методы противодействия им, пресечения и расследования); 3) новые технологии как эффективное средство контроля за преступностью на всех стадиях, начиная с допреступного поведения (безопасность в широком смысле) и заканчивая исполнением приговора суда (развитие альтернативных наказаний, исполнению которых должно способствовать внедрение новых технологий) [9, с. 50].

В равной мере уже сейчас необходимо развивать и внедрять в практику новые технологии как эффективное средство контроля за преступностью. Наряду с экономией государственных расходов в данной сфере это должно привести к общему снижению уровня преступности и дальнейшему цикличному высвобождению государственных ресурсов. К числу таких

крупных корректирующих шагов можно отнести, в частности, такое направление, как деформализация, то есть снижение требований к оформлению документов, внедрение более простых способов фиксации (включая аудио/видео, цифровые и прочие современные способы фиксации информации без бумажных носителей), нацеленность на быструю передачу в суд [3, с. 54].

Представляется, что реализовать вышесказанное становится возможным при решении следующих стратегически важных вопросов:

– переход на фиксацию хода процессуальных, в том числе следственных, действий с помощью технических средств и сохранение результатов в электронном виде;

– внедрение в уголовно-процессуальную материю удобную и надежную технологию удостоверения процессуального документа любым участником уголовного процесса вместо его обычной подписи;

– разработка «Электронное уголовное дело» и использование его на всех стадиях уголовного судопроизводства;

– широкое применение дистанционных форм проведения процессуальных действий, включая участие в судебных заседаниях всех заинтересованных лиц;

– предоставление потерпевшему в режиме онлайн через Интернет возможности отслеживать движение уголовного дела от подачи заявления в электронном форме до вынесения приговора;

– использование электронного помощника судьи для оценки фактических данных, имеющихся в уголовном деле, а также при назначении научно обоснованного и соразмерного совершенному противоправному деянию наказания.

Перечисленные направления представляют собой некоторую программу минимум, которая может дополняться и видоизменяться. В любом случае их можно комментировать.

В настоящее время приоритетным способом фиксации хода процессуальных, в том числе следственных, действий является составление бумажных протоколов. Технические средства выполняют факультативную роль. Высказаться в пользу перехода на электронный способ отображения процессуальной деятельности хочется, воспользовавшись аргументами других авторов. Так, существует мнение, что это позволит оптимизировать работу участников уголовного процесса, повысить качество выполнения поставленных задач [8, с. 28]. В перспективе технические средства копирования, хранения, передачи электронной информации сделают ненужными бумажные уголовно-процессуальные документы, то есть возможен переход исключительно на электронный документооборот [8, с. 165].

В этой связи следует согласиться с тем, что необходимо регулирование, в первую очередь, основных начал проведения следственных действий и иной деятельности с использованием информационных технологий и электронных документов путем формулирования норм о гарантиях подлинности электронных доказательств, например, о ее неизменности, защите от возможных посягательств и доступности для последующего изучения, депонировании электронных копий, обязательном участии специалиста при проведении следственных или судебных действий, связанных с копированием, депонированием, осмотром, изъятием электронной информации [8, с. 128].

Формирование материалов дела не только в бумажном виде, но и в форме электронного уголовного дела, несомненно, упростит реализацию ст. 158.1 УПК РФ, в соответствии с которой восстановление утраченного уголовного дела либо его материалов производится по постановлению руководителя следственного органа, начальника органа дознания, а в случае утраты уголовного дела или материалов в ходе судебного производства — по решению суда, направляемому руководителю следственного органа или начальнику органа дознания для исполнения. Это, в свою очередь, позволит не прибегать к применению ч. 4 ст. 158.1 УПК РФ,

а именно не освобождать обвиняемого в случае, если по утраченному уголовному делу истек предельный срок содержания под стражей [10, с. 174].

В.В. Зозуля предлагает на законодательном уровне предусмотреть возможность осуществления видеозаписи при проведении следственных действий с автоматической системой видеозаписи в служебных помещениях органов предварительного расследования в уведомительном порядке [4, с. 50]. Соглашаясь с этим в принципе, имеет смысл бумажный тип документирования в уголовном процессе пора признать не иначе, как архетипом.

Положение п. 18 постановления Пленума Верховного Суда РФ от 13 декабря 2012 г. № 35 «Об открытости и гласности судопроизводства и о доступе к информации о деятельности судов» определяет: при наличии технической возможности судам надлежит осуществлять фиксацию хода судебного разбирательства с использованием средств аудиозаписи и иных технических средств, а в случае недостаточной вместимости зала судебного заседания, в котором проводится слушание дела, осуществлять в здании суда трансляцию хода судебного заседания в режиме реального времени с использованием технических средств. Материалы фиксации хода судебного разбирательства, осуществляемого судом (например, носитель аудиозаписи), приобщаются к делу.

Согласно ч. 2 ст. 6 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия.

Внедрение в уголовно-процессуальную материю технологии удостоверения процессуального документа любым участником уголовного процесса вместо его обычной подписи позволит в режиме онлайн осуществлять процессуальные действия и подтверждать их. Это дает широкие возможности по дистанционному обеспечению прав и законных интересов участников. Многие страны уже ушли далеко вперед в этом.

В США система видео-конференц-связи с момента появления в судах прошла значительную технологическую эволюцию: современное качество связи существенно отличается от того, которое было доступно десять или двадцать лет назад. В настоящее время оно обеспечивает беспрерывную связь с высоким качеством разрешения, которое способно обеспечить полноценное присутствие лица в зале суда [11, с. 2].

Система электронного документооборота в этой стране нового поколения заключается в том, что регистрация в электронной системе управления электронным делопроизводством является обязательной для адвокатов и всех должностных лиц, осуществляющих судопроизводство. Каждый участник уголовного процесса несет ответственность за поддержание электронного почтового адреса, своей учетной записи, необходимой для получения электронного уведомления о движении дела и принимаемых решениях. Если адвокат не подает документы в электронном виде, то он должен получить на это разрешение суда и объяснить причины несоблюдения обязательной электронной подачи материалов. Если суд разрешил подачу материалов в не электронной форме, то он может отозвать это разрешение в любое время и обяжет адвоката подать документы с использованием системы электронного документооборота [5, с. 24].

В 2016 г. органами общественной безопасности КНР была создана интернет-платформа по приему заявлений о нарушениях закона, получившая название «cyberpolice». Данный сайт

принимает к регистрации информацию о распространении порнографических материалов, вовлечении в занятие проституцией, распространении компьютерных вирусов, мошеннических действиях в сети Интернет, организации азартных игр, продаже оружия, боеприпасов к нему, а также торговле документами, фальшивыми деньгами, человеческими органами, распространении запрещенной информации о религиозных культах. В то же время разработчики сайта поощряют передачу любой информации о деятельности организации «Исламское движение Восточного Туркестана» и иной информации о вооруженно-террористических организациях, целью которых является создание фундаменталистского исламского государства. Процедура подачи сообщения о преступлении достаточно проста: зарегистрированный на сайте пользователь заполняет типовой бланк и отправляет электронное сообщение, после чего получает логин и пароль для отслеживания хода рассмотрения своего заявления. В период с мая по июль 2019 г. на данном сайте зарегистрировано 127 175 пользователей. В указанный период был дан ответ на 21 213 обращений, подготовлено 40 990 материалов для возбуждения уголовного дела, из которых 22 042 — об организации незаконной игорной деятельности (53,8%), 11 468 — о сексуальных домогательствах и распространении порнографических материалов (28%) [5, с. 159].

В декабре 2017 г. в Уголовно-процессуальный кодекс Республики Казахстан были внесены изменения, позволяющие проводить расследование по уголовным делам в электронном формате. Согласно материалам сайта Верховного Суда Республики Казахстан, первое электронное уголовное дело было рассмотрено уже в январе 2018 г. В этом же году расследовано свыше 15 000 электронных уголовных дел по проступкам и преступлениям небольшой тяжести, из которых более 4 000 направлено в суд [5, с. 199].

Ю.Н. Познанский убеждает в необходимости формирования уголовного дела на всех стадиях досудебного и судебного производства в электронном виде (например, в формате PDF); законодательном закреплении возможности изучения материалов уголовного дела в электронном виде такими участниками уголовного процесса, как следователь, дознаватель, эксперт, прокурор, судья в случаях, когда изучение материалов уголовного дела не требует проведения каких-либо экспертиз либо иного анализа материалов уголовного дела на бумажном носителе [7, с. 42].

В научных кругах необходимость и возможность активного использования «электронных уголовных дел» в уголовном судопроизводстве обсуждается многими авторами. Имеются уже и попытки создания подобного рода программ [10].

Широкое применение дистанционных средств проведения процессуальных действий на любой стадии уголовного судопроизводства, включая участие в судебных заседаниях всех заинтересованных лиц — это перспективное направление развития. В связи с этим целесообразно дополнить содержание диспозиции ст. 278.1 УПК возможностью использования видео-конференц-связи не только в судебном заседании, но и на предварительном расследовании [2, с. 19].

Вместе с тем необходимо отметить, что расширение возможностей информационных технологий уголовного процесса путем совершенствования программы реализации видеоконференц-связи (проведение с использованием данной технологии таких следственных действий, как допрос, очная ставка, опознание, частичное упразднение института понятых), должно осуществляться при решении вопросов, связанных с обеспечением достоверности и допустимости полученной таким образом информации, ее безопасности и сохранности, тайны следствия, с соблюдением прав и законных интересов человека и гражданина [8, с. 27–28].

Прежде всего, необходимо предоставить потерпевшему в режиме онлайн через Интернет возможность отслеживать движение уголовного дела, начиная от подачи заявления в электронной форме — важное направление развития информационных технологий в уголовном судопроизводстве.

На сегодня заявление о преступлении может поступить в правоохранительные органы через сайт государственных услуг. Однако заявитель не имеет четко определенный УПК РФ перечень прав, не может потребовать от правоохранительных и иных государственных органов быть своевременно информированным о движении уголовного дела. Представляется, что, используя определенную программу, он мог бы получать всю информацию о принятых решениях, о передаче материалов следователю или дознавателю, о сроках расследования и других процессуальных моментах. Также следует предоставить потерпевшему возможность ознакомления с материалами уголовного дела через Интернет. С другой стороны, необходимо устанавливать различного рода фильтры на «отсев» ложной и второстепенной информации. В этом плане интерес представляет опыт зарубежных стран. Например, имеются технологии, позволяющие воспрепятствовать злоупотреблению правом при обращении в правоохранительные органы, пресечь случаи подачи заведомо ложных заявлений. В частности, ученые из Мадридского университета имени Карла III и Кардиффского университета в Уэльсе разработали искусственный интеллект — алгоритм VeriPol, способный выявлять ложные заявления в полицию на основании их содержания. Эта технология была протестирована полицией Испании в 2017 г. в двух полицейских департаментах Малаги и Мурсии [1].

Идея принятия юридических решений в уголовном судопроизводстве с использованием математических методов и алгоритмизации не нова и имеет как своих противников, так и сторонников. Отдельно взятая такая идея проигрывает при столкновении с противниками, которые боятся потерять усмотрение правоприменителя, обладающего в то же время высокой степенью коррупционного риска. Однако в общем контексте разработки использования электронных (цифровых) средств уголовного судопроизводства все выглядит вполне логично. О необходимости использования в юриспруденции математических методов и алгоритмов говорилось достаточно давно, задолго до современного развития информационных технологий. К сторонникам данного направления развития юридической науки и практики следует отнести следующих ученых А.А. Арямов, Д.С. Дядькин, В.И. Курляндский, С.Г. Ольков, Н.Д. Оранжиреев, Чижов М.В. и других. Не углубляясь в конкретные разработки математических методов назначения наказаний и обобщив их принципиальные подходы, можно выделить следующие направления: балльная система; шкалирование; выстраивание отношений с помощью математических формул.

Проблема освободить судью при вынесении приговора от усмотрения является краеугольным камнем системы уголовного правосудия в странах общего права. Ряд авторов создали информационную систему наказаний для предоставления судьям юридических, фактических и статистических данных. Цель системы — не лишить судью своего усмотрения, но лучше информировать его, и таким образом добиться согласованности подходов по всей юрисдикции. В их работе на конкретных примерах показано, как применяется такая информационная система.

Вышесказанное требует дальнейшего развития в плане использования информационных технологий в уголовном судопроизводстве. Этому может способствовать научная разработка концепции формирования единой цифровой среды уголовного судопроизводства [12].

Все это свидетельствует о необходимости больше внимания уделять цифровой уголовно-процессуальной политике. При этом надо учитывать, что внедрение информационных

технологий, кроме определенных сложностей технического оснащения властных органов судопроизводства, повлечет некоторые проблемы непосредственного восприятие новых форм информационных коммуникаций, которое сопровождается различными, и не всегда положительными, психофизиологическими реакциями у участников процессуальных отношений. Все это обусловлено еще и требованиями по сохранению традиционных ценностей права, успешно создающих чувство доверия граждан к порядку отправления правосудия, соблюдению законности и справедливости, гарантии защищенности.

Список литературы

1. Александров А.С., Андреева О.И., Зайцев О.А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестник Томского государственного университета. 2019. № 448. С. 199-207.
2. Дмитриева А.А. Теоретическая модель безопасного участия личности в уголовном судопроизводстве: дисс. … д-ра юрид. наук. М., 2017. 52 с.
3. Есаков Г.А., Долотов Р.О., Филатова М.А., Редчиц М.А., Степанов П.П., Цай К.А. Уголовная политика: дорожная карта (2017-2025 гг.). М., 2017. URL: https://www.csr.ru/ uploads/2017/04/Report-CP.pdf
4. Зозуля В.В. К вопросу о применении видеозаписи при производстве следственных действий с участием несовершеннолетних // Уголовно-процессуальная охрана прав и законных интересов несовершеннолетних. 2016. № 1 (3). С. 47-51.
5. Информационные технологии в уголовном процессе зарубежных стран. М., 2020. 216 с.
6. Кувычков С.И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: дисс. … канд. юрид. наук. Нижний Новгород, 2016. 273 с.
7. Познанский Ю.Н. Электронное уголовное дело в решении проблемы расследования уголовного дела в разумные сроки // Труды академии управления МВД России. 2015. № 1 (33). С. 41-44.
8. Развитие информационных технологий в уголовном судопроизводстве. М., 2018. 248 с.
9. Смирнова И.Г. Уголовно-процессуальная политика: некоторые суждения о ее сущности, социальной обусловленности и месте в уголовной политике // Криминологический журнал Байкальского государственного университета экономики и права. 2010. № 3. С. 61–67.
10. Янушко А.В., Бабанин А.В., Кузнецова О.А., Петрушенко С.В., Чекмарев М.Ю. Защищенный аппаратно-программный комплекс центра хранения электронных копий материалов уголовного дела // Безопасность информационных технологий. 2011. № 1. С. 21-29.
11. Enhancing Courts and Justice with Technology. A Polycom Perspective. White Paper. Polycom. 2016. URL: https://www.polycom.com/content/dam/polycom/common/documents/ white-papers/courtroom-video-applications-whitepaper-enus.pdf
12. Potas I., Ash D., Sagi M., Cumines S., Marsic N. Informing the discretion: the sentencing information system of the judicial commission of New South Wales // International Journal of Law and Information Technology. 1998. Vol. 6 (2). P. 99-124.

И.М. Комаров, *д.ю.н., заведующий кафедрой криминалистики МГУ им. М.В. Ломоносова, г. Москва*

НЕКОТОРЫЕ ПРОБЛЕМНЫЕ ВОПРОСЫ «ЦИФРОВИЗАЦИИ» В КРИМИНАЛИСТИКЕ

«Цифровую» криминалистику можно считать реалиями сегодняшнего дня. Мы придерживаемся этого понятия по причине того, что оно отражает сущность соответствующего его содержания, обусловленного двоичным кодом. Специалистами в этой отрасли криминалистического знания к настоящему времени уже сделано достаточно, чтобы можно было констатировать факт создания научных основ, согласно которым этот раздел криминалистической техники мог бы гармонично развиваться в соответствии с запросами правоприменительной практики, и не только связанной с уголовным судопроизводством.

Вместе с тем логика научного познания связана не столько с накоплением суммы новых знаний, сколько приведением этих знаний в стройную структурированную систему, способную обеспечить его дальнейшее поступательное развитие с учетом теоретических исследований и запросов правоприменительной практики.

В этой связи, на наш взгляд, есть несколько проблемных моментов, требующих обсуждения научной общественности.

1. Логика научного познания требует от криминалистического сообщества четкого обоснования объекта и предмета исследования, которые бы соотносились с понятиями «цифровой» криминалистики. Это как бы заданные на сегодняшний день границы, «коридор», в пределах которого должно продолжать формироваться определенное знание. Понятно, что эти границы будут меняться в соответствии с суммой накопленного знания. Однако сейчас это является актуальным для того, чтобы «цифровые» исследования в криминалистике приобрели характер системного знания.

2. В соответствии с вышеизложенным сразу следует отметить, что имеется проблема относительно субъекта исследований, связанных с «цифровой» криминалистикой. Специалисты традиционной криминалистики, а их в нашем научном сообществе большинство, не всегда способны проводить подобные качественные научно-практические исследования. Причин этому достаточно, и мы не станем на них подробно останавливаться, они всем хорошо известны. Однако эти специалисты обладают достаточными традиционными криминалистическими знаниями, чтобы в творческом тандеме со специалистами в области «цифровых» знаний разрабатывать ситуационно определенные типовые рекомендации относительно методов, способов и приемов решения правоприменителями конкретных тактических задач.

3. Как никогда становится актуальной проблема соотнесения языка традиционной и «цифровой» криминалистики. Как должна протекать их интеграция? Проведенный нами в этой связи анализ свидетельствует о том, что в криминалистический оборот уже введены новые понятия и их определения, которые у традиционного криминалиста (если это понятие считать допустимым) вызывают затруднения для понимания, что требует его обращения к источникам, толкующим эти понятия. Без этого не представляется возможным «встраивать» их в криминалистические системы (рекомендации и т.п.) как для теоретических, образовательных целей, так и для правоприменительной деятельности.

Уверен, что не все криминалисты моего поколения знакомы с такими понятиями, как dos-атаки; дефейс; вредоносные атаки; кардерство; мошенничество с трафиком; нарушения авторских прав в офлайне; нарушения авторских прав в Сети; фишинг; скимминг; киберсквоттинг, кейлогер и пр., а таких понятий много и, что хуже того, они пополняют словарь «цифровой» криминалистики.

Соответствующие проблемы возникают и у правоприменителей, которые не всегда понимают, о чем идет речь и как оценивать тот или иной факт, отраженный в процессуальном документе, например, в заключении судебно-компьютерной экспертизы. Практики эту проблему решают на основе привлечения соответствующих специалистов, однако это не выход, следователь должен владеть этим языком сам, так как это знание определяет оперативность принятия решений и отражает требования процессуальной и иной экономии при расследовании преступлений и отправлении правосудия.

Первое, что приходит в качестве способа и средства решения вопроса — формализация этого нового для криминалистического употребления языка на основе совместной деятельности в данном направлении криминалистов и математиков, при соблюдении криминалистических приоритетов относительно значимости того или иного понятия для элементов криминалистической систематики. Задача непростая, если иметь в виду динамику постоянных изменений, происходящих собственно в «цифровом» языке с учетом того, что среди криминалистов имеется немного специалистов, готовых правильно отражать эти изменения с пониманием того, насколько они могут быть полезны собственно криминалистике. В этой связи нам представляется более целесообразным обратное отношение этого взаимодействия по формуле — математики объясняют понятие через его определение, криминалисты принимают и «встраивают» («не встраивают») понятие в элементы системы криминалистических данных. Возможны и другие варианты решения этой «языковой» криминалистической проблемы.

Развитие языка важно для любой науки, так как он относится к одному из фундаментальных факторов, ее характеризующих, которые наряду с объектом, предметом, методами и прочими основаниями делают совокупность знаний собственно наукой, то есть областью человеческой деятельности, направленной на выработку и систематизацию объективных знаний о действительности. В основе этой деятельности всегда лежит сбор фактов, их постоянное обновление и систематизация, критический анализ и на этой основе — синтез новых знаний или обобщений, которые не только описывают наблюдаемые природные или общественные явления, но и позволяют построить причинно-следственные связи с конечной целью прогнозирования.

4. Традиционный ряд закономерностей предмета криминалистики, характеризующий преступную деятельность, в настоящее время содержательно по умолчанию подразумевает и «цифровые» следы-последствия преступной деятельности. Но криминалистами они практически изучены очень плохо и для их изучения делается недостаточно.

Данный факт определяет необходимость выдвижения для последующего изучения соответствующей гипотезы относительно понятия «цифровых» следов-последствий, закономерностей их образования в процессе преступной деятельности и т.п. положений, которые на основе их опытно-фактического криминалистического подтверждения будут обоснованы и сформулированы в виде закономерных явлений, что станет способствовать использованию этого знания в процессе правоприменительной деятельности.

5. Элементы системы криминалистики структурно связаны между собой и традиционно криминалисты выделяют четыре элемента науки (общая теория, криминалистические техника, тактика и методика). В соответствии с этой системой, полагаем, и следует развивать знание о «цифровых» следах-последствиях преступлений, где были использованы соответствующие компьютерные технологии и средства для достижения преступных целей. На наш взгляд, широту и глубину этой проблемы в настоящее время представить себе достаточно трудно, так как, в первую очередь, в современной криминалистике отсутствуют фундаментальные теоретические знания, объясняющие эту проблему. Их накопление, систематизация и описание должно протекать в соответствии и на основе данных анализа судебно-следственной практики, где усматривается использование компьютерных технологий в процессе подготовки,

совершения и сокрытия преступлений. Но соответствующее криминалистическое теоретическое исследование должно проводиться криминалистами во взаимодействии и тесном сотрудничестве с математиками, специалистами в области IT-технологий.

Можно дальше раскрывать недостатки современной криминалистической теории относительно отсутствия в ее содержании данных о «цифровых» следах-последствиях преступлений и компьютерных технологиях, используемых при их совершении, однако мы не преследуем в настоящей публикации эту цель. Для нас важно обратить внимание криминалистов и, в первую очередь, молодых криминалистов (традиционные криминалисты в силу ряда причин неспособны решать эту задачу) на давно назревшую проблему, которая уже много лет находится в состоянии застоя и никак не решается и, возможно, этой публикацией хотя бы немного «сдвинуть» ее с места. Разрыв между практикой расследования преступлений, где имеют место «цифровые» следы-последствия преступной деятельности, и теорией криминалистики, связанной с обучением и образованием будущих правоприменителей, с каждым днем все больше увеличивается. Между тем в современной правоохранительной практике все чаще «цифровые» технологии становятся предметом следственной деятельности по расследованию преступлений, и в этой связи следователи действуют не по криминалистическому алгоритму, который для этих ситуаций не разработан, а интуитивно, как «бог на душу положит», чего в принципе быть не может.

В.Е. Козлов, *к.ю.н., Академия МВД Республики Беларусь, г. Минск*

ОБ ОТДЕЛЬНЫХ АСПЕКТАХ КРИМИНАЛИСТИЧЕСКОГО И ОПЕРАТИВНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Проводившиеся нами исследования проблемных вопросов осуществления противодействия преступлениям, совершаемым с использованием средств компьютерной техники (СКТ), позволили выявить ряд проблемных вопросов, возникающих на его различных уровнях и нуждающихся в разрешении. Так, на государственном уровне объектом познания выступали собственно социальное явление «компьютерная преступность», процессы, протекающие в ходе моделирования противодействия ей различными субъектами. Моделирование осуществлялось с целью формулирования основ познавательной и предметно-практической составляющих деятельности субъектов, осуществляющих искомое противодействие [1]. Выявленные системные проблемные вопросы позволили констатировать наличие проблемы, заключающейся в несоответствии сложившегося уровня развития общественных отношений в рассматриваемой предметной области, уровню, необходимому и достаточному для осуществления эффективного контроля над «компьютерной преступностью» со стороны государства. Таким образом, стала очевидна актуальность подобных исследований, их научная новизна и практическая значимость, а также то, что последующие результаты проводимых исследований будут детерминированы эффективностью построения и исследования информационных моделей как искомой системы в целом, так и ее подсистем.

Нами рассмотрены константы и переменные, описывающие объекты, связи между ними, входные и выходные параметры объектов, динамику изменения входных и выходных величин, детерминируемую возможными состояниями объектов. В качестве подсистем были исследованы модели подсистемы компьютерной безопасности (КБ), а также осуществления противодействия «компьютерной преступности» правоохранительными органами [2], включающую модели криминалистического (КО) и оперативно-технического обеспечения (ОТО).

Результаты исследования позволили сформулировать проблемные вопросы, присущие именно им. Так, для КО таковыми являются следующие [3].

1. Вопрос криминалистического толкования терминов «компьютерное преступление» («высокотехнологичное преступление») и «компьютерная информация» (КИ) — основополагающий, являющийся базовым для разрешения иных проблем, возникающих в процессе осуществления искомого противодействия, и связанных с ними вопросов использования криминалистических и других знаний о «высокотехнологичной преступности» при осуществлении предупреждения, выявления, раскрытия и расследования общеуголовных, экономических и иных преступлений, в особенности транснациональных, совершаемых организованными преступными группами.

2. Вопросы непрерывного анализа современных угроз информационной безопасности личности, общества, государства в условиях изменяющейся оперативной обстановки и связанный с ними комплекс вопросов по совершенствованию систем КБ в условиях массового использования СКТ в соответствии с криминалистическими рекомендациями и требованиями по оказанию содействия субъектам, осуществляющим ОТО искомого противодействия.

3. Вопросы организации деятельности субъектов, ответственных за КБ во взаимосвязи с органами уголовного преследования.

4. Вопросы разработки и совершенствования тактики использования научно-технических средств (НТС) — специализированных программных и аппаратных средств, предназначенных для обнаружения, фиксации и изъятия следов «высокотехнологичных преступлений», а также создания условий для дополнительного следообразования, при производстве следственных действий (СД) и проведении оперативно-розыскных мероприятий (ОРМ), а также связанные с ними вопросы тактики применения специальных знаний (СЗ и совершенствования тактики назначения и производства судебной компьютерно-технической экспертизы по делам рассматриваемой категории.

5. Вопросы совершенствования основных положений тактики производства СД и проведения ОРМ по делам рассматриваемой категории, в целом — методики выявления, раскрытия и расследования таких преступлений, и связанные с ними вопросы допустимости и относимости вещественных доказательств, полученных при производстве СД и проведении ОРМ.

6. Вопросы совершенствования национальной системы противодействия «высокотехнологичной преступности» в целом и связанные с ними вопросы научного и организационно-методического обеспечения специализированных подразделений правоохранительных органов.

Аналогичным образом формулировалось проблемное поле и для разработки основ ОТО [4].

1. Непрерывный рост уровня «высокотехнологичной преступности», проникновение преступности в информационную сферу жизни общества, усиливающийся криминальный контроль над информационными ресурсами.

2. Расширяющееся применение информационных (компьютерных) технологий (ИТ) в криминальной деятельности, сращивание «компьютерной» и общеуголовной преступности. Применяемые преступниками современные технологии разнообразны по структуре, содержанию и зачастую эффективнее технологий правоохранительной деятельности, в том чиле технологий оперативно-розыскного назначения. Отмечено использование технологий информационного противодействия правоохранительным органам.

3. Повышение «криминальной квалификации» субъектов совершения преступлений, совершенствование СКТ, используемых в качестве орудия их совершения, исследование организации работы с конфидентами оперативных подразделений правоохранительных органов, и, как следствие, совершенствование конспиративности действий правонарушителей, направленных на подготовку и совершение преступлений, активное противодействие проведению ОРМ.

4. Совершенствование способов криминогенных воздействий средств массовой информации, в том числе использование глобальных телекоммуникаций в ходе подготовки

и совершении преступлений. Активное дискуссионное обсуждение характерных ошибок преступников, моделирование определенных информационных объектов и отношений, благоприятствующих решению противоправных задач.

Очевидно, что одной из ключевых категорий при осуществлении противодействия преступлениям, совершаемым с использованием СКТ, являются «технология», а также производные от нее, в том числе «технология борьбы с преступностью», «технология оперативно-розыскного назначения», «высокая технология» и т.д.

Допустим, что технология (Т) — система методов (М), средств (Ср) и субъектов (Сб) их применения, необходимая и достаточная для достижения поставленной цели, основанная на применении научного знания (1).

$$Т=М\&Ср\&Сб \quad (1)$$

Тогда существующую технологию можно представить в следующем виде (2):

$$Т_1=М_1\&Ср_1\&Сб_1 \quad (2)$$

А возникающую новую, «новейшую», «высокую» и т.д., как (3).

$$Т_2=М_2\&Ср_2\&Сб_2 \quad (3)$$

Очевидно, что технология изменится (становится «новой», «новейшей», «высокой») лишь при соблюдении условия подстановки новых значений средств, методов и субъектов их применения (конъюнкция). Следовательно, новые технологии возникают при условии появления нового средства деятельности, новой методики применения данного средства для достижения поставленной цели, а также субъекта, имеющего необходимый и достаточный уровень знаний, умений, навыков, необходимых для применения средств в соответствии с методикой. Кроме того, этот уровень знаний должен быть использован также для совершенствования средств деятельности и методики их применения. Справедливо и обратное утверждение — применение технологии эффективно в случае, если владеющий современными знаниями, умениями и навыками субъект использует современные средства и владеет методикой их применения. Отступление от этих логических выводов в практике противодействия «высокотехнологичной преступности» приводит к распространенному результату — у правонарушителей вызывает смех, а у специалистов (прежде всего в области ИТ) — слезы. Этот результат наиболее очевиден при разработке и внедрении нормативных правовых актов, наставлений и инструкций.

Применительно к КО раскрытия и расследования преступлений, совершаемых с использованием СКТ, НТС прежде всего, должны обеспечивать выполнение следующих действий [5, с. 171-178], например, при производстве осмотра места происшествия:

– внутренний осмотр помещений, в которых расположены СКТ и линий связи для выявления каналов утечки информации;

– определение свойств, качеств и технических характеристик СКТ с протоколированием сведений о состоянии аппаратных и программных ресурсов сетевого окружения СКТ;

– выявление каналов утечки информации в сетевой среде, что необходимо для последующего эффективного построения версий о совершенном противоправном деянии в отношении КИ;

– полноценную работу с имеющейся КИ.

Необходимо отметить, что детальный перечень НТС формируется при анализе обстановки (оперативной обстановки), сложившейся на момент производства СД или проведения ОРМ. Правообоснованность их применения как в случае КО, так и ОТО детерминируется следующими обстоятельствами допустимости:

– по субъекту — участие категорий лиц, предусмотренных законодательством;

– по средству (технологии) — применения технологий, определенных (не запрещенных) действующим законодательством;

– по методу — использования методов, допускающих включение в уголовное судопроизводство полученных материалов (прежде всего КИ) либо служащих для планирования проведения последующих ОРМ.

Отсюда вытекают рекомендации по привлечению специалистов к производству СД и проведению ОРМ, например, справедливо утверждение, что специалиста в области ИТ не существует, а можно вести речь лишь о специалисте, компетентном в области конкретном СКТ (операционной системе, прикладном программном обеспечении, низкоуровневых функциях, отдельных аппаратных реализациях и т.д.). Использование же СЗ следователем либо оперативным работником процесс гораздо более сложный. Их система должна способствовать созданию целостного представления о произошедшем событии, роли и месте всех его участников, возможности применения НТС, оценки оперативной обстановки и привлечении иных специалистов. Таким образом, содержание деятельности по использованию СЗ в процессе противодействия (в узком смысле) «компьютерной преступности» можно представить в виде рисунка 1.

Рис. 1. Содержание деятельности по использованию СЗ
в процессе противодействия «компьютерной преступности»

Такой системно-структурный подход, по нашему мнению, может являться основой разработки научно обоснованных рекомендаций по эффективному использованию СЗ в процессе противодействия «компьютерной преступности», позволит повысить эффективность практической составляющей такого противодействия. Отметим, что средства и методы ОТО противодействия преступлениям, совершаемым с использованием СКТ, отнесены к государственной тайне России и государственным секретам Беларуси, соответственно, в полном объеме не могут быть рассмотрены в данной статье. Однако они достаточно тесно интегрированы в подсистему КО, различаясь, прежде всего, целью применения, соответственно решаемыми задачами и, следовательно, функциями (рис. 2, 3). Очевидно, что в процессе искомого противодействия исключительно важное значение приобретает интеграция знаний различный отраслей науки. Эффективность их практической реализации во многом зависит от решения проблемных вопросов организационного и научно-методического обеспечения системы подготовки кадров для правоохранительных органов, главным образом, их оперативных и следственных подразделений. Одним из путей их разрешения является введение в учебные планы юридических вузов новых учебных дисциплин (см., например, [6]), что предопределяет необходимость

проведения организационных мероприятий, обеспечивающих их изучение, прежде всего, необходимый и достаточный на первоначальном этапе внедрения учебной дисциплины уровень знаний выпускников в области предупреждения, выявления, раскрытия и расследования «высокотехнологичных» преступлений. Целью преподавания подобных учебных дисциплин является формирование у обучающихся теоретических знаний, практических умений и навыков по правовым, организационным, тактическим, программным, аппаратным и иным технологическим аспектам применения современных технологий в оперативно-розыскной, следственной и оперативно-служебной деятельности подразделений правоохранительных органов.

В результате изучения учебной дисциплины обучающиеся должны: знать сущность современных ИТ как новой информационно-технологической концепции; виды ИТ, их основные признаки и характеристики; систему и основные положения нормативных актов, регулирующих применение ИТ в ОРД и в ходе осуществления предварительного расследования; вопросы организации и тактики использования ИТ при проведении ОРМ и производстве СД; уметь характеризовать соотношение используемых категорий, понятий, определений, современный уровень и перспективы использования ИТ-технологий оперативными подразделениями; правомерность применения технологий в оперативно-служебной деятельности; уметь анализировать возможные варианты использования результатов применения технологий в оперативно-розыскном и уголовно-процессуальном производстве; роль и место ИТ в правоохранительной деятельности; приобрести навыки самостоятельного использования ИТ; подготовки оперативно-служебных документов, составляемых в процессе их применения; технической культуры; конспирации.

Рис. 2. Система ОТО противодействия преступлениям, совершаемым с использованием СКТ

Полагаем, что учебный материал должен изучаться слушателями на лекционных, семинарских, практических занятиях, обсуждаться на круглых столах, а также в процессе самостоятельной работы. Контроль полученных знаний должен осуществляется путем проведения зачета (экзамена).

Рис. 3. Система КО противодействия преступлениям, совершаемым с использованием СКТ

Методика обучения должна быть сориентирована на формирование и закрепление в ходе аудиторных занятий знаний, умений и навыков использования ИТ в ОРД, а также деятельности органов, ведущих уголовный процесс, с учетом разнообразных оперативно-розыскных и следственных ситуаций, возникающих в практике подразделений правоохранительных органов.

Таким образом, анализ роли КО и ОТО в национальной системе противодействия преступлениям, совершаемым с использованием СКТ позволяет сделать следующие выводы.

1. Подсистемы КО и ОТО противодействия преступлениям, совершаемым с использованием СКТ, участвует в непрерывном процессе перехода количества знаний смежных отраслей науки (например, ИТ, КБ) в качество (постепенная интеграция их в криминалистику и теорию ОРД), в результате они становятся собственно криминалистическими; справедливо признание также обратного процесса.

2. Полученные в процессе информационного обмена научные знания внедряются в практическую деятельность субъектов путем непрерывного специализированного образования в системе КО и ОТО.

3. Разработанные модели имеют выраженную практическую направленность. Результатом деятельности подсистем в единой системе противодействия являются с одной стороны, — обеспечение заданного уровня КБ, с другой — выявление, предупреждение, раскрытие и расследование преступлений, совершаемых с использованием СКТ.

Список литературы

1. Козлов В.Е. Противодействие компьютерной преступности: проблемные вопросы и пути их разрешения: монография / М-во внутр. дел Респ. Беларусь, Акад МВД. Минск: Акад. МВД Респ. Беларусь, 2006. 256 с.
2. Козлов В.Е. Использование моделирования в изучении функционирования системы противодействия компьютерной преступности // Законность и правопорядок. 2007. № 1. С. 56-61.
3. Козлов В.Е. Об отдельных аспектах криминалистического обеспечения противодействия преступлениям, совершаемым с использованием средств компьютерной техники // Вестник Академии МВД Респ. Беларусь. Научно-практический журнал № 1 / М-во внутр. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». Минск: Акад. МВД, 2018. С. 86–92.
4. Козлов В.Е. О функциях оперативно-технического обеспечения противодействия преступлениям, совершаемым с использованием средств компьютерной техники // Проблемы борьбы с преступностью и подготовки кадров для правоохранительных органов: тез. докл. междунар. науч.-практ. конф. (Минск, 21 февраля 2019 г.) / учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь»; А.В. Яскевич (отв. ред.) и др. Минск: Академия МВД, 2019. С. 120-121.
5. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия — Телеком, 2002. 336 с.
6. Козлов В.Е. Об учебной дисциплине «Облачные технологии в правоохранительной деятельности» // Вестник Академии МВД Респ. Беларусь. Научно-практический журнал № 2 (34) / М-во внутр. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». Минск: Акад. МВД, 2017. С. 202-206.

О.С. Кучин, *д.ю.н., профессор кафедры судебных экспертиз и криминалистики Российского государственного университета правосудия, г. Москва*

О НЕКОТОРЫХ ТЕНДЕНЦИЯХ РАЗВИТИЯ МИРОВОЙ КРИМИНАЛИСТИКИ

Происходящие в настоящее время в мире процессы глобализации, неразрывно связанные с ускоряющимся развитием научно-технического прогресса, неизбежно приводят к негативным количественным и качественным изменениям преступности. В ее структуре все больший вес приобретают преступления, являющиеся финансовой базой для большинства иных видов преступности, в том числе для ее организованных форм, а также для терроризма, сепаратизма, бандитизма, коррупции.

Организованные преступные сообщества с успехом осваивают достижения научно-технического прогресса, активно используя в своей деятельности современные средства связи, транспорта, возможности Интернета, компьютерных технологий. Они активно действуют в сфере криминального бизнеса, связанного с оборотом наркотиков, оружия, с сокрытием доходов от налогов, с «отмыванием грязных денег» и, наконец, с коррупцией, приобретшей в нашей стране, по мнению многих аналитиков, ужасающий и системный характер. Современная преступность активно использует нейросети для достижения своего криминального результата или как места и способа его получения.

Роль современной криминалистики в этом процессе является уникальной, поскольку только она в пределах своего предмета, как никакая другая наука, непосредственно причастна

к решению всех названных выше насущных проблем. Перспективы развития криминалистики специалисты не без оснований связывают с дальнейшим освоением возможностей компьютерной техники и современных информационно-цифровых технологий, с созданием автоматизированных информационно-поисковых систем технико-криминалистического назначения, с разработкой искусственного интеллекта и роботизацией умственного криминалистического процесса. Факт создания таких систем обусловливает необходимость повышения качества и содержательности сосредотачиваемой в них информации, в частности, о различных цифровых следах преступлений. Таким образом, инициируется разработка новых и совершенствование традиционных методов и средств собирания и исследования таких следов.

В последнее время большое значение получили различные криминалистические компьютерные и цифровые технологии, используемые в борьбе с преступностью. Вместе с тем следует отметить, что российское понятие «цифровая криминалистика», известное в зарубежных странах как digital forensics, на самом деле представляет собой раздел криминалистической техники, посвященный восстановлению и исследованию доказательств, обнаруженных на цифровых устройствах или в Интернете, как правило, в связи с расследованием киберпреступлений (преступления, совершаемые в нейросетях или с использованием электронных технических средств для проникновения в эти нейросети) и никакого отношения к подлинной digital forensics не имеет, так как просто исследует различные носители цифровой информации и учит следователя, как с ними работать в ходе расследования того или иного преступления, где эти носители фигурируют в различном качестве. Последнее утверждение, впрочем, не должно восприниматься как отождествление цифровой криминалистики и киберпреступности. Цифровая криминалистика вполне успешно применяется и при расследовании традиционных преступлений в случаях, когда часть доказательств имеет цифровую форму — например, в виде электронной переписки, перевода денежных средств с использованием систем дистанционного банковского обслуживания (далее — ДБО) и т.д. Именно поэтому внутренняя классификация цифровой криминалистики довольно сложна и варьируется в зависимости от объекта и предмета исследования, вида преступлений и преступности, особенностей исследования цифровых следов и т.п.

В ряде стран, таких как США, Республика Корея, КНР, Япония известная нам криминалистическая экспертиза, в том числе экспертиза цифровых носителей информации и различных устройств, не существует в качестве отдельного процессуального действия, имеющего определенные временные границы назначения, проведения и дачи заключения. На смену такой экспертизе пришло постоянное сопровождение процесса выявления, раскрытия и расследования преступлений специалистами в сфере компьютерных (цифровых) технологий. С целью обеспечения такого непрерывного процесса сопровождения криминальной деятельности киберпреступников в этих странах создаются центры цифровой криминалистики (например, Национальный центр цифровой криминалистики при Прокуратуре Республики Корея), исследовательские институты (такие как Исследовательский центр цифровой криминалистики при Университете Корё), сотрудниками которых разрабатываются не методики расследования преступлений и экспертизы, в нашем российском понимании, а алгоритмы криминалистического сопровождения, то есть специальные системы и программные обеспечения, гарантирующие постоянный доступ субъекта расследования к цифровому анализу. Основой таких систем являются анализ больших данных, анализ работы систем дистанционного банковского обслуживания (далее — ДБО), искусственный интеллект и применение программного обеспечения (далее — ПО) на основе нейросетей. Сравнительно небольшое количество сотрудников, разработанные ими алгоритмы и программы автоматически обнаруживают и фиксируют цифровые следы при совершении различных видов преступлений посредством автоматического изучения активности вредоносных программ, логов, сетей, больших данных. Соответственно,

сбор информации и ее документирование осуществляется не человеком, т.е. специалистом, детективом, сотрудником полиции, прокурором или следователем прокуратуры, а специализированным программным обеспечением (ПО), фактически цифровым роботом. На основе анализа собранной информации следственная команда или детектив получает необходимые им данные по заданной комбинации и критериям анализа, которые могут быть использованы не только для расследования конкретного деяния, но для выявления и предотвращения преступлений вообще.

Таким образом, принятое в Российской Федерации толкование «цифровой криминалистики» как направленного исследования электронных доказательств (носителей цифровой информации) с помощью специалистов и экспертов, неверно или просто ошибочно.

Настоящая цифровая криминалистика представляет собой сложную систему, включающую совокупность постоянно работающих программных обеспечений (программ) для исследования цифрового пространства в целях предотвращения и выявления преступлений, анализ цифрового материала, а также направленного исследования конкретных носителей цифровых данных или самих данных (например, логов) для выявления следов конкретного преступления. При этом ведущую роль в цифровой криминалистике, в отличие от науки криминалистики «традиционного» типа, играет именно специализированное программное обеспечение (ПО) и широта его возможностей, а не специалист или эксперт, а проще сказать, не человек (следователь, детектив, полицейский).

Объясняется это тем, что сложность и многослойность цифровых устройств, их технические характеристики, а также действия преступников в цифровом пространстве настолько ускорены и усовершенствованы возможностями этого пространства, что человеческий мозг не в силах противостоять им в одиночку. Таким образом, специалист-криминалист превращается, по сути, в обслуживающий персонал при инструменте криминалистического исследования.

Поэтому сейчас все шире используются возможности компьютеров, снабженных соответствующим программным обеспечением. В США, в Республике Корея, в Японии, в Китае и в ряде других технически развитых странах уже разработаны и успешно работают специальные компьютерные программы, которые сами автоматически обнаруживают и фиксируют следы при совершении различных видов киберпреступлений. То есть документирование электронных следов киберпреступлений осуществляется не лично самим детективом-полицейским, а специальным компьютерным, цифровым роботом. У нас же в стране эту инновацию не совсем верно назвали «цифровой криминалистикой», определив ее предназначение только в исследовании цифровых электронных носителей информации с помощью специалистов в области IT-технологий. Это в корне неверно. На самом же деле «цифровая криминалистика» — это специальное программное обеспечение или его аналог.

Автор статьи считает, что российский термин «цифровая криминалистика» является неверным, так как априори такой криминалистики в природе не существует. На самом же деле «цифровая криминалистика» — это digital forensics, специальная компьютерная программа или программное обеспечение, разработанная в ряде развитых стран, направленная на автоматическое обнаружение, фиксацию и документирование цифровых следов преступлений.

Также следует отметить, что во всем мире вещественным доказательством является именно носитель цифровой информации (флэш-карта, диск, телефон, смартфон, айфон, планшет, компьютер и т.п.), а вот полученная из него цифровая информация становится доказательством только после исследования самого носителя специалистом или посредством заключения эксперта. Поэтому цифровая информация становится доказательством только в виде заключения эксперта или специалиста, т.е. после ее специальной обработки и исследования. В этом ее особенность и отличие, например, от письменного документа, который сам

и изложенная в нем информация являются самостоятельным и совместным доказательством, не требующим обязательного экспертного исследования.

До сих пор остается весьма актуальной разработка компьютерной системы для автоматического распознавания папиллярных узоров и их цифрового кодирования. Создание такой программной системы позволило заменить традиционную десятипальцевую систему регистрации монодактилоскопической и ввести ее в память компьютера, способного на автоматический поиск следов пальцев рук, сходных с обнаруженными на месте происшествия или в других местах.

При изучении организации борьбы с организованной преступностью рассматривается взаимодействие полицейских и иных государственных органов с негосударственными, в том числе с частными детективными агентствами, организациями самозащиты граждан, союзов по защите граждан от мошенничества в области кредитных операций и других подобных организаций, в настоящее время повсеместно распространенных за рубежом.

Значительное внимание специалистами в современной зарубежной криминалистике уделяется использованию средств массовой информации и коммуникации в расследовании преступлений, а в ходе изучения криминалистики в зарубежных полицейских академиях учебные программы направлены на формирование профессиональных качеств и навыков у детектива и полицейских в работе с компьютерами и носителями различной цифровой информации. Поэтому технико-криминалистические и иные компьютерные методы и средства собирания и исследования материальных носителей цифровой и иной электронной информации, их оценки и использования найдут еще более широкое применение в уголовном судопроизводстве.

В практику расследования уголовных дел, в частности для фиксации вербальной криминалистически значимой информации, все более активно внедряются средства аудио- и видеотехники, а также электронно-цифровые способы передачи данной информации. Цифровые и компьютерные технологии в настоящее время прочно заняли ведущее место в криминалистической технике и в тактических рекомендациях. В связи с развитием технического прогресса и IT-технологий в различных сферах правоприменительной деятельности в настоящее время в теории науки криминалистики активно рассматривается вопрос о проведении в ходе расследования уголовных дел онлайн-допроса (интернет-допроса, web-допроса, допроса с помощью видеоконференцсвязи), который представляет собой специальный метод получения криминалистически значимой и доказательственной информации, осуществляемый на основе использования интернет-технологий. Надо отметить, что онлайн-исследования проводятся в мире уже более 20 лет, и все эти годы ведутся споры об их качестве. В современной России попытки использования онлайн-методов в процессе различных исследований начались в конце XX века. Они уже активно используются судами при рассмотрении уголовных и гражданских дел. Сейчас эти исследования пытаются внедрить в криминалистическую и следственную практику.

Согласно проведенному анализу, практические работники считают, что в настоящее время допрос потерпевшего, свидетеля, а также подозреваемого и обвиняемого может быть произведен с использованием в режиме онлайн с вызовом их в орган расследования (дознания) определенного района, области, города республиканского значения, столицы, на территории которых они находятся на момент производства данного следственного действия. В ходе дистанционного допроса участники этого процессуального действия в прямой трансляции непосредственно воспринимают показания допрашиваемого лица.

Онлайн-допрос (допрос с помощью видеоконференцсвязи) можно проводить в ходе досудебного производства, непосредственно следователем или дознавателем. Аргументов в пользу того, чтобы предусмотреть в российском уголовно-процессуальном законодательстве использование систем видео-конференц-связи на стадии предварительного расследо-

вания, можно привести немало. Но современный российский законодатель этого не учитывает, ограничивая возможность проведения дистанционного онлайн-допроса случаями, необходимыми для обеспечения безопасности свидетелей и потерпевших и то только в ходе судебных заседаний.

Российский законодатель должен понимать, что онлайн-допрос направлен, прежде всего, на процессуальную экономию, оперативность, сокращение сроков досудебного производства. Очевидно, что производство допроса или очной ставки посредством видео-конференц-связи позволило бы следователю существенно сэкономить время расследования и повысить его эффективность.

Производство дистанционного допроса должно допускаться только в случаях, прямо предусмотренных действующим уголовно-процессуальным законом. Суть онлайн-допроса заключается в том, что допрашивающее лицо находится в помещении органа, который ведет расследование по делу, а допрашиваемое лицо — в ином следственном органе, на территории которого он находится либо проживает. Допрос проводится с помощью видео-конференц-связи с соблюдением требований, предъявляемых к производству допроса в целом.

Регламентация в действующем УПК РФ использования систем видео-конференц-связи при проведении допроса в ходе предварительного расследования приблизит наше законодательство к законодательству многих современных зарубежных государств, где дистанционный допрос давно уже предусмотрен и успешно проводится. Такая унификация отечественного уголовно-процессуального законодательства, в частности, позволит российским следователям и дознавателям в рамках запросов о международной правовой помощи при необходимости лично допрашивать лиц, находящихся за пределами Российской Федерации.

В завершение хотелось бы отметить, что использование систем онлайн-связи в ходе судопроизводства, а также криминалистическое исследование цифровых технологий и использование их данных в расследовании преступлений является объективным и необходимым требованием настоящего времени. Поэтому криминалисты вправе рассчитывать на то, что уже в ближайшем времени законодателем будут внесены соответствующие дополнения в действующее законодательство, помещения органов следствия, дознания, полиции и судов оборудуют надежными системами онлайн-связи, а в штат всех правоохранительных и следственных органов непосредственно войдут специалисты в области цифровых IT-технологий, которые будут напрямую помогать следователям в расследовании уголовных дел.

Высказанные предложения и рекомендации криминалистов могут в дальнейшем быть учтены российским законодателем, что позволит сократить время и повысить эффективность судопроизводства в целом.

В.А. Мещеряков, *д.ю.н., Воронежский государственный университет, г. Воронеж*
О.Ю. Цурлуй, *к.ю.н., Центральный филиал Российского государственного университета правосудия, г. Воронеж*

НЕКОТОРЫЕ ВОПРОСЫ ФИКСАЦИИ И ИЗЪЯТИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ С ЦИФРОВЫХ НОСИТЕЛЕЙ ПРИ ПРОИЗВОДСТВЕ ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

В соответствии с нормами ст. 74 УПК РФ доказательством по уголовному делу могут стать любые сведения, на основании которых суд, прокурор, следователь или дознаватель

могут установить наличие или отсутствие обстоятельств, имеющих значение для уголовного дела.

При этом данные сведения могут быть зафиксированы не только в виде протоколов и заключений, предусмотренных частью 2 названной выше статьи, но и представлены в форме иных документов, выполненных как в письменном, так и ином виде. На основании части 2 ст. 84 УПК РФ материальными носителями таких сведений могут выступать материалы фото- и киносъемки, аудио- и видеозаписи, а также иные носители информации, полученные, истребованные или представленные в порядке, установленном ст. 86 УПК РФ. Исходя из смысла данной статьи, законодатель не делает различий в формах представления фото- и киносъемки, аудио- и видеозаписи. Они могут быть закреплены как в традиционной аналоговой, так и в современной цифровой форме.

Особое место в этом ряду занимают электронные документы.

Согласно п. 11.1 ст. 2 Федерального закона от 27.07.2006 № 49-ФЗ «Об информации, информационных технологиях и защите информации», электронный документ — это «документированная информация, представленная в электронном формате, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах».

В соответствии с ГОСТ 2.051-2013 электронный документ получают с помощью программно-технических средств в результате автоматизированного проектирования (разработки) или преобразования документов, выполненных в бумажной форме, в электронную форму. Попутно следует отметить, специфика электронного документа такова, что содержание бумажного и электронного документа могут в значительной мере отличаться друг от друга. Этот факт обязательно необходимо учитывать при копировании электронных документов.

Местом размещения (хранения и воспроизведения) электронного документа является электронный носитель информации.

Согласно п. 3.1.9 ГОСТ 2.051-2013 электронный носитель — это материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники, то есть устройств, конструктивно предназначенных для постоянного или временного хранения данных в виде, пригодном для их использования в электронных вычислительных машинах, а также передачи по информационно-телекоммуникационным сетям.

Вот уже здесь, отмечая возможность использования различных носителей компьютерной информации при ее копировании в ходе следственных действий, следует обратить внимание на **первую особенность,** которой уделяется непростительно мало внимания при производстве следственных действий, но которая имеет исключительно важное криминалистическое значение.

Эта особенность заключается в виртуальном представлении значимых для расследуемого уголовного дела сведений, зафиксированных на материальном носителе в цифровом виде. При этом основное смысловое значение имеют не зафиксированные свойства материального носителя, всего лишь структура и последовательность цифровых данных, отражающих параметры формализованной модели, описывающей интересующее следствие явление.

Несмотря на значительное количество публикаций, посвященных данной теме [1, с. 165; 2, с. 35-37; 4, с. 34-35; 3, с. 49; 7, с. 56; 8, с. 161-163; 9, с. 42; 10, с. 14; 11, с. 196; 12, с. 123; 13, с. 8], остановимся на сути этой особенности более подробно.

Основной задачей предварительного расследования является формирование в установленном действующим уголовно-процессуальным законом порядке доказательств, на основа-

нии которых суд будет принимать решение о событии преступления и всех его неотъемлемых атрибутах.

Доказательства формируются надлежащими субъектами на основе следов, выявляемых на материальных объектах окружающей обстановки. При этом следами признается любая информация, возникшая в результате взаимного отражения объектов материального мира, которую мы умеем (в результате знания вида и природы взаимосвязи) связать с фактами, событиями и обстоятельствами, имеющими отношение к расследуемому уголовному делу.

Аргументы в пользу возможности отделения формы путем ее копирования (например, изготовления в нашем случае гипсового слепка) не принимаются, поскольку в ходе изготовления копии мы, с одной стороны, ухудшаем качество запечатленной формы (причем тем хуже, чем крупнее будут части вещества применяемого для изготовления слепка), а с другой — привносим свои дополнительные изменения за счет несовершенства используемых инструментов и навыков человека, изготавливающего копию. В любом случае изготовить копию без потери качества никогда не получится, а изготовление копии с копии вообще может привести к тому, что получившийся результат будет непригоден для решения не только идентификационных, но и диагностических криминалистических задач.

Принципиально иная схема отображения возникает при формировании виртуальных следов (цифровую форму фиксации которых мы получаем с компьютерных носителей). Возьмем случай, когда реальное явление (например, тот же удар топором по доске) фиксируется видеорегистратором. В ходе этой фиксации происходит электронно-цифровое отображение, основанное на использовании формальной модели реального явления, подлежащего регистрации, обладающее рядом весьма значимых для криминалистики свойств.

Во-первых, отображение происходит в искусственной среде формальной (чаще всего математической) модели, которая отражает с заданным качеством одни признаки и свойства моделируемого явления и абсолютно игнорирует другие. В результате фиксируются не все существующие в природе виды взаимодействия объектов окружающего мира, а лишь только те, которые были предусмотрены создателем этой искусственной среды.

Например, видеорегистратор, созданный для фиксации изображений в инфракрасном диапазоне электромагнитных волн, будет хорошо видеть теплые объекты и совершенно не регистрировать холодные (совпадающие по температуре с окружающей средой).

Причем качество регистрации изменений в искусственной среде обусловлено будет техническими возможностями (в нашем примере — разрешающей способностью, углом обзора объектива) или настройками регистратора (например, если видеорегистратор запускается от датчика движения, то в зависимости от настроек этого датчика он может вообще не зафиксировать медленно происходящие изменения, такие как разворачивание цветков растений, изменение положения солнечной тени и т.п.)

Во-вторых, регистрации на материальном носителе подлежит не сама формализованная модель (она, как правило, заложена в конструкцию или программное обеспечение средства регистрации) наблюдаемого явления, а только ее параметры в объеме и качестве, позволяющем в дальнейшем сформировать представление о зафиксированном явлении. В результате зафиксированные в цифровой форме виртуальные следы могут копироваться сколь угодно раз без потери их криминалистического качества.

В-третьих, семантическая сущность (смысловое значение) виртуальных следов, зафиксированных в цифровой форме, закреплена не в материале носителя, как в случае с материальными следами, а в структуре и последовательности и значении цифровых данных. В результате связь следа с событием, имеющим отношение к расследуемому уголовному делу, не определяется свойствами его материального носителя. Например, изображение с одинаковым качеством может быть зафиксировано как на оптическом диске (где физическим носителем

информации выступает наличие/отсутствие дырок в отражающем слое), так и на магнитном диске (где физическим носителем информации выступает магнитный домен) или полупроводниковой NAND-памяти флеш-накопителя. Более того, при определенных условиях без потери криминалистических качеств фиксации следов возможно преобразование форматов этого изображения (например, JPEG в TIFF и т.п.).

Таким образом, при производстве копирования компьютерной информации при соблюдении определенных технологических требований (иногда различных для различных криминалистических задач) без потери криминалистического качества возможно использование материальных носителей различного вида, объема и формата (используемой файловой системы) в том числе и некоторого их количества.

Второй особенностью, на которую следует обратить внимание при копировании компьютерной информации в ходе отдельных следственных действий, является уровень подготовки и технического оснащения специалиста, привлекаемого для производства необходимых технологических действий.

Анализ правоприменительной практики показал, что материальными носителями, наиболее часто встречающимися в ходе расследования уголовных дел, а также направляемых на исследование в рамках судебной компьютерной экспертизы являются следующие объекты [5]:

– компьютерные устройства (рабочие станции, персональные компьютеры, ноутбуки, планшеты и т.п.);
– SIM-карты;
– мобильные телефоны, пейджеры, смартфоны, диктофоны;
– флэш-карты, оптические диски;
– контрольно-кассовые машины;
– отдельные компьютерные программы или их системы, а также иные объекты авторских прав и т.п.

Одно разнообразие перечисленных объектов уже отражает широту спектра знаний, которыми должны обладать специалисты для производства копирования компьютерной информации из них. Упоминание о различных состояниях этой техники (исправен/неисправен, включен/выключен) только расширяет круг востребованных знаний, умений и технического оснащения.

Положения действующего уголовно-процессуального законодательства предусматривают следующий перечень следственных действий, выступающих в качестве способов собирания доказательств по уголовному делу, в ходе которых возможно получение (копирование или изъятие) компьютерной информации, хранящейся на электронных носителях:

• осмотр (места происшествия, предметов или документов);
• допрос (в случаях предоставления допрашиваемым лицом документа на электронном носителе и приобщения его к протоколу);
• обыск;
• выемка.

Учитывая специфику формирования и преобразования информации, хранящейся и передаваемой в электронной форме, названные следственные действия производятся в установленном соответствующими уголовно-процессуальными нормами порядке, с обязательным участием специалиста, обладающего соответствующими специальными знаниями, необходимыми для производства требуемых действий программно-техническими средствами, а также навыками их использования и достаточной квалификацией.

Таким образом, категорически нельзя согласиться с тем, что требование уголовно-процессуального законодательства по привлечению специалиста для изъятия электронных носи-

телей информации является чрезмерным и не соответствует современному уровню технической грамотности всего населения. Высказываемые некоторыми авторами мнения о том, что современные информационные технологии настолько просты в обращении, что практически не требуют специальных умений и знаний по их корректному использованию, нам представляются необоснованными [6, с. 42].

Положения части 3 ст. 164.1 УПК РФ закрепляют право следователя в ходе производства следственного действия осуществить копирование информации, содержащейся на электронном носителе. При этом в протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. К протоколу прилагаются электронные носители, содержащие информацию, скопированную с других электронных носителей, обнаруженных в ходе производства следственного действия.

На наш взгляд, самостоятельное копирование следователем информации с электронных носителей допустимо в исключительных случаях, когда полученная информация будет использоваться исключительно в качестве ориентирующей и в последующем не станет объектом экспертного исследования.

Проиллюстрируем сказанное примером. Камерой наружного наблюдения зафиксировано убийство, совершенное у входа в здание. Доступ к камере имели сотрудники охраны учреждения, расположенного в этом здании. В ходе производства расследования следователь самостоятельно в отсутствие юридического основания и надлежащего процессуального оформления скопировал видеофайл момента убийства с камеры наблюдения на флеш-накопитель и приобщил его к материалам уголовного дела. Ввиду грубейшего нарушения требований уголовно-процессуального законодательства приобщенная копия видеозаписи, хранящаяся на флеш-накопителе, не может выступать в качестве объекта экспертного носителя.

Отдельного разговора требует уровень технического оснащения специалиста, привлекаемого для решения задач копирования компьютерной информации. Это в первую очередь касается используемых им средств вычислительной техники (переносных компьютеров, ноутбуков, планшетов), вспомогательного коммутационного (различного рода кабели, переходники и адаптеры) и периферийного оборудования (копираторы, концентраторы и разветвители), а также специального программного обеспечения.

Диапазон такого оборудования крайне широк и представлен как открытыми (Open-Source), так и проприетарными разработками. Поскольку нормативно установленных требований по выбору состава и характеристик такого оборудования не существует, то их выбор осуществляется самим специалистом исходя из собственного опыта и удобства использования для решения поставленных задач.

Третьей особенностью копирования компьютерной информации в ходе отдельных следственных действий является необходимость определения условий формирования виртуальных следов, изъятие которых осуществляется.

В ряде случаев для решения определенной категории вопросов, возникающих в ходе расследования уголовного дела, требуется не только сам скопированный набор цифровых данных, но и оборудование, которое осуществляло регистрацию реального процесса, а также исходный физический носитель, на который проводилась соответствующая запись.

Изложенное весьма наглядно подтверждается следующим примером следственно-экспертной практики.

К эксперту-видеотехнику на исследование поступил файл с записью автомобильного видеорегистратора и заключение видеотехнической экспертизы по данному материалу, из которого следовало, что скорость автомобиля в момент съемки значительно превышала раз-

решенный порог движения по городу — 60 км/ч — со всеми вытекающими правовыми последствиями. Примененная методика исследования была типичной для подобных экспертиз. В интересующий момент времени на видеозаписи были найдены два соседних кадра, на которых были запечатлены неподвижные объекты. Для этих объектов определен размер их линейного смещения.

Из надписи на шильдике видеорегистратора установлена скорость записи — 30 fps. В результате скорость движения автомобиля, на котором был размещен видеорегистратор, была определена как размер вычисленного смещения неподвижных объектов на двух соседних кадрах, умноженных на 30 и 3600 (для получения пройденного расстояния в час).

Основанием для производства повторной экспертизы послужило разительное отличие установленной скорости от той, о которой говорил водитель, управлявший автомобилем.

Эксперт-видеотехник запросил на исследование не только файл с видеозаписью, но и сам видеорегистратор, а также SD-карту, на которую эта запись осуществлялась.

Исследовав SD-карту и видеорегистратор неизвестных китайских производителей, эксперт убедился, что в погоне за объемом хранимой информации при малой стоимости карты ее класс скорости записи был крайне низок. В результате несложных подсчетов стало ясно, что картинка установленного в файле видеозаписи разрешения пишется на SD-карту с плавающей скоростью всегда меньше заявленных 30 fps.

Как следствие, получившаяся оценка скорости движения оказалась завышенной, что полностью изменило квалификацию содеянного.

Последняя особенность, на которую необходимо обратить внимание при копировании компьютерной информации в ходе отдельных следственных действий, является требование обеспечения неизменности полученной цифровой копии.

Одним из наиболее простых и достаточно эффективных способов подтверждения неизменности скопированной в ходе производства следственных действий компьютерной информации выступает подсчет и фиксация контрольной суммы (хэш-функции) файла.

В соответствии с п. 3.1.5 ГОСТ Р 34.11-2012, хэш-код(hash-code) это строка бит, являющаяся выходным результатом вычисления хэш-функции. Данная функция позволяет построить однозначное соответствие любого набора цифровых данных (одного или нескольких файлов и даже всего материального носителя цифровой информации) и строки бит установленной длины. При этом вероятность того, что различным наборам данных будет соответствовать одно и то же значение хэш-функции, ничтожна мала, а изменение хотя бы одного бита в исходном наборе данных приводит к кардинальному изменению значения хэш-функции.

Использование данной технологии позволяет всем участникам уголовного преследования убедиться в том, что изъятая в ходе следственного действия информация в дальнейшем была неизменной.

В связи с этим, на наш взгляд, в протоколе следственного действия в ходе производится копирование компьютерной информации (цифровая видео- или аудиозапись, компьютерная программа, база данных и т.п.), необходимо обязательно отражать значение хэш-функции изымаемых информационных объектов, а также сообщать его лицу, у которого этот информационный объект был скопирован, с обязательной отметкой об этом в протоколе следственного действия.

Таким образом, обязательное участие специалиста в производстве следственных действий по осмотру и изъятию информации, содержащейся на электронных носителях, является положительным законодательным требованием. Обусловлено это еще и с позиции тактики следственного действия, поскольку специалист может заметить то, что скрыто ввиду отсутствия специальных познаний от следователя. В работе с электронными носителями информации следователю недостаточно общих криминалистических знаний.

В связи с изложенным предлагаем дополнить положения уголовно-процессуального законодательства нормой следующего содержания.

В протоколе следственного действия должны быть указаны аппаратные и программные средства, использованные при осуществлении копирования информации, порядок их применения, используемые электронные носители информации и их характеристики, а также значения хэш-сумм, скопированных в ходе следственного действия информационных объектов.

Список литературы

1. Борисов В.В. Особенности фиксации информационных следов в практике защиты информации // Известия Южного федерального университета. Технические науки. Т. 94, 2009. № 5. С. 164–168.
2. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: монография. Волгоград, ВА МВД России, 2008. 401 с.
3. Гаврилин Ю.В., Лыткин Н.Н. Понятия, свойства и криминалистическое значение компьютерно-технических следов преступления // Вестник криминалистики. 2005. № 4. С. 49-55.
4. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: учеб. пособие / под ред. Н.Г. Шурухнова. М.: Книжный мир, 2001. 88 с.
5. Зазулин А. Обзор судебной практики по участию специалиста и производству судебных экспертиз при исследовании цифровой информации. URL: https://zakon.ru/blog/2018/05/06/obzor_sudebnoj_praktiki_po_uchastiyu_specialista_i_proizvodstvu_sudebnyh_ekspertiz_pri_issledovanii_ (дата обращения 04.01.2020).
6. Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации // Законность. 2019. № 5. С. 40-43.
7. Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений: дис. … канд. юрид. наук. М., 1997. 215 с.
8. Лушин Е.А. О термине «электронно-цифровые следы» // Расследование преступлений: проблемы и пути их решения. 2017. № 4 (18). С. 161-163.
9. Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности: дис. ... канд. юрид. наук. М.: Московский университет МВД России, 2007. 201 с.
10. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. … д-ра юрид. наук. Воронеж, 2001. 39 с.
11. Островский О.А. Алгоритм выявления временных характеристик исследуемого факта преступления на основе анализа компьютерных следов // Проблемы формирования правового социального государства в современной России: материалы XIII всероссийской национальной научно-практической конференции. Новосибирск: Новосибирский государственный аграрный университет, 2017. С. 195-198.
12. Поляков В.В., Шебалин А.В. К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2013. № 11-1. С. 123-125.
13. Тулупьева Т.В., Суворова А.В., Азаров А.А., Тулупьев А.Л., Бордовская Н.В. Возможности и опыт применения компьютерных инструментов в анализе цифровых следов студентов-пользователей социальной сети // Компьютерные инструменты в образовании. 2015. № 5. С. 3-13.

И.Д. Милич, *ассистент кафедры уголовного права Юридического факультета Государственного университета в г. Нови-Сад, Республика Сербия, г. Нови-Сад*

ПРИШЛО ЛИ ВРЕМЯ ДЛЯ НОВОГО УГОЛОВНОГО НАКАЗАНИЯ В РЕСПУБЛИКЕ СЕРБИЯ — ЗАПРЕТА ДОСТУПА В ИНТЕРНЕТ?

К совершившим уголовные преступления лицам в ходе уголовного процесса применяется уголовное наказание. Одной из целей применения наказания является и специальная превенция. Таким образом, воздействие наказания на осужденное лицо способствует предотвращению совершения уголовных преступлений в будущем. В Республике Сербия Уголовным кодексом предусмотрены следующие виды наказания, которые могут быть применены к совершеннолетним лицам, совершившим уголовные преступления: штрафы, предупреждения и меры, гарантирующие безопасность [1]. В соответствии с законом наказание в виде тюремного заключения является самым строгим уголовным наказанием в Республике Сербия — особенно с 1 декабря 2019 г., когда было введено наказание в виде пожизненного лишения свободы. Так, до 1 декабря 2019 г. уголовное законодательство Республики Сербия предусматривало не наказание в виде пожизненного тюремного заключения, а наказание в виде лишения свободы на срок от 30 до 40 лет.

Однако иногда и другие виды уголовного наказания могут оказать значительное воздействие на лицо, совершившее уголовное преступление. Например, лишение права занимать определенные должности или заниматься определенной деятельностью, депортация иностранцев, запрет на посещение мест проведения официальных спортивных соревнований. Иногда и сам факт внесения информации о совершившем уголовное преступление лице в соответствующий реестр может иметь для него более тяжелые последствия, чем применение определенных мягких наказаний. Таким образом, одно и то же наказание может оказывать различное воздействие на лицо, совершившее уголовное преступление.

Места лишения свободы в Сербии переполнены, а количество лиц, вновь совершающих уголовные преступления, из года в год не уменьшается. Государство разными способами пытается снизить уровень криминала. Прежде всего, имеет место применение «уголовно-правовых мер», которые, как предполагается, способствуют снижению количества совершаемых уголовных преступлений, а тем самым и количества вновь совершаемых уголовных преступлений. За последние несколько лет Уголовный кодекс в Республике Сербия неоднократно менялся и дополнялся. Эти изменения и дополнения, по большей части, касаются определения новых уголовных преступлений, изменения существующих определений, ужесточения наказаний, запретов на смягчение наказания и другое. Помимо этого, принимаются и новые законы, которые «определяют уголовно-правовой материал». Необходимо подчеркнуть, что множество подобных изменений и дополнений Уголовного кодекса, как и принятие закона, который «определяет уголовно-правовой материал», было введено в правовую систему под влиянием широкой общественности, без критической оценки профессионалов и без серьезного — прежде всего криминалистического — исследования. В отдельных случаях причиной для такой законодательной интервенции становилось совершение отдельных вызвавших широкий общественный резонанс уголовных преступлений, ход расследования и судебный процесс по которым освещались в СМИ ежедневно.

Классические уголовные преступления (например, убийства и кражи) существовали всегда. Вместе со всесторонним развитием общества увеличивается и количество инкриминаций. Например, нельзя было инкриминировать преступления, связанные с нарушениями безопасности дорожного движения во времена, когда дорожного движения не было, или уголовные

преступления против безопасности компьютерных данных во времена, когда компьютерные данные не существовали.

С другой стороны, и уголовное наказание меняется. Распространенные некогда смертную казнь, изгнание и нанесение увечий заменили «гуманные наказания», прежде всего, наказание в виде лишения свободы. Со временем были введены и иные виды наказания, посредством которых ограничивают или лишают прав лиц, совершивших уголовные преступления, препятствуют реализации ими определенных прав, назначают лечение и другое. Для исполнения наказания в виде лишения свободы для особо опасных преступников формируют специальные отделения в тюрьмах [2]. Обобщенно можно сказать, что одновременно с возникновением некоторых прав и свобод вводятся и уголовные наказания, которые реализуются в форме ограничения или лишения этих прав и свобод.

Меняются способы и средства совершения уголовных преступлений. Средства, которые используются для совершения уголовных преступлений, могут быть изъяты в ходе уголовного процесса. Наряду с классическими средствами совершения уголовных преступлений, сегодня преступниками чаще и чаще используется Интернет. Все большее количество уголовных преступлений можно совершить с помощью доступа в Интернет. Например: преследование; несакционированный доступ к защищенному компьютеру, компьютерной сети или электронной базе данных; раскрытие личной и семейной информации; посредничество в проституции; демонстрация, приобретение и хранение порнографических материалов и вовлечение малолетних лиц в порнографический бизнес; провокация паники и общественных беспорядков. Сегодня все чаще с помощью Интернета совершается мошенничество, как и вымогательство, шантаж, а также другие уголовные преступления. Необходимо отметить, что посредством использования Интернета реализуется подготовка к совершению уголовного преступления — таким образом, что с его помощью обеспечивается доступ к определенной информации. Обеспечивается доступ к данным жертв уголовных преступлений. С помощью Интернета осуществляется подстрекательство к совершению уголовных преступлений. Нередко через Интернет формируются криминальные группировки, особенно те, которые имеют международный характер. Их коммуникация, планирование, как и совершение уголовного преступления, было бы невозможно (или было бы затруднено) без обращения к технологии Интернета.

Возможно, уголовное наказание в виде запрета на доступ в Интернет повлияло бы на снижение количества уголовных преступлений, а вместе с тем и на снижение количества вновь совершаемых преступлений. Особое место тут нашла бы специальная превенция. Лица, которым запрещено использовать Интернет, лишаются возможности повторить уголовное преступление, которое можно совершить с его помощью. Таким образом, они лишаются «средства» совершения уголовного преступления, аналогично тому, как в соответствии с действующими порядками у совершившего уголовное преступление лица изымаются вещи в ходе исполнения мер по обеспечению безопасности (ст. 87 Уголовного кодекса). То же самое имеет место в случае наказания в виде «лишения права занимать определенные должности или заниматься определенной деятельностью», так как тот, кто «злоупотребил положением» посредством этого наказания, на определенное время лишается права в будущем осуществлять определенную деятельность, что означает, что он «лишается возможности» повторить «злоупотребление положением» (ст. 85 Уголовного кодекса). Также и наказание в виде изъятия водительских прав применяется к лицам, которые использовали транспортное средство для совершения уголовного преступления (ст. 53 Уголовного кодекса). Схож с мерой обеспечения безопасности и запрет на управление транспортным средством, так как в этом случае правонарушителю запрещается управлять транспортным средством, если он нарушил безопасность дорожного движения (ст. 86 Уголовного кодекса). Введение запрета на доступ в Интернет

в определенном смысле стало бы уголовно-правовой реакцией в отношении совершивших уголовное преступление лиц, которые совершили его посредством использования Интернета.

Важно напомнить, что на основе Закона об уголовном процессе Республики Сербия в одном случае можно ввести запрет на использование Интернета [3]. Речь идет о случае, когда «лицу, которому предъявлено обвинение» (но которое не осуждено), определяется мера пресечения в виде домашнего ареста (это мера, с помощью которой обеспечивается присутствие обвиняемого лица и беспрепятственная реализация уголовного процесса), так как тогда одновременно можно ввести запрет на использование обвиняемым Интернета. Таким образом, если запрет на использование Интернета может быть применен в отношении обвиняемого лица, то это может стать одним из аргументов в пользу того, что такой же запрет может быть применен и в отношении осужденного лица.

Если бы законодательно было принято решение о применении запрета на доступ в Интернет, то это решение необходимо было бы реализовать посредством установления новой меры обеспечения безопасности — запрета на доступ в Интернет. В этом случае данная мера исполнялась бы как наказание и мера по обеспечению безопасности. В любом случае, нужно было бы предвидеть, что время отбытия наказания в местах лишения свободы не будет засчитано в качестве времени действия меры по запрету доступа в Интернет. Это относилось бы к осужденным лицам, которые отбывают свое наказание в виде лишения свободы в тюрьмах. Упомянем лишь, что в тюрьмах Сербии заключенные не могут пользоваться Интернетом. Необходимо выделить и то, что в Республике Сербия наказание в виде лишения свободы может отбываться в тюрьмах или в помещении, где осужденный проживает (так называемое домашнее заключение). Существует возможность, что осужденный, которому назначено наказание в виде лишения свободы сроком менее одного года при определенных условиях, отбывает данное наказание в помещении, в котором проживает (в своей квартире или доме). В этот период по решению суда осужденный может быть и под электронным надзором. Представляется, что было бы оправдано в этом случае, чтобы мера в виде запрета на доступ в Интернет применялась одновременно с исполнением наказания в виде лишения свободы — наказания в виде так называемого домашнего заключения. Было бы нелогично, если бы осужденный во время отбытия наказания в виде домашнего заключения имел доступ в Интернет, а после отбытия наказания началось применение меры по запрету. Требовалось бы определить и санкции за нарушение осужденным меры запрета [4].

В Республике Сербия довольно часто выносится условный приговор. Так, в 2009 г. было вынесено 23 382 условных приговора, в то время как в том же году было вынесено 9 763 приговора к тюремному заключению [5]. В связи с этим запрет доступа в Интернет мог бы быть предусмотрен как вид защитного контроля. В этом случае реализацию защитного контроля необходимо было бы предусмотреть как причину отмены условного осуждения с тем, что необходимо было бы определить, будет ли отмена условного осуждения обязательной или факультативной.

Самое большое право, которое может получить осужденное лицо, которое наказание в виде лишения свободы отбывает в тюрьме — это условное освобождение. В том же 2009 г. из тюрем было выпущено 1735 осужденных лиц [6]. В связи с этим, вероятно, было бы оправдано предусмотреть возможность, чтобы осужденному лицу, которое получило условное освобождение, была вменен и уголовно-правовой обязательный запрет на доступ в Интернет (при условии, что ему не запрещен доступ в Интернет в виде меры обеспечения безопасности). Если бы осужденный нарушил запрет и вышел в Интернет, то это нужно было бы рассматривать как основание отмены условного освобождения. Также необходимо было бы предусмотреть, будет ли в этом случае отмена условного освобождения обязательной или факультативной.

Если бы законодательно был введен запрет на доступ в Интернет, потребовалось бы определить и обязательный или необязательный характер вынесение запрета на доступ в Интернет. Возможно, следует предусмотреть обязательный запрет на доступ в Интернет или факультативный. Мы склонны сделать вывод о том, что было бы оправдано предписать только факультативное вынесение запрета, чтобы оставить судье возможность принять решение о применении или неприменении запрета на использование Интернета. Таким образом, судья на основании независимого судебного заключения принимал бы решение о том, будет ли применен запрет на доступ в Интернет, что зависело бы от характера и тяжести уголовного преступления и личности лица, его совершившего [7]. Суд обязан соответствующим образом изучить личность совершившего уголовное преступление лица и после этого исследования реализовать индивидуализацию уголовного наказания [8].

То, насколько данное уголовное наказание может подействовать на совершившее уголовное преступление лицо, зависит от многих критериев. Самым важным вопросом тут является то, насколько Интернет необходим лицу, совершившему уголовное преступление. Особенно это затронуло бы лица, чья трудовая деятельность невозможна без использования Интернета. В этом случае запрет имел бы соответствующее влияние и на трудовые отношения осужденного, а вместе с тем и на его существование, как и на существование членов его семьи. Однако и при вынесении других уголовных наказаний встает вопрос о трудовых отношениях осужденного, его существовании и существовании членов его семьи. Например, если осужденному назначат меру по обеспечению безопасности в виде запрета на управление транспортным средством или наказание в виде лишения водительских прав, оно будет влиять на трудовые отношения осужденного, а вместе с тем и на существование его и членов его семьи. С другой стороны, эта мера меньше бы задела тех осужденных, чьи трудовые отношения не обусловлены использованием Интернета. Возможно, законодательство должно было бы предвидеть в случае принятия решения о введении запрета на доступ в Интернет возможность, чтобы осужденный все-таки в определенных случаях, при соответствущих условиях, в определенное время и под надзором уполномоченных органов мог использовать Интернет. Решение об этом опять должен был бы принять суд посредством судебного решения. Таким образом, существовала бы возможность, чтобы осужденный, даже если ему вынесен запрет на доступ в Интернет, при определенных условиях мог им пользоваться.

Исполнение наказания следует после того, как судебное решение вступит в силу и будет подлежать исполнению. Процесс исполнения уголовных наказаний в Республике Сербия определяется, прежде всего, Законом об исполнении уголовных наказаний [9]. В связи с этим если бы законодательно был предусмотрен и запрет на доступ в Интернет, то необходимо было бы определить и сам способ исполнения этого наказания. Представляется, что процесс исполнения был бы достаточно сложным. Таким образом, то, что лица, которым назначен запрет доступа в Интернет, находятся на свободе, усложняет контроль того, используют или не используют они Интернет.

Список литературы

1. Уголовный кодекс, Служебный вестник Республики Сербия, № 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019.

2. Милич Д. Иван. Где отбывают тюремное заключение самые опасные заключенные в Республике Сербия? Уголовная политика и культура противодействия преступности: материалы Междунар. науч.-практ. конф., 20 сент. 2019 г.: в 2 т. / редкол.: А.Л. Осипенко, К.В. Вишневецкий, В.С. Соловьев и др. Краснодар: Краснодарский университет МВД России, 2019. Т. I. С. 44-50.

3. Кодекс уголовного процесса, Служебный вестник Республики Сербия, № 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019.

4. Милич И. О последствиях нарушения запрета, который введен в качестве меры, обеспечивающей безопасность // Сборник трудов Юридического факультета государственного Университета в городе Нови-Сад. 2018. № 3. С. 1269–1281.

5. Бюллетень «Совершеннолетние лица, совершившие уголовные преступления в Республике Сербия: заявления, обвинения и приговоры. URL: https://publikacije.stat.gov.rs/G2019/Pdf/G20195653.pdf (дата обращения: 01.02.2020).

6. Годовой отчет Управления исполнения уголовных наказаний за 2009 год. URL: http://reforma.bezbednost.org/wp-content/uploads/downloads/2012/09/2009-Godisnji-izvestaj-Ministarstvo-pravde-Uprava-za-izvr%C5%A1enje-krivi%C4%8Dnih-sankcija.pdf (дата обращения: 01.02.2020).

8. Милич И. Индивидуализация тюремного заключения — криминологические, уголовно-правовые аспекты и аспекты наказания. Нови-Сад, 2017. С. 109-114.

7. Милич И. О необходимости исследования личности обвиняемого в уголовном процессе. Актуальные проблемы права иправоприменительной деятельности на современном этапе: материалы Международной научно-практической конференции. Краснодар, 25-26 сентября 2014. С. 192-196.

9. Закон о применении уголовных наказаний, Служебный вестник Республики Сербия, № 55/2014, 35/2019.

В.В. Поляков, *к.ю.н., доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*

АЛГОРИТМИЗАЦИЯ РАЗРЕШЕНИЯ КРИМИНАЛИСТИЧЕСКИХ СИТУАЦИЙ ПРИ РАССЛЕДОВАНИИ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРЕСТУПЛЕНИЙ

Последние десятилетия характеризуются взрывным технологическим прорывом в информационной сфере. Это явление оказало существенное влияние на различные общественные отношения, в том числе привело к появлению новой опасной разновидности преступности. Анализ судебно-следственной практики, результатов анкетирования, отчетов ведущих российских компаний, специализирующихся на обеспечении информационной безопасности, а также опубликованных исследований приводит к выводу, что для преступлений, связанных с использованием компьютерных и информационно-телекоммуникационных средств, может быть выделена группа наиболее общественно опасных преступлений, способ которых может быть назван высокотехнологичным. В высокотехнологичных преступлениях присутствует групповая форма совершения, при этом в состав группы входит специалист в сфере компьютерных технологий, используется информационная сеть для удаленного доступа к компьютерной информации, применяются специально разработанные или модифицированные программно-аппаратные средства, причем способ преступления является полноструктурным [1]. Выделение высокотехнологичных способов и соответствующих им высокотехнологичных преступлений имеет важное значение для криминалистической теории и практики, поскольку оно лежит в основе разработки частной криминалистической методики расследования этих преступлений, обладающих существенной спецификой [2].

Нужно признать, что в силу стремительности происходящих изменений и современные правовые теории, и практическая деятельность правоохранительных и судебных органов оказались не готовы к противодействию высокотехнологичной преступности. Полагаем, что значительную роль в таком противодействии может сыграть привлечение ситуационного подхода. Этот подход, зародившийся в рамках частной теории криминалистических ситуаций, по мнению отечественных ученых-криминалистов, вошел практически во все разделы криминалистики. Так, В.К. Гавло и Д.В. Ким отмечали, что «именно ситуационный подход является основополагающим во всех разделах криминалистики» [3]. На эту его роль обращал внимание Р.С. Белкин, еще в начале 2000-х писавший: «В криминалистике утвердился ситуационный подход к реализации в практике разрабатываемых ею рекомендаций» [4, с. 116].

Полагаем, что для применения ситуационного подхода к разработке частной методики расследования высокотехнологичных преступлений необходимо последовательное решение следующих задач [5].

I. Прежде всего нужно провести накопление эмпирического материала, относящегося к практике расследования высокотехнологичных преступлений. Этот материл представляет собой совокупность конкретных ситуаций, возникавших в процессе расследования на всех его этапах, включая проверочный, предшествующий возбуждению уголовного дела, этапы предварительного расследования и судебного разбирательства [6]. Отметим, что серьезной проблемой при решении этой исходной задачи является относительно малый объем следственной и судебной практики, которые находятся в стадии формирования.

II. При наличии статистически значимого объема информационных данных о конкретных ситуациях расследования высокотехнологичных преступлений должна быть проведена обработка этих данных, по итогам которой будут выявлены основные закономерности расследования. В результате будут выделены наборы типовых и типичных ситуаций расследования [7]. Полученные типовые и типичные ситуации являются той основой, которая призвана обеспечить разработку криминалистических методических рекомендаций для практики. Кроме того, будет проведен анализ оптимальных способов благоприятного разрешения проблемных и конфликтных ситуаций, отличающих расследование высокотехнологичных преступлений.

III. Заключительная группа задач включает в себя разработку конкретных криминалистических методов и тактических приемов, обеспечивающих благоприятное разрешение ситуаций, возникавших на том или ином этапе в процессе расследования. Одновременно предполагается также выработка рекомендаций, определяющих последовательность предлагаемых к использованию тактических решений [8, с. 56].

После того как описанные задачи будут реализованы, действия субъектов расследования по разрешению ситуаций с помощью аппарата криминалистической ситуалогии могут быть алгоритмизированы. Целесообразность такой алгоритмизации обусловлена тем, что каждому шагу алгоритма соответствует применение вполне определенных тактических приемов. Учеными-криминалистами неоднократно подчеркивалось положительное влияние алгоритмизации на результативность действий следователя, который постоянно сталкивается с проблемой выбора конкретных следственных действий и очередности их проведения [9, с. 25-26]. С.И. Давыдов отмечал, что «частная криминалистическая методика должна выглядеть как своеобразная программа (алгоритм) действий следователя» [10].

Опишем в наиболее общем и формализованном виде алгоритм, представляющий последовательность этапов, раскрывающих применение ситуационного подхода к разрешению криминалистических ситуаций, формирующихся в процессе расследования высокотехнологичных преступлений.

Этап 1. На первом этапе субъектом ситуации проводится анализ имеющейся в наличии информации об обстановке и обстоятельствах преступления, а также оцениваются условия

и возможности расследования. Фактически на данном этапе определяется содержание конкретной ситуации и ее особенности.

Этап 2. На втором этапе проводится соотнесение конкретной ситуации с известным набором типовых и типичных ситуаций, характерных для высокотехнологичных преступлений и описанных криминалистической теорией. Этот набор выступает как обобщение самых общих и характерных свойств статистически значимого числа конкретных ситуаций данного вида. Другими словами, осуществляется, по словам Ю.А. Головина, соотнесение «конкретной сложившейся по делу ситуации с признаками различных классификационных видов» ситуаций [11, с. 48]. На этом этапе субъект ситуации определяет, насколько возникшая конкретная ситуация соответствует имеющемуся набору, является она типичной или атипичной и т.д.

Этап 3. На основании проведенного на предыдущем этапе анализа субъект ситуации выбирает набор и последовательность наиболее эффективных тактических приемов, рекомендуемых криминалистической теорией, то есть проводит индивидуализацию имеющихся в его распоряжении рекомендаций. Можно сказать, что на этом этапе общего алгоритма формулируется своеобразный частный алгоритм, раскрывающий план применения конкретных тактических приемов для данного момента расследования.

Этап 4. Данный этап отражает практическую реализацию криминалистических действий, алгоритм которых был выработан на предыдущем этапе. Этот этап обеспечивает получение нового объема информационных данных об обстоятельствах преступления и доказательствах по уголовному делу, а также об изменившихся вследствие реализации этапа условиях расследования.

Этап 5. На последнем этапе проводится обработка полученных новых информационных данных, оценивается, насколько удалось достичь поставленные цели расследования. Осуществляется прогноз ситуаций, которые могут возникнуть при дальнейшем развитии расследования. Завершение этого этапа означает разрешение первоначальной конкретной ситуации и формирование новой ситуации, характеризующейся новой совокупностью информационных данных по делу и изменившимися условиями расследования.

Далее алгоритм повторяется, то есть осуществляется качественно та же последовательность действий, но только для новой ситуации. Повторение всего цикла продолжается вплоть до окончательного разрешения ситуаций, формирующихся при расследовании преступления.

Полагаем, что описанный подход к расследованию высокотехнологичных преступлений, основанный на алгоритмизации процесса разрешения криминалистических ситуаций, может быть применен и к ситуациям оперативно-розыскной деятельности. Как отмечал С.И. Давыдов, «если не придавать оперативно-розыскным рекомендациям форму алгоритма или программы, трудно будет добиться их безусловной ориентации на реальные оперативно-розыскные ситуации и, соответственно, на решение задач, стоящих перед оперативным сотрудником» [10].

В случае высокотехнологичных преступлений применение ситуационного подхода сталкивается со специфической трудностью, характерной для новых видов преступности и заключающейся в недостаточности имеющейся правоохранительной практики. Преодоление данной трудности может, как мы полагаем, быть осуществлено следующим образом.

Во-первых, должна проводиться последовательная работа по созданию новых и модернизации имеющихся теоретических разработок криминалистической ситуалогии. Она должна включать в себя выработку новых критериев типизации ситуаций расследования высокотехнологичных преступлений, адекватно отражающих их специфику [12]. Далее, необходимо описать типовые и типичные ситуации, возникающие не только для наиболее исследованного этапа предварительного расследования, но и для других этапов. Особенно важным представляется провести типизацию ситуаций, возникающих при судебном разбирательстве. Наконец,

предстоит обратить внимание на совершенствование рекомендуемых тактических приемов, которые должны соответствовать новым техническим средствам и способам, используемым для совершения и сокрытия преступлений. Для этого нужно расширять технические возможности для отдельных криминалистических действий, в частности, непрерывно совершенствовать методики проведения компьютерно-технических экспертиз [13].

Во-вторых, предстоит повышать роль творческой деятельности субъектов ситуации, прежде всего следователей и оперативных сотрудников, в процессе анализа ими складывающихся ситуаций расследования. Возрастание этой роли связано с особой криминалистической сложностью расследования высокотехнологичных преступлений и, как следствие, объективной трудностью принятия решений при анализе конкретной ситуации [14]. Кроме того, в силу недостаточной разработанности методических рекомендаций или их полного отсутствия субъекту ситуации приходится творчески определяться, какие коррективы требуется внести в набор известных тактических приемов при реализации общего алгоритма расследования, основанного на ситуационном подходе. Значение творческой составляющей в деятельности субъектов ситуации, в свою очередь, означает необходимость их профессиональной подготовки и регулярной переподготовки [15].

Список литературы

1. Поляков В.В., Слободян С.М. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации // Известия Томского политехнического университета. 2007. Т. 310, № 1. С. 212-216.
2. Поляков В.В. Основы формирования криминалистической методики расследования высокотехнологичных преступлений // Уголовное судопроизводство: правовое, криминалистическое и оперативно-розыскное обеспечение: монография / под ред. С.И. Давыдова. Барнаул: Изд-во Алт. ун-та, 2019. Гл. 2 п. 2.2. С. 114-126.
3. Гавло В.К., Ким Д.В. Некоторые вопросы дальнейшего развития ситуационного подхода в расследовании преступлений // Уголовно-процессуальные и криминалистические чтения на Алтае: материалы ежегодной региональной научно-практической конференции. Вып. 2. Барнаул: Изд-во Алт. ун-та, 2003. С. 37-41.
4. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М.: НОРМА, 2001. 240 с.
5. Поляков В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. № 1 (21). С. 46-50.
6. Князьков А.С., Ондар Д.С. Проблемы этапности криминалистической деятельности в контексте ситуационного подхода // Вестник Томского государственного университета. Право. 2018. № 30. С. 34-52.
7. Волчецкая Т.С. Криминалистическая ситуалогия: монография / под ред. проф. Н.П. Яблокова. Москва; Калинингр. ун-т. Калининград, 1997. 248 с.
8. Комаров И.М. Криминалистические операции и следственные ситуации в системе криминалистической характеристики расследования преступлений // Вестник Московского ун-та. Сер. 11. Право. 2014. № 4. С. 50-61.
9. Шаталов А.С. Проблемы алгоритмизации расследования преступлений: автореф. дис. … д-ра юрид. наук. М., 2000. С. 25-26.
10. Давыдов С.И. Ситуационные аспекты алгоритмизации оперативно-розыскной деятельности органов внутренних дел // Юридическая наука и правоохранительная практика. 2008. № 2 (5). С. 80-86.

11. Головин А.Ю. Теоретические основы и актуальные проблемы криминалистической систематики на современном этапе развития криминалистики: автореф. дис. … д-ра юрид. наук. М., 2003. 57 с.

12. Поляков В.В. Начальные следственные ситуации расследования высокотехнологичных преступлений // Цифровые технологии в юриспруденции: генезис и перспективы: материалы I Международной межвузовской научно-практической конференции (28 февраля 2020 г., Москва) / НИУ МИЭТ, Краснояр. гос. аграр. ун-т, 2020. С. 123-127.

13. Судебная компьютерно-техническая экспертиза / Е.Р. Россинская, А.И. Усов. М.: Право и закон, 2001. 414 с.

14. Зеленский В.Д. Криминалистические проблемы организации расследования преступлений: дис. … д-ра юрид. наук. Краснодар, 1991. 323 с.

15. Поляков В.В. Особенности подготовки специалистов для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации // Известия Алтайского государственного университета. 2010. № 2/1. С. 96-97.

А.Е. Федюнин, *д.ю.н., профессор кафедры уголовного процесса*
Саратовской государственной юридической академии, г. Саратов
Н.М. Перетятько, *к.ю.н., доцент кафедры уголовного процесса*
Саратовской государственной юридической академии, г. Саратов
В.Ю. Алферов, *к.ю.н., доцент кафедры правосудия и правоохранительной деятельности*
Саратовского социально-экономического института (филиал) РЭУ им. Г.В. Плеханова,
г. Саратов

ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ (НАБЛЮДЕНИЕ) С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

В рамках осуществления оперативно-розыскной деятельности, в том числе и оперативно-розыскного сопровождения расследования уголовных дел, наиболее широкие возможности для применения различных технических средств предоставляются оперативным работникам при осуществлении наблюдения — оперативно-розыскного мероприятия (ОРМ), предусмотренного п. 6 ст. 6 Федерального закона «Об оперативно-розыскной деятельности» (далее — ФЗ «Об ОРД») [1]. К сожалению, ФЗ «Об ОРД» не дает даже краткого определения данному мероприятию, оставляя его на усмотрение правоприменителя и ведомственного нормативно-правового регулирования. Из многочисленных комментариев к данному Закону, а также сложившейся практики оперативной работы его в общем можно охарактеризовать как негласное слежение за лицами, подозреваемыми в совершении преступлений, которое может проводиться в различных местах и способами, не противоречащими действующему законодательству.

Уточняя сущность данного ОРМ, отметим, что оно заключается в получении сведений об объекте посредством визуального, слухового, электронного, радиолокационного и иных способов контроля в помещениях, на транспорте и в иных условиях его нахождения [2, с. 171]. В качестве объекта наблюдения выступают лица, транспортные средства, различные помещения, места сбыта или хранения похищенного и др.

С.Д. Ковалев и Е.В. Полуянова относят наблюдение к разновидности оперативно-технических мероприятий, проводимых негласно с использованием специальных технических средств и направленные на получение и фиксацию информации, необходимой для реализации задач ОРД. По их мнению, в данном случае технические средства применяются для «тайного слежения (наблюдения) за действиями, операциями, разговорами и местами нахождения проверяемых (разрабатываемых) лиц в жилых и нежилых помещениях (служебных, общественных, спортивно-оздоровительных, культурно-просветительских), в транспортных средствах и на открытой местности. Указанное оперативно-техническое мероприятие проводится специальными оперативно-техническими и оперативно-поисковыми подразделениями с возможным привлечением должностных лиц оперативных подразделений соответствующих государственных органов. Специальные технические средства, предназначенные для аудио- и видеозаписи могут использоваться для наблюдения за разрабатываемыми лицами, подозреваемыми в совершении преступлений» [3, с. 69].

В современных условиях рассматриваемое мероприятие практически всегда осуществляется с применением технических средств различного назначения, используемых как гласно, так и под прикрытием, с применением легендирования действий оперативных сотрудников. Основным требованием к порядку его проведения является непрерывность, в связи с чем наблюдение чаще всего может осуществляться как по месту работы, жительства, учебы, отдыха проверяемых и разрабатываемых лиц, так и в их в транспортных средствах, на маршрутах передвижения и в других местах их нахождения. Естественно, что проведение такого рода мероприятий в определенных ситуациях сопряжено с необходимостью передачи и обработки информации и применением информационно-телекоммуникационных технологий.

В юридической и специальной литературе многие авторы, например В.В. Николюк [4, с. 216], В.М. Мешков, В.Л. Попов [5, с. 32], В.В. Каминский, В.В. Коряковцев, К.В. Питулько [6] классифицируют наблюдение на три вида: физическое, электронное и комплексное. Аналогичная классификация принята уже давно в законодательстве США [7, с. 55], которые являются лидером как по уровню технического обеспечения данного мероприятия, так и по накопленному опыту его применения начиная с 30-х годов прошлого века. В то же время следует отметить, что исходя из смысла и содержания данного оперативно-розыскного мероприятия, рассматриваемое нами деление представляется достаточно условным, поскольку его проведение в существующих реалиях практически никогда не бывает в «чистом виде», как без использования арсенала различных технических средств, так и органов восприятия наблюдателя.

Представляется, что в современных условиях быстрого развития техники и средств коммуникаций данное ОРМ следует рассматривать как комплексное, с использованием различных видов технических средств, непосредственно предназначенных для наблюдения, средств фиксации наблюдаемых событий на материальные носители, а также средств телекоммуникаций, позволяющих в реальном времени удаленно наблюдать за происходящим и при необходимости корректировать действия сотрудников, непосредственно осуществляющих мероприятие. Особенно важное значение для дальнейшей реализации полученных материалов в ходе уголовного судопроизводства и приобщения их к уголовному делу в качестве доказательств имеет документальное оформление организации подготовки и проведения данного ОРМ, поскольку полное документирование и фиксация всех действий с реальной привязкой к временной шкале позволит в полной мере гарантировать придание результатам ОРД всех необходимых свойств доказательств.

Значительный вклад в решение данного вопроса внес Конституционный Суд РФ, который в своих Определениях от 21 октября 2008 г. № 862-О-О [8]; от 17 июля 2007 г. 3 597-О-О [9]; от 20 марта 2007 г. № 178-О-О [10]; от 16 ноября 2006 г. № 454-О [11]; от 11 июня 2006 г.

№ 268-О [12] указал, что по смыслу законодательства об оперативно-розыскной деятельности применение средств аудио- и видеозаписи наблюдаемых событий, если они не ограничивают конституционные права человека и гражданина, не требуют вынесения специального судебного решения.

Оперативно-розыскное наблюдение, проводимое в широком смысле электронным (комплексным) способом, является действием, в определенных ситуациях и определенной степени ограничивающим конституционные права граждан, в связи с чем на его санкционирование, планирование и проведение должны налагаться соответствующие ограничения, исключающие возможность нарушения закрепленных в Конституции гражданских прав. Согласно ст. 9 Закона «Об ОРД», наблюдение, ограничивающее закрепленные в Конституции РФ основные права граждан, к которому в силу вышеупомянутых причин относятся виды электронного (комплексного) наблюдения с использованием технических средств, а также наблюдение, связанное с ограничением права на неприкосновенность частной жизни и жилища, должно проводиться исключительно на основании судебного решения.

Между тем действующее законодательство ограничивает не только пределы проведения рассматриваемого мероприятия с использованием технических средств, но также и варианты использования полученной информации. Так, п. 4 Определения Конституционного Суда РФ от 14 июля 1998 г. гласит, что «при проведении наблюдения не допускается сбор, хранение, использование и распространение информации о частной жизни проверяемого лица, если это не связано с выявлением, предупреждением, пресечением и раскрытием преступлений или решением других задач оперативно-розыскной деятельности» [13]. Таким образом, анализ решений Конституционного Суда РФ позволяет сделать вывод о том, что проведение всех оперативно-розыскных мероприятий, и в частности, наблюдения, связанного с ограничением неприкосновенности жилища, допустимо только по тем деяниям, по которым предварительное следствие обязательно, и не допускается без решения суда.

По общему правилу, закрепленному в ст. 89 УПК РФ, результаты наблюдения с использованием технических средств, так же как и все другие результаты оперативно-розыскной деятельности, передаваемые органам предварительного расследования в соответствии со ст. 11 ФЗ «Об ОРД», могут использоваться в доказывании по уголовным делам, если порядок их получения и документирования не противоречит требованиям к доказательствам, предъявляемым УПК РФ.

По данному вопросу Ю.В. Кореневский и М.Е. Токарева отмечают, что «в некоторых случаях проведение оперативно-розыскного мероприятия под названием наблюдение может ограничивать права граждан на неприкосновенность жилища» [14, с. 70]. Данное мнение мы полностью разделяем, поскольку независимо от того, осуществляется ли нарушение неприкосновенности жилища путем физического проникновения в него человека, либо это происходит путем использования технических средств, на данное ОРМ должны распространяться все ограничения, установленные ст. 23 и 25 Конституции РФ и ч. 2 ст. 8 Закона «Об ОРД», то есть судебный порядок санкционирования его проведения. На данную проблему обращали внимание также и другие авторы В.В. Каминский, В.В. Коряковцев, К.В. Питулько [6], которые связывали возможность осуществления оперативного наблюдения в местах работы и проживания разрабатываемых лиц, а следовательно, с нарушением конституционного права на неприкосновенность жилища и частной жизни.

Проблема регламентации порядка и условий дистанционного получения информации о происходящем в помещениях при производстве оперативно-розыскных мероприятий остается актуальной на протяжении как минимум последних 20 лет и единого решения, которое удовлетворило бы всех заинтересованных, до настоящего времени не найдено. Например, еще в 2001 г. в научном докладе «Теория и практика применения органами внутренних дел Закона

«Об оперативно-розыскной деятельности»» [15, с. 5] отмечалось, что ни Закон «Об ОРД», ни ведомственные нормативные акты не регламентируют порядок и условия такого способа получения информации. В связи с чем возникают затруднения при отнесении этих действий к определенному виду ОРМ (прослушивание телефонных переговоров или обследование помещений, зданий, сооружений) и остаются неясными вопросы: будут ли в подобных ситуациях иметь доказательственную силу результаты ОРМ, проведенного без судебного решения, и не подпадают ли действия оперативных работников под признаки преступления, предусмотренного ст. 138 УК РФ?

В этой связи представляет интерес точка зрения А.А. Максимова, который указывает на недопустимость оформления результатов оперативного эксперимента в качестве иных оперативно-розыскных мероприятий, поскольку «оперативными сотрудниками при отсутствии возможности санкционировать проведение оперативного эксперимента производится его документальное оформление по факту проведения в качестве комплекса оперативно-розыскных мероприятий, зачастую включающего в себя опрос (или проверочную закупку) и наблюдение с использованием технических средств фиксации. Подобная практика приводит к признанию полученных сведений незаконными» [16, с. 58].

Из-за отсутствия в Законе «Об ОРД» и вообще в действующем законодательстве четкого определения понятия «нарушение неприкосновенности жилища» неясно, требуется ли судебное решение для визуального или слухового контроля за поведением и разговорами разрабатываемых без проникновения в их жилища.

Однако несмотря на то, что рассматриваемая нами проблема имеет довольно большую историю, в действующем законодательстве до сих пор не закреплена обязательность судебного санкционирования оперативно-розыскных мероприятий, связанных с удаленным получением аудиовизуальной информации в жилище, а также местах нахождения граждан, но и не определено само понятие «неприкосновенность», которое позволило бы связать конституционные нормы с уголовно-процессуальным и оперативно-розыскным законодательством в сфере регулирования правоотношений, связанных с ограничением неприкосновенности жилища. В связи с тем, что законодательное закрепление понятия неприкосновенности жилища в настоящее время отсутствует, ряд авторов делает предположение о возможности нарушения неприкосновенности жилища не только путем физического проникновения в него человека, но и при помощи технических средств, управляемых дистанционно путем средств телеуправления, а также получения информации с помощью средств телекоммуникаций [17, с. 203].

Мы поддерживаем данную точку зрения и полагаем, что современный уровень развития систем передачи информации и в целом технических средств вполне допускает нарушение неприкосновенности жилища без физического проникновения в него человека, путем дистанционной установки в его границах устройств, позволяющих вести аудиальное и визуальное наблюдение за происходящим внутри и передавать полученную информацию на любое расстояние с последующей ее записью и хранением. Кроме того, современные и перспективные разработки в области получения информации позволяют вести наблюдение за происходящим в жилище без физического нарушения его границы, находясь как в непосредственном контакте с границами жилища, так и вне его пределов, что по своей сути является тем же самым нарушением неприкосновенности жилища, которое, однако, находится вне сферы судебного контроля и санкционирования.

Таким образом, по нашему мнению, в настоящее время имеется необходимость законодательного определения понятия «неприкосновенность жилища» применительно к сфере оперативно-розыскной деятельности и уголовного судопроизводства, с целью охвата всех правоотношений связанных с получением информации, находящейся внутри жилища судебным контролем. В связи с этим следует дополнить ст. 139 УК РФ примечанием 2 следующего

содержания: «Под нарушением неприкосновенности жилища в настоящей статье, а также в других статьях настоящего Кодекса понимается всякое открытое или тайное вторжение в него лиц, которые по закону не вправе находиться в нем, а также установка и использование внутри жилища, либо вне его технических средств, предназначенных для негласного получения информации о происходящем внутри жилища помимо воли проживающих лиц, либо без решения суда».

Список литературы

1. Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 02.08.2019) «Об оперативно-розыскной деятельности» // СЗ РФ. 1995. № 33. Ст. 3349.
2. Маркушин А.Г. Оперативно-розыскная деятельность: учебник для вузов. М.: Юрайт, 2012. С. 171.
3. Ковалев С.Д., Полуянова Е.В. О соотношении понятий оперативно-розыскных мероприятий и оперативно-технических мероприятий // Борьба с пенитенциарной преступностью: опыт, проблемы, перспективы: материалы межвуз. науч.-практ. конф. Владимир, 2013. С. 69.
4. Научно-практический комментарий к Федеральному закону «Об оперативно-розыскной деятельности» / под ред. В.В. Николюка. М.: Спарк, 2000. С. 216.
5. Мешков В.М., Попов В.Л. Оперативно-розыскная тактика и особенности легализации полученной информации в ходе предварительного следствия: учебно-практическое пособие. М.: Щит-М, 1999. С. 32.
6. Каминский В.В., Коряковцев В.В., Питулько К.В. Законодательное и организационное обеспечение расследования и судебного разбирательства по уголовным делам, связанным с организованной преступной деятельностью // С.П.Б.: Санкт-Петербургский Центр по изучению организованной преступности и коррупции, 2001. URL: http://law.edu.ru/doc/document.asp?docID=1116155. (дата обращения: 18.03.2020).
7. Пешков М. Прослушивание и электронное наблюдение в уголовном процессе США // Российская юстиция. 1997. № 4. С. 55-56.
8. Определение Конституционного Суда РФ от 21.10.2008 № 862-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Камалиева Марата Дамировича на нарушение его конституционных прав статьей 6 Федерального закона «Об оперативно-розыскной деятельности» // URL: https://legalacts.ru/doc/opredelenie-konstitutsionnogo-suda-rf-ot-21102008-n-862-o-o-ob/ (дата обращения: 18.03.2020).
9. Определение Конституционного Суда РФ от 17.07.2007 № 597-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Дахкуряна Сурена Николаевича на нарушение его конституционных прав частями второй и четвертой статьи 8 и частью третьей статьи 11 Федерального закона «Об оперативно-розыскной деятельности». URL: https://www.glavbukh.ru/npd/edoc/96_902068340. (дата обращения: 18.03.2020).
10. Определение Конституционного Суда РФ от 20.03.2007 № 178-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Донского Александра Павловича на нарушение его конституционных прав пунктами 4 и 6 части первой и частью третьей статьи 6 Федерального закона «Об оперативно-розыскной деятельности» и статьями 13, 89 и 186 Уголовно-процессуального кодекса Российской Федерации». URL: https://legalacts.ru/doc/ opredelenie-konstitutsionnogo-suda-rf-ot-20032007-n-178-o-o-ob/. (дата обращения: 18.03.2020).
11. Определение Конституционного Суда РФ от 16.11.2006 № 454-О «Об отказе в принятии к рассмотрению жалобы гражданки Дьячковой Ольги Геннадьевны на нарушение ее конституционных прав пунктами 6 и 14 части первой и частью четвертой статьи 6, пунктом 3 статьи 7, частью второй статьи 8 Федерального закона «Об оперативно-розыскной деятельности», частью второй статьи 7, пунктом 4 части второй статьи 38, статьями 125, 140 и 146

Уголовно-процессуального кодекса Российской Федерации». URL: https://legalacts.ru/doc/opredelenie-konstitutsionnogo-suda-rf-ot-16112006-n-454-o-ob/. (дата обращения: 18.03.2020).

12. Определение Конституционного Суда РФ от 11.07.2006 № 268-О «По жалобам гражданина Уразова Сергея Владимировича на нарушение его конституционных прав положениями статей 49, 91, 92, 227, 228, 229, 255 и 355 Уголовно-процессуального кодекса Российской Федерации и статей 6, 8 и 10 Федерального закона «Об оперативно-розыскной деятельности» // ВКС РФ. 2006. № 6.

13. Определение Конституционного Суда РФ от 14.07.1998 № 86-О «По делу о проверке конституционности отдельных положений Федерального закона «Об оперативно-розыскной деятельности» по жалобе гражданки И.Г. Черновой» // ВКС РФ. 1998. № 6.

14. Кореневский Ю.В., Токарева М.Е. Использование результатов оперативно-розыскной деятельности в доказывании по уголовным делам: методическое пособие. М.: Юрлитинформ, 2000. С. 70.

15. Теория и практика применения органами внутренних дел закона «Об ОРД»: научный доклад. М.: ВНИИ МВД России, 2001. С. 5.

16. Максимов А.А. Условия обеспечения законности проведения оперативного эксперимента // Российская юстиция. 2019. № 5. С. 57-59.

17. Постатейный комментарий к Конституции Российской Федерации / под общ. ред. В.Д. Карповича. М.: Юрайт-М, 2002. С. 203.

РАЗДЕЛ 1. ПРОБЛЕМЫ КВАЛИФИКАЦИИ, КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ

М.Г. Ермаков, *к.ю.н., старший преподаватель кафедры криминалистики Омской академии МВД России, г. Омск*

«ТЕЛЕФОННОЕ» МОШЕННИЧЕСТВО

Как показывает практика, большинство пользователей социальных сетей подвержены деятельности мошенников: преступники, пользуясь низкой компьютерной грамотностью или доверчивостью людей, придумывают все новые способы совершения подобных преступлений. Причиной «популярности» у криминалитета такого способа хищения денежных средств у граждан является широкая распространенность и относительная доступность для большинства населения услуг мобильной связи, сети Интернет [1, с. 382]. Массовый характер приобрели такие действия, которые обычно называются «дистанционные преступления», где в качестве главного «орудия» совершения преступления выступают средства мобильной связи и всемирная информационно-коммуникационная сеть Интернет. Для общения с потенциальной жертвой «дистанционные мошенники» используют:

– телефонный звонок — позволяет манипулировать человеком при разговоре, но при таком общении можно разоблачить мошенника правильным вопросом;

– SMS-сообщения — это мошенничество «вслепую»: такие сообщения рассылаются в большом объеме в надежде на доверчивого получателя;

– размещение объявлений о продаже или покупке товаров, услуг в сети Интернет;

– вредоносное программное обеспечение, которое, проникая в операционную систему мобильного телефона или компьютерной техники, передает информацию о банковских счетах, паролях к ним и иные данные, которые могут быть использованы злоумышленниками [2, с. 332].

Основная цель «дистанционных мошенников» — заставить потерпевшего добровольно передать свои денежные средства. Для этого используются различные схемы «телефонного мошенничества», основными из которых являются [3] следующие.

1. Обман по телефону.

Требование выкупа или взятки за освобождение якобы из отделения полиции родственника или знакомого. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции за совершение того или иного преступления (совершил ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и др.). Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Но если раньше деньги привозили непосредственно ему, то сейчас так делать нельзя, так как он «боится потерять погоны». Деньги необходимо привезти в определенное место, передать какому-либо человеку или перевести на определенный счет. Общественная опасность подобных преступлений заключается в том, что помимо причинения материального ущерба потерпевшим, дискредитируются правоохранительные органы, в частности полиция.

2. SMS-просьба о помощи.

Требование перевести определенную сумму на указанный номер (как правило, используется обращение «мама», «друг», «сынок» и т.п.). Абонент получает на мобильный телефон SMS-сообщение: «У меня проблемы, позвони по такому-то номеру, если номер недоступен, положи на него определенную сумму и перезвони».

3. Выигрыш в лотерею и т.п.

На мобильный телефон абонента приходит СМС-сообщение о крупном выигрыше (телефон, ноутбук и др.) в лотерее, организованной каким-либо известным брендом, чтобы получить приз, необходимо дозвониться на радиостанцию. Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия игры: просит представиться и назвать год рождения; грамотно убеждает в честности акции (никаких взносов, переигровок и т.д.). Сначала просят перевести налог 13% на указанные ими реквизиты, затем потерпевший переводит деньги на указанные последним счета банковских карт, электронные кошельки и счета абонентов операторов сотовой связи, но товар или услугу не получает и контакт с ним прекращается.

4. При продаже потерпевшими товаров или услуг мошенники под предлогом перевода денег в виде предоплаты за покупку путем обмана получают от последних информацию о банковских картах и паролях к ним или к системе «Мобильный банк», личным кабинетам пользователей услугами банков «онлайн» и с помощью полученной информации похищают деньги потерпевших.

5. Использование вредоносного программного обеспечения. На мобильный телефон, компьютер потерпевшего приходят сообщения различного содержания, уже содержащие «вирус» или содержащие ссылку на интернет-сайт, при переходе на который в операционную систему телефона или компьютера приникает вредоносное программное обеспечение, которое передает информацию о банковских счетах, страницах социальных сетей, пароли к ним и иную информацию, которые используются злоумышленниками для хищения денежных средств потерпевших или взлома страниц социальных сетей, электронных почтовых ящиков, при помощи которых происходит хищение денежных средств путем обмана из числа знакомых потерявшего от имени последнего.

В большинстве случаев на момент поступления заявления неизвестно, кто совершил «телефонное» мошенничество. Для успешного раскрытия и расследования такого преступления необходим тесный контакт следователя с сотрудниками, производящими оперативно-розыскные и технические мероприятия. На стадии возбуждения уголовного дела материалы доследственных проверок, как правило, содержат заявление потерпевшего, объяснение и запросы в БСТМ МВД России (без ответов). Неустановление в кратчайшие сроки принадлежности абонентских номеров телефонов и банковских карт, с использованием которых совершаются преступления, не дает возможности установить виновных и пресечь противоправную деятельность преступных групп.

Анализ сложившейся оперативной обстановки на территории России показал, что изъятие денежных средств у потерпевших в основном происходит тремя способами:

1. Зачислением на номера мобильных телефонов, указанных мошенником (как правило, используются операторы сотовой связи ПАО «Мобильные ТелеСистемы» (МТС), ПАО «ВымпелКом» (Билайн), ПАО «Мегафон» и т.п.), что определяется развитием сотовой связи в конкретном регионе). На официальном интернет сайте Федерального агентства связи (Россвязь) www.rossvvaz.ru следователь самостоятельно может определить по номеру телефона оператора связи, которому он принадлежит, с получением данных субъекта Российской Федерации, в котором он зарегистрирован.

2. Осуществлением блиц-перевода через систему «Колибри» Сбербанка России, «Юнистрим» и «Золотая корона», электронные платежные системы «Лидер», «Контакт» (Contact), ЗАО «Киви Банк» и других организаций, осуществляющих денежные переводы на территории России.

3. Перевод с использованием системы «мобильный банк» и «банк онлайн».

4. Передачей посреднику (например, таксисту) или лицу, выполняющему курьерские услуги (родственнику или знакомому).

Преступники, пользуясь бесконтрольностью операторов сотовой связи, при совершении преступлений используют абонентские номера мобильных телефонов, зарегистрированные на случайных лиц, по утерянным или похищенным паспортам, вымышленным данным, а также корпоративные номера, в связи с чем для установления использующих их лиц требуется проведение комплекса оперативно-розыскных мероприятий.

Основными субъектами Российской Федерации, откуда совершаются телефонные звонки, являются: г. Москва, Московская, Самарская, Пензенская, Кемеровская области, Республики Башкортостан, Татарстан. Вместе с тем представления о принятии мер по устранению обстоятельств, способствовавших совершению преступлений, в компании сотовой связи вносятся в единичных случаях либо носят формальный характер.

Как показывает анализ расследования уголовных дел и проведенных оперативно-розыскных мероприятий, в большинстве случаев посредники осведомлены о преступном характере своей деятельности. Однако без наличия результатов оперативно-технических мероприятий возникает сложность в опровержении ложных показаний посредника и привлечении его к уголовной ответственности. В ходе доследственной проверки и расследования не прорабатываются варианты проведения оперативных экспериментов в отношении данных лиц.

При установлении факта нахождения мобильного номера телефона в зоне действия базовых станций, расположенных вблизи исправительных учреждений, оперативным службам ФСИН России не всегда своевременно направляются соответствующие информационные письма, содержащие номер мобильного телефона, его идентификационный номер (IMEI) и наименование модели для установления причастности к совершенным преступлениям лиц из числа осужденных, у которых изымались мобильные телефоны. По изъятым мобильным телефонам необходимо исследовать историю IMEI и работавшие сим-карты. Изучение представленных материалов показало, что в целях изобличения лиц, причастных к совершению преступлений, в том числе участвующих в обналичивании денежных средств, полученных преступным путем, целесообразно истребовать сведения:

– из коммерческой организации о движении денежных средств по счету номера мобильного телефона, с которого производился звонок преступника, и номера мобильного телефона, на баланс которого переведены денежные средства;

– из компании оператора сотовой связи информации о соединениях абонентского номера, с которого производился звонок, а также месторасположение и номер базовой станции, с помощью которой производилось соединение (телефонный звонок), с целью получения информации о месте, откуда производятся мошеннические действия.

При установлении личности курьера, получившего денежные средства от потерпевшего, и достаточных основаниях полагать о его причастности к совершенному преступлению необходимо провести обыски по месту его регистрации (жительства) и изъять его мобильные средства связи.

При совершении мошенничества из мест лишения свободы осужденный привлекает посредника. В роли посредников выступают родственники или знакомые осужденного, друзья

по переписке (случайное знакомство по телефону, через объявление или Интернет-сайт), таксисты и лица, выполняющие курьерские услуги.

Выявленные в учреждениях ФСИН преступные группы, как правило, имеют однотипную структуру:

– «контролер» — осужденный, занимающийся сбором информации на граждан, в отношении которых планируется преступное посягательство, фиксацией необходимых данных в период преступного посягательства и ведением «бухгалтерского» учета;

– «разводящие» — осужденные, осуществляющие звонки на телефоны граждан и вымогающие денежные средства от имени родственников или сотрудников правоохранительных органов;

– «координатор» — осужденный, занимающийся поиском посредников «на воле», их руководством и координацией по получению и дальнейшему движению денежных средств.

Факты использования осужденными, содержащимися в учреждениях ФСИН России, мобильных средств связи являются грубыми нарушениями Уголовно-исполнительного кодекса Российской Федерации и правил внутреннего распорядка исправительных учреждений и свидетельствуют о ненадлежащем исполнении своих должностных обязанностей сотрудниками указанных учреждений.

В этой связи в процессе расследования дел о «телефонном» мошенничестве необходимо выявлять обстоятельства, способствующие совершению преступлений, установив которые, принимать меры по их устранению, для чего вносить представления в соответствующие государственные (в том числе учреждения ФСИН России) или иные организации (в том числе операторы мобильной связи и компании-дилеры, действующие от их лица) для устранения выявленных причин и условий, способствующих совершению преступления. Представляется необходимым в целях профилактики преступлений данной категории, через средства массовой информации с населением проводить разъяснительную работу. Для этого о фактах совершения «телефонного» мошенничества, о неблаговидной роли отдельных должностных лиц и граждан, чье поведение способствовало совершению преступления, сообщать в печать, по радио и телевидению. Вместе с тем актуальной проблемой на сегодняшний день остаются нераскрытые кражи, совершенные путем внедрения и использования вредоносных программ в сотовые телефоны с абонентскими номерами, подключенными к услуге «мобильный банк» или «Сбербанк онлайн». Число зарегистрированных заявлений и сообщений по данным преступлениям постоянно растет. Используемые злоумышленниками способы маскировки преступных действий и противодействия расследованию существенно затрудняют борьбу органов внутренних дел с преступлениями данного вида.

Проведенный анализ сложившейся оперативной обстановки в Омской области в 2019 г. по данным видам преступлений показал, что совершение таких преступлений стало возможным в связи с доверчивостью граждан из-за их неграмотности в сфере пользования ресурсами сети Интернет, в том числе мобильными устройствами и программами. Подобным бесконтактным преступлениям подвергаются граждане в возрасте 20-50 лет, что связано с пользованием последними сайтами по продаже товаров в сети Интернет или бесплатных объявлений, например, «Авито», а также общением в социальных сетях и т.п.

Раскрытие рассматриваемой категории преступлений серьезно затруднено установлением лица, причастного к совершению данного преступления, так как зачастую звонки потерпевшим происходят с мобильных телефонов, зарегистрированных на подставных или несуществующих лиц, а банки информацию о движении денежных средств предоставляют с большим опозданием (2-6 месяцев), иногда запросы игнорируются или остаются без ответа. К тому же платежные системы, в свою очередь, информацию о движении денежных средств

предоставляют не в полном объеме. Также очень часто в схеме обналичивания денежных средств задействуется несколько платежных систем и различные электронные кошельки, что делает весьма затруднительным и долговременным установление держателей счетов, получивших денежные средства. Это является проблемой, создающей трудности в раскрытии данного вида преступлений. В связи с этим можно с большой долей вероятности прогнозировать рост данной разновидности преступлений. При этом интенсивность и темпы их роста будут постоянно увеличиваться.

Список литературы

1. Карамышева М.С. Некоторые проблемы латентности неправомерного доступа и мошенничества, совершаемых посредством социальных сетей // Современные научные исследования и разработки. 2016. № 7. С. 382-384.

2. Иванов С.А., Крюков А.А. Телефонное мошенничество // Электронный научный журнал. 2016. № 5. С. 332-339.

3. Орлов П. Звонок прямым в голову // Общественно-политическая газета «Труд». 20.04.2012. № 55. URL: http://www.trud.ru/article/20-04-2012/275294_zvonok_ prjamym_ v_golovu.html (дата обращения: 05.05.2020).

М.А. Иващенко, *младший научный сотрудник Научно-исследовательского института Московской академии Следственного комитета РФ, аспирант Московской академии Следственного комитета РФ, г. Москва*

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ЭКСТРЕМИСТСКИХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СЕТИ ИНТЕРНЕТ

В нашем государстве признается идеологическое многообразие. Никакая идеология не может устанавливаться в качестве государственной или обязательной. Запрещается создание и деятельность общественных объединений, цели или действия которых направлены на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, подрыв безопасности государства, создание вооруженных формирований, разжигание социальной, расовой, национальной и религиозной розни [1].

Однако вопреки конституционным принципам, преступления экстремистской направленности в Российской Федерации совершались и совершаются в настоящее время. Несмотря на увеличение их числа почти в два раза за последнее десятилетие (с 548 в 2009 г. до 1265 в 2018 г.), доля преступлений экстремисткой направленности, по которым установлены виновные лица, остается постоянно высокой: на протяжении рассматриваемого временного промежутка она составляла около 85%, редко (в 2011 г. — 81%, в 2013 г. — 82,9%, 2016 г. — 83,2%) опускаясь ниже данного значения [2].

Анализ уголовных дел экстремисткой направленности показал, что одним из способов приобщения жителей нашей страны к экстремистской идеологии является размещение неустановленными лицами в сети Интернет текстов, видеороликов, изображений и комментариев экстремистского содержания.

Пленум Верховного Суда РФ принял 20 сентября 2018 г. Постановление № 32 «О внесении изменений в Постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности». Необходимость дополнительных разъяснений по вопросам применения

антиэкстремистского уголовного законодательства была вызвана сложностями, возникающими при правовой оценке деяний, совершенных с использованием информационно-телекоммуникационных сетей.

Представляя проект Постановления на заседании Пленума Верховного Суда РФ (далее — Пленум), судья Верховного Суда О.К. Зателепин подчеркнул, что примерно 90% дел о преступлениях экстремистской направленности касаются размещения материалов в сети Интернет [3]. В первую очередь это относится к деяниям, предусмотренным ст. 280, 282 УК РФ, которые составляют подавляющее большинство уголовных дел указанной категории. Именно по этой причине Пленум сосредоточил свое внимание на вопросах квалификации состава возбуждения ненависти или вражды, а равно унижения человеческого достоинства, совершенного с использованием информационно-телекоммуникационных сетей (ст. 282 УК РФ).

Большая часть преступлений, совершаемых с использованием сети Интернет, являются корыстными — кражи, мошенничество, вымогательство. Однако с использованием высоких технологий возможны призывы к осуществлению, помимо прочего, экстремистской деятельности, то есть деяний, направленных на подрыв общественной безопасности, основы конституционного строя и безопасность государства. При этом возникают проблемы правильной квалификации содеянного, эффективного расследования совершенных деяний, поскольку преступность в виртуальном пространстве — новое явление.

Выделим следующие проблемы, которые возникают при квалификации преступлений экстремисткой направленности, совершенных с использованием сети Интернет:

1. Определение обстоятельств, подлежащих доказыванию, или предмета доказывания.
2. Основания привлечения к уголовной ответственности за «репосты».
3. Неограниченный доступ к материалам, размещаемым в сети Интернет.
4. Широкая географическая распространенность сети Интернет.

Обстоятельства, подлежащие доказыванию определены в ст. 73 УПК РФ.

Особенности квалификации преступлений экстремистской направленности, совершенных с использованием сети Интернет, рассмотрим на примере ч. 2 ст. 280 УК РФ.

Публичные призывы к осуществлению экстремистской деятельности, совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети Интернет (ч. 2 ст. 280 УК РФ).

О**бъектом** выступают общественные отношения, складывающиеся по поводу охраны конституционного строя, политической системы и безопасности РФ, прав и свобод человека и гражданина и обеспечивающие недопущение экстремистской деятельности.

Квалифицирующие признаки (ч. 2 ст. 280 УК РФ) с использованием:

– средств массовой информации;
– информационно-телекоммуникационных сетей, в том числе сети Интернет.

Согласно п. 6 Постановления Пленума Верховного Суда РФ от 28.06.2011 № 11 (ред. от 20.09.2018) «О судебной практике по уголовным делам о преступлениях экстремистской направленности», при решении вопроса об использовании средств массовой информации либо информационно-телекоммуникационных сетей, включая сеть Интернет, следует учитывать положения Закона РФ от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» и Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Определения «средств массовой информации» и «информационно-телекоммуникационных сетей» даны выше по тексту.

Периодическим печатным изданием являются газета, журнал, альманах, бюллетень, иное издание, имеющее постоянное наименование (название), текущий номер и выходящее в свет не реже одного раза в год.

Сетевое издание представляет собой сайт в информационно-телекоммуникационной сети Интернет, зарегистрированный в качестве СМИ.

Под **радио-, теле-, видео-, кинохроникальной программой** понимается совокупность периодических аудио-, аудиовизуальных сообщений и материалов (передач), имеющих постоянное наименование (название) и выходящих в свет (в эфир) не реже одного раза в год.

Объективная сторона преступления, предусмотренного ст. 280 УК РФ, состоит в публичных призывах к осуществлению экстремистской деятельности [4]. Разберем более подробно каждый из признаков объективной стороны указанного деяния:

– **наличие призывов** как психического воздействия на сознание и волю людей с целью побудить их к совершению определенных действий. **Призыв** — это форма психического воздействия на сознание и волю людей с целью побудить их к совершению определенных действий;

– **публичность призывов**, то есть выраженные в любой форме (устной, письменной, с использованием технических средств, информационно-телекоммуникационных сетей общего пользования, включая сеть Интернет) обращения к другим лицам с целью побудить их к осуществлению экстремистской деятельности. Более того, надо понимать, что публичность призывов предполагает, что призывы обращены к широкому кругу людей. Наиболее характерными примерами публичности являются выступления на собраниях, митингах и других массовых мероприятиях, использование экстремистских лозунгов во время демонстраций, шествий, пикетирования и т.д. В каждом конкретном деле вопрос о публичности призывов решается с учетом всех обстоятельств дела. В том числе должно быть установлено, что публика воспринимала призывы;

– **время (период времени)** совершения преступления. Временем совершения преступления будет являться то конкретное время, с точностью до минуты, которое указано на странице пользователя в сети Интернет в момент опубликования им сообщения, поста, аудиозаписи, видеозаписи, подтверждающих факт совершения публичных призывов к экстремистской деятельности. Например, запись на стене социальной сети «ВКонтакте» опубликована 10 декабря 2019 г. в 16 часов 45 минут. В случае если это была единственная запись пользователя, содержащая признаки рассматриваемого преступления, то именно 16 часов 45 минут будет считаться временем совершения преступления. Однако пользователь может неоднократно публиковать подобные записи в сети Интернет, и если они относятся к одному и тому же событию преступления, то время совершения преступления следует указывать как период времени. Например, в период времени с 16 часов 45 минут 10 декабря 2019 г. по 23 часа 05 минут 20 декабря 2019 г.;

– **место** совершения преступления. Изучив судебную практику, можно прийти к выводу, что местом совершения преступления экстремистской направленности, совершенном с использованием сети Интернет, является то фактическое место нахождения человека, где он находился в момент опубликования (направления, распространения) соответствующей записи в сети Интернет. Как правило, это либо место его проживания, где имеется выход в сеть, либо кафе, рестораны, иные заведения, где он может пользоваться сетью;

– обстановка публичных призывов (собрание, митинг, демонстрация и т.п.). Обстановкой будет признаваться сама сеть Интернет и конкретная социальная сеть, где эти призывы размещены;

– **способ публичных призывов**, например, распространение листовок, вывешивание плакатов, нанесение на стенах надписей, рисунков; размещение обращения в информационно-

телекоммуникационных сетях общего пользования, включая сеть Интернет, например на сайтах, в блогах (личных электронных дневниках, размещенных в сети Интернет для всеобщего пользования) или на форумах, распространение обращений путем веерной рассылки электронных сообщений и т.п.);

– **форма публичных призывов** (устная, письменная, с использованием различных изобразительных форм, с помощью технических средств). Формой публичных призывов, совершенных с использованием сети Интернет, будет признаваться, как правило, письменная форма с использованием сети Интернет;

– **отсутствие у призывов персонифицированного характера** (обращены к неопределенному кругу лиц: тем или иным группам населения (молодежи, представителям какой-либо профессии, социального слоя, национальности и другое); участникам различных мероприятий (зрителям, слушателям, избирателям, делегатам и другое); членам организаций, работникам предприятий, учреждений, военнослужащим и другое). Когда в сети Интернет совершается указанное преступление, то оно практически всегда направлено к неопределенному кругу лиц.

Субъективная сторона публичных призывов характеризуется виной в форме умысла. Призывая к осуществлению экстремистской деятельности, субъект всегда осознает общественную опасность своих действий.

Мотив и цели такой деятельности могут быть различными (националистические, корыстные, хулиганские и другие) и не влияют на квалификацию, но учитываются при индивидуализации уголовного наказания.

Сознательное размещение материалов экстремистского характера не в сугубо памяти своего персонального компьютера, а в популярной социальной сети с круглосуточным доступом к ним неограниченного числа лиц, о чем лицу, размещающему такие материалы, достоверно известно, свидетельствует о фактической реализации им намерений поделиться с пользователями сети Интернет возможностью просмотра данных материалов, что указывает на наличие прямого умысла на совершение указанного преступления.

Субъект публичных призывов общий, то есть физическое вменяемое лицо, достигшее 16-летнего возраста.

При совершении публичных призывов к осуществлению экстремистской деятельности путем массовой рассылки сообщений абонентам мобильной связи или с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет, преступление следует считать **оконченным** с момента размещения обращений в указанных сетях общего пользования (на сайтах, форумах или в блогах), отправления сообщений другим лицам.

Изготовление, размножение или хранение материалов с целью последующего их использования для пропаганды экстремизма не влечет уголовной ответственности, так как стадия приготовления к данному преступлению в силу ч. 2 ст. 30 УК ненаказуема (приготовление ведется к совершению преступления средней тяжести). По тому же основанию ненаказуема в уголовном порядке и подготовка к совершению указанного преступления при отягчающих обстоятельствах (с использованием СМИ либо информационно-телекоммуникационных сетей, в том числе сети Интернет).

При совершении публичных призывов к осуществлению экстремистской деятельности путем массовой рассылки сообщений абонентам мобильной связи или с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет, преступление следует считать оконченным с момента размещения обращений в указанных сетях общего пользования (например, на сайтах, форумах или в блогах), отправления сообщений другим лицам.

По приговору Северо-Кавказского окружного военного суда от 23 января 2019 г. С. признан виновным в размещении с целью ознакомления неограниченного круга лиц на личной интернет-странице, открытой для общего доступа: 21 октября 2014 г. видеоматериала, содержащего призывы к осуществлению террористической деятельности и оправдание терроризма; 23 ноября, 15 декабря 2014 г. и 26 декабря 2015 г. — видеоматериалов, содержащих призывы к осуществлению экстремистской деятельности, которые стали доступны пользователям социальной сети.

По совокупности преступлений, предусмотренных ч. 1 ст. 205.2 (в редакции Федерального закона от 7 декабря 2011 г. № 420-ФЗ) и ч. 2 ст. 280 УК РФ, С. осужден в соответствии с ч. 2 ст. 69 УК РФ путем частичного сложения назначенных наказаний к лишению свободы на срок 4 года с лишением права заниматься деятельностью, связанной с администрированием сайтов электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет, на срок 1 год.

В соответствии со ст. 70 УК РФ к наказанию, назначенному С. по приговору окружного военного суда, частично присоединена неотбытая часть наказания по приговору Кизлярского городского суда Республики Дагестан от 18 июня 2009 г. и окончательное наказание ему назначено в виде лишения свободы на срок 5 лет в исправительной колонии строгого режима с лишением права заниматься деятельностью, связанной с администрированием сайтов электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет, на срок 1 год.

Таким образом, можно заключить, что проблемы квалификации преступлений экстремистской направленности, совершенных с использованием сети Интернет, на практике имеют место быть. Важно предвидеть их и уметь грамотно дать правильную оценку квалификации того или иного деяния.

Список литературы

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (ст. 13 Конституции РФ).

2. Состояние преступности в России за период с 2009 по 2019 г. // Генеральная прокуратура Российской Федерации. Главное управление правовой статистики и информационных технологий.

3. Заседание Пленума Верховного Суда РФ 20 сентября 2018 г. Выступление О.К. Зателепина, судьи Верховного Суда РФ. URL: https://www.youtube.com/watch?v =YwrXBxTtI1M&index=1&list=PLludGApopXaX YOtWdxMqVnMlWOcGua4D.

4. Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 (ред. от 20.09.2018) «О судебной практике по уголовным делам о преступлениях экстремистской направленности».

5. Власов В.И. Экстремизм: сущность, виды, профилактика: учебно-методическое пособие / под ред. Р.Г. Абдулатипова. М.: Изд-во РАГС, 2003.

6. Зеленков М.Ю. Экстремизм в современном мироустройстве и Российской Федерации XXI века. Политико-правовой аспект: монография. М.: ЮНИТИ-ДАНА: Закон и право, 2018.

Я.О. Кучина, *к.ю.н., LL.M., докторант университета Макао (Макао, САР КНР), профессор РАЕ*

НЕКОТОРЫЕ ОСОБЕННОСТИ ОБЪЕКТА ПРЕСТУПЛЕНИЯ В СТ. 274.1 УК РФ «НЕПРАВОМЕРНОЕ ВОЗДЕЙСТВИЕ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Статья 274.1 УК РФ («Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации») была введена в Особенную часть Уголовного кодекса РФ 26.07.2017 г. одновременно с принятием Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — Федеральный закон № 187).

Объектом преступления, запрещенного ст. 274.1 УК РФ, выступают отношения в сфере безопасности критической информационной инфраструктуры (далее — КИИ), что прямо следует из названия статьи и из текста диспозиций ч. 1–5. В них везде используется термин «критическая информационная инфраструктура», который отсылает нас к Федеральному закону № 187.

Согласно п. 6 ст. 2 Федерального закона № 187 критическая информационная инфраструктура — *это объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.*

Под объектами критической информационной инфраструктуры подразумеваются *информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры* (п. 6 ст. 2). Таким образом, в целом критическая информационная инфраструктура представляет собой *информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия этих объектов.*

Анализ текста Федерального закона № 187 показывает, что отношения в сфере безопасности критической информационной инфраструктуры регулируются сложной системой нормативно-правовых актов и локальных нормативных актов, которые принимаются соответствующим субъектом критической информационной инфраструктуры (физическим или юридическим лицом, которому принадлежит объект КИИ). Благодаря чему дабы определить, что конкретно является объектом преступления в ст. 274.1 УК РФ, необходимо проанализировать все действующее законодательство о КИИ.

Если следовать смыслу ст. 2 Федерального закона № 187, критическая информационная инфраструктура формируется из двух составляющих ее элементов:

1) из объектов КИИ, к которым относятся:

1.1. информационные системы,

1.2. информационно-телекоммуникационные сети,

1.3. автоматизированные системы управления;

2) из сетей электросвязи, при помощи которых осуществляется взаимодействие объектов КИИ в разных комбинациях в зависимости от архитектуры.

Иными словами, критическая информационная инфраструктура — это цифровые системы, выполняющие определенную функцию и состоящие, как и любые другие системы подобного рода, из конструктивных материальных частей (деталей, устройств), программных частей (программного обеспечения) и системы электросвязи (о том, что может подразумеваться под системой электросвязи, подробно указано в ст. 12. Федерального закона от 07.07.2003 № 126-ФЗ «О связи»).

При этом не любые системы, устройства, сервисы могут признаваться объектами КИИ с юридической точки зрения. Исходя из положений п. 8 ст. 2 Федерального закона № 187,

объекты КИИ — это те объекты, которые функционируют в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Кроме того, текст Федерального закона № 187, а также иные нормативные акты (Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»; Приказ Федеральной службы по техническому и экспортному контролю от 06.12.2017 г. № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»; Приказ ФСБ России от 19.06.2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» и ряд других) позволяют сделать вывод, что объект критической информационной инфраструктуры — это общая категория, подразделяемая на виды.

Согласно положениям ст. 2 Федерального закона № 187, таких видов два:

1) значимый объект критической информационной инфраструктуры первой, второй или третьей категории (ч. 3 ст. 2);

2) незначимый объект критической информационной инфраструктуры (ч. 4 ст. 7).

Присвоение категории (категорирование) значимым объектам КИИ производится на основе следующих показателей критической значимости:

1) социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;

2) политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;

3) экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;

4) экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;

5) значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

Вопрос о том, к какому из видов относится объект критической информационной инфраструктуры, решается в процессе категорирования объектов КИИ, общий порядок которого определен в ст. 7 Федерального закона № 187 и уточнен Постановлением Правительства от 08.02.2018 г. № 127 [1].

В упрощенном виде категорирование подразделяется на четыре этапа:

1) присвоение категории значимости (первой, второй или третьей) объекту субъектом критической информационной инфраструктуры;

2) обращение субъекта с подготовленными результатами присвоения в уполномоченный орган государственной власти для проверки правильности категорирования (Федеральная служба по техническому и экспортному контролю (ФСТЭК);

3) проверка результатов присвоения категории органом государственной власти (ФСТЭК) и принятие решения о присвоении категории значимости или об отказе в таком присвоении;

4) внесение значимых объектов в реестр значимых объектов критической информационной инфраструктуры или возврат документов с мотивированным отказом в случае, если объект признается незначимым [2.].

Из положений Постановления Правительства от 08 февраля 2018 г. № 127, равно как из положений Федерального закона № 187 следует, что значимым объект КИИ становится только *после внесения его в реестр*, а незначимым — *после мотивированного отказа* в присвоении категории *и отказа во* внесении в реестр. От факта, является ли объект значимым или нет, зависят меры безопасности конкретной критической информационной инфраструктуры, права и обязанности конкретного субъекта. Это же непосредственным образом отражается на процессе квалификации деяний, запрещенных ст. 274.1 УК РФ.

Так, незначимый объект КИИ должен быть в обязательном порядке подключен к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Это изложено в разделе 2 Приказа ФСБ России от 06.05.2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты», а также в Приказ ФСБ России от 24.07. 2018 г. № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

На данный момент периферийный центр ГосСОПКА может быть реализован субъектом КИИ как самостоятельно (с использованием собственных технических и кадровых ресурсов), так и с привлечением сторонних специалистов (так называемый аутсорсинг услуг) [1]. Иные меры безопасности незначимых объектов определяются субъектом КИИ также самостоятельно, а права и обязанности устанавливаются ст. 9 Федерального закона № 187 в усеченном виде.

Что касается значимых объектов КИИ, то система безопасности таких объектов представляет собой целый комплекс мер, которые в кратком виде можно описать следующим образом:

1) создание системы безопасности значимого объекта КИИ;

2) реагирование на компьютерные инциденты в порядке, установленном Федеральной службой безопасности [3];

3) предоставление беспрепятственного доступа к значимому объекту КИИ лицам, уполномоченным на проведение плановых и внеплановых проверок (ФСТЭК, ФСБ); выполнение предписаний по результатам проверок.

В результате ст. 274.1 УК РФ предусматривает наличие двух видов защищаемых общественных отношений — тех, что касаются защищенных объектов КИИ, и тех, что касаются незащищенных объектов КИИ. Правовой режим и установление принадлежности к конкретному из видов имеют слишком существенные различия, чтобы считать их единым целым.

То есть мы видим, что объект преступления ст. 274.[1] УК РФ, в отличие от объектов преступлений ст. 272-274 УК РФ, не включает в себя технической составляющей. Объект ст. 274.1 УК РФ имеет классическое определение, признанное уголовно-правовой наукой, в силу бланкетного характера самой статьи и обширного перечня актов, к которым отсылает диспозиция каждой из частей. При этом даже упомянутая в этих частях компьютерная информация прежде всего регулируется этими актами, и только потом к ней могут (если возникнет необходимость) применяться правила определения правового режима компьютерной информации в том смысле, в котором сама компьютерная информация определена в Приложении к ст. 272 УК РФ.

Список литературы

1. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

2. Приказ Федеральной службы по техническому и экспортному контролю от 6 декабря 2017 г. № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».

3. Приказ ФСБ России от 19 июня 2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».

В.А. Мазуров, *к.ю.н., доцент кафедры уголовного права и криминологии Алтайского государственного университета, г. Барнаул*
М.А. Стародубцева, *преподаватель Алтайского государственного университета, г. Барнаул*

О НЕКОТОРЫХ АСПЕКТАХ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ

Терроризм — это глобальное явление, выходящее за рамки национальных границ. Компьютерные сети и компьютерные данные, которые также игнорируют физические границы, создали глобальное киберпространство. Кроме того, компьютерные сети, такие как Интернет, позволяют разработать новые формы технологий, помогающие пользователям сохранять свою анонимность, заниматься скрытым общением. Таким образом, глобальное киберпространство обеспечивает уникальную среду, в которой и осуществляется кибертерроризм.

В результате этих специфических особенностей компьютерных сетей открылись основные направления террористической деятельности в Интернете: совершение деструктивных атак с помощью сети Интернет; массовое распространение нелегального контента через Интернет; использование Интернета для индивидуального общения между террористами. В первом случае *разрушительные атаки против компьютерных систем, осуществляемых с помощью сети Интернет* (кибертерроризм), могут привести не только к разрушению, коррупции и блокированию производственных процессов, банковских систем. Интернет-атаки также могут нанести физический ущерб собственности и человеческим жизням, если, например, атакованный сервер отвечает за управление атомной электростанцией, системой управления полетом, компьютерами больницы или военными системами вооружения. Так как многие аспекты современного общества сильно зависят от компьютерных систем, риски, связанные с этим видом преступной деятельности, являются значительными. Однако в то же время известно достаточно мало случаев, связанных с такими видами нападений [1, с. 34].

Напротив, террористическое использование Интернета и других электронных систем связи во второй из этих сфер — *распространение незаконного контента* — это обычное дело. Как результат, Интернет стал важным инструментом, с помощью которого террористы посылают свои послания широкой аудитории. Также Интернет и другие компьютерные системы играют значительную роль в создании третьей сферы, упомянутой выше, *технической подготовки террористических преступлений*, включая внутреннюю связь, приобретение информации (например, о создании бомбы, захвате заложников или угоне самолета), анализ целевых показателей и другие формы сбора информации.

Уголовное преследование большинства из этих преступлений является сложным и технически практически неосуществимым. Расследование и судебное преследование в этой области требуют, прежде всего, адекватного материально-правового уголовного регулирования, а также адекватных процедурных возможностей, таких как полномочия и технические возможности идентификации злоумышленников, сохранение компьютерных данных, право требовать от операторов выдачи указанных данных.

Во многих случаях эти действия имеют международный охват, который может потребовать согласованного расследования во многих странах. Вследствие этого преследование и предотвращение террористической деятельности в Интернете в значительной степени зависит от наличия соответствующих международных конвенций.

Национальные материально-правовые нормы уголовного права и различные рассматриваемые международные стандарты характеризуются следующими особенностями: там описываются прежде всего деяния, результаты и намерения. Таким образом, проведенное расследование применимости этих положений к террористическим актам в сети Интернет требует систематического анализа не только самих актов, но и в особенности самого процесса их применения.

В процессе нашей работы мы изучили варианты террористических действий в сети Интернет.

Первичный результат всех разрушительных действий против компьютерной системы, осуществляемых посредством сети Интернет, это *помехи с данными*, то есть разрушение, изменение, подавление или же уничтожение недоступных данных [2, с. 37].

- *Вторичными результатами* такого рода вмешательства в данные могут быть: видимый в *двух видах ущерб*: цифровой (или нематериальный) ущерб в том случае, если данные будут недоступны или обработаны таким образом, что услуги больше не могут быть оказаны, или если компьютерная система скомпрометирована, подобно классической жертве преступления. Физический (или материальный) ущерб может быть нанесен, например, если в администрировании используется атакованная компьютерная система (например, обрушен сервер гидроэлектростанций или электростанций).
- При причинении этих первичных и вторичных результатов исполнитель намерен добиться *третьего результата*, а именно осуществления *политических целей* (таких как запугивание населения, принуждение правительства к действию определенным образом или дестабилизация политической ситуации).

Можем выдвинуть гипотезу о том, что кибертерроризму можно противостоять с помощью «компьютерного» подхода к обработке данных (с упором на нематериальный ущерб) и/или с использованием подхода, предусматривающего «конкретный террористический материальный ущерб» (сосредотачиваясь на физическом вреде и политических целях).

Эти два возможных подхода будут проанализированы более подробно на основе соответствующих международных конвенций, т.е. Конвенция о киберпреступности Совета Европы, ЕС, Рамочного решения Совета о нападениях на информационные системы, а также различных конвенций ООН, обязывающих государства ввести в действие материально-правовые нормы уголовного права.

Конвенция Совета Европы о киберпреступности является наиболее полным из всех существующих международных документов, касающихся компьютерной преступности. Она включает обязательства в отношении материального уголовного права, уголовное судопроизводство и международное сотрудничество [3, с. 28].

В области материального уголовного права (глава II, раздел 1), ст. 4 и 5 касаются «причинения ущерба, исключения, ухудшения состояния, изменения или подавления компьютерных данных» и «серьезные затруднения ... функционировании компьютерной системы путем

ввода искаженной информации, передача, повреждение, удаление, ухудшение, изменение компьютерных данных»:

Таким образом, ст. 4 и 5 Конвенции о киберпреступности охватывают все виды помех с данными и вычислительными системами, которые, как показано, есть обязательное условие для совершения терактов на компьютерные системы, осуществляемые с помощью сети Интернет.

Кроме того, Статьи 2 и 3 Конвенции о киберпреступности охватывают методы взлома и перехвата компьютерных данных (например, с помощью технических манипуляций).

Эти положения расширены по своему охвату правилами, касающимися покушения, пособничества и подстрекательства (ст. 11) и корпоративной ответственности (ст. 12) и поддерживаются правилами, требующими эффективного, пропорционального воздействия, включая лишение свободы (ст. 13). Кроме того, ст. 6 «О неправомерном использовании устройств» направлена на «криминализацию действий, подготовительных к вторжению, таких как незаконное производство, продажа, закупка для использования или иное изготовление компьютерных программ, разработанных или приспособленных в первую очередь для совершения любого из преступлений, установленных в соответствии со статьями 2-5».

Таким образом, в отношении террористических нападений через Интернет ст. 2, 3 и 6 дают дополнительную защиту, позволяющую привлечь виновных к ответственности в кратчайшие сроки.

Как следствие, имплементационные требования к Конвенция о киберпреступности в области материального уголовного права требуют широкой криминализации ИТ-ориентированных террористических актов в российском законодательстве. Как было показано выше, физический вред не является обязательным условием для наказания в соответствии с Конвенцией о киберпреступности, но приводит к необходимости применения дополнительной квалификации деяний по национальному уголовному законодательству. Таким образом, Конвенция о киберпреступности описывает компьютерные атаки с помощью так называемого «подхода через данные», она не оценивает материальный вред, нанесенный хакерской атакой или политические цели исполнителя.

Рамочное решение Совета ЕС о нападениях на информационные системы основывается на Конвенции о киберпреступности и, как и в Конвенции, обеспечение незаконного доступа к информационным системам (ст. 2), незаконное вмешательство в работу систем (ст. 3) и незаконное вмешательство в учет данных (ст. 4) наказуемы как уголовные преступления [3, с. 41].

В дополнение, Решение включает четкие требования, касающиеся криминализации таких преступлений, как подстрекательство, пособничество и покушение.

Однако в отличие от Конвенции основное внимание в Рамочном решении уделяется не вмешательству в работу с базами данных или хакерским атакам, но результату действий преступника и его намерениям.

Статья 1 Рамочного Решения гласит: каждое государство-участник принимает необходимые меры для обеспечения противодействия умышленным действиям, упомянутым ниже ..., которые, учитывая их природу или контекст, могут нанести серьезный ущерб стране или международному сообществу, и совершаются с целью:

- серьезного запугивания населения;
- неоправданного принуждения правительства или международной организации к совершению или отказу от совершения какого-либо действия;
- серьезной дестабилизации политической обстановки в стране,

признаются террористическими преступлениями:

d) причинение значительного ущерба правительству или общественности, транспортной системе, *объекту инфраструктуры, в том числе: информационной системе,* или частной

собственности, которое может представлять опасность для жизни человека или *привести к крупным экономическим потерям …*

i) угроза совершения любого из деяний, перечисленных в подпунктах a) - h).

Статьи 2 и 4 содержат дополнительные правила, касающиеся квалификации соучастия (в том числе предоставления информации, материальных ресурсов или финансирования) и покушения на акт кибертерроризма.

Таким образом, в Рамочном решении применяется так называемый «телесный подход к ущербу», который фокусируется на самом террористическом акте, ущербе, им причиняемом и его мотивировке.

Принимается во внимание следующее: «террористический» умысел исполнителя понимается как отягчающее обстоятельство. Статья 5 Рамочного решения требует, чтобы такие преступления наказывались более длительными сроками лишения свободы, чем те, которые могут быть назначены в соответствии с национальным законодательством за совершение преступлений без подобного умысла [4, с. 42].

Организация Объединенных Наций разработала многочисленные многосторонние конвенции и протоколы, касающиеся борьбы государств с кибертерроризмом.

Конвенция о борьбе с незаконным *захватом имущества, находящегося в государственной собственности,* криминализирует некоторые деяния, такие как захват воздушного судна, применение насилия в отношении лица, находящегося на его борту; уничтожение воздушных судов или аэронавигационных средств и другие подобные преступления. Покушение на подобное преступление, а также соучастие в нем тоже наказуемы. Это положение может применяться, например, в случаях захвата компьютерной системы управления полетом в самолетах или аэропортах.

- Конвенция о предупреждении *преступлений в отношении лиц, пользующихся международной защитой,* обязывает стороны: ввести уголовную ответственность за некоторые деяния, направленные против глав государств, глав правительств, а также дипломатических представителей, такие как убийство, похищение, некоторые насильственные нападения, угрозы и попытки их. Такое нападение может быть совершено, например, путем манипулирования компьютерной системой для покушения на подобную жертву.
- Международная Конвенция о борьбе с *захватом заложников* наказывает «любое лицо, которое захватывает или задерживает и угрожает убить, травмировать или продолжать задерживать другого человека ... для того, чтобы принуждать третью сторону ... делать или воздерживаться от совершения какого-либо действия в качестве посредника, и это будет явное или неявное условие освобождения заложника». Положения этой конвенции могут применяться, например, в том случае, когда террористы передают требования о выкупе по электронной почте.
- Конвенция о физической *защите ядерного материала*. Статья 7 охватывает «деяние, совершенное без законного основания, которое представляет собой получение, владение, использование, передачу, изменение, удаление или рассеивание ядерного материала и которое вызывает или вероятно вызовет, смерть или серьезные травмы для любого человека или существенный ущерб имуществу». Конвенционное преступление может быть совершено, например, террористами при манипулировании компьютерной системой атомной электростанции с намерением похищения ядерного материала [4, с. 48].
- Конвенция о борьбе с незаконными актами, направленными против безопасности *морского судоходства* стабилизирует правовой режим применимо к актам, угрожающим безопасности международных морских перевозок. Она аналогична правилам, применяемым к актам, угрожающим безопасности полетов международной авиации. Захват судна может быть произведен террористами, например, путем манипулирования электронной системой управления кораблем.

В отношении кибертерроризма и использования сети Интернет в террористических целях важно отметить, что все положения, содержащиеся в конвенциях и протоколах, рассмотренных выше, сформулированы в общих чертах. Они применимы независимо от того, как эти действия совершаются, то есть независимо от того, совершены ли они традиционными средствами или с помощью ИТ-атак. Например, положения, требуемые вышеупомянутыми конвенциями ООН, применимы, если сеть Интернет используется для получения контроля над аэропортом или судовой навигационной системой, если используется компьютерная сеть для атаки на самолет или если компьютерные манипуляции предпринимаются для того, чтобы передать ядерный материал [5, с. 19].

Мы можем сделать вывод о том, что все серьезные атаки на компьютерные системы и объекты инфраструктуры охватываются составами, указанными в международных конвенциях и документах, рассмотренных выше.

Конвенция Совета Европы по киберпреступности также уделяет большое внимание практическим аспектам международного сотрудничества. Она предусматривает организацию «сети 24/7» с контактом между правоохранительными органами государств-участников Конвенции, доступным двадцать четыре часа в сутки, семь дней в неделю. Статья 35 требует, чтобы каждая сторона назначала «пункт связи, работающий на круглосуточной основе, с тем чтобы обеспечить незамедлительное предоставление информации; помощь в проведении расследований или разбирательств в отношении уголовных преступлений, связанных с компьютерными системами». Такая помощь включает в себя предоставление технических консультаций, сохранение данных в соответствии со статьями 29 а также 30, сбор доказательств, предоставление юридической информации, а также информации о местонахождении подозреваемых.

Список литературы

1. Bassiouni C. International Terrorism : Multilateral Conventions (1937-2001), 3 т., New York 2001/2002.
2. Goodman M., 2015. Future crimes: inside the digital underground and the battle for our connected world. New York: Anchor Books.
3. Greene A. (2017). TERRORISM DEFINITION: ONE SIZE FITS ALL? International and comparative law quarterly, 66 (2), 411-440. doi: 10.1017 / S0020589317000070
4. Rao A.S., and Verweij G., 2018. Sizing the prize. What's the real value of AI for your business and how can You capitalize? New York: PWC. Rastorguev, S. P., and Litvinenko, M. V., 2014. Informatsionnye operatsii v seti Internet [Information operations on the Internet]. Edited by A. B. Mikhailovsky. Moscow: The Centre of Strategic Assessment and Forecasts.
5. Sieber U. « International cooperation against terrorist use of the internet », Revue internationale de droit pénal, 2006/3 (Vol. 77), p. 395-449. DOI: 10.3917 / ridp.773.0395. URL: https://www.cairn.info/revue-revue-internationale-de-droit-penal-2006-3-page-395.htm
6. Sieber U. the Threat of Cybercrime, in : Council of Европа (ред.), Organized Crime in Europe, Strasbourg 2005, Pp. 81-218 (173-175)
7. Sieber U. Punishment of Serious Crimes, Vol. 1, Freiburg 2004, PP. 26 ff.
8. Waddel K., 2018. The impending war over deepfakes. Axios [online]. Available at: [Accessed 31 January 2019]. World Economic Forum, 2016. The future of job employment, skills and workforce strategy for the fourth industrial revolution. Executive summary. Geneva: World Economic Forum.

Т.А. Савчук, *к.ю.н., доцент кафедры правового обеспечения правоохранительной деятельности Академии управления при Президенте Республики Беларусь, г. Минск*
М.А. Городецкая, *магистр юридических наук, старший преподаватель кафедры правового обеспечения правоохранительной деятельности Академии управления при Президенте Республики Беларусь, г. Минск*

ОБЗОР НАЦИОНАЛЬНОЙ СИТУАЦИИ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Активный рост киберугроз в мировом масштабе ставит перед каждым государством задачу — обеспечить информационную безопасность, повысить уровень защищенности граждан современного информационного общества. При этом в качестве приоритетных видятся вопросы правового регулирования борьбы с киберпреступлениями на национальном и международном уровне, квалифицированной кадровой обеспеченности сферы информационной безопасности, установления единых подходов к определению родового объекта киберпреступности в уголовном законе. Происходящие в обществе процессы информатизации оказали существенное влияние на преступность и ее качественные и количественные показатели.

Как заметил Президент Республики Беларусь А.Г. Лукашенко в своем выступлении, посвященном Дню Независимости Республики Беларусь 1 июля 2012 г., «новые информационные технологии, колоссальная мощь Интернета, опутавшего сетью всю планету, вместе с невиданными ранее возможностями таят прямые угрозы суверенитету не только отдельных государств, но и каждой отдельной личности». Опасность современной киберпреступности состоит в способности ее проникновения во все сферы жизни общества, а также в быстрой приспособляемости к новым условиям. Комплекс причин и условий, способствующих совершению киберпреступлений, включает: высвобождение и сложности трудоустройства в условиях кризиса высокоинтеллектуальной части населения, связанной с компьютерными технологиями; возможность быстрого обогащения путем компьютерных хищений с незначительной вероятностью разоблачения ввиду высокой латентности компьютерных преступлений; недостаточная защищенность автоматизированных систем обработки данных; лояльное отношение общества к такого рода преступлениям ввиду использования лицами, их совершающими, интеллектуального способа обогащения; отсутствие должного противодействия.

Отметим, что первое высокотехнологичное преступление на территории Республики Беларусь было зарегистрировано 20.11.1998. Внедрив в программное обеспечение «компьютера-жертвы» вредоносную программу типа «троянский конь» под названием «BackOrifice», злоумышленник осуществил несанкционированный доступ к сетевым реквизитам пользователей глобальной сети Интернет из числа клиентов крупнейшего в республике столичного сервис-провайдера [1].

Впервые столкнувшись с преступлениями в информационном пространстве в 1998 г., органы внутренних дел Республики Беларусь начали борьбу с ней при помощи традиционных правовых норм, но такой подход оказался не вполне удачен ввиду того, что многие компьютерные преступления не охватывались традиционными составами преступлений. Поэтому закономерно, что законодателю и правоохранительным органам Беларуси на определенном этапе пришлось столкнуться с выбором одного из двух вариантов реагирования на новые угрозы. Первый вариант состоял в признании существования нового явления — киберпреступности, выработке и реализации новых эффективных методов борьбы с данным явлением, включая законодательную и материально-техническую составляющие, направляя их на нужды следственной и оперативно-розыскной деятельности. Второй вариант предполагал игнорирование такого явления, тем более что масштабы выявления его, особенно в регионах республики относительно

иных категорий преступлений, были некритичны. Исходя из реалий был выбран первый вариант, что потребовало обновления законодательной базы и совершенствование кадрового обеспечения процесса противодействия новым вызовам и угрозам.

В этой связи в Республике Беларусь (как и во многих государствах-участниках СНГ) в 2012 г. было создано Управление по раскрытию преступлений в сфере высоких технологий Министерства внутренних дел Республики Беларусь («Управление «К»), основной задачей которого является оказание содействия в выявлении и раскрытии преступлений против информационной безопасности и в сфере телекоммуникаций; преступлений, где электронная информация является орудием (средством) совершения другого преступления; преступлений, совершаемых с использованием в той или иной мере компьютерной и другой электронной техники; преступлений, связанных с распространением в сети Интернет детской порнографии. Управление «К» определено головным подразделением в системе органов внутренних дел, отвечающим за организацию борьбы с преступлениями, предусмотренными ст. 212, 349-355 Уголовного кодекса Республики Беларусь (далее — УК Республики Беларусь), а также координирующим деятельность подразделений главного управления криминальной милиции Министерства внутренних дел Республики Беларусь и органов внутренних дел при выявлении ими преступлений против информационной безопасности.

В настоящее время, согласно официальной статистике Управления «К», отмечается стремительный рост киберпреступлений. Так, если в 2006 г. было зарегистрировано 334 таких преступлений, то в 2016 г. — 2 471 преступление, в 2017 г. — 3 099, в 2018 г. — 4 741, в 2019 г. — 10 567. Таким образом, с 2018 г. по 2019 г. их число увеличилось в 2,2 раза (с 4 741 до 10 539 преступлений) и составило 11,9% от общей численности зарегистрированных в Республике Беларусь преступлений. Между тем приведенные цифры охватывают лишь составы, предусмотренные УК Республики Беларусь: преступления против информационной безопасности (ст. 349–355); хищение путем использования компьютерной техники (ст. 212), что позиционирует киберпреступность как явление. При этом около 75% совершенных преступлений составляют хищения с использованием компьютерной техники, остальные — преступления против информационной безопасности. Прирост преступлений против информационной безопасности обусловлен увеличением случаев несанкционированного доступа к компьютерной информации (например, в 2017 г. в Беларуси было зарегистрировано 462 таких преступлений, в 2018 г. — 912, в 2019 г. — 2 185). Такая ситуация наблюдается как по Республике Беларусь в целом, так и по отдельным ее регионам: количество выявленных преступлений против информационной безопасности (ст. 349–355 УК Республики Беларусь) увеличилось в целом по республике, поскольку в 2017 г. было зарегистрировано 781 такое преступление, в 2018 г. — 1 156; в 2019 г. — 2 492.

Не вызывает сомнений, что количественные показатели лишь частично отражают сущность киберпреступности как правового явления, а действующая система учета преступлений не отражает реальной картины киберпреступности в республике. Исследование состояния, структуры и динамики киберпреступности представляет определенную сложность, ведь в современных условиях возрастает количество преступлений, совершаемых с использованием информационно-коммуникационных технологий (например, доведение / склонение / пропаганда самоубийства; незаконный оборот наркотических средств …; изготовление и распространение порнографических материалов, предметов порнографического характера с изображением несовершеннолетнего; компьютерное вымогательство; «кардинг»), выявление, раскрытие и расследование которых вызывает определенные практические трудности. Справедливо отмечает Е.А. Русскевич, что информационно-коммуникационная трансформация преступности является объективным и неизбежным следствием вступления в эпоху информа-

ционного общества [2, с. 10]. В рассматриваемом контексте представляется важным рассмотреть сущность киберпреступности для осмысления ее как явления правовой действительности.

Прежде всего отметим, что в правовой литературе кроме термина «киберпреступность» употребляются различные его аналоги: «компьютерные преступления», «преступления против информационной безопасности», «преступления в сфере высоких (информационных) технологий», «цифровая преступность», «преступления в сети Интернет». М.А. Дубко указывает, что такое разнообразие обусловлено отсутствием единых подходов на основания отнесения противоправных деяний к исследуемым преступлениям в связи с совершенствованием информационных компьютерных технологий и отличающимися национальными подходами в определении родового объекта таких преступлений [3]. Наиболее приемлемым, на наш взгляд, является термин «киберпреступность», официальное толкование которого выработало международное сообщество: киберпреступлениями являются деяния, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а также злоупотребления такими системами, сетями и данными (Будапештская конвенция, 2001); киберпреступность — это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, сетей и данных (проект ООН «Всестороннее исследование проблемы киберпреступности», 2013). Такой подход позволяет расширительно толковать противоправные деяния, подпадающие под киберпреступления, для целей развития уголовного законодательства и установления единых критериев их мониторинга.

Я.И. Гилинский указывает, что снижение уровня преступности и большинства ее видов в мировом пространстве «является следствием, во-первых, «ухода» основного субъекта уличной преступности — подростков и молодежи — в Интернет; во-вторых, «замещения», «вытеснения» традиционной преступности высоколатентной и малоизученной киберпреступностью» [4, с. 178]. Считаем, что основной чертой киберпреступности является ее гиперлатентность, ведь большая ее часть остается за рамками официальной уголовной статистики (считается, что в официальную статистику попадает в лучшем случае 20% таких деяний [5, с. 51]; а по оценкам экспертов, латентность киберпреступлений в США равна 80%, в Великобритании — 85%, в ФРГ — 75%, в России — более 90% [6, с. 371]). Киберпреступности присущи и иные характеристики, отражающие ее правовую природу, а именно:

– популярность и стремительный рост, обусловленные невероятной прибыльностью киберпреступности как «бизнеса», минимальным риском и малозатратностью совершения таких преступлений, относительной комфортностью — их подготовка и совершение осуществляются, практически не отходя от «рабочего места»;

– сверхизменчивость, связанная со стремительным и непрерывным совершенствованием технологий, что предопределяет динамичный процесс обновления киберпреступности и форм ее проявления;

– гипертаргетированность, состоящая в том, что киберпреступности свойственна нацеленность на большое количество потерпевших (по данным международной службы по обеспечению безопасности в области киберугроз Symantec Securiti, каждую секунду в мире подвергаются кибератаке 12 чел., ежегодно в мире совершается около 556 млн киберпреступлений, ущерб от которых составляет более 100 млрд дол. США» [6, с. 371]);

– мультипликативность (самовоспроизводство), которое в научной среде позиционируется как перманентный признак преступности (на это указывают российские криминологии: А.И. Долгова, С.М. Иншаков, В.Н. Кудрявцев, В.В. Лунеев, Г.Ф. Хохряков). Но приме-

нительно к киберпреступности данный признак приобретает новое содержание и наиболее ярко проявляется на примере распространения вредоносных компьютерных программ;

– транснациональный характер (экстерриториальность) и связь с организованной преступностью. Киберпреступность является одним из видов транснациональной преступности, исполнители и жертвы которой могут находиться в любой точке мира, где есть подключение к глобальной сети Интернет. Экстерриториальный характер интернет-коммуникаций и, как следствие, рост киберпреступности убеждает в недостаточности региональных и (или) внутригосударственных мер.

Как отмечает международный эксперт по гармонизации законодательства в сфере киберпреступности Ш. Шьольберг, «киберпространство, как пятое общее пространство, после наземного, морского, воздушного и космического, требует координации, сотрудничества и особых правовых мер на международном уровне» [6, с. 370]. Иными словами, борьба с трансграничной киберпреступностью должна осуществляться при хорошо скоординированной работе правоохранительных органов различных стран, включает разработку нормативных актов и общих рекомендаций, внедрение эффективных моделей организационного взаимодействия между государствами.

Республика Беларусь уделяет пристальное внимание борьбе с киберпреступностью на национальном уровне и активно развивает международное сотрудничество в сфере противодействия киберугрозам, в основном используя традиционные механизмы такого сотрудничества — разработку правовых основ, запросы и взаимопомощь, совместные мероприятия, обмен информационными услугами и другие подобные инструменты.

На национальном уровне приняты и действуют нормативные правовые акты, определяющие правовой режим информации, порядок ее предоставления и распространения, правовой режим информационных ресурсов и порядок их регистрации, а также порядок создания, использования и регистрации информационных систем. К наиболее значимым из них относятся: Концепция информационной безопасности (утв. постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1); Указы Президента Республики Беларусь от 01.02.2010 № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет», от 08.11.2011 № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь»; от 05.01.2015 № 4 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность»; Законы Республики Беларусь от 19.07.2005 № 45-З «Об электросвязи»; от 10.11.2008 № 455-З «Об информации, информатизации и защите информации». Реализация положений названных нормативных правовых актов осуществляется системой государственных, главным образом — правоохранительных органов, где ведущее место отводится Генеральной прокуратуре Республики Беларусь, являющейся координатором деятельности по борьбе с преступностью на государственном уровне.

В данном контексте отметим, что Генеральной прокуратурой Республики Беларусь ведется активная работа в получении положительного зарубежного опыта в борьбе с киберпреступностью и формировании устойчивой платформы собственных мероприятий в данном направлении. Так, в сентябре 2019 г. в Генеральной прокуратуре Республики Беларусь состоялась встреча с представителями проекта Совета Европы и Европейского Союза «КиберВосток» в странах «Восточного партнерства», цель которого — выработать конкретные меры по гармонизации законодательства Армении, Азербайджана, Беларуси, Грузии, Молдовы и Украины с положениями Конвенции Совета Европы о преступности в сфере компьютерной информации (2001), повышение эффективности международного взаимодействия между поставщиками информационных услуг, судебными и правоохранительными органами в сфере уголовного правосудия, борьбы с киберпреступлениями и сбора электронных доказательств. В числе

основных вопросов были затронуты проблемы подготовки сотрудников правоохранительных органов и идея создания обучения прокурорских кадров, специализирующихся на вопросах борьбы с киберпреступностью [7]. Несомненно, что квалифицированная кадровая обеспеченность сферы информационной безопасности — это один из важнейших факторов, влияющих на результативность борьбы с киберугрозами.

Основные направления стратегии борьбы с киберпреступностью на национальном уровне определены Программой по борьбе с преступностью и коррупцией на 2020–2022 гг., утвержденной решением Республиканского координационного совещания по борьбе с преступностью и коррупцией от 18.12.2019 № 20 (раздел 5.3 «Предупреждение и пресечение преступлений в информационной сфере»). Так, названной Программой предусмотрены следующие значимые направления противодействия киберпреступности:

1) обобщение практики рассмотрения заявлений и сообщений о преступлениях, предусмотренных ст. 208, 209, 212 УК Республики Беларусь, совершаемых в компьютерных системах, социальных сетях и глобальной компьютерной сети Интернет, следственной и судебной практики по делам о преступлениях указанной категории;

2) обеспечение взаимодействия с представителями бизнес-сообществ в целях разработки и внедрения специализированного сетевого ресурса по противодействию и профилактике противоправных деяний в информационном пространстве;

3) подготовка рекомендаций по определению порядка реагирования сотрудниками служб безопасности банков на преступления в банковской и кредитно-финансовой сферах, осуществляемая совместно с Национальным банком Республики Беларусь;

4) проведение комплексных межведомственных оперативно-профилактических операций и мероприятий, направленных на противодействие преступлениям в информационной сфере;

5) анализ уголовного законодательства государств-участников СНГ в сфере противодействия преступлениям против информационной безопасности в целях выработки предложений по его унификации.

Национальная стратегия по противодействию киберугрозам строится на основе международных стандартов и положительного зарубежного опыта в данной сфере. Необходимость развития и использования международных инструментов в борьбе с киберпреступностью особенно стала заметна после принятия соглашений, призванных установить глобальные стандарты в борьбе с преступностью в информационном пространстве, а именно: Конвенции Совета Европы о киберпреступности (подписана 23.11.2001 в Будапеште и открыта для подписания как государствами-членами Совета Европы, так и государствами, не являющимися его членами, которые участвовали в ее разработке), Соглашения о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001). Конвенция Совета Европы о киберпреступности является первым международным договором о преступлениях, совершенных через глобальную компьютерную сеть Интернет и другие компьютерные сети, регламентирующим, в частности, нарушения авторских прав, компьютерных мошенничеств, детской порнографии и нарушений безопасности сети. Данный международный документ устанавливает определенные полномочия и предусматривает такие процедуры, как обыск компьютерных сетей и перехват [8].

Отмечая значимость данной Конвенции, к сожалению, следует отметить, что в настоящее время Республика Беларусь не является ее участницей. Это обстоятельство наряду с другими порождает в исследовательской среде мнение о неэффективности уголовной политики и отставании уголовного законодательства от стремительного развития компьютерных технологий [9, с. 98].

Вышеизложенное приводит к следующим выводам:

1. Для определения правильной стратегии борьбы с транснациональными киберпреступлениями на первое место выходит проблема гармонизации законодательства всех государств в мировом масштабе с положениями Конвенции Совета Европы о преступности в сфере компьютерной информации (2001), на которую нами указывалось ранее, и унификации родового объекта киберпреступлений в уголовном законодательстве.

2. Сложность, опасность и транснациональность киберпреступлений указывает, что крайне важным является выработка не только совместных действий ученых-правоведов и законодателей, но и специалистов в сфере компьютерных технологий, направленных на противодействие таким преступлениям в глобальных информационных сетях. Принимая во внимание особенность Интернета как трансграничного информационного ресурса, мировому сообществу необходимо консолидировать свои усилия с привлечением технических специалистов и выработать Единую концепцию противодействия на пользователей глобальной сети Интернет.

3. Основное ядро сотрудничества и взаимодействия государств с преступлениями транснационального характера, включая киберпреступления, составляет обмен актуальной информацией и соблюдение законодательных предписаний, ее устанавливающих. В качестве развития такого взаимодействия можно рассмотреть вопрос о создании межгосударственных банков данных для регистрации компьютерных преступлений, способов и других обстоятельств их совершения, учета компьютерных преступников [10].

4. Координация борьбы с транснациональными киберпреступлениями требует новых подходов в подборе и подготовке квалифицированных национальных кадров, представители которых будут задействованы в области кибербезопасности.

Список литературы

1. Управление «К» МВД Беларуси отметило 10-летие. URL: https://42.tut.by/322679. (дата доступа: 11.11.2019).

2. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения. М.: ИНФРА-М, 2019. 227 с.

3. Дубко М.А. Уголовное законодательство государств-участников Содружества Независимых Государств, предусматривающее ответственность за неправомерное завладение компьютерной информацией: сравнительно-правовой анализ [Электронный ресурс] [по состоянию на 05.01.2015 г.] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2020.

4. Гилинский Я.И. Современное состояние и перспективы российской криминологии // Рос. журн. правовых исследований. 2014. № 4. С. 175–180.

5. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1. С. 45–55.

6. Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью // Криминолог. журн. Байкальс. гос. ун-та экономики и права. 2016. Т. 10, № 2. С. 369–378.

7. Киберпреступность не знает границ. Представители Генпрокуратуры и Совета Европы развивают сотрудничество в рамках проекта «КиберВосток». URL: https://www.prokuratura.gov.by. (дата доступа: 04.03.2020).

8. Управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь (Управление «К»). URL: https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/istoriya-urpsvt. (дата доступа: 11.11.2019).

9. Джансараева Р.Е., Аратулы К. Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ // Криминологический журн. ОГУЭП. 2012. № 3. С. 95–99.

10. Старичков М.В. Вопросы международного информационного обмена в раскрытии и расследовании преступлений в сети «Интернет». URL: https://cyberleninka.ru/article/n/ voprosy-mezhdunarodnogo-informatsionnogo-obmena-v-raskrytii-i-rassledovanii-prestupleniy-v-seti-internet. (дата доступа: 08.05.2020).

С.С. Симонова, *к.ю.н., доцент кафедры уголовного права, уголовного процесса и криминалистики Волгоградского института управления (филиал РАНХиГС), г. Волгоград*

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ОСОБЕННОСТИ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПЕРИОД COVID-19

Проблема преступлений, совершаемых в сети Интернет, остается актуальной, поскольку киберпреступления обладают высокой латентностью. В настоящее время киберпреступность настолько широко распространена, что рассматривать проблему ее предупреждения следует в трех аспектах: международном, федеральном и региональном.

Обратимся к статистическим данным. Количество киберпреступлений в России в 2019 г. выросло на 68,5% по сравнению с 2018 годом и составило 294,4 тыс. случаев. Каждые 4 секунды в мире рождается вредоносный файл, который может заразить организацию, личную почту человека и потом предоставить доступ преступников к данной информации.

МВД РФ зафиксировало резкий роста числа преступлений, совершенных через Интернет либо с использованием средств мобильной связи. За первые три месяца 2020 года их выявлено 101,5 тыс., почти вдвое (на 83,9%) больше, чем в первом квартале 2019 года. В общем объеме преступности их доля выросла в годовом исчислении с 11 до 20%. По данным МВД, 78% таких преступлений было совершено с целью кражи или мошенничества, а еще 10% — с целью незаконного производства, сбыта или пересылки наркотических средств. При этом преступлений на улицах стало меньше на 3,3%. [1]

Ущерб от киберпреступлений составляет 1 трлн 700 млн долларов. Средняя сумма хищений в день у юридических лиц с троянами для ПК составляет 250 000 рублей, у физических лиц с Android-троянами — 440 000 рублей, фишинг приносит злоумышленникам 348 000 рублей в день, а обналичивание похищаемых денег составляет 467 100 рублей ежедневно.

В марте 2020 г. в структуре Следственного комитета появился отдел по расследованию киберпреступлений и преступлений в сфере высоких технологий.

Уголовная ответственность за совершение киберпреступлений (преступлений в сфере компьютерной информации) регламентируется Главой 28 Уголовного кодекса Российской Федерации. В рассматриваемой Главе предусмотрены следующие составы преступлений:

- Статья 272. Неправомерный доступ к компьютерной информации.
- Статья 273. Создание, использование и распространение вредоносных компьютерных программ.
- Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
- Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации(введена в действие в 2017 г.) [2].

1 апреля Президент России Владимир Путин подписал закон об ужесточении наказания за распространение заведомо ложной информации, которое привело к тяжким последствиям. В обзоре практики, который был опубликован 21 апреля, Верховный суд изложил правила привлечения к уголовной ответственности за недостоверную информацию о коронавирусе. Речь идет о статьях Уголовного кодекса: 207.2 УК («Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия»).

Верховный суд разъяснил, что обстоятельства распространения новой коронавирусной инфекции (COVID-19) относятся к «обстоятельствам, представляющим угрозу жизни и безопасности граждан». Ведь это повлекло и еще может повлечь человеческие жертвы, значительные материальные потери и нарушение условий жизнедеятельности населения [3].

Верховный суд также разъяснил, в чем заключается преступление по ст. 207.1 УК. Это «публичное распространение под видом достоверных сообщений заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, в том числе об обстоятельствах распространения новой коронавирусной инфекции (COVID-19) на территории Российской Федерации, и (или) о принимаемых в связи с этим мерах по обеспечению безопасности населения и территорий, приемах и способах защиты от указанных обстоятельств». При этом судам следует учитывать условия, цель и мотивы совершения преступления (например, чтобы спровоцировать панику и нарушить правопорядок). Такая информация может распространяться не только через СМИ, но и путем выступлений на собрании, митинге, распространения листовок, вывешивания плакатов.

Необходимо отметить, что уголовная ответственность возможна только за те деяния, которые совершили после вступления статей УК РФ в силу, то есть с 1 апреля 2020 года. Соответственно, нельзя наказать за действия, которые были совершены до этого, пусть даже общественно опасные последствия наступили после.

За совершение данных преступлений Уголовный кодекс предусматривает штрафы от 300 000 до 1,5 млн руб., обязательные, исправительные работы или лишение свободы до трех лет (в зависимости от последствий).

Уже имеется практика возбуждения уголовных дел по ст. 207.1 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан». В частности, в Твери возбудили дело за фейк об умерших в больнице от коронавируса, распространенный в социальных сетях.

13 апреля Генпрокуратура выявила в Интернете ложные сообщения о «сотнях погибших от коронавируса в ряде регионов». Недостоверные публикации обнаружили в Республике Башкортостан, Северной Осетии, Волгоградской и Свердловской областях. Так, в Волгограде пользователем видеохостинга YouTube был размещен ролик, где он рассказывает о сотне умерших в Волгограде. Надзорное ведомство попросило Роскомнадзор принять меры по ограничению доступа к фейкам, а при переносе аналогичных материалов на другие сайты ограничить к ним доступ.

В условиях распространения коронавируса в мире наблюдается повышение активности киберпреступников. В начале апреля Европейское полицейское агентство опубликовало доклад, в котором сообщается о росте числа киберпреступлений в связи с коронавирусом. Киберпреступники «быстро адаптировались» в условиях пандемии коронавируса и стали использовать ее в своих целях. Злоумышленники пользуются увеличением количества людей в Интернете и играют на беспокойстве в обществе. В частности, увеличилось распространение программ-вымогателей, а также атак, приводящих к недоступности веб-сайтов. Также, по данным Европола, значительно ухудшилась ситуация в таких сферах, как сексуальная эксплуатация детей; использование темного Интернета (сегмент всемирной паутины, куда можно попасть

лишь с помощью специального программного обеспечения, где можно сохранять полную анонимность и где осуществляется торговля нелегальными товарами).

Пандемия коронавируса стала причиной возникновения в сети нового типа мошенничества, который связан с темой распространения инфекции. Киберпреступники пытаются по максимуму воспользоваться ситуацией, когда множество людей работает и учится из дома с использованием устройств с устаревшими системами безопасности.

Киберпреступники очень быстро адаптировались и начали использовать пандемию в своих целях, в том числе играя на беспокойстве и страхе людей. С учетом значительно увеличившегося числа потенциальных жертв, сидящих дома и использующих различные онлайн-услуги, они не только все активнее используют старые методы, но и изобретают все новые способы получения выгоды от ситуации.

Следует отметить, что проблема киберпреступности в связи с короновирусом затронула и Россию. Аферисты оперативно подстраиваются под текущую ситуацию и изобретают новые способы обмана людей. Фальшивые уведомления о штрафах за нарушение самоизоляции стали получать россияне через мессенджеры и СМС-сообщения. В таких сообщениях мошенники ссылаются на несуществующее постановление ФСИН. Угрожая возбуждением уголовного дела, аферисты требуют в течение суток уплатить штраф переводом на номер абонента. Если же человек перезванивал, ему отвечали якобы специалисты справочной службы МВД РФ [4].

В России среди наиболее частых случаев мошенничества — продажа фальшивых лекарств от коронавируса и тестов на наличие инфекции, фейковые интернет-магазины. Мошенники также представляются сотрудниками коммунальных служб и собирают плату за ЖКХ. Отмечены также случаи появления людей в униформе полицейских или росгвардейцев, которые берут с прохожих штрафы наличными за появление в общественных местах. Мошенники активно пользуются темой пандемии и рассылают огромное количество соответствующих спам-писем. Преступники выдают себя за представителей Всемирной организации здравоохранения (ВОЗ) и осуществляют рассылку указаний, касающихся мер безопасности. Однако при активации ссылки пользователя «перебрасывает» на фишинговый сайт, где ему предлагают поделиться персональной информацией.

После всех действий личные данные оказываются в пользовании мошенников. От киберпреступников также приходят вредоносные письма, в которых они обещают рассказать об источниках распространения коронавируса и поделиться более подробной информацией о нем. Если пользователь заинтересуется и перейдет по ссылке (или откроет вложение), вирус будет загружен на его компьютер. Как правило, используются вирусы-вымогатели или другие вредоносные кампании.

Не менее важной представляется и такая проблема: многие люди перешли на удаленную работу, и в результате открылось значительно большее число сервисов для дистанционной работы, а множество из них до сих пор не обновлены. В результате количество взломов увеличилось.

Банк России фиксирует новые мошеннические схемы для хищения денег с банковских счетов с применением приемов социальной инженерии. При этом преступники активно используют тему коронавирусной инфекции.

Мошенники обзванивают граждан, обещая отсрочки по выплате кредитов, разного рода компенсации, пособия, возврат денег за авиационные билеты, услуги по диагностике заражения коронавирусной инфекцией, волонтерство. Все в итоге сводится к тому, что человек должен под тем или иным предлогом сообщить данные своей банковской карты, пароль из СМС либо самостоятельно осуществить платеж на некий счет. Для того чтобы выманить у граждан данные банковских карт и убедить человека открыть вложение или перейти по ссылкам на

зараженные сайты, киберпреступники часто подделывают бренд и фирменный стиль известных организаций (Министерство здравоохранения, Роспотребнадзор, Банк России, Всемирная организация здравоохранения и другие). Всплески аналогичных атак фиксируются и в других государствах.

Далее рассмотрим, какие меры предупреждения преступлений, совершаемых в сети Интернет, являются наиболее эффективными, особенно в период распространения коронавирусной инфекции.

Банк России рекомендует не сообщать посторонним людям и не вводить на неизвестных сайтах данные своей банковской карты, пароли из СМС-сообщений, под каким бы предлогом эти данные ни пытались узнать.

Луис Корронс, представитель компании Avast, отмечает, что для борьбы с преступлениями в Интернете рекомендуется устанавливать системы безопасности на свое устройство, которые умеют блокировать фишинговые атаки [5]. Руслан Сулейманов, директор управления информационных технологий компании ESET считает, что нужно уничтожать сообщения от неизвестных адресатов. Для этого сначала необходимо проверить, куда ведет ссылка в письме: нужно навести курсор мыши на ссылку — таким образом адрес отобразится. URL из сервиса коротких ссылок, среди которых окончание типа is.gd. Is.gd, bit.ly, является признаком фишинг-ресурса.

Роскомнадзор разместил на своем официальном сайте Памятку по поиску достоверной информации о COVID-19. Также помимо обращения в Полицию, потерпевшим от киберпреступлений рекомендуется обращаться на Горячую линию Роскомнадзора.

Таким образом, в условиях пандемии короновируса важно сохранять спокойствие, не поддаваться панике и доверять только официальной информации, а не фейковым новостям, а также помнить о правилах, помогающих не стать жертвой киберпреступлений.

Список литературы

1. Уличных преступлений стало меньше на фоне резкого роста киберпреступности / Сайт РБК URL:: https://www.rbc.ru/society/23/04/2020/5ea174a69a79471358c0459d?fromtg=1 (дата обращения: 16.06.2020).

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 07.04.2020) // СПС КонсультантПлюс. URL: http://www.consultant.ru/document/ cons_doc_ LAW_10699/(дата обращения: 15.06.2020).

3. Обзор № 1 по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) (утвержден Президиумом Верховного Суда Российской Федерации 21 апреля 2020 года. URL: http://vsrf.ru/files/28856/ (дата обращения: 15.06.2020).

4. Мошенники начали рассылать фальшивые сообщения о штрафах за карантин // Волгоградская правда. Вып. от 12.04.2020 г. URL: https://vpravda.ru/proisshestviya/moshenniki-prisylayut-falshivye-sms-uvedomleniya-o-shtrafah-za-karantin-87230/ (дата обращения: 16.06.2020).

5. Эксперты предупредили россиян о начале «киберкоронавируса» киберпреступности // Сайт РИА Новости. URL: https://ria.ru/20200317/1568703266.html (дата обращения: 11.06.2020).

В.В. Поляков, *к.ю.н., доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*
С.Н. Толстошеев, *начальник отдела «К» ГУВД МВД России по Алтайскому краю, г. Барнаул*

НЕКОТОРЫЕ ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 273 УК РФ

В последние десятилетия происходит стремительное развитие новых компьютерных технологий и их внедрение в различные сферы человеческой жизни. Зачастую эти технологии вначале внедряются и реализуются на практике и только после этого обеспечиваются полноценной защищенностью от использования в неправомерных целях. В этой связи возрастает потребность в том, чтобы новые компьютерные технологии, включая используемые средства компьютерной техники и программное обеспечение, удовлетворяли следующим требованиям: отсутствие незадекларированных возможностей, не указанных в описании; безопасность и стабильность работы при взаимодействии с другими программными и аппаратными средствами; устойчивость от несанкционированного доступа, а также обеспечение качественной работы при различных обстоятельствах и условиях. Перечисленные требования в определенной мере могут быть решены путем тестирования новых программно-аппаратных средств в специальных условиях, в том числе при так называемых стрессовых нагрузках. Важность такого решения для улучшения защищенности объектов информатизации обусловлена также тем обстоятельством, что недостатки и бреши в защищенности позволяют злоумышленникам получать несанкционированный доступ к компьютерной информации и использовать ее для совершения преступлений. Одной из причин, способствующих подобному развитию событий, являются пробелы в правовом регулировании отношений в этой области уголовным законодательством.

В 1997 г. в Уголовный кодекс Российской Федерации была включена статья 273, которая криминализировала «1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации…». Появление этой статьи было вполне обосновано с позиций противодействия распространению преступлений в сфере компьютерной информации. При применении ст. 273 УК РФ возникают определенные трудности, что отмечалось рядом исследователей (например, [1, с. 138]). Правоприменителю весьма сложно разграничивать негативные преступные действия по созданию, использованию и распространению вредоносных компьютерных программ от позитивных естественных и технически необходимых действий по исследованию защищенности компьютерных систем от всевозможных угроз. Это связано с тем, что на практике для анализа защищенности, как правило, применяется программное обеспечение под названием «тестирование на проникновение», или «пентест», которое, по сути, использует те же алгоритмы, что и вредоносные компьютерные программы [2, 3]. В связи с этим возникают вопросы относительно диспозиции ст. 273 УК РФ и реальных возможностей доказывания в целом и по отдельным частям этой статьи. В частности, это относится к совершению преступления группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинте-

ресованности, а также когда преступные действия повлекли тяжкие последствия или создали угрозу их наступления.

Изложенное означает, что существуют проблемы, связанные с несовершенством законодательного регламентирования ст. 273 УК РФ и практикой расследования преступлений, подпадающих под эту статью [4; 5, с. 164]. Эта проблема проявляется в виде двух взаимосвязанных негативных факторах.

Первый фактор связан с тем, что специалисты, добросовестно работающие в области защиты компьютерной информации, оказываются под реальной угрозой уголовного преследования. Это вызвано с тем, что в силу недостаточной точности формулировки замысла законодателя, изложенного в ст. 273 УК РФ, работа этих специалистов по исследованию защищенности программно-аппаратных средств может подпадать под действие данной статьи. Опасаясь такого преследования, многие специалисты выполняют свою работу с существенными ограничениями или же в той или иной степени уклоняются от нее. Это представляется недопустимым и тормозит применение передовых информационных технологий в сфере защиты информации. Полагаем, что данная проблема может быть в значительной степени решена при учете в уголовном законодательстве Российской Федерации ст. 6 Конвенции о компьютерной преступности Совета Европы [6], в которой говорится, что уголовная ответственность не наступает, если не преследовалась цель совершения преступления. Например, это имеет место при санкционированном тестировании, производимом в целях обеспечения защиты работы компьютерной системы [7, с. 40].

Второй фактор заключается в том, что при предварительном расследовании и судебном разбирательстве высокотехнологичных преступлений [8], совершаемых в групповой форме, высока вероятность использования в защитительных целях действующей формулировки ст. 273 УК РФ таким образом, чтобы продемонстрировать недостатки в доказывании, особенно в связи с неотносимостью и недопустимостью используемых в деле доказательств. Это приводит к тому, что преступники могут избежать уголовной ответственности как раз за наиболее сложные и опасные компьютерные преступления, что косвенным образом стимулирует дальнейший рост высокотехнологичной преступности. Отметим, что оба указанных фактора имеют тенденцию к росту.

Полагаем, что для разрешения указанных проблем, а также в профилактических целях положительную роль могли бы сыграть следующие правовые меры.

1. **Лицензирование деятельности** в области разработки и использования программного обеспечения, предназначенного для проверки защищенности программных и программно-аппаратных средств от несанкционированного воздействия. Это позволит государству и правоохранительным органам в большей степени контролировать разработку и использование соответствующего специализированного программного обеспечения. Мы согласны с тем, что «…назначение и способность уничтожить, блокировать, модифицировать, копировать информацию вполне могут быть в определенных сочетаниях и для определенных ситуаций функциями легальных программ…» [9, 10; 1, с. 141]. Так, распространенные коммерческие программы «Cobalt Strike», «Metasploit Framework Pro», «Metasploit Pro», предназначенные в том числе и для проведения тестов на уязвимость программного обеспечения, при их продаже проверяются на благонадежность покупателей только со стороны самих производителей. Однако данные программы обладают практически всеми нужными возможностями для осуществления неправомерного доступа к компьютерной информации. Именно в связи с этим они стали использоваться (иногда со незначительной модификацией) международными сетевыми преступными группами и сообществами. Например, их использовали такие преступные группы

как «Cobalt», «Winnti», «APT17», «Carbanak», «Silence», «TreasureHunter», о чем свидетельствует отчет компании «Positive Technologies», занимающейся вопросами информационной безопасности в России [11, с. 34].

Фактически любое лицо, планирующее осуществление деятельности в данной области, должно будет получить разрешение в виде лицензии, в противном случае это будет нарушением закона. Отсутствие лицензии станет веским аргументом в доказывании умысла (виновности) именно на совершение преступления.

Следует отметить, что лицензирование также будет способствовать облегчению работы следственных и оперативно-розыскных органов, так как при соответствующем запросе может быть получена криминалистически и оперативно значимая информация о разработчиках, а в дальнейшем — и заказчиках программного обеспечения, фигурирующего в уголовном деле или оперативном учете. В связи с этим, по нашему мнению, желательно, чтобы программная продукция подобного назначения получала более защищенную индивидуализацию в целях обеспечения ее учета. При такой индивидуализации следственным и оперативным органам будет легче получать результаты идентификационных исследований по выявлению тождества между оригинальным программным обеспечением и его модификацией, осуществленной преступниками. Это связано с тем, что в техническом плане программный код (зачастую являясь неизменным ядром программы) даже в случае его модификации может сохранить определенные криминалистически значимые данные, например, идентификационные признаки. Установление тождества вредоносного программного обеспечения с зарегистрированным программным обеспечением поможет в выдвижении и проверке криминалистических версий о том кем, от кого и как было получено законное программное обеспечение, зачем, когда и кто мог его использовать или модифицировать в преступных целях, а также ряде других важных вопросов.

Таким образом, лицензирование и индивидуализация специализированного программного обеспечения, предназначенного для проверки защищенности используемых компьютерных средств, может позволить правоохранительным органам получить важные ориентирующие и доказательственные данные, повысит эффективность выдвижения криминалистических версий, будет способствовать повышению качества расследования уголовных дел, предусмотренных ст. 273 УК РФ.

2. Второй правовой мерой **является дифференциация ответственности** по рассматриваемой статье. На наш взгляд, следует разделять преступную деятельность, направленную на создание, использование и распространение вредоносных компьютерных программ, за которую должна наступать уголовная ответственность, и близкие к ней, но менее значимые негативные действия, не являющиеся в такой же степени общественно опасными. В первом случае умысел направлен на совершение преступлений, а во втором — на незаконное осуществление действий, которые подлежат лицензированию. Во втором случае может быть предусмотрена менее суровая административная ответственность, для чего потребуется принятие новой статьи в КоАП РФ. Полагаем, что благодаря дифференцированному правовому регулированию сократится необоснованное уголовное преследование специалистов в области информационной безопасности, невиновных в совершении преступлений, предусмотренных ст. 273 УК РФ.

Таким образом, предложенные правовые меры могут повысить эффективность противодействия преступности, связанной с разработкой, использованием и применением в преступных целях вредоносного программного обеспечения, а также улучшить практику расследования таких дел. Полагаем также, что для большего эффекта не следует ограничиваться только

правовыми мерами, целесообразно использовать комплексный подход, включающий в себя также технические, методически и организационные составляющие.

Список литературы

1. Энгельгардт А.А. Компьютерная информация как предмет преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации // Право. Журнал Высшей школы экономики. 2014. № 4. 136-145.
2. Киздермишов А.А. К вопросу о применении CVE-совместимых сетевых сканеров // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2015. № 1 (154). С. 136-140.
3. Зинкевич А.В., Михайлов М.С. Аудит информационной безопасности // Ученые заметки ТОГУ. 2018. № 1. С. 307-312.
4. Копырюлин А.Н. Квалификация преступлений в сфере компьютерной информации // Законность. 2017. № 2. С. 18-19.
5. Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2 (32). С. 162-166.
6. The Convention on Cybercrime of the Council of Europe (CETS No.185). Budapest, 23/11/2001. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTM Content?documentId=0900001680081561. Загл. с экрана.
7. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. № 2. С. 37-44.
8. Поляков В.В. О высокотехнологичных способах совершения преступлений в сфере компьютерной информации // Уголовно-процессуальные и криминалистические чтения на Алтае: материалы ежегодной Всеросс. науч.-практ. конф., посвященной 50-летию юридического факультета и 40-летию Алтайского государственного университета. Барнаул: Изд-во Алт. ун-та, 2012. Вып. 11-12. С. 123-126.
9. Уголовное дело № 1-765/2015. Приговор Октябрьского районного суда г. Барнаула от 15 марта 2015 года.
10. Уголовное дело № 1-267/2016. Приговор Центрального районного суда г. Барнаула от 21 апреля 2016 года.
11. POSITIVE RESEARCH 2020: аналитическая статья. Электр. дан. 2020. URL: https://www.ptsecurity.com/ru-ru/research/analytics/positive-research-2020/. Загл. с экрана.

РАЗДЕЛ 2. КРИМИНАЛИСТИЧЕСКОЕ И ОПЕРАТИВНО-РОЗЫСКНОЕ ОБЕСПЕЧЕНИЕ УГОЛОВНОГО СУДОПРОИЗВОДСТВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Р.Г. Драпезо, *старший преподаватель кафедры уголовного процесса и криминалистики Кемеровского государственного университета, г. Кемерово*

ОПЕРАТИВНО-РАЗЫСКНАЯ ХАРАКТЕРИСТИКА «НАЕМНОГО ФАКЕЛА» В СЕТИ ИНТЕРНЕТ С НЕКОТОРЫМИ ЭЛЕМЕНТАМИ ТАКТИКИ

Ранее мы показали [1, 2], что оперативно-разыскная характеристика преступления (ОРХП) представлена совокупностью информационных признаков конкретной категории преступления, которые, с одной стороны, находятся в определенной (корреляционной) зависимости между собой, с другой — обладают поисковыми качествами. Такая информационно-поисковая совокупность в первую очередь должна быть направлена на обеспечение прогнозирования (типового и атипичного) поведения преступника, возможных путей его отхода с места преступления, наступления оперативных рисков (расконспирации и т.п.), а также должна способствовать выработке (типовых и атипичных) оперативно-разыскных ситуаций, версий и типовых комплексов по разрешению последних. Другими словами, исходя из определения сущности ОРХП, последняя должна содержать в себе элементы не только информационно-поисковой, но и поисково-тактической направленности. Ситуации, версии, типовые комплексы и тактика выступают основными элементами частных оперативно-разыскных методик выявления, раскрытия, предупреждения преступлений, о чем неоднократно упоминал в своих трудах С.И. Давыдов [3]. Все это делает ОРХП не фантомом от науки ОРД [4], а вполне сформированной самостоятельной научной категорией.

Часть ученых при этом являются сторонниками о включении в ОРХП специфических элементов, которые характерны только для ОРД [5-7 и др.], например, таких как: оперативная обстановка (время, место, способы совершения преступления, состояние преступности и т.п.), оперативно значимое поведение объектов и субъектов, представляющих оперативный интерес, доступность для оперативного внедрения, оперативные риски и т.п. Другая часть ученых говорит о включении в состав ОРХП наравне с аналогичными категориями уголовно-правовых, криминолого-криминалистических и специальных оперативно-разыскных элементов [8, 9 и др.]. Однако во втором случае речь идет не о бездумном включении вышеперечисленных элементов, а только тех, которые способствуют решению задач ОРД и прямо или косвенно обладающими поисково-разведывательными и информационно-тактическими качествами.

Не являясь сторонниками ни первого, ни второго подходов, тем не менее, скажем, что та категория преступлений, которую мы затрагиваем в настоящей статье, подпадает под конструкцию второго подхода. Итак, первый элемент в структуре ОРХП (согласно второму подходу) — это структура и динамика преступления (часть авторов [10, 11] под этим элементом подразумевает состояние оперативной обстановки, но суть от этого не меняется). Ряд исследователей склонны игнорировать данный элемент, так как последний не обладает ни поисковыми качествами и не способствует выработке оперативной тактики в целом. Как мы покажем, данная позиция ошибочна, как минимум, для оперативно-разыскной характеристики криминальной деятельности «наемного факела» в информационно-телекоммуникационном пространстве (далее — сети Интернет).

Мы формулируем **гипотезу**, которую постараемся обосновать: убийства, где огонь выступает как орудие (способ) сокрытия преступления (далее — убийства, сопряженные с огнем) или криминальные пожары (поджоги) без жертв, становятся профессиональными благодаря появлению относительно новой криминальной специализации, такой как «наемные факелы», опасность которых усугубляется уходом их деятельности в анонимную сеть Интернет.

Опасность заключается в следующем:

1) «наемные факелы» профессионально уничтожают следы преступления с помощью огня [12, 13], сами при этом следов своего присутствия практически не оставляют, за исключением следов, которые остаются от огня. Это существенно затрудняет решение задачи ОРД по выявлению, предупреждению, пресечению и раскрытию преступлений;

2) «наемные факелы» никак не связаны с потерпевшими и не формируют классическую в криминалистике связь «преступник — жертва». Все это затрудняет поиск источников оперативно значимой информации и в конечном итоге формированию доказательной базы. Из немногочисленных зарубежных источников [14] нам также известно, что «наемные факелы» сами не имеют отношения к убийству или другому тяжкому преступлению, но уничтожают их следы посредством огня за вознаграждение;

3) криминальная деятельность носит заказной характер. Причем если ранее услугами «наемных факелов» пользовалась только криминальная среда либо «наемные факелы» уже входили в состав преступной группы, то сейчас наймом занимаются обычные законопослушные граждане;

4) преимущественное использование сети Интернет как основного средства коммуникации с заказчиком убийства или сокрытия следов убийства (либо другого тяжкого преступления) с помощью огня и транзакций за свою криминальную деятельность.

Исследование эмпирической базы[2] показало существование как минимум двух видов отношений: а) классическая связь «заказчик-исполнитель («наемный факел»)», либо б) «заказчик, он же исполнитель — пособник («наемный факел»)». Последнее отношение формируется в ситуации, когда имеет место только консультация заказчика лицом («наемным факелом») посредством защищенных каналов сети Интернет. Вопросы консультирования касались моментов профессионального применения огня и источников возгорания, и в процентном отношении (процент указывается от обнаруженных нами ресурсов сети darknet как по Российской Федерации, так и по Сибирскому федеральному округу) распределись следующим образом:

а) консультирование по сокрытию следов преступления (чаще всего «наемных факелом» нанимают на сокрытие следов убийства, хотя этот вид консультирования не всегда связан с его сокрытием, как, например, в ситуации с осуществлением заказа поджога автомобиля конкурентов по бизнесу) посредством огня — 17%;

б) консультирование по вопросам маскировки преступления под несчастный случай (например, как создать «простые» технические или химические устройства, имитирующие замыкание в электропроводке или самовозгорание; каким образом поместить обгоревший труп потерпевшего в пространстве, чтобы это походило на инсценировку несчастного случая; какое горючее вещество лучше использовать и каким образом при этом создать оптимальный приток кислорода воздуха с тем, чтобы в крови или перикардиальной жидкости потерпевшего был обнаружен карбоксигемоглобин (от 40% и выше), или наоборот, чтобы при определенных ситуациях он не был обнаружен и т.п. [15]), самоубийство — 10%;

[2] Были изучены материалы 353 уголовных дел, возбужденных по факту убийств, сопряженных с огнем и по которым имеются судебные решения за период с 1989 по 2019 года; порядка 80 актов судебно-медицинского исследования обгоревших трупов Бюро су-дебно-медицинской экспертизы города Кемерово за период с 2005 по 2018 год; данные статистики с официальных сайтов МВД России, МЧС России и международных официальных баз данных правовой статистики убийства (например, «UNODC» (http://www.unodc.org/gsh/)); материалы судебной практики с официального интернет-портала «Судебные и нормативные акты РФ» (http://sudact.ru); форумы и аккаунты соответ-ствующих onion-ресурсов сети darknet (например, «Medusa»), где можно оставить заказ «наемному факелу».

в) консультирование относительной возможности полного сжигания тела (например, создание условия непрерывного и достаточного притока кислорода воздуха с использованием горючих материалов, обладающих длительным термическим эффектом и высокой энергоемкостью. Как показала эмпирическая база исследования, шины большегрузных автомобилей одновременно обеспечивают оптимальный приток воздуха и обладают высокой температурой горения. Сделанные нами расчеты в соответствии с рекомендациями ученых в области судебной медицины прошлого столетия [16-18] позволяют говорить о высокой вероятности сжигания тела массой 70 кг до состояния озоления в среднем от 4 до 6 ч) — 61%;

г) консультирование по вопросам сокрытия следов биологического и иного происхождения, указывающие на присутствие лица, совершившего преступление, — 12%.

Кроме того, опасность криминальной деятельности «наемных факелов» заключается еще и в использовании последними так называемых зашифрованных каналов связи (например, мессенджеры Telegram, Viber, Vipol), иных средств анонимизации в сети Интернет (сеть darknet, его структурное ответвление deep web, VPN-подключения, использование удаленных серверов и т.п.).

Анализ судебно-следственной практики по уголовным делам о криминальном применении «наемными факелами» огня в качестве орудия либо средства сокрытия следов преступления показал нам следующую структуру: 1) ч. 1 или ч. 2 ст. 105 УК РФ в совокупности с ч. 2 ст. 167 УК РФ либо только ч. 2 ст. 167 УК РФ либо только ч. 1 или ч. 2 ст. 105 УК РФ (когда обгоревший труп обнаруживают на открытой территории либо в помещении, которое от огня пострадало не сильно). Нами было установлено, примерно в 20% случаев, убийству предшествовали угрозы физической расправы над потерпевшим (например, угрозы сожжения заживо), поэтому для целей оперативной работы важно в структуру включить такой состав преступления, как ст. 119 УК РФ. При этом в 12% случаев потерпевшие расценивали такую угрозу как реальную, исходя из двух оснований: а) потерпевшие после высказывания виновным угрозы испытывали тревогу, дискомфорт; б) личность виновного (имеется судимость за убийство, либо за иные составы преступлений, агрессивность в поведении); 2) ч. 1 ст. 111 либо ч. 4 ст. 111 УК РФ чаще всего в совокупности с ч. 2 ст. 167 УК РФ; 3) ч. 2 ст. 110.1 УК РФ («Склонение к совершению самоубийства или содействие совершению самоубийства»); 4) ч. 2 ст. 178 УК РФ («Ограничение конкуренции, сопряженные с уничтожением или повреждением чужого имущества либо с угрозой его уничтожения или повреждения»); 5) ч. 1 ст. 195 УК РФ («Неправомерные действия при банкротстве»); 6) ст. 243 УК РФ («Уничтожение или повреждение объектов культурного наследия …»); 7) ст. 261 УК РФ («Уничтожение или повреждение лесных насаждений»).

Как можно видеть, это так называемые сопутствующие преступления, то есть то, что желают достичь заказчики посредством огня. Однако первое место занимает другая криминальная цель — сокрытие следов тяжкого преступления (чаще всего убийства), убийства и/или причинения тяжкого вреда здоровью, причинения значительного ущерба имуществу, сокрытие следов хищения, растраты и присвоения, уничтожение следов преднамеренного банкротства. Жертвами становятся конкуренты по общему делу, должники, те граждане, кому завидуют, граждане, кому жаждут отомстить за причиненные обиды. В последнее время в качестве жертв стали встречаться социально незащищенные слои населения, например, одинокие пенсионеры, лица с ограниченными возможностями здоровья, лица с психическими отклонениями здоровья, у которых нет родственников, а также лица без определенного рода занятий (асоциальные граждане), как правило, употребляющие спиртные напитки, наркотики и у которых также нет ближайших родственников, но имеется собственность в распоряжении. Речь идет о так называемых «черных риелторах», которые все чаще прибегают к услугам «наемных факелов».

Так, в г. Белово Кемеровской области в 2015 г. гр. А. мошенническим путем пытался завладеть квартирой [19]. Собственнику квартиры периодически привозил алкоголь. Впоследствии обманным путем оформил право собственности на себя. Заказав «наемного факела» для

сокрытия следов убийства, вывез потерпевшего в садовый участок, причинив последнему смерть путем огнестрельного ранения. «Наемным факелом» были организованы условия для практически полного уничтожения тела потерпевшего огнем. Мягкие ткани, а также кости на 50-60% подверглись обугливанию. Поэтому поступление в оперативные подразделения информации о вероятно совершаемых незаконных сделках купли-продажи квартир, о подозрительном поведении собственника квартиры и подозрительных новых знакомых должно послужить сигналом для проведения оперативно-разыскных мер профилактической направленности.

Также в качестве жертв выступают сожительницы, чаще всего вместе с детьми, и близкие родственники, которые имеют неразрешенные вопросы совместной собственности.

Если рассмотреть динамику преступлений по Российской Федерации, статистика по которым была нами взята с официальных отечественных и международных источников[3], то получим следующую структуру, которая отражена ниже в таблицах 1 и 2. Видно, что по поджогам, в отличие от большинства преступлений, обнаруживается существенная разница между количеством зарегистрированных и раскрытых поджогов. Далее, если мы обратимся к статистике вынесенных обвинительных приговоров судами общей юрисдикции по первой инстанции, то обнаружим нисходящую линию тренда по данному статистическому показателю примерно в 1,5-2 раза (то есть дальнейшее снижение показателя). По убийствам, в отличие от поджогов, разница между зарегистрированными и раскрытыми преступлениями незначительна, примерно 10-15%. Однако если мы обратимся к показателям медико-демографической и международной баз правовых данных, то можем прийти к выводу о существовании диссонанса по основным показателям криминогенной обстановки. Как нам видится, причин этому множество: методологическая, терминологическая, манипуляция статистическими данными на уровне национальных учетов, укрывательство преступлений от учетов.

Таблица 1

Показатели правовой статистики по поджогам и убийствам за период 2015-2019 гг. в Российской Федерации

Годы	Поджоги (ч. 2 ст. 167 УК РФ)			Убийства (включая покушение на убийство)		
	зарегистрировано сообщений	раскрыто	Вынесено обвинительных приговоров по 1-й инстанции	зарегистрировано сообщений	раскрыто	Вынесено обвинительных приговоров по 1-й инстанции
2015	13560	2400	1846	11496	9763	8928
2016	11988	2330	1475	10444	9441	9147
2017	11597	2031	1255	9738	8612	8219
2018	10854	2060	997	8574	7632	7399
2019	10202	1912	1165	7948	6773	5828

[3] Были изучены материалы 353 уголовных дел, возбужденных по факту убийств, сопряженных с огнем и по которым имеются судебные решения за период с 1989 по 2019 года; порядка 80 актов судебно-медицинского исследования обгоревших трупов Бюро су-дебно-медицинской экспертизы города Кемерово за период с 2005 по 2018 год; данные статистики с официальных сайтов МВД России, МЧС России и международных официальных баз данных правовой статистики убийства (например, «UNODC» (http://www.unodc.org/gsh/)); материалы судебной практики с официального интернет-портала «Судебные и нормативные акты РФ» (http://sudact.ru); форумы и аккаунты соответ-ствующих onion-ресурсов сети darknet (например, «Medusa»), где можно оставить заказ «наемному факелу».

Таблица 2

Сопоставление других видов официальной статистики убийств
за период 2014-2018 гг. в Российской Федерации*

Виды официальной статистики убийств	Годы				
	2014	2015	2016	2017	2018
1. Медико-демографическая (статистика убийств)	45200	41700	37800	34300	31800
2. Международная статистика (статистика убийств)#	~ 23 тыс. / 17425	~ 40 тыс. / 16273	~ 54 тыс. / 14380	~ 47 тыс. / 13439	~ 45 тыс. / 12600

*За 2019 г. по указанным статистическим базам данные пока отсутствуют.
#Зарегистрированных сообщений по убийствам / количество зарегистрированных убийств.

В 97-98% случаев от возникших пожаров отказывают в возбуждении уголовных дел, из них в более чем 82% случаев причины пожаров не установлены [21]. И дело здесь не только в латентности преступлений (имеется в виду убийств, сопряженных с огнем) и отсутствием соответствующего показателя в статистической отчетности, как справедливо отмечает Э.В. Лантух [20], но в их укрывательстве, включая убийства, замаскированные под неосторожное обращение с огнем, что убедительно описано в монографии А.Л. Протопопова [21]. По данным международной статистики количество зарегистрированных убийств оказываются в 2-4 раза меньше по сравнению с количеством зарегистрированных сообщений по убийствам. Более существенные расхождения мы встречаем в немногочисленных работах зарубежных авторов [22].

В таблице 3, таким образом, суммируем, что такой элемент ОРХП, как структура и динамика криминальной деятельности «наемных факелов», обладают поисковыми и тактическими качествами. Можно видеть, что знание оперативными работниками сопутствующих убийствам, сопряженных с огнем преступлений уже в своей основе содержит первоначальные поисковые и тактические качества.

Таблица 3

Фрагмент элемента структуры и динамики преступлений и их связь
с поисковыми и тактическими качествами

Структура и динамика	Описание поисковых и тактических качеств
1. Статья 119 УК РФ («Угроза убийством или причинением тяжкого вреда здоровью»)	Знание этого элемента имеет существенное тактическое значение. От угрозы до реализации умысла может пройти от нескольких часов до нескольких дней, либо этот период растягивается на месяцы и даже годы. Поэтому оперативным работникам важно знать, что первым (сигнальным) поисковым признаком может оказаться угроза. Если угроза высказана недавно, то оптимально будет предупредить вероятное преступление путем профилактических бесед. В данном случае можно предложить склонить лицо оперативной заинтересованности к отказу от совершения подобных действий. Если угрозы, длящиеся во времени, тогда можно спланировать оперативную разработку, направленную на пресечение преступного замысла
2. Статья 159 УК РФ	Особенно мошенничество в сфере купли-продажи квартир также имеет как поисковое, так и тактическое значение. В данном случае

	оперативным подразделениям необходимо проводить постоянный мониторинг оперативной обстановки, работу с агентурным аппаратом (например, сотрудники риелторских агентств)
3. Часть 1 статьи 105 УК РФ	В основном убийства, сопряженные с огнем, совершаются с особой жестокостью, общеопасным способом, то есть квалифицируются по соответствующему пункту ч. 2 ст. 105 УК РФ. Но бывает, что потерпевший не испытывал особых мучений и страданий (в ситуации, если в атмосферу огня попал уже труп потерпевшего) и для сжигания не был использован общеопасный способ. Тогда квалификация идет по ч. 1 ст. 105 УК РФ. Просматривается закономерность в том, что если результаты судебно-медицинского исследования покажут отсутствие в крови или перикардиальной жидкости жертвы карбоксигемоглобина, то есть вероятнее всего в атмосферу огня попал уже труп потерпевшего и если при этом будут обнаружены специфические горючие материалы, то оперативные работники могут выдвинуть версию о возможном участии «наемного факела». Скорее всего, нанятого через сеть Интернет

Таким образом, в целом мы подтверждаем нашу гипотезу, выдвинутую в начале статьи. Действительно, большая часть «наемных факелов» успешно осваивает скрытый сектор сети Интернет, а также и то, что в своей криминальной теме последние становятся более профессиональными, что требует от научного сообщества дальнейшего исследования и взаимодействия с сотрудниками правоохранительных органов.

Список литературы

1. Драпезо Р.Г. Модель оперативно-разыскной характеристики убийств, где огонь применяется как орудие (способ) сокрытия преступления // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: материалы семнадцатой междунар. науч.-практ. конф. / под ред. С.К. Бурякова. Барнаул: БЮИ МВД России, 2019. Ч. 1. С. 5-6.
2. Драпезо Р.Г. Нюансы построения оперативно-розыскной характеристики убийств, где огонь применяется как средство сокрытия преступления // Правовые проблемы укрепления российской государственности: сборник статей / под ред. О.И. Андреевой, С.А. Елисеева, А.С. Князькова и др. Томск, 2019. С. 149-150.
3. Давыдов С.И. Некоторые проблемные вопросы развития теории оперативно-розыскной методики раскрытия преступлений // Российский следователь. 2008. № 8. С. 25-28.
4. Исиченко А.П. Оперативно-разыскная характеристика преступлений: фантом или реальность? // Российский следователь. 2015. № 13. С. 41-45.
5. Шойжилцыренов Б.Б., Ступницкий А.Е. Проблемные вопросы структурных элементов оперативно-розыскной характеристики преступлений // Российский следователь. 2009. № 14. С. 22-25.
6. Водько Н.П. Правовые и организационные основы оперативно-разыскной деятельности органов внутренних дел по борьбе с организованной преступностью: автореф. дисс. ... д-ра юрид. наук. М., 2002.
7. Осипенко А.Л. Оперативно-разыскная деятельность органов внутренних дел по борьбе с преступностью в глобальных компьютерных сетях: автореф. дис. ... д-ра юрид. наук. Омск, 2010.
8. Ларичев В.Д. Оперативно-розыскная характеристика экономических преступлений: понятие и содержание // Оперативник (сыщик). 2009. № 1 (18). С. 11-16.
9. Гребельский Д.В. О соотношении криминалистических и оперативно-розыскных характеристик // Криминалистическая характеристика преступлений: труды Академии МВД СССР. М., 1984. С. 70-73.

10. Гаджиев В.Э., Мкртычян Б.А. Уголовная ответственность за кражи скота и оперативно-розыскное обеспечение борьбы с ними. Новосибирск: Изд-во юрид. фак. НГАУ, 2011. 225 с.

11. Федоров А.Н. К вопросу о понятии и содержании оперативно-розыскной характеристики мошенничества, совершенного с использованием средств мобильной связи // Уголовно-исполнительная система: право, экономика, управление. 2016. № 6. С. 16-19.

12. Ахмедшин Р.Л. Криминалистическая характеристика личности преступника: дис. ... д-ра юрид. наук. Томск, 2006. 413 с.

13. Драпезо Р.Г., Гольдшмидт Е.С. Социально-криминалистический профиль индивидуальности убийц, применяющих огонь как орудие (способ) сокрытия преступления // Психология и право. 2020. Т. 10, № 1. С. 55-72.

14. Criminal Profiling: An Introduction to Behavioral Evidence Analysis // Brent E. Turvey. Hardcover, 462 pages. Published by Academic Press, June, 1999.

15. Drapezo R., Shevchuk D. Mortality rates caused by gunshot injuries and fires associated with killings as the markers of socially negative development in a megapolis // Всборнике: Advances in social science, education and humanities research Proceedings of the International Conference on Sustainable Development of Cross-Border Regions: Economic, Social and Security Challenges (ICSDCBR 2019). Altai State University. 2019. С. 565-569.

16. Таге-Иенсен С. К главе о сожжении трупов // Архив криминологии и судебной медицины. Т. 1. Кн. 2-3. Харьков, 1927. С. 777-780.

17. Кубицкий Ю.М. О криминальном сожжении трупов // Труды государственного научно-исследовательского института судебной медицины. М.: МЕДГИЗ, 1949. С. 195-197.

18. Шупик Ю.П. К вопросу о криминальном сожжении трупов // Судебная медицина и реаниматология: материалы расширенной конференции судебных медиков Татарии (научные труды). Казань, 1969. Т. 26. С. 84-86.

19. Номер уголовного дела 12082810. Архив уголовных дел Кемеровского областного суда за период с 1989 по 2019 года.

20. Лантух Э.В. Методика расследования убийств, сопряженных с поджогом: дисс. ... канд. юрид. наук. СПб., 1998. 154 с.

21. Протопопов А.Л. Расследование серийных убийств. СПб.: Изд. дом СПбГУ, 2006. С. 246.

22. Lysova, Alexandra. (2018). Challenges to the veracity and the international comparability of Russian homicide statistics. European Journal of Criminology. 2018. Pp. 1-21.

Д.В. Емельяненко, *аспирант кафедры уголовного процесса и криминалистики Алтайского государственного университета, директор АНО «Сибирский центр судебной экспертизы и криминалистики», г. Барнаул*

ПРОБЛЕМЫ СОБЛЮДЕНИЯ ТАЙНЫ КОММУНИКАЦИИ ПРИ НАЗНАЧЕНИИ СУДЕБНОЙ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

Из результатов исследования Всероссийского центра изучения общественного мнения (ВЦИОМ), проведенного в 2018 г., следует, что 45% опрошенных россиян старше 18 лет пользуются хотя бы одной из социальных сетей почти каждый день, 62% — хотя бы раз в неделю [1].

Всероссийский опрос «Левада-центра», проведенный в 2020 г., показал, что продолжается рост числа пользователей социальных сетей. Также растет число тех, кто пользуется

социальными сетями каждый день (51%, +5 п.п.). Число россиян, которые не пользуются интернет-мессенджерами, сократилось по сравнению с прошлым годом на 8 п.п. (29%) [2].

В характеристике состояния преступности в стране за январь-июнь 2020 г. Генеральная прокуратура Российской Федерации отмечает, что массив преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, за последние 5 лет увеличился более чем в шесть раз — с 43,8 тыс. преступлений в 2015 г. до 294,4 тыс. в 2019 г. По итогам первого полугодия 2020 г. их количество возросло почти на 92% (до 225,5 тыс.). Если годом ранее такими деяниями было каждое девятое регистрируемое преступление, то сегодня это уже каждый пятый факт (22,3%) [3].

Приведенные статистические данные показывают значительную вовлеченность граждан в цифровой формат общения, обусловленную, прежде всего, неминуемой цифровизацией общества, которая приобретает все больший масштаб. Неизбежным следствием этого является рост числа преступлений с использованием информационно-телекоммуникационных технологий. Одновременно с этим усиливается и актуальность соблюдения конституционных прав участников уголовного судопроизводства.

Статьей 23 Конституции РФ гарантировано право на неприкосновенность частной жизни, личную и семейную тайну (п. 1). А также на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения (п. 2).

Таким образом, в Конституции РФ приведен перечень видов тайн, находящихся под охраной Основного закона. Следует обратить внимание, что, во-первых, данный перечень является открытым, а, во-вторых, в нем не упоминается тайна связи. Наличие неисчерпывающего перечня видов тайн позволяет относить к данной правовой конструкции новые способы передачи сообщений, появляющиеся в результате технического прогресса.

Законодатель предусмотрел ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений положениями ст. 138 УК РФ.

Названием ст. 63 ФЗ «О связи» законодатель ввел понятие «тайна связи», однако не дал ему четкого определения ни в этом федеральном законе, ни в каком-либо ином нормативно-правовом акте. Данное обстоятельство привело к путанице в понятийном аппарате, относящемся к сфере охраняемых законов сведений, и породило многочисленные споры правоведов, которые продолжаются до сих пор.

Некоторую ясность в 2018 г. внес Пленум Верховного Суда РФ [4], который разъяснил, что под иными сообщениями следует понимать сообщения граждан, передаваемые по сетям электрической связи, например СМС- и ММС-сообщения, факсимильные сообщения, *передаваемые посредством сети Интернет мгновенные сообщения*, электронные письма, видеозвонки, а также сообщения, пересылаемые иным способом.

В целом можно отметить, что группа прав, перечисленных во п. 2 ст. 23 Конституции РФ, нуждается в обобщении, и наиболее удачный вариант встречается у М.А. Мещеряковой [5], М.З. Шварц [6], которые объединяют описываемые конституционные права термином «тайна коммуникации».

По мнению автора настоящей статьи, тайну связи составляют сведения, полученные оператором связи при осуществлении своей деятельности. Таким образом, тайна связи относится к группе профессиональных видов тайн, наряду с банковской, адвокатской, врачебной и другими.

В случае когда указанные сведения покидают канал оператора связи, прекращает действовать и тайна связи. При этом такие сведения продолжают составлять тайну коммуникации. Стоит обратить внимание, что конституционным правом является право на тайну коммуникации, а не на тайну связи.

В этой связи нельзя согласиться с А.Л. Карловым [7], который полагает, что информация, сохранившаяся на электронном носителе любого устройства пользователя, уже не может

относиться к тайне связи, а является личной тайной, правовой режим доступа к которой существенно отличается.

Сведения, составляющие личную и семейную тайну и содержащиеся, например, в переписке, могут относиться и к авторской тайне. Однако авторская тайна может включать неограниченно широкий вид сведений, которые при этом могут составлять как другие виды профессиональных тайн, так и не относиться к ним.

Таким образом, конфиденциальную информацию относят к личной или семейной тайне по принципу характера ее содержания, а к тайне коммуникации — по принципу способа передачи такой информации. Иными словами, любые сведения, которые гражданин передает посредством переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, относятся к тайне коммуникации.

В данном контексте интересным представляется постановление Президиума Владимирского областного суда [8], диспозиция ч. 1 ст. 138 УК РФ не ограничивает уголовную ответственность за нарушение тайны переписки лишь наличием в ней сведений, составляющих личную либо семейную тайну, а уголовная ответственность по данной статье наступает за нарушение права лица на тайну (конфиденциальность) переписки, имеющей личный характер, независимо от того, составляют ли передаваемые сведения его личную или семейную тайну или нет.

Согласно статистике по АНО «Сибирский центр судебной экспертизы и криминалистики», наиболее часто встречаемым объектом исследования при проведении судебных компьютерно-технических экспертиз (далее — СКТЭ) выступает информация, размещенная на жестком диске или твердотельном накопителе (в составе компьютера или отдельно), а также в смартфоне.

Один из наиболее частых вопросов, который ставится на разрешение эксперта, — «Имеются ли сведения о переписке, осуществляемой с использованием интернет-мессенджеров?» с указанием на необходимость приведения такой переписки в случае ее обнаружения.

Очевидно, что проведение такой экспертизы сопряжено с получением судебным экспертом доступа к охраняемой законом информации. При этом эксперт является безусловным исполнителем постановления о назначении судебной экспертизы в силу положений ст. 16 ФЗ «О государственной судебно-экспертной деятельности в РФ»: эксперт обязан принять к производству порученную ему руководителем соответствующего государственного судебно-экспертного учреждения судебную экспертизу, а также провести полное исследование представленных ему объектов и материалов дела, дать обоснованное и объективное заключение по поставленным перед ним вопросам.

Исключение составляют случаи, когда поставленные вопросы выходят за пределы специальных знаний эксперта, объекты исследований и материалы дела непригодны или недостаточны для проведения исследований и дачи заключения и эксперту отказано в их дополнении, современный уровень развития науки не позволяет ответить на поставленные вопросы. Из чего следует, что проверка законности ограничения конституционных прав участников судопроизводства находится за пределами ведения судебного эксперта.

В контексте приведенных правовых норм выглядит логичным, что эксперт не может являться субъектом совершения преступления, ответственность за которое предусмотрена ст. 138 УК РФ в случае, если получение сведений о переписке, телефонных переговорах, почтовых, телеграфных или иных сообщениях необходимо ему для разрешения поставленных вопросов.

По мнению А.Н. Яковлева [9], как только данные, отправляемые пользователями сети Интернет, оказываются вне границ технической ответственности операторов связи — на серверах правообладателей коммуникационных сервисов, на компьютерных средствах пользователей, они могут быть получены лицом, проводящим расследование, в порядке ст. 86 УПК РФ

в ходе следственных действий, а также истребованием от правообладателя коммуникационного сервиса. Решения суда при этом не требуется.

Такая позиция не согласуется с правоприменительной практикой и может привести к плачевным последствиям, если ей руководствоваться при проведении предварительного расследования.

Конституционный Суд РФ [10] в 2018 г. указал, что по смыслу ч. 5 ст. 177 УПК РФ на производство осмотра жилища требуется разрешение суда, если хотя бы одно из проживающих в нем лиц возражает против осмотра (п. 8 Постановления Пленума ВС РФ от 01.06.2017 № 19).

Проведение осмотра с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий *в установленном законом порядке*, не предполагает вынесения об этом специального судебного решения. Лица же, полагающие, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения способны причинить ущерб их конституционным правам, в том числе праву на тайну переписки, почтовых, телеграфных и иных сообщений, могут оспорить данные процессуальные решения и следственные действия в суд в порядке, предусмотренном ст. 125 УПК РФ (определение Конституционного Суда РФ от 25.01.2018 № 189-О).

Следует учитывать, что представляющие интерес для следствия предметы могут быть изъяты и без санкции суда, но при этом и без нарушения установленного законом порядка. К таким ситуациям можно отнести изъятие предметов не в жилище, а в нежилом помещении. Зачастую обыск проводится не только по месту проживания или пребывания лица, которое может быть причастно к совершению преступления, но и по месту его работы. Уголовно-процессуальные нормы для приведенного случая не предусматривают обязательное получение судебного согласия на производство обыска.

Кроме того, не стоит забывать о добровольной выдаче предметов, имеющих значение для расследуемого уголовного дела, которая оформляется выемкой в порядке ст. 183 УПК РФ. При таком варианте развития событий участник следственного действия выражает согласие на изъятие у него определенных предметов, документов — производит их добровольную выдачу. Вместе с тем следует учитывать, что в ходе выемки лицо выдает лишь физический предмет — вещь (например, смартфон как носитель информации, содержащий переписку — сведения, составляющие тайну коммуникации), что не может приравниваться к предоставлению права на ознакомление с охраняемой законом информацией, содержащейся в таком предмете. Боле того, уголовный процессуальный закон не предусматривает документального закрепления подобного волеизъявления в ходе производства выемки.

Однако если в приведенных в предыдущих абзацах ситуациях следователь самостоятельно проведет осмотр изъятых предметов или вынесет постановление о назначении СКТЭ и передаст объекты исследования эксперту — произойдет ознакомление с конфиденциальной информацией, составляющую тайну коммуникации. Тем самым будет незаконно ограничено, нарушено неотчуждаемое конституционное право лица, участвующего в уголовном судопроизводстве.

Хотелось бы отметить, что какой бы ценной ни была добытая экспертом при проведении СКТЭ информация, какой бы интерес она ни представляла для следствия, какое бы полное ни было проведенное исследование — из-за несоблюдения процессуальных норм такое заключение эксперта будет считаться полученным с нарушением закона. Согласно ст. 75 УПК РФ, подобное заключение эксперта как доказательство не будет иметь юридической силы и не может быть положено в основу обвинения, а также использоваться для доказывания любого из обстоятельств, предусмотренных ст. 73 Кодекса.

Резюмируя все вышесказанное, подчеркнем обязательную необходимость предварительного судебного контроля ограничения конституционного права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Список литературы

1. Результаты опроса ВЦИОМ. URL: wciom.ru/index.php?id=236&uid=116691 (дата обращения: 01.09.2020).
2. Результаты опроса «Левада-центр». URL: levada.ru/2020/04/28/rossijskij-medialandshaft-2020/ (дата обращения: 01.09.2020).
3. Состояние преступности в России за январь-июнь 2020 г. URL: genproc.gov.ru/upload/iblock/4fb/sbornik_6_2020.pdf (дата обращения: 01.09.2020).
4. О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации): постановление Пленума Верховного суда Российской Федерации от 25.12.2018 №46. URL: scfec.org/lib/sudact/pvs_25-12-18 (дата обращения: 01.09.2020).
5. Мещерякова М.А. Конституционное право на тайну коммуникации: понятие и содержание // Юридическая наука и правоохранительная практика. 2020. № 3 (53). С. 127-137. URL: scfec.org/lib/art/Meshcheryakova_20 (дата обращения: 01.09.2020).
6. Шварц М.З. К вопросу о тайне личной коммуникации в контексте правил доказывания в гражданском судопроизводстве // Закон. 2018. № 4. С. 56-63.
7. Карлов А.Л. Использование в доказывании по уголовным делам сведений, составляющих тайну связи, расположенных в сети интернет // Вестник СибЮИ ФСКН. России. 2015. № 2 (19). С. 142-146. URL: scfec.org/lib/art/Karlov_15 (дата обращения: 01.09.2020).
8. Постановление Президиума Владимирского областного суда от 19.11.2018 г. № 44у-40/2018. URL: scfec.org/lib/sudact/pvos_19-11-18 (дата обращения: 01.09.2020).
9. Яковлев А.Н. Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: «Электронная почта» // Вестник ВИ МВД России. 2014. № 4. С. 42-48. URL: scfec.org/lib/art/Yakovlev_14 (дата обращения: 01.09.2020).
10. Об отказе в принятии к рассмотрению жалобы гражданина Сидак Константина Петровича на нарушение его конституционных прав частью шестой статьи 164 и статьей 177 Уголовно-процессуального кодекса Российской Федерации: определение Конституционного Суда Российской Федерации от 17.07.2018 №1955-О. URL: scfec.org/lib/sudact/oks_17-07-18 (дата обращения: 01.09.2020).

К.А. Ерина, *преподаватель кафедры уголовно-процессуального права и криминалистики юридического факультета ВЮИ ФСИН России, г. Владимир*

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЦЕЛЯХ ПОЛУЧЕНИЯ ПОКАЗАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Вопросы повышения результативности и эффективности деятельности в процессе сбора, проверки и оценки доказательств зависит от ряда объективных и субъективных факторов. В их числе следует указать информатизацию и цифровизацию досудебного производства по уголовному делу, а также применение высокотехнологичной криминалистической техники, автоматизированных баз данных и иных информационных технологий. Неслучайно Председатель Следственного комитета Российской Федерации А.И. Бастрыкин справедливо отмечал, что «внедрение в следственную практику новейших цифровых технологий является одним из основополагающих направлений развития ведомства» [4]. В этой связи более эффективное внедрение в работу субъектов, осуществляющих предварительное расследование по уголовному делу, современных технологий, в частности современных информационных средств, исполь-

зуемых при доказывании, предоставит возможность вывести процесс установления обстоятельств, характеризующих противоправные деяния на качественно новый уровень.

При этом в условиях современных способов обеспечения коммуникативной связи, используемых при совершении преступления (мобильных устройств, мессенджеров, закрытых каналов связи и иных электронных ресурсов), т.е. в цифровом будущем, следователь находится в условиях «растерянности». Так, для правоприменителя, которым и выступает субъект предварительного расследования, с безусловными плюсами применения новых информационных технологий проявляются и новые сложности, например, отсутствие в уголовно-процессуальном законе прямых предписаний по обеспечению возможности использования информационно-телекоммуникационных технологий при производстве отдельных следственных действий, порядка протоколирования указанного алгоритма и т.д.

Поэтому, по нашему мнению, внедрение информационных технологий в «быт» следователя необходимо производить постепенно, путем их использования в привычных его действиях. Таким действием может выступать допрос.

Производство допроса участников уголовно-процессуальных отношений является одним из ключевых следственных действий, на основе которого:

– выдвигаются криминалистические версии;

– осуществляется планирование и проведение дальнейших следственных действий, оперативно-поисковых (розыскных) мероприятий, оперативно-тактические комбинации;

– определяется выбор тактики всего расследования в целом.

Отметим, что рассматриваемое следственное действие обладает не только сугубо процессуальным аспектом и составляет информативно-значимое процессуальное общение, но и психолого-криминалистическим.

Следует подробнее рассмотреть его с точки зрения судебной психологии, прежде чем анализировать возможность его информатизации и технологизации. Так, допрос возможно рассматривать как процесс специфического общения допрашивающего с допрашиваемым, который подразумевает психологическое явление, связанное с проявляющимися в процессе допроса закономерностями человеческой психики [7, с. 10].

Особенность получения информации в ходе допроса при расследовании трудновыявляемых преступлений, к примеру, киберпреступлений, коррупционных, экономических, должностных преступлений состоит в том, что ее источником является человек с заранее скрытой и скрытной, отклоняющейся моделью поведения. В связи с этим допрос следует отождествлять и с социальным явлением, имеющим этическую и профилактическую (воспитательную) стороны.

Поэтому среди условий, определяющих специфику рабочего этапа производства допроса, особую роль играет психологическая составляющая в связи с тем, что психология, психическое состояние допрашиваемого лица предопределяет его позицию по делу, а потому и характер показаний, и в целом их достоверность.

Для субъектов допроса характерны следующие психологические особенности дачи показаний [5, с. 218]:

1. Защитная реакция допрашиваемого, действующая с момента осознания своего положения. Иначе ее называют оборонительной доминантой. Через призму оборонительной доминанты преломляются восприятие и оценка обстановки допрашиваемым, регуляция его поведения.

2. Повышенная потребность в информации об осведомленности следователя. В зависимости от того, каков объем доказательственной базы, допрашиваемый выбирает линию поведения. На этой особенности строится применение психологических реагентов.

3. Отношение к допрашивающему как к источнику опасности, от действий и осведомленности которого зависит возможность вынесения судом обвинительного приговора, а во многом и характер уголовного наказания.

4. Прямая заинтересованность в исходе дела.

5. Активная позиция в расследовании, содействие следователю в выявлении фактов преступления, возможных соучастников совершения преступления.

6. Повышенная возбудимость, взволнованность, нервозность.

Названные особенности психологии допрашиваемого, сама специфика его правового статуса определяют производство допроса как тактическую борьбу двух сторон с противоположными интересами. Стремление следователя раскрыть преступление сталкивается с намерением допрашиваемых лиц оказать противодействие: скрыть информацию, следы, повести следствие по ложной версии [6, с. 72]. Ведь выражение цели допроса невозможно без использования языковой единицы — слова. Слово как единица языка закрепляет понятие — единицу знания. А взаимосвязь слов и понятий не означает их тождества [3, с. 229]. Лишь добавим, что в условиях современной борьбы с преступностью задачи следователя по получению показаний в ходе допроса должны быть более амбициозными.

Обозначенные условия свидетельствуют о том, что следователь зачастую сталкивается с «информационным вакуумом» при производстве допроса, формами противодействия со стороны допрашиваемых, невозможностью объективной оценки и предоставления информации о произошедшем преступном событии.

В связи с этим представляется закономерным рассмотрение вопросов использования современных научно-технических средств получения информации при производстве допроса, а именно устройств психофизиологический исследований, основанных на действиях искусственного интеллекта.

К примеру, существует революционная платформа «151EYE», которая даже по телефонному устройству, аудиозаписи, голосу имеет возможность отследить 151 психофизиологический параметр и с вероятностью до 90% определить подлинность показаний [1]. Исследование по времени занимает от 15 минут до получаса.

Исследователи и разработчики платформы отмечают, что голос — это продукт деятельности мышц человека, которые управляются от полушарий головного мозга до спинного мозга, поэтому при улавливании малейших его изменений возможного говорить о результате исследования. При этом национальность, этнос, уровень владения русским языком не имеет значения. В настоящее время программа используется в основном в целях обеспечения кадровой работы, но, по нашему мнению, имеется возможность его приспособления в целях выявления и установления обстоятельств преступного события.

Также следует отметить об использовании так называемого видеополиграфа, в возможности которого входит распознавание микроэмоции на лице, которые длятся всего 5-7 миллисекунд, а также пульса человека по видеоизображению [8]. Совершенно справедливо перспективы применения указанного исследования, отмечал А.И. Баянов, через призму обеспечения криминалистической детализации как универсального средства раскрытия и расследования преступлений, при котором «обнаружение микровыражений позволяет решить важную задачу допроса — диагностировать ложные показания, если остальные средства не позволяют этого сделать» [2, с. 15]. Так, результатом указанного исследования будет являться подлинность или ложность показаний, представленных на допросе с использованием видеозаписывающих устройств. При этом представляется закономерным отметить, что, в первую очередь, в обеспечение применения вышеуказанных технологий и исследований станет возможным при производстве допроса с применением аудио-, видеозаписи, к которой следователь прибегает не так часто.

Также имеются процессуальные препятствия использования указанных исследований. Они напрямую не могут быть использованы в качестве доказательств, а носят лишь ориентирующее значение, что в этой связи требует не только изыскания новых способов получения правдивых показаний с помощью современных информационно-технических средств, но

и преобразования всей системы уголовно-процессуального доказывания по уголовному делу в сторону их расширения и оптимизации использования.

Список литературы

1. Автоматизация оценки персонала. URL: https://151eye.ru/. (дата обращения: 15.03.2020).
2. Баянов А.И. Криминалистическая детализация — метод криминалистики и универсальное средство раскрытия и расследования преступлений // Уголовно-процессуальные и криминалистические чтения на Алтае / под ред. О.В. Кругликовой. Барнаул: Барнаульский юридический институт МВД России, 2016. С. 13-15.
3. Баянов А.И., Емельянова О.Н. Общая правовая цель допроса 6 лингвистический и юридический аспекты // Пробелы в российском законодательстве. 2014. № 2. С. 229-231.
4. Кто вне закона? Никто // Российская газета. URL: https://rg.ru/2020/01/14/bastrykin-predlozhil-uprostit-proceduru-zaderzhaniia-lic-s-osobym-statusom.html. (дата обращения: 24.04.2020).
5. Порубов Н.И. Допрос в советском уголовном судопроизводстве. Минск, 1976. 368 с.
6. Порубов Н.И. Научные основы допроса на предварительном следствии. Минск, 1978. 175 с.
7. Ратинов А.Р. Судебная психология для следователей. М., 1967. 290 с.
8. Уникальная российская разработка помогает ловить преступников по голосу и видеоизображению // Российская газета. URL: https://rg.ru/2020/03/05/rossijskaia-razrabotka-pomozhet-lovit-prestupnikov-po-golosu-i-video.html. (дата обращения: 15.03.2020).

И.Г. Иванова, *к.ю.н., доцент кафедры уголовного процесса и криминалистики Юридического института Сибирского федерального университета, г. Красноярск*

НЕКОТОРЫЕ ПРОБЛЕМЫ НАЗНАЧЕНИЯ И ПРОИЗВОДСТВА СУДЕБНОЙ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ МОБИЛЬНЫХ ТЕЛЕФОНОВ

В связи с повсеместным распространением средств мобильной коммуникации все чаще следователям при расследовании уголовных дел приходится назначать судебную компьютерно-техническую экспертизу изъятых мобильных телефонов.

Судебные компьютерно-технические экспертизы проводятся в целях выявления и изучения роли мобильных устройств в расследуемом преступлении, а также получения доступа к содержащейся в них информации с последующим всесторонним ее исследованием [1, с. 458-459].

На разрешение экспертов в этом случае ставятся следующие типичные вопросы:

1) Какой IMEI у представленного на экспертизу телефона?

2) Имеется ли в памяти представленного на экспертизу телефона телефонная книга (список контактов), входящие, исходящие и пропущенные вызовы, SMS-сообщения в явном либо удаленном виде?

3) Есть ли в памяти представленного на экспертизу телефона переписка посредством обмена электронными сообщениями?

4) Имеются ли в памяти представленного на экспертизу телефона приложения-мессенджеры, в том числе «WhatsApp», «Telegram»?

5) Имеются ли в приложениях-мессенджерах, в том числе «WhatsApp», «Telegram», входящие, исходящие и пропущенные вызовы, текстовые (графические, аудио, видео) сообщения в явном либо удаленном виде?

6) Имеются ли в памяти представленного на экспертизу телефона графические, текстовые и видеофайлы?

7) Имеется ли в памяти представленного на экспертизу телефона история браузера? Если да, то какие интернет-ресурсы и когда посещал пользователь данного телефона?

8) Имеются ли на представленном на экспертизу телефоне sim-карта, если да, то каковы ее международный код (IMSI) и серийный номер (ICCID)?

9) Имеется ли в памяти sim-карты телефонная книга (список контактов), входящие, исходящие и пропущенные вызовы, SMS-сообщения?

Здесь необходимо отметить, что при подготовке и назначении судебной компьютерно-технической экспертизы у следователей (дознавателей) нередко возникают затруднения как в формулировании выносимых на разрешение эксперта вопросов, так и в оформлении направляемых на экспертизу материалов [2, с. 83].

На судебную компьютерно-техническую экспертизу направляются сами мобильные телефоны, которые должны быть надлежащим образом упакованы и опечатаны. Однако в практике повсеместно распространены случаи ненадлежащей упаковки средств мобильной коммуникации, отправляемых на исследование. Так, нередко телефоны упаковываются в прозрачные пакеты из полимерного материала, которые не ограничивают доступ к содержимому памяти мобильных телефонов: их можно включить и выполнить любую модификацию информации в них, т.е. скопировать, удалить, изменить информацию и т.п.

В постановлениях о назначении судебной компьютерно-технической экспертизы мобильных телефонов следователи «забывают» дать разрешение эксперту на изменение внешнего вида или основных свойств исследуемых объектов (мобильных телефонов). В связи с этим эксперт при проведении исследования фактически вынужден изменять свойства компьютерной информации в мобильных телефонах без разрешения следователя.

В соответствии с ч. 1 ст. 8 ФЗ «О государственной судебно-экспертной деятельности в РФ» № 73-ФЗ от 31.05.2001 г. эксперт проводит исследования объективно, всесторонне и в полном объеме. Однако большинство (6 из 8) проанализированных нами экспертных заключений не удовлетворяли этим требованиям полноты, всесторонности и объективности экспертной оценки по различным основаниям. К таким основаниям мы отнесли следующие:

1. Применяемые экспертами аппаратно-программные комплексы и программное обеспечение для исследования мобильных телефонов не позволяют решить поставленные перед экспертом вопросы в полном объеме. Так, аппаратно-программный комплекс (АПК) «UFED Touch 2» и программное обеспечение «UFED Physical Analyzer», используемые практически всеми экспертами Сибирского федерального округа, не позволяют ответить на все перечисленные выше типичные вопросы судебной компьютерно-технической экспертизы в полном объеме. Например, с их помощью невозможно извлечь данные из программ «WhatsApp», «Viber», «Telegram», «VeChat», а также сведения о посещенных интернет-ресурсах, имеющиеся на мобильном телефоне, если эти сведения хранятся в телефоне в защищенной области. В настоящее время разработано специальное программное обеспечение, такое как «Мобильный криминалист 2019 Детектив», «Belkasoft», которые позволяют решить указанные задачи, но они отсутствуют на вооружении экспертов.

2. Эксперты в заключениях не приводят полных сведений об установленном программном обеспечении («мессенджерах») для обмена электронными сообщениями (о зарегистрированном пользователе, версии, дате установки и т.п.), имеющемся на исследуемом телефоне.

3. В заключении формально указывается время производства экспертизы, которое не соответствует реальным срокам ее производства. Нам встречались заключения, где срок экспертизы одного мобильного устройства составил более двух месяцев. Очевидно, что время производства экспертизы не может занимать такое количество времени. Однако в заключении не указаны промежутки времени, когда производство экспертизы было прервано по каким-либо причинам: больничный, срочные (внеочередные экспертизы), командировки и иные причины.

4. Часто исследовательская часть заключений страдает неполнотой, так как в ней не указывается следующая информация:

- сведения о системном программном обеспечении («прошивке») мобильного телефона;
- сведения об установленном системном времени и дате в мобильном телефоне (соответствует/отстает/опережает);
- сведения о содержимом памяти мобильного телефона (всего/свободно/занято байт);
- сведения о зарегистрированном пользователе («аккаунте»);
- сведения об установленных интернет-мессенджерах (версия, дата установки, пользователь и т.п.);
- содержимое памяти мобильного телефона на предмет «вредоносного программного обеспечения».

5. Выводы, сделанные в заключении, часто абсолютно не проверяемы. Это происходит потому, что в исследовательской части отсутствуют какие-либо сведения об обнаруженной информации, а с помощью файлов-отчетов (обычно прилагаемых к заключению в виде компакт-дисков) проверить это невозможно, так как в них приводится неполная информация.

Высказанные замечания в совокупности свидетельствуют о том, что у многих экспертов, проводящих компьютерно-техническое исследование мобильных телефонов, имеются существенные пробелы в специальных знаниях, демонстрируется недостаточное знание ими организационно-правовых, научных и методических основ такого вида исследований.

При наличии указанных недостатков заключение судебной компьютерно-технической экспертизы не будет соответствовать требованиям ст. 8 ФЗ-73 «О государственной судебно-экспертной деятельности в РФ», а в соответствии с постановлением Пленума Верховного суда РФ № 28 от 21.12.2010 г. такие заключения следует считать необоснованными, что ставит под сомнение допустимость экспертного заключения как доказательства.

Список литературы

1. Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. М.: Норма, 2005. 656 с.

2. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учебное пособие / В.Ф. Васюков, Б.Я. Гаврилов, А.А. Кузнецов и др.; под общ. ред. Б.Я. Гаврилова. М.: Проспект, 2017. 160 с.

П.П. Ищенко, *к.ю.н., старший преподаватель кафедры организации судебной и прокурорско-следственной деятельности Московского государственного юридического университета им. О.Е. Кутафина, г. Москва*

ХВАТИТ ЛИ «ИНТЕЛЛЕКТУАЛЬНЫМ АГЕНТАМ» ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, ЧТОБЫ ЗАМЕНИТЬ СЛЕДОВАТЕЛЯ?*

Широкое распространение общедоступных цифровых технологий, именуемое «четвертой промышленной революцией», стремительно изменяет не только технологический базис общества, но и весь социум [1]. Самостоятельный во всем индивид ныне остался в прошлом. Наш современник почти постоянно «подключен» к глобальной сети, чем бы он ни занимался: там он работает и отдыхает, общается и враждует, творит и разрушает. Там же совершаются преступления и осуществляется деятельность по их раскрытию.

Компьютерные технологии, сети и программное обеспечение обеспечивают функционирование глобальной искусственной среды коммуникации, действующей по своим специфическим законам. Уже первые преступления, совершенные при помощи или в самой сети Интернет, поставили вопрос о необходимости экспертной интерпретации следов преступления лицами, сведущими в указанной области для их использования в качестве судебных доказательств. Распечатка логов соединений сервера, даже по делу о банальном хищении трафика, выявленного службой безопасности провайдера, не более понятна суду, чем шумерская клинопись. Компьютерно-техническая экспертиза, включающая в себя исследование технических средств, программного обеспечения и компьютерных сетей, стала первым специализированным «инструментом», позволяющим правосудию «увидеть» «виртуальные» следы преступления.

Распространение Интернета и предоставляемых им возможностей, в совокупности с анонимностью пользователей, не могло не привлечь общеуголовную преступность, в том числе и организованную. На смену «компьютерным гениям», писавшим вредоносные программы и взламывавшим сайты крупных корпораций «из спортивного интереса», пришли новые уголовники, модернизировавшие привычные способы незаконного извлечения прибыли с помощью современных IT-технологий. Возникли десятки новых криминальных «профессий», действующих исключительно в «виртуальном» пространстве, способных, однако, причинить немалый и вполне материальный ущерб.

Новые информационные технологии более всего ориентированы на обеспечение потребностей бизнеса. Именно поэтому организованная преступность, экономическая функция которой состоит в удовлетворении потребности общества в нелегальных товарах и услугах [2, 3], по достоинству оценила эти новые открывшиеся перед ней возможности. Буквально на наших глазах в глобальную сеть переместилась почти вся торговля наркотиками, порнографией, краденым и запрещенным контентом, контрафактной продукцией, незаконными услугами и товарами, изъятыми из легального оборота, а также «отмывание» денег, полученных от преступной деятельности. В глобальной сети появились целые «торговые площадки», на которых функционируют сотни интернет-магазинов, осуществляющих торговлю незаконными товарами и услугами в автоматическом режиме практически без участия человека.

Так, правоохранительные органы США много лет пытались ликвидировать интернет-магазин «Silk road» (Шелковый Путь), который осуществлял торговлю наркотиками по всему миру, принимая к оплате практически любую конвертируемую валюту, в том числе электронную. Действовал он автоматически, почти без вмешательства оператора или администратора. Оплаченный заказ программа сама направляла поставщику, который отправлял «товар» покупателю по почте, под видом обычного почтового отправления. По оценке исследователей,

* *Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-011-00896.*

общий доход продавцов на «Silk road» составлял в месяц более 1,2 млн долл. США, а комиссионные администраторов — более 92 тыс. долл. США [4]. Аналогичные интернет-площадки существуют и в России. Несколько крупных уголовных дел о преступных сообществах, занимавшихся «сетевой» торговлей наркотиками на торговых площадках LegalRC.biz, shaman26.com, RAMP и других, было расследовано Следственным управлением Следственного Департамента ФСКН России в последние годы существования данного ведомства [5].

Общеуголовная преступность в значительной своей части стала «сетецентрической»: все, что нужно для совершения преступления, можно найти, «собрать» и привести в действие, не вставая с кресла перед компьютером. Для того чтобы ограбить современный банк, «медвежатник» с его слесарными инструментами уже не требуется. С точки зрения современных профессионалов — это «динозавр преступного мира», вызывающий любопытство лишь как музейный экспонат. Сегодня для этого непростого дела необходим целый набор профессионалов иного рода:

- «кодер» — программист, создающий вирусную программу, современную «отмычку» банковских сейфов;

- «тестировщик», который эту программу проверит в необходимой программной среде;

- «трафогоны», «фишеры» и прочие специалисты в области социального инжиниринга, которые помогут инфицировать банковскую систему подготовленным вирусом, который откроет брешь в защите системы;

- «заливщик» — специалист по выведению средств из банка на счета похитителей;

- «дроповоды», «дропы» и прочие «денежные мулы» — специалисты по «отмывке» и обналичиванию похищенных средств и т.д. Все указанные «специалисты» предлагают свои «услуги» в сети. Многие из них работают сдельно, требуя за свою работу фиксированную оплату. Самое известное дело этой категории — дело группировки «Carbanak», участниками которой было похищено по разным оценкам от 300 тыс. до 1 млрд евро [6].

Происшедшие изменения преступности и необходимость новых технологичных способов борьбы с ней произвели сильное впечатление на некоторых ученых. Можно услышать мнения о том, что правоохранительные органы якобы бессильны перед новой компьютерной преступностью. Для исправления ситуации предлагается реформировать уголовный процесс по американскому образцу: ввести исковой порядок возбуждения уголовного судопроизводства, отказаться от уголовного дела и предварительного расследования [7]. Расследование преступлений предлагается поручить роботам — полицейским, «интеллектуальным агентам, способным установить IP-адрес, с которого последовала команда, осуществлена транзакция криминального характера», а также узкоспециализированным органам, «в которых вместе работают технари и оперативные сотрудники криминальной полиции» [8].

Представляется, что предлагаемые реформы уголовного судопроизводства возымеют эффект, прямо противоположный ожиданиям авторов. Целесообразность «американизации» российского уголовного судопроизводства, отстаиваемая авторами и сторонниками «Доктринальной модели уголовно-процессуального доказательственного права», более обоснована риторическими тезисами, нежели логическими аргументами.

Личный опыт расследования преступлений, связанных с использованием цифровых технологий, показывает, что «установление IP-адреса» само по себе не решает проблемы установления личности преступника, а сотрудничество «технарей» и оперативников при всей своей результативности производит информацию, в большинстве случаев для суда непонятную. Более того, они сами порой не в состоянии оценить юридический смысл и доказательственное значение установленных ими обстоятельств. Изучение дел оперативного учета почти всегда позволяет найти в них ценную информацию, которую оперативные сотрудники сочли недостаточно важной и потому не представили следователю. Полномасштабное расследование организованной преступной деятельности, предполагающее методичное и целена-

правленное вскрытие всей структуры преступного формирования, вообще невозможно без руководящих и направляющих подсказок и поручений следователя [9].

Устранение процессуальной фигуры следователя точно не приведет к улучшению раскрываемости преступлений, но гарантированно «обрушит» действующую систему уголовного правосудия. Реформы в этой социально-чувствительной сферы государственной деятельности должны руководствоваться врачебным девизом «не навреди». Это означает, что для повышения эффективности выявления и расследования новых технологичных преступлений оперативным и следственным органам нужны не очередные шоковые преобразования, а новые, в том числе процессуальные, инструменты, легализующие результаты применения современных программно-технических средств в уголовном судопроизводстве. Однако вопрос, поставленный С.В. Власовой, о возможностях и пределах применения современных информационных технологий в уголовном судопроизводстве чрезвычайно интересен и заслуживает внимательного рассмотрения.

Известно, что методика расследования преступления определяется способом его совершения. Преступления, совершаемые в сети Интернет, особенно связанные с автоматизированной торговлей незаконными товарами и услугами, имеют одно важное свойство, позволяющее автоматизировать их выявление. Все они предельно алгоритмизированы, т.е. постоянно воспроизводят одну и ту же последовательность операций типа: поступление заказа, оплата товара, отправка товара получателю и сообщение о месте и способе его получения. Если сумма оплаты кратна стоимости запрещенного товара (например, дозе разового потребления наркотика), а семантика лексических единиц, входящих в оформление сайта, подтверждает криминальные цели его существования, есть основания полагать, что каждый «технологический цикл», зафиксированный в логах соответствующих серверов, является совершенным преступлением. То же самое относится к любой более или менее «автоматизированной» преступной деятельности, осуществляемой в глобальной сети.

Другой особенностью организованной преступной деятельности является формирование устойчивых регулярных коммуникативных структур. Еще в 1992 г. нами отмечалось, что совокупность следов коммуникации (в то время — биллингов соединений сотовой связи) между участниками преступного формирования точно отражает его структуру [10]. Организованные преступные формирования устойчивы, равно как и порядок осуществления связи между его членами. Это означает, что следы коммуникативного взаимодействия соучастников, оставляемые в информационной среде, имеют характерный «рисунок», обладающий признаком повторяемости или «регулярности». Обычным людям в процессе общения нет нужды формировать связанные между собой устойчивые «тройки», «пятерки» или «десятки», однако это весьма характерно для организованной преступности, террористов, экстремистов и разного рода военизированных формирований.

Перечисленные и подобные им закономерности позволяют автоматизировать процесс выявления преступной деятельности в сети Интернет. Имеющиеся технологии и обширные электронные ресурсы создают практически реализуемую возможность создания обучаемой электронной системы, действующей на основе технологий искусственного интеллекта, которая будет способна устанавливать участников криминальной активности и собирать об этом потенциально доказательственную информацию. Однако является ли данная техническая возможность реальным предвестником «интеллектуальных агентов», способных заменить следователя?

В компьютерной науке под интеллектуальным агентом понимается программа, самостоятельно выполняющая задание (например, поиск и сбор информации в сети Интернет), указанное пользователем, в течение длительного промежутка времени. В сфере искусственного интеллекта (ИИ) под интеллектуальными агентами понимаются вычислительные системы, помещенные во внешнюю среду, способные взаимодействовать с ней, совершая автономные рациональные действия для достижения определенных целей [11]. Автономность деятельности

таких агентов обеспечивается совокупностью заложенных правил «событие-действие», типа «если А, то В» (агенты с простым поведением), либо заложенных моделей, которые позволяют системам действовать в среде, лишь частично доступной для наблюдения. Идентифицируя установленную часть ситуации с какой-либо имеющейся у нее моделью, система «дорисовывает» недоступную для восприятия часть «картины» и сообразно этому выбирает модель своего дальнейшего поведения.

Правоохранительной практике известны случаи создания и использования таких систем. В 2012 г. в 30 городах и округах КНР была запущена в «пилотном» варианте основанная на технологии искусственного интеллекта система «Zero Trust», предназначенная для выявления несоответствий доходов и расходов государственных чиновников в связи с осуществляемой ими служебной деятельностью. Первоначально алгоритм обучали сотрудники отдела внутренних расследований Коммунистической партии Китая, обучая систему выявлять типичные несоответствия в документах, указывающие на допущенные нарушения. Затем объем доступной системе информации стали увеличивать, постепенно доведя его 150 баз данных федерального и регионального уровней. В результате систему научили эффективно выявлять типичные правонарушения: незаконную передачу права собственности, махинации с землей, участие в конкурсных процедурах подставных фирм или родственников ответственного чиновника и др. При необходимости система способна самостоятельно проверять по спутниковым фотоснимкам, действительно ли построен числящийся сданным объект или деньги попросту украдены.

С 2012 по 2019 г. система «поймала за руку» 8721 чиновника, которых обвинили в злоупотреблении властью, нецелевом расходовании средств или в превышении полномочий. Однако реальное наказание понесли лишь небольшая часть уличенных в правонарушениях, большинство «отделались» лишь выговорами [12]. Чрезвычайно мягкая карательная практика известного своей непримиримой борьбой с коррупцией Китая не может не вызывать вопросов. Сами чиновники чрезвычайно возмущались тем, что для доступа к их данным компьютерной системе не требовались ни санкции руководства, ни судебные решения. Однако нет оснований полагать, что власти КНР, принимая в 2019 г. решение о свертывании этой, казалось бы, эффективной системы, руководствовались интересами защиты прав коррумпированных чиновников.

Представляется, что ответ на этот вопрос можно найти в Европейской этической хартии об использовании искусственного интеллекта в судебных системах и окружающих их реалиях [13] (далее — Этическая хартия) и заключается он в свойствах ИИ как инструмента познания. Искусственный интеллект не является разумом и не воспроизводит человеческое мышление. Он неспособен воспроизвести рассуждения судьи или иного субъекта процессуального доказывания. Авторы Этической хартии отмечают, что «знаменитый юридический силлогизм является скорее способом представления юридического обоснования, нежели его формальным переводом. Он не отражает в полной мере аргументацию судьи, которая фактически состоит из множества влияющих на принятие решения факторов, не может быть априори формализована, а иногда и основана на усмотрении». При этом работ в направлении формализации юридических оснований для нужд машинного обучения даже не ведется [13, с. 32].

Системы искусственного интеллекта делятся на «слабые» — обучаемые человеком, и «сильные» — способные к самообучению, обладающие сознанием и способные постичь мир во всей его сложности. «Сильных» систем искусственного интеллекта в реальности не существует. Все системы, в том числе и описанная выше «Zero Trust», относятся к «слабым» ИИ. Они способны эффективно анализировать большие объемы данных, выявлять сложные тенденции, точно прогнозировать события. Однако у них, как и у их предшественников — экспертных систем, есть существенное ограничение. После «усвоения» 200-300 правил анализа информации логика системы становится недоступной для ее разработчиков [13, с. 28]. То есть ИИ комбинирует сформулированные человеком правила своим, «нечеловеческим» образом,

что обесценивает полученный результат с точки зрения его осмысленного, доказательного применения в уголовном судопроизводстве. Ученые, участвовавшие в разработке Этической хартии, отмечают, что современные большие системы обработки данных не пытаются воспроизвести человеческую модель познания, а сами создают контекстную статистику на новых объемах данных и используют ее для анализа без какой-либо реальной гарантии исключения ложных корреляций. При этом чем больше анализируемая база данных, тем больше вероятность ошибок [13, с. 30-31]. Это означает, что проблема получения «недоступных для понимания» результатов работы ИИ сохраняется.

Именно поэтому важны утверждаемые Этической хартией принципы прозрачности, беспристрастности и достоверности, требующие, чтобы методы обработки данных были понятными и доступными, в том числе для внешней проверки. В судопроизводстве вообще, а в уголовном — тем более, не может использоваться информация, происхождение которой недоступно пониманию. Как и все сложные логические построения, выводы ИИ должны проверяться «практикой» — соответствием их объективной реальности. Далеко не всегда для этого достаточно обратиться к спутниковым снимкам или записям видеокамер. И стандарты уголовно-процессуального доказывания, и криминалистические рекомендации требуют проверять полученную информацию путем проведения следственных действий. Это позволяет классифицировать информацию, полученную при помощи ИИ, как ориентирующую, содержащую сведения о возможном источнике доказательств.

Полученные выводы ни в коей мере не означают, что применение ИИ или иного специализированного программного обеспечения для нужд раскрытия и расследования преступлений бесполезно, а их разработка и совершенствование не имеют смысла. Напротив, работы в данном направлении открывают замечательные возможности по борьбе с современной, в том числе компьютеризованной преступностью. Технологии машинного поиска, анализа и обработки информации чрезвычайно успешно используются в оперативно-следственной практике. Существующая система следственных действий позволяет не только использовать непосредственно, но и вводить посредством процессуальной проверки результаты применения информационных технологий в уголовное судопроизводство. А вот планы по замене следователей «интеллектуальными агентами» придется отложить на неопределенный срок, не только ввиду отсутствия необходимых для этого технологий. Представляется, что в уголовном судопроизводстве «человечность» решения важнее его технологичности.

Список литературы

1. Шваб К. Четвертая промышленная революция. М.: Эксмо, 2016. 138 с.
2. Минна Р. Мафия против закона. М.: 1988. С. 184.
3. Шнайдер Г.Й. Криминология. М.: 1994. С. 49-51.
4. Nicolas Christin Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. Cornell University Library. URL: http//arxiv.org/abs/1207.7139 (дата обращения: 12.07.2019).
5. Уголовное дело № 143158 //Архив Индустриального районного суда г. Ижевска, 2019 г.; уголовное дело № 676074 // Архив Шпаковского районного суда Ставропольского края, 2018 г.
6. Большое банковское ограбление: APT-кампания Carbanak. URL: https://securelist.ru/bolshoe-bankovskoe-ograblenie-apt-campaniya-carbanak/25106/ (дата обращения: 18.06.2020).
7. Александров А.С. и др. Доктринальная модель уголовно-процессуального доказательственного права Российской Федерации и комментарии к ней. М.: Юрлитинформ, 2015. 304 с.
8. Власова С.В. К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. 2018. № 1. С. 9-18.

9. Ищенко П.П. Преступные сообщества (преступные организации) в сфере незаконного оборота наркотиков: методика расследования: науч.-практ. пособие. М.: Юрлитинформ, 2017. С. 110-143.

10. Ищенко П.П. О необходимости создания нового криминалистического учета для борьбы с организованной преступностью // Актуальные проблемы борьбы с правонарушениями. Екатеринбург, 1992. С. 66-70.

11. Alan-Jerome Fougeres. A Modeling Approach Based on Fuzzy Agents // International Journal of Computer Science Issues, November, 2012.

12. Носков А. В Китае отключают слишком крутую ИИ-систему борьбы с коррупцией // Хайтек+ от 04.02.2019. URL: https://hightech.fm/2019/02/04/zerotrust (дата обращения: 18.06.2020).

13. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях. Принята на 31-м пленарном заседании ЕКЭП (Страсбург, 3-4 декабря 2018 г.). URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4 (дата обращения: 18.06.2020).

А.Н. Калюжный, *к.ю.н., сотрудник Академии Федеральной службы охраны Российской Федерации, г. Орел*

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ОСМОТРА ДАННЫХ, ОБНАРУЖЕННЫХ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ ПО ДЕЛАМ О ПОСЯГАТЕЛЬСТВАХ НА СВОБОДУ ЛИЧНОСТИ

Происходящие в современном мире процессы, связанные с развитием информационно-коммуникационных технологий, привели к значительному развитию и распространению электронных устройств, использование которых стало обыденным и повсеместным. В настоящее время человек не представляет свою деятельность без использования средств сотовой связи, камер видео-наблюдения, видеорегистраторов, возможностей информационно-телекоммуникационной сети Интернет. Преобладающая в конце XX столетия точка зрения о делении следов на материальные и идеальные трансформировалась, дополнившись отдельной категорией следовой информации — электронной, находящей свое выражение на различных магнитных носителях, страницах сайтов интернет-ресурсов, средствах сотовой связи и т.п.

Получившие существенное развитие информационно-коммуникационные технологии стали повсеместно использоваться не только в целях развития общества и государства, создания комфортных условий жизнедеятельности населения, но и активно применяться в ходе совершения преступлений, образовав собой отдельное направление преступной деятельности — сферу компьютерной информации, а также иных преступлений, совершенных посредством (с использованием) указанных технологий.

В числе таких преступлений оказались и посягательства на свободу личности, совершение которых находит прямое либо косвенное отражение в данных: детализации телефонных соединений абонентов, посредством которых осуществлялся их контакт, высказывались требования передачи имущества или денежных средств, выкупа за похищенную жертву; записей камер видеонаблюдения, фиксировавших факты перемещения, передвижения виновных и жертв; информации передаваемой посредством сети Интернет: с помощью электронной почты, социальных сетей, систем мгновенного обмена сообщениями и других.

Выявление и расследование преступлений, направленных на свободу личности, становится невозможным без использования современных криминалистических средств и примене-

ния тактических приемов, выступающих основой производства отдельных следственных и процессуальных действий, особое значение среди которых принадлежит осмотрам [1, с. 74].

Изучение материалов уголовных дел о преступлениях, направленных на свободу личности, а также данные анкетирования сотрудников правоохранительных органов, занимающихся их выявлением и расследованием свидетельствуют, что наиболее типичными объектами, зафиксировавшими контакты преступников и их жертв, являются: CD-диски с данными детализацией телефонных переговоров фигурантов дела, средства мобильной связи виновных и потерпевших, а также записи камер видеонаблюдения. Тактические особенности их осмотра и выступили предметом настоящей статьи, получив развитие в ее содержании.

Итак, механизм совершения преступлений, направленных на свободу личности, обусловливает на этапах подготовки, совершения и сокрытия исследуемых преступлений к активному использованию средств сотовой связи в целях: выманивая жертв из мест их нахождения; предъявления потерпевшим требований передачи имущества, совершения определенных действий, угроз и т.п.; выдвижения близким и родственникам похищенных требований об уплате выкупа, совершения определенных действий; приискания средств совершения преступления, средств удержания жертв; подыскания сообщников преступной деятельности; координации преступной деятельности соучастников; организации деятельности по уничтожения следов преступной деятельности, оказания противодействия расследованию и другие.

Изложенное указывает, что одним из наиболее распространенных и типичных объектов осмотра по делам о посягательствах, направленных на свободу личности, являются средства сотовой связи — мобильные телефоны преступников и их жертв, данные которых содержат не только информацию о соединениях фигурантов дела, но и также сведения, передаваемые с помощью MMS-, SMS-сообщений, материалы переписки с использованием мессенджеров, а также иную криминалистически значимую информацию, размещенную в социальных сетях.

Тактические особенности осмотра данных, содержащихся в мобильных аппаратах виновных и их жертв, по посягательствам на свободу личности предопределяют необходимость отражения в протоколе осмотра предметов следующей информации, имеющей значение для уголовного дела:

а) марку телефона, его заводской номер, цвет, состояние внешнего вида и индивидуальные характеристики (наличие царапин, использование чехла и т.п.);

б) сведения о входящих и исходящих звонках, содержащиеся в «журнале звонков», с описанием времени и дат контактов подозреваемых (обвиняемых) друг с другом, с жертвой, его близкими или родственниками;

в) данные о наличии (отсутствии) фигурантов в списке контактов «телефонной книги» [2, с. 262];

г) содержание информации MMS и SMS-сообщений, сделанных за определенный период виновными и жертвами (переписка соучастников; тексты требований, угроз, ультиматумов, выдвинутых и пересланных потерпевшему, его близким или родственникам);

д) сведения, имеющиеся в интернет браузерах, установленных в мобильном аппарате (Opera, Яндекс браузер, Google Chrome и др.), история просмотренных сайтов, приискания орудий и средств совершения преступлений, аренды транспорта, жилых и нежилых помещений и иная имеющая к делу информация;

е) информации, содержащаяся в установленных на мобильном аппарате мессенджерах (WhatsApp, Telegram, WeChat и др.), а также опубликованная в социальных сетях (Facebook, Instagram, Twitter и т.п.), отражающая факты общения фигурантов преступления друг с другом и с потерпевшими (содержание переданной или размещенной текстовой информации, переданные фото- и видеофайлы, данные геолокации, сведения о подключениях к сетям Wi-Fi и др.) [3, с. 3]. Пристальное внимание необходимо уделить информации о местонахождении виновных в определенные периоды времени (время совершения преступления) и обоснование их корреляций с данными о местоположении жертв, местами их удержания и эксплуатации;

ж) фото-, видеофайлы, находящиеся в «камере» и «галерее» мобильного аппарата.

Отраженная в протоколах осмотра предметов информация, характеризующая данные, содержащиеся в мобильных телефонах преступников и жертв имеет существенное значение, доказывая причастность виновных к совершенным преступлениям, изобличая их в преступных деяниях, свидетельствуя о нахождении виновных и их жертв в одно и то же время и месте, а также иным образом характеризуя преступные действия фигурантов дела.

Например, в протоколе осмотра предметов, одним из которых явился мобильный телефон, была зафиксирована следующая криминалистически значимая информация: телефон марки NOKIA X1-01, черного цвета, с IMEI номером 358604… В меню вызовов в 20.53 имеется один вызов на номер 8-928-059…, принадлежащий Ж. В меню принятые вызовы в 01.32 имеются один вызов с номера 8-916-018…, принадлежащего Р. Данная информация отражает факт общения преступников друг с другом и с потерпевшим [4].

Кроме того, механизм совершения преступлений, направленных на свободу личности, и имеющаяся вероятность удаления некоторых данных с мобильного устройства предопределяют необходимость получения информации о соединениях между абонентами или абонентскими устройствами и последующего осмотра данных детализации телефонных соединений преступников и их жертв, как правило, содержащихся на CD-дисках.

Специфика осмотра CD-дисков с материалами детализации телефонных соединений преступников и их жертв предполагает фиксацию в протоколах осмотров предметов следующих, имеющих значение для уголовного дела данных:

а) паспортных данных фигурантов уголовного дела, на которых зарегистрированы интересующие абонентские номера;

б) корреляционных взаимосвязей абонентских номеров виновных и их жертв;

в) принадлежности участникам уголовного дела кодов IMEI их телефонов;

г) время и даты соединений фигурантов уголовного дела друг с другом, с потерпевшими; их близкими или родственниками;

д) время, даты и содержание полученных и отправленных фигурантами MMS и SMS-сообщений;

е) звонки, сделанные виновными и их жертвами, соединения по которым не были достигнуты;

ж) о работе средств сотовой связи виновных и их жертв относительно базовых станций [5, с. 101].

Также необходимо отразить в протоколе осмотра криминалистически значимую информацию, относящуюся к осматриваемому CD-диску:

а) изготовитель (наименование) диска, его серийный номер и содержащиеся надписи;

б) техническое устройство (ноутбук, персональный компьютер и т.п.) с помощью которого он был осмотрен;

в) количество файлов, содержащиеся на CD-диске, их название и размер занимаемых данных.

Зафиксированная в протоколе осмотра предметов вышеуказанная информация позволяет доказать механизм преступных действий виновных, количество соучастников преступления, роль каждого из них в совершенном деянии, установить источники подыскания мест удержания потерпевших, источники приискания средств и орудия совершения рассматриваемых преступлений, а также обосновать нахождение виновных вместе с потерпевшим в местах завладения, перевозки, удержания или освобождения.

Например, выявленные в ходе осмотра предметов (CD-диска) данные детализации телефонных номеров, зарегистрированных на Ж., Г. и потерпевшего А., доказывают факт похищения потерпевшего, исходя из того, что телефонные номера виновных находились в зоне действия единой с потерпевшим базовой станций, что нашло отражение в протоколе [6].

Развитие информационно-телекоммуникационных технологий и исследование преступлений, направленных на свободу личности, заставляют нас обратить внимание на тактические особенности осмотра записей камер видеонаблюдения, получившие свое широкое распространение в общественной жизнедеятельности и являющихся типичными для доказывания преступной деятельности виновных.

Преобладающее количество уголовных дел о преступлениях, направленных на свободу личности, содержали данные о приобщении к материалам уголовных дел записей камер видеонаблюдения путем производства выемок и находившихся на DVD-дисках. В ходе проведения осмотра записей камер видео-наблюдения обязательному отражению, кроме данных, индивидуализирующих конкретный DVD-диск и указанных нами ранее, подлежит следующие сведения, имеющие значение для дела:

а) время и дата имеющихся событий, запечатленных на видео;

б) характер и содержание происходящих действий;

в) последовательность действий, имеющихся на видео [7, с. 196].

Например, в ходе осмотра DVD-диска с видеозаписями камер наружного наблюдения, в протоколе осмотра предметов нашла отражение следующая информация: на записи от 20.04.2009 г. отображен подъезд дома по улице… В 4:22 мин. запечатлен факт захвата тремя людьми потерпевшего С., путем причинения последнему телесных повреждений в виде шести ударов руками в область лица и головы, с последующим помещением С. в автомашину, государственные регистрационные знаки на которой не видны [6].

Подводя итоги изложенному, отметим, что данные, содержащиеся на магнитных дисках и представленные в виде информации с детализацией телефонных переговоров (соединений), записей камер видеонаблюдения, а также содержащиеся в мобильных телефонах преступников и их жертв являются наиболее типичными объектами осмотров по посягательствам на свободу личности. Применение современных криминалистических средств и тактических приемов производства осмотра указанных предметов позволяет изобличить преступную деятельность виновных, зафиксировать имеющую значение для уголовного дела доказательственную информацию и решить задачи, возложенные на уголовное судопроизводство.

Список литературы

1. Волков А.С. Правовые и криминалистические проблемы выявления и раскрытия похищения человека: дис. … канд. юрид. наук. Самара, 2002. 192 с.

2. Гаврилин Ю.В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы: дис. … д-ра. юрид. наук. М., 2010. 404 с.

3. Васюков В.Ф., Булыжкин А.В. Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел // Российский следователь. 2014. № 2. С. 2-4.

4. Архив Перовского районного суда г. Москвы // Уголовное дело № 1-197/2013.

5. Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: монография. Екатеринбург: УрЮИ МВД России, 2014. 209 с.

6. Архив Гагаринского районного суда г. Москвы // Уголовное дело № 1-480/2014.

7. Тушев А.А., Назаров Н.А. Информация как основа всех видов доказательств в уголовном процессе // Общество и право. 2012. № 3 (40). С. 195-197.

В.М. Кондратьев, *адъюнкт кафедры оперативно-разыскной деятельности в ОВД Санкт-Петербургского университета МВД России, г. Санкт-Петербург, заместитель начальника Управления по контролю за оборотом наркотиков ГУ МВД России по Кемеровской области, г. Кемерово*

НЕКОТОРЫЕ ОСОБЕННОСТИ ОПЕРАТИВНО-РОЗЫСКНОГО ВЫЯВЛЕНИЯ, ПРЕСЕЧЕНИЯ И РАСКРЫТИЯ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Угроза появления в России новых видов наркотических средств и психотропных веществ вошла в число первоочередных проблем в сфере противодействия незаконному обороту наркотиков. Наркобизнес ускоренными темпами переходит от распространения таких традиционных наркотиков, как героин и марихуана, к производству и сбыту синтетических видов наркотических средств, а также новых потенциально опасных психоактивных веществ, в том числе так называемых «дизайнерских» наркотиков.

Стремительное развитие информационно-телекоммуникационных технологий, электронных платежных систем безналичных переводов денежных средств, несовершенство действующего законодательства активно используются наркосбытчиками для организации бесконтактного распространения наркотических средств, психотропных веществ, их аналогов, новых потенциально опасных психоактивных веществ (далее — наркотики).

Бесконтактный способ реализации наркотиков с использованием электронных платежных систем в условиях отсутствия эффективного государственного контроля над сферой электронных платежей позволяет злоумышленникам в значительной степени создавать препятствия в проведении многих оперативно-розыскных мероприятий сотрудниками оперативно-розыскных органов.

Р.Г. Драпезо и В.Н. Шелестюковым отмечается такая негативная тенденция последних лет, как уход наркобизнеса в так называемый Darknet (темный Интернет), в котором с помощью обычных браузеров нельзя воспользоваться его ресурсами. Только используя специальные браузеры, такие как Tor, можно воспользоваться onion-ресурсами, но и зарегистрировать интернет-магазин по незаконной продаже наркотиков. Браузер Tor обеспечивает анонимное подключение к onion-ресурсам не только клиентов и пользователей, но и серверов, что делает отслеживание адресатов по IP-адресам практически невозможным [1, с. 24].

Как показала практика выявления и расследования преступлений рассматриваемой категории, решению задач по выявлению, пресечению и раскрытию наркопреступлений, совершаемых с использованием информационно-телекоммуникационных систем, препятствует ряд обстоятельств, среди которых особо выделяется необходимость привлечения к указанной деятельности значительного количества сил и средств, главным образом со стороны подразделений, осуществляющих оперативно-технические мероприятия. Тем не менее правильно организованное наблюдение за сетевыми ресурсами в Интернете и грамотное проведение в сети комплексных оперативно-розыскных мероприятий позволяют оперативным сотрудникам выявлять и задерживать лиц, причастных к незаконному обороту наркотических средств указанным способом [2, с. 35].

В настоящее время любое причастное к наркобизнесу лицо может после виртуальной переписки посредством сети Интернет заказать из-за рубежа партию наркотического средства, получив ее в международном почтовом отправлении, в целях дальнейшего потребления или сбыта бесконтактным способом. Основное преимущество такой формы приобретения наркотиков — минимальный риск разоблачения преступной деятельности, ведь физического перемещения подконтрольных веществ через таможенную границу не происходит, а при заказе

наркотика и внесении за него платы фигурант действует завуалировано, не идентифицируя себя. Незаконный сбыт наркотических средств через сеть Интернет имеет те же черты обезличенности, позволяя наркосбытчику при минимальном риске разоблачения своей преступной деятельности длительное время распространять в наркосреде синтетические наркотики, внедряя в криминальный наркооборот их новые виды [3, с. 29].

Структура бесконтактного сбыта наркотиков включает в себя:

– коммуникационную систему для связи между участниками противоправной деятельности (мобильная связь, IP-телефония, интернет-мессенджеры);

– финансовый инструментарий в виде комплекса электронных средств платежа различных категорий, банковских карт и иных средств;

– структуру логистического обеспечения, в том числе транспортного;

– штат криминального персонала для сетевого сбыта с четким распределением функций (программисты, координаторы, диспетчеры, закладчики, кладовщики, финансисты и др.), систему подбора персонала и деятельность по его обучению криминальным навыкам.

В этой связи на постоянной основе необходимо осуществлять не только анализ состояния, структуры, динамики сферы бесконтактного сбыта наркотиков с использованием информационно-телекоммуникационных технологий, но и текущий мониторинг особенностей его финансовой составляющей (типологических особенностей финансовых операций, региональной специфики отраслей легального бизнеса и т.д.).

Полученные в результате проведения комплексного анализа и оценки сведения являются основой для своевременного прогнозирования криминальных тенденций с выявлением новых вызовов и угроз, выработки актуальных организационно-правовых мер воздействия на состояние оперативной обстановки в сфере незаконного оборота наркотиков, направленных на устранение причин и условий, способствующих совершению наркопреступлений.

Огромную и важную роль в деятельности правоохранительных органов в выявлении, пресечении и раскрытии незаконного сбыта наркотиков, совершаемого с использованием инормационно-телекоммуникационных технологий, играет использование сил и средств оперативно-розыскной деятельности как особого вида государственной деятельности, направленной на борьбу с преступностью.

Только путем применения негласных оперативно-розыскных методов и специальных познаний в сфере высоких информационных технологий возможно достигнуть положительных результатов в рассматриваемом направлении противодействия наркопреступности.

Так, на первоначальном этапе осуществления оперативно-розыскной деятельности по выявлению преступлений, связанных с незаконным сбытом наркотиков с использованием информационно-телекоммуникационных систем, необходимо установить:

– регистратора доменных имен (юридическое лицо, аккредитованное координатором для оказания услуг регистрации доменных имен);

– провайдера хостинга (т.е. лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет);

– интернет-провайдера, который в конечном счете и может сообщить IP-адрес конкретного пользователя, точнее, точки доступа в сеть Интернет.

Это позволяет установить фактическое местонахождение компьютера, мобильного устройства, точки доступа в Интернет, с неограниченным числом пользователей (например, через wi-fi-роутеры).

Однако при регистрации доменного имени, сайта или регистрационного аккаунта на ресурсе в качестве пользователя проверка подлинности представленных данных не проводится, что не позволяет достоверно установить лицо, разместившее информацию в сети Интернет.

Кроме того, на первоначальном этапе выявления рассматриваемого вида преступлений особое значение приобретает поиск первичной оперативной информации в сети Интернет и ее проверка, проведение которых предполагает наличие у оперативного сотрудника специальных знаний. Для выявления информации, представляющей оперативно-розыскной интерес, в первую очередь используется поиск по информационным ресурсам Интернета с применением разного рода поисковых систем (Google, Yandex, Rambler и прочие). В ходе этого выявляются сайты, связанные с преступными организациями, а также информационные ресурсы, содержащие запрещенную к распространению информацию. По результатам поиска принимаются меры к установлению личности организаторов сайтов. Однако использование только такого подхода не может обеспечить достаточной эффективности информационного поиска в киберпространстве, поскольку в нем существуют обширные закрытые для поисковых серверов зоны, которые могут использоваться в деструктивных целях (в том числе и для распространения наркотиков). В целях более эффективного выявления наркопреступлений в сети Интернет предлагается проводить оперативно-розыскной мониторинг сетевого информационного пространства, который предполагает сбор, обработку и анализ информации о явлениях криминального плана, представляющих интерес для оперативно-розыскной деятельности, оценку и прогноз изменения оперативной обстановки под воздействием криминогенных факторов. После выявления ресурсов, через которые организован оборот наркотических средств, важно обеспечить установление контакта с продавцами (диспетчером), выяснение способов связи с ними и данных контактов, в том числе номеров мобильных телефонов, электронных кошельков, банковских счетов и т.п. Необходимо принять меры к определению местонахождения устройств, с помощью которых преступниками осуществляется выход в сеть Интернет, установлению всех участников преступной деятельности, а также выяснению роли каждого из соучастников в сбыте наркотиков, определить места закладок наркотических средств, каналы поставок, способы обналичивания и распределения денежных средств, а также иные обстоятельства, свидетельствующие о преступной деятельности. Проводимый комплекс оперативно-розыскных мероприятий должен включать несколько проверочных закупок, осуществляемых на различных этапах оперативной проверки. По итогам первичной проверочной закупки целесообразно представить следователю часть результатов оперативно-розыскной деятельности для решения вопроса о возбуждении уголовного дела. Наличие уголовного дела позволяет более оперативно получать доказательства вины участников группы путем осуществления не только оперативно-розыскных мероприятий, но и следственных действий, таких как допросы, выемки, обыски и др. После того как основные участники организованной преступной группы установлены и их преступные действия надлежащим образом зафиксированы, следует переходить к реализации материалов оперативной разработки и задержанию фигурантов. Большую актуальность приобретает вопрос первоначальных следственных действий, обусловленных способом совершения преступления. Особое внимание на первоначальном этапе необходимо уделить обыску по месту жительства подозреваемого, необходимо изучить рабочее место — используемый персональный компьютер с его периферийными устройствами, иные устройства, обеспечивающие доступ к Интернету. Объектами поиска при незаконном распространении наркотиков посредством глобальной сети Интернет в зависимости от конкретных обстоятельств являются: наркотические средства, психотропные и сильнодействующие вещества — переписка, почтово-телеграфная корреспонденция, записные телефонные книжки, другие документы, свидетельствующие о связях между преступниками, а также между ними и их клиентами; квитанции, чеки, бланки, счета оплаты перевода, отправления, получения денежных средств, электронных переводов, пластиковые карты, договоры на открытия счетов и т.д. [2, с. 37–38].

Н.Т. Кузьмин обоснованно полагает, что причины повышенного интереса наркопреступников к Интернету заключаются в том, что в этой среде имеются особые условия для обеспечения конспирации участников незаконного оборота наркотиков. Использование нарко-

дилерами последних достижений в телекоммуникационных технологиях позволяют преступникам исключать прямой контакт с покупателем. Таким образом:

– повышается безопасность наркосбытчиков;

– появляются новые преступные группы в рамках сетевой системы сбыта наркотиков;

– за счет увеличения преступных групп, сбывающих наркотики, расширяется розничная сеть наркодилеров [4, с. 43–44].

Для достижения максимальной безопасности при сбыте наркотиков преступниками применяется хорошо продуманная система безопасности, где существуют несколько уровней защиты, препятствующей документированию преступных действий разрабатываемых.

1-й уровень — на этапе связи:

– исключены личные встречи между членами преступной группы;

– исключены встречи между сбытчиком и покупателем;

– контакты осуществляются с помощью мобильной связи, SMS сообщений, систем Skype, Jabber, Viber;

– абонентские номера зарегистрированы на подставных лиц или не имеют официальной регистрации;

– используемые SIM-карты и телефонные аппараты мобильной связи периодически меняются;

– информация о смене телефонных номеров рассылается заинтересованным лицам только с помощью SMS.

2-й уровень — поставка наркотиков от организатора к «закладчику»:

– «закладчик» лично не знаком с организатором и «диспетчером»;

– «закладчик» подобран из числа потребителей;

– вовлечение в сбытовую сеть осуществляется с помощью коммерческого предложения через SMS или сеть Интернет;

– «закладчик» получает телефонный аппарат с SIM-картой и наркотики через закладки в тайниках;

– наркотики, заложенные в тайниках, уже заранее расфасованы на условные единицы веса (дозы).

3-й уровень — на этапе осуществления закладок:

дозы наркотиков дополнительно маскируются, упаковываются во фрагменты газет, мятые сигаретные пачки, затем помещаются в тайники;

– закладки в тайники осуществляются заранее;

– места тайников не повторяются;

– используются общедоступные места (полости под подоконниками, вывесками, в подъездах за мусоропроводами, почтовыми ящиками, возле гаражей и т.д.);

4-й уровень — этап контакта «диспетчера» с покупателем:

– контакт между «диспетчером» и покупателем осуществляется с помощью мобильной связи посредством SMS, систем Skype, Jabber, Viber и др.;

– при заказе покупатель указывает количество и вид желаемого наркотика;

– «диспетчер» называет цену и способ оплаты;

– при получении информации о поступлении денежных средств «диспетчер» сообщает о месте нахождения тайника.

5-й уровень — на этапе оплаты:

– без предварительной оплаты наркотики не отпускаются;

– информация о месте нахождения закладки направляется только после подтверждения о произведенной оплате;

– для оплаты наркотиков покупатели используют общедоступные платежные терминалы (предназначенные для моментальной оплаты телефонов, коммунальных платежей и других услуг), переводя денежные средства на банковские счета;

– банковские счета оформляются на подставных лиц с подключением услуги «мобильное информирование», при которой информация о движении денежных средств отправляется на абонентский номер мобильного телефона в виде SMS;

– виртуальные счета открываются обезличенным способом через Интернет в системах Яндекс.Деньги, Webmoney, проверка поступления денежных средств осуществляется «диспетчером» с помощью компьютера, имеющего выход в сеть Интернет;

– с учетом наличия суточного лимита по сумме наличных денежных средств по банковским и виртуальным счетам наркосбытчики используют несколько счетов, номера которых «диспетчер» сообщает покупателям непосредственно перед сделкой.

6-й уровень — на этапе обналичивания денежных средств:

– для получения банковского счета одному из покупателей наркотиков направляется SMS с предложением открыть на себя такой счет, оформить банковскую карту и обменять ее через закладку на наркотики;

– при использовании электронного счета виртуальные деньги с помощью компьютера, имеющего выход в сеть Интернет, переводятся на один или несколько банковских счетов;

– непосредственное обналичивание денежных средств осуществляется в банкоматах с использованием банковских карт, не «привязанных» к преступникам.

В целях сокрытия доходов преступниками используются схемы многоходовых переводов денежных средств через электронные платежные системы. Создается определенное количество интернет-кошельков QIWI, один или несколько из которых используются в рекламе интернет-магазина, реализующего наркотики. Консолидация денежных средств осуществляется путем их перечисления через другие интернет-кошельки с последующим переводом на расчетный счет либо карту. Представленная схема бесконтактного сбыта наркотиков может видоизменяться с учетом технических возможностей, образовательной подготовки участников преступной группы и используемых конспиративных мер [4, с. 46–47].

Именно на все вышеуказанные факторы и должно быть обращено первоочередное внимание сотрудников оперативно-розыскных органов в целях правильного планирования комплекса необходимых оперативно-розыскных мероприятий, направленных на выявление, пресечение и раскрытие незаконного сбыта наркотиков с использованием информационно-телекоммуникационных систем.

Итак, проводя анализ всего вышесказанного, следует сделать вывод, что основными видами оперативно-розыскных мероприятий, проводимых оперативно-розыскными органами при выявлении, пресечении и раскрытии наркосбыта с использованием информационно-телекоммуникационных технологий, являются:

1) «наведение справок», в ходе которого устанавливаются IP-адреса, интернет-провайдеры, модели и номера средств связи, используемые объектами оперативной заинтересованности, их телефонные и иные соединения, используемые ими электронные и банковские счета, совершенные финансовые операции с наркодоходами, а также иные сведения;

2) «опрос», в ходе которого устанавливаются оперативно значимые сведения об объектах оперативной заинтересованности, об их связях, личностных характеристиках, чертах характера, а также каких-либо иных обстоятельствах произошедших событий и явлений, представляющих оперативный интерес;

3) «исследование предметов и документов», в ходе которого добывается оперативно значимая информация, содержащаяся в сотовых телефонах и иных мультимедийных устройствах, имеющих выход в сеть Интернет, используемых объектами оперативной заинтересованности, а также путем исследования иных предметов и документов, с использованием

специальных познаний и привлечением к проведению оперативно-розыскного мероприятия специалистов соответствующих профилей;

4) «наблюдение», в результате которого устанавливаются места пребывания, частого времяпровождения, работы, проведения досуга, адреса жительства объектов оперативной заинтересованности, используемые ими транспортные средства, гаражи, автостоянки, а также преступные и иные связи проверяемых и разрабатываемых лиц, места сбыта и хранения наркотиков;

5) «проверочная закупка» и «оперативный эксперимент», основной целью которых является установление способов и механизма сбыта наркотиков, движение денежных средств, задержание объектов оперативного интереса с поличным при совершении наркосбыта;

6) «прослушивание телефонных переговоров» и «снятие информации с технических каналов связи» позволяют получить необходимые сведения о преступных намерениях проверяемых и разрабатываемых лиц и принимать соответствующие и своевременные меры реагирования на различные предпринимаемые ими факты преступных проявлений, а также позволяют установить связи объектов оперативной заинтересованности, места сбыта и хранения наркотиков, конкретное местонахождение объектов в определенный период времени;

7) «обследование помещений, зданий, сооружений, участков местности и транспортных средств» способствует обнаружению и изъятию оперативно значимых предметов, веществ и материалов, используемых объектами оперативной заинтересованности в противоправной деятельности (наркотические средства, мобильные устройства сотовой и интернет-связи, денежные средства, иное имущество, добытое преступным путем, документы и т.д.);

8) «получение компьютерной информации», в результате которого путем применения специальных познаний добываются оперативно значимые сведения, содержащиеся в используемых объектами оперативной заинтересованности компьютерами, планшетами, смартфонами, а также иными устройствами с функциями накопления, обработки и передачи данных.

Список литературы

1. Драпезо Р.Г., Шелестюков В.Н. Особенности нового оперативно-разыскного мероприятия — получение компьютерной информации (на примере незаконной торговли наркотическими и психоактивными веществами) // Оперативник (сыщик). 2018. № 1 (54). С. 23-26.

2. Анисова И.А. Выявление, раскрытие и расследование наркопреступлений, совершаемых с использованием информационных технологий // Национальный и международный уровни противодействия наркоугрозе и взаимодействие в сфере реабилитации и ресоциализации наркопотребителей: материалы XIII международной научно-практической конференции (16-17 апреля 2015 г.): в 2 ч. / отв. ред. И.А. Медведев; СибЮИ ФСКН России. Красноярск: СибЮИ ФСКН России, 2015. Ч. 2. С. 34-38.

3. Шарманкин С.В. Практика расследования уголовных дел о преступлениях в сфере незаконного оборота синтетических наркотических средств, совершенных с использованием сети Интернет (на примере деятельности Управления ФСКН России по Приморскому краю) // Вестник Сибирского юридического института ФСКН России. 2015. № 3 (20). С. 28-32.

4. Кузьмин Н.Т. Некоторые особенности бесконтактного сбыта наркотиков // Национальный и международный уровни противодействия наркоугрозе и взаимодействие в сфере реабилитации и ресоциализации наркопотребителей: материалы XIII международной научно-практической конференции (16-17 апреля 2015 г.): в 2 ч. / отв. ред. И.А. Медведев; СибЮИ ФСКН России. Красноярск: СибЮИ ФСКН России, 2015. Ч. 2. С. 43-47.

Е.А. Королева, *аспирант кафедры криминалистики Московской академии Следственного комитета РФ, старший следователь отдела по расследованию особо важных дел следственного управления по Западному административному округу Главного следственного управления Следственного комитета РФ в г. Москве, г. Москва*

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПОЛОВЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ НЕСОВЕРШЕННОЛЕТНИМИ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Широкая популяризация всемирной компьютерной сети, ее доступность и динамическое омоложение пользователей привело к тому, что в состав лиц, реализующих объективную сторону общественно-опасных деяний, предусмотренных ст. 135 Уголовного кодекса РФ, вошли несовершеннолетние. Развратные действия, за совершение которых наступает уголовная ответственность как по вышеуказанной статье Уголовного кодекса РФ, так и по п. «б» ч. 4 ст. 132 Уголовного кодекса РФ, могут выражаться в физической или интеллектуальной форме. При этом интеллектуальная форма, о которой пойдет речь в данной статье, подразумевает циничные разговоры с малолетним лицом на сексуальные темы, а также демонстрация ему материалов порнографического содержания (фото- и видеоматериалов).

Психологическими предпосылками виктимизации, а также криминализации личности несовершеннолетних является тот факт, что дети допубертатного возраста (10-12 лет) в большей степени ориентированы на социальные отношения, они начинают испытывать осознанные сексуальные чувства и порывы. В это время закладываются основные модели и схемы сексуального поведения, которые проявятся в период полового созревания и позже (в возрасте от 12-13 лет и старше). В связи с тем, что сексуальные темы вызывают у несовершеннолетних неподдельный интерес, но его обнаружение обществом, в том числе и в лице родителей, родственников, педагогического состава учебного учреждения и иными лицами, представляется им крайне нежелательным и пугающим, активность подростков в этой теме полностью актуализируется на просторах Глобальной сети. Несовершеннолетний (как потерпевший, так и преступник), находясь еще в периоде интенсивного физического и нравственного развития, опасается любого наказания, в том числе и в виде общественного порицания, следствием чего является высокая степень латентности данного вида преступлений [1]. Интернет-форумы, чаты, социальные сети при этом дают возможность несовершеннолетним совершать интеллектуальные развратные действия (иными словами, познавать и реализовывать себя как субъекта сексуальной жизни) в психологически комфортной для них обстановке, то есть дома, наедине, не привлекая внимания общественности и правоохранительных органов.

Так, Следственным управлением Следственного комитета РФ по Тамбовской области в 2016 г. прекращено уголовное дело по основанию, предусмотренному п. 2 части 1 ст. 24 Уголовно-процессуального кодекса РФ, то есть в связи с отсутствием в действиях несовершеннолетнего Ф., 1999 года рождения, состава преступления, предусмотренного ч. 2 ст. 135 Уголовного кодекса РФ, так как он не достиг возраста привлечения к уголовной ответственности. По материалам следствия несовершеннолетний Ф. в октябре 2015 г., находясь в не установленном следствием месте, используя учетную запись «М» в социальной сети «ВКонтакте» сети Интернет, ведя переписку с пользователем учетной записи «Д», используемой малолетним К, 2001 года рождения, заведомо зная о недостижении им четырнадцатилетнего возраста, совершил с последним развратные действия без применения насилия, путем склонения к совершению действий сексуального характера [2].

В следственной практике также получили распространение случаи непривлечения к уголовной ответственности несовершеннолетних по причине обоснованных заблуждений последних относительно возраста потерпевших.

Так, следственным управлением Следственного комитета РФ по Саратовской области в 2015 г. вынесено постановление об отказе в возбуждении уголовного дела в отношении несовершеннолетнего А. 2000 года рождения по факту противоправных действий в отношении несовершеннолетней Б. 2003 г.р. По материалам следствия несовершеннолетний А. путем шантажа заставил малолетнюю Б. сделать фотографии интимного характера, после чего распространил их через социальные сети на сайт школы, а также требовал от нее услуг сексуального характера под угрозой размещения данных фотографий в социальных сетях. В действиях А. формально усматриваются признаки составов преступлений, предусмотренных ст. 133, 135, 137, 242, 242.1 и 242.2 Уголовного кодекса РФ, однако субъектом уголовной ответственности по ним является лицо, достигшее 16-летнего возраста, а по статье 135 Уголовного кодекса РФ лицо, достигшее 18-летнего возраста. Несмотря на то, что потерпевшая не достигла двенадцатилетнего возраста, несовершеннолетний А. не был привлечен к уголовной ответственности по п. «б» ч. 4 ст. 132 Уголовного кодекса РФ, так как он добросовестно заблуждался в возрасте Б., что подтвердилось осмотром интернет-страницы с персональными данными последней, где дата ее рождения указана как 02.07.2001 г.

Наибольшую общественную опасность представляют несовершеннолетние лица, которые целенаправленно и осознанно вступают в контакт с малолетними, не достигшими возраста двенадцати лет. Процесс ускоренной криминализации такой личности демонстрирует следующее высказывание одного из гостей интернет-форума, посвященного теме сексуальных отношений с малолетними: «Совершенно точно понял, что тянет к мальчикам, в 13 лет … Причем, как и у большинства тогда, ни Интернета, ни других источников информации у меня не было. От незнания поначалу было жутко… Ну а то, что я БЛ, я осознал, когда появился Интернет. И случилось это уже годам к 16…» [4].

Таких фигурантов относят к категории педофилов. Педофилия — это сексуальное предпочтение детям обычно препубертатного или раннего пубертатного возраста. Чаще всего в результате производства комплексных психолого-психиатрических экспертиз несовершеннолетним подозреваемым по анализируемому виду преступлений не выявляется наличие постоянной или доминирующей наклонности, необходимой для постановки соответствующего диагноза (F65.4 по МКБ-10).

Следует отметить, что срок наказания по п. «б» ч.4 ст. 132 Уголовного кодекса РФ уголовным законом установлен в пределах от 12 до 20 лет, что равноценно наказанию за реальное изнасилование или иные насильственные действия сексуального характера и намного суровее, чем за совершение убийства.

Основываясь на вышесказанном, следует отметить, что при расследовании уголовных дел в отношении несовершеннолетних, фактически совершивших действия, подпадающие под признаки преступления, предусмотренные ст. 135 Уголовного кодекса РФ, но при наличии к тому оснований (возраст потерпевшего), квалифицирующихся по п. «б» ч. 4 ст. 132 Уголовного кодекса РФ, во всех случаях следует принимать исчерпывающие меры для установления, к какой конкретно категории преступников относится подозреваемое лицо, доказывая всеми доступными следствию средствами факт осознания несовершеннолетним малолетнего возраста потерпевшего, в том числе и исходя из характера переписки.

В ходе расследования такого рода преступлений, учитывая их анонимность и удаленность в пространстве, следователи сталкиваются с препятствиями, успешное преодоление которых сопряжено с применением выработанных следственной практикой криминалистических тактик проведения конкретных следственных действий, а также криминалистических методик расследования данного типа преступлений.

В связи с тем, что, как правило, место совершения преступных действий в значительной степени удалено от места наступления последствий, следственная практика идет по пути возбуждения уголовного дела по месту выявления фактических признаков преступления, чаще всего по месту нахождения потерпевшего лица, и последующей передаче уголовного дела

в следственный орган по месту установления подозреваемого лица, что в том числе обусловливает длительный срок следствия по данной категории уголовных дел.

Однако наибольшую сложность для следователей при таком межрегиональном характере расследования представляет правильная своевременная и достаточная фиксация доказательств причастности конкретного несовершеннолетнего лица к совершению расследуемого преступления.

Принципиально важным на первоначальном этапе расследования является установление IP-адресов, с которых осуществлялся выход в сеть Интернет на страницу в социальной сети, либо с которого зарегистрирована страница, которая используется преступником, а также MAC-адреса (физический адрес) оконечного оборудования. С помощью IP-адресов необходимо установить, какой организации-провайдеру они принадлежат (данную информацию можно получить самостоятельно, к примеру, на сайте http://xinit.ru), истребовать в этой организации сведения о том, кому и на основании какого договора присвоены данные IP-адреса, о дате, времени выхода в сеть Интернет и др. (с приобщением копии договора и иной имеющейся документации). Затем на основании полученного в установленном порядке судебного решения необходимо произвести выемку информации, содержащей личную переписку подозреваемого лица, а также иного содержимого его аккаунта в социальной сети.

По MAC-адресу можно определить производителя сетевого оборудования. Изъяв впоследствии в ходе осмотра места происшествия или обыска роутер, ADSLмодем, персональный компьютер (ноутбук) или иное сетевое оборудование и имея сведения о MAC-адресе сетевого оборудования, при помощи которого осуществлялся доступ к сети Интернет, можно идентифицировать подозреваемого и место совершения им преступления, даже если искомые медиафайлы или переписка были им намеренно удалены и не подлежат восстановлению.

Кроме того, необходимо получить сведения о данных, указанных проверяемым лицом при регистрации аккаунта (номер телефона, электронная почта). По указанным идентификационным данным также на основании запросов и судебных решений (в случаях, предусмотренных законодательством) следует:

– произвести снятие информации с технических каналов связи сотовых компаний, с указанием сведений о принадлежности абонентского номера мобильного телефона, собеседниках, типах и направлениях вызова, дате, времени и длительности соединений, а также о присвоенных в период интернет-сессии (GPRS-сессии) IP-адресах и адресах посещенных интернет-узлов (данная информация позволит подтвердить выход с мобильного телефона на сайт социальной сети при помощи мобильного приложения или мобильного браузера и будет соответствовать IP-адресу, сообщенному администрацией сайта);

– получить данные о пользователях, зарегистрированных с использованием полученных идентификационных данных на страницах других социальных сетей, у администраторов которых также произвести изъятие информации о содержимом его аккаунта;

– произвести арест электронной корреспонденции с последующим ее осмотром и выемкой в порядке ст. 185 УПК РФ.

В целях фиксации размещенных на странице подозреваемого сведений, интересующих следствие, рекомендуется, не дожидаясь фактического изъятия информации у администратора сайта, производить ее осмотр с привлечением понятых. В ходе осмотра следует описывать все данные, содержащиеся на странице пользователя, обращая внимание на количество «подписчиков», «друзей», указанный «регион», «последнее посещение страницы пользователем», дату размещения фотоснимков и видеозаписей, «количество просмотров» фото- и видеоматериалов, размещенных на странице, количество «лайков». В обязательном порядке в ходе осмотра следует сохранять на отдельном носителе информации, прилагающимся к протоколу осмотра, снимки экрана монитора (скриншоты), что позволит избежать утраты доказательств в случае дальнейшего удаления аккаунта пользователем. Закрепление в протоколе осмотра указанных

обстоятельств может доказать факт распространения запрещенной информации неопределенному кругу лиц, выявить подлинную дату и время совершения преступления (в случае доказывания факта публикации, распространения фото- и видеоматериалов порнографического содержания).

Вышеуказанные мероприятия по сбору доказательств преступной деятельности несовершеннолетнего подозреваемого направлены на закрепления фактов склонностей и интересов несовершеннолетнего, в том числе и в сфере сексуальных отношений. Характерной чертой преступников данного типа является безразличие к последствиям собственных действий, умаление значимости (общественной опасности) совершаемых им действий и, как следствие, неспособность в должной мере контролировать свои интересы и желания. Указанные особенности приводят к множественности адресатов сексуальной активности несовершеннолетнего, к определенным формам сексуального взаимодействия со сверстниками, к общению на страницах различных форумов, а также сохранению на электронных носителях различного контента соответствующего содержания (аудио-, видеоинформация и фотоизображения). Несовершеннолетний педофил, как правило, даже при скудности обратной связи (в случае когда малолетний потерпевший не поддерживает активную переписку и не проявляет очевидный интерес к сексуальной теме) продолжает периодически направлять ему сообщения соответствующего содержания. Очевидно, что данные неосмотрительные действия делают такого преступника уязвимым для следственных органов.

Подросток также не заботится о сокрытии виртуальных следов своих преступлений, что в значительной мере облегчает получение и закрепление доказательств его преступной деятельности.

В связи с этим следующим этапом закрепления доказательственной базы должен стать обыск в квартире, откуда несовершеннолетний осуществляет свою преступную деятельность.

При подготовке к производству обыска, учитывая, что целью данного следственного действия является в большей степени обнаружение и изъятие цифровой и компьютерной техники, следует привлечь специалистов. Помимо специалиста, обладающего знаниями в области информационных технологий, целесообразно также привлечь эксперта-криминалиста с целью обнаружения и изъятия на цифровой и компьютерной технике следов папиллярных узоров рук. Совпадение отпечатков пальцев с предполагаемым преступником косвенным образом подтвердит имеющиеся в отношении него подозрения в совершении преступления. Более того, факт принадлежности и фактическом пользователе конкретного технического средства целесообразно выяснять в период проведения обыска с занесением в протокол данных в ходе данного следственного действия пояснений участвующих лиц.

В следственной практике представлены факты совершения актов мастурбации преступником непосредственно за рабочим местом возле компьютера. Поэтому необходимо в ходе обыска также обследовать рабочий стол, стул (кресло), за которыми обычно сидит проверяемое лицо за компьютером, клавиатуру, пол, ковер, мусорное ведро, шторы и прочее на предмет обнаружения следов спермы и последующего их изъятия, с целью в том числе проведения сравнительной молекулярно-генетической экспертизы для установления тождества.

При производстве обыска целесообразно обнаружить и фактически изъять с участием специалиста все компьютеры и иные устройства, имеющие выход в Интернет, которыми мог пользоваться преступник, а также все цифровые накопители (флэш-карты, карты памяти, диски, SIM-карты и пр.). При обнаружении мобильного телефона подозреваемого следователю необходимо произвести фиксацию в протоколе следственного действия и фотофиксацию места расположения телефона, произвести описание его повреждений, информационного табло, всех слотов, модели, IMEI и других сведений о телефоне, а также всех внешних источников (SIM-карты, карты памяти), батареи, чехла. Прежде чем выключить телефон, необходимо просмотреть и зафиксировать последние контакты, перевести телефон в авиарежим

(авторежим), исключив сетевую активность и выяснить, синхронизирован ли аппарат с компьютером пользователя. Далее необходимо выключить-включить телефон и убедиться, отсутствует ли пароль на включение-активацию. В случае наличия пароля, ПИН-кода выяснить его у владельца и занести в протокол [4, с. 213-216].

Обнаруженные и изъятые предметы (содержимое памяти устройств), а также полученное в ходе выемок содержимое аккаунтов подозреваемого в ходе дальнейшего расследования становится объектом компьютерно-технической судебной экспертизы, а также комплексной судебной психолого-лингвистической (по переписке и предположительно порнографическим материалам).

Список литературы

1. Плюгина И.О., Фомин С.А. Использование социальных сетей как способ совершения развратных действий в отношении лиц, не достигших 16 лет // Криминалистика и судебно-экспертная деятельность в условиях современности: материалы II Всероссийской научно-практической конференции. Краснодар, 2014. С. 412-414.

2. Методические рекомендации по расследованию преступлений против половой неприкосновенности несовершеннолетних, совершенных посредством глобальной сети «Интернет» / под ред. и.о. ректора ФГКОУ ВО «Академия Следственного комитета Российской Федерации» к.ю.н. А.М. Багмета. М.: Академия Следственного комитета Российской Федерации, 2016.

3. Holmes, Ronald M., Stephen T. Holmes. Current perspectives on sex crimes (неопр.). SAGE, 2002. С. 165.

4. Интернет-страница «Мониторинговый центр по выявлению опасного и запрещенного законодательством контента». URL: http://www.pedofilov.net/news/ (дата обращения: 28.06.2020).

5. Технико-криминалистическое сопровождение расследования преступлений: учебное пособие / под ред. канд. юрид. наук А.М. Багмета. М.: Юрлитинформ, 2016. 256 с.

Е.Е. Космодемьянская, *к.ю.н., доцент кафедры криминалистики Сибирского юридического института МВД России, доцент кафедры уголовного процесса и криминалистики Юридического института СФУ, г. Красноярск*

Е.А. Межинский, *слушатель Сибирского юридического института МВД России, г. Красноярск*

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ КОРЫСТНО-НАСИЛЬСТВЕННЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В УСЛОВИЯХ НЕОЧЕВИДНОСТИ

Как показало изучение статистических данных, в 2019 г. на территории России было зарегистрировано 2024,3 тыс. преступлений. При этом более половины всех зарегистрированных преступлений (53,5%) составляют хищения чужого имущества, совершенные путем грабежа — 45,8 тыс., разбоя — 6,7 тыс. Статистика на текущее время показывает, что каждый двадцать пятый грабеж (3,9%), каждое девятое разбойное нападение (11,4%) были сопряжены с незаконным проникновением в жилище, помещение или иное хранилище. Зарегистрировано 404,6 тыс. преступлений, совершенных на улицах, площадях, в парках и скверах, в том числе 19,4 тыс. грабежей, 2,3 тыс. разбойных нападений. Не раскрыто 915,2 тыс. преступлений, что на 6,4%

больше показателя 2018 г. Из этого количества на долю тяжких и особо тяжких преступлений приходится 26,9% (2018 г. — 23,1%). Остались нераскрытыми 13,6 тыс. грабежей, 1116 разбойных нападений. 895 тыс. преступлений (+6,6%) остались нераскрытыми в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого[4].

В Красноярском крае в 2019 г. было зарегистрировано 46 530 преступлений, из них 862 грабежа, 160 разбойных нападений[5]. Анализ данных показателей в сравнении с показателями 2018 г. позволяет сделать вывод, что количество совершенных грабежей и разбоев имеет тенденцию к небольшому снижению, однако тяжесть этих общественных деяний в каждом конкретном случае выше, чем было еще несколько лет назад. При этом происходит увеличение количества нераскрытых преступлений анализируемого вида, что свидетельствует о несомненной актуальности проблематики исследования и ее практической востребованности.

Ранее нами уже проводились исследования в аспекте изучения как традиционных средств поиска преступников, совершивших данные виды преступлений, так и нетрадиционных поисковых средств [4].

Как показал анализ судебно-следственной практики, в качестве первых наиболее часто выступают следующие мероприятия: постановка на розыскной учет похищенных и изъятых предметов (на учет ставятся только номерные вещи); ориентирование негласных сотрудников оперативного подразделения на установление контактов с лицами, которые могут располагать интересующей информацией; распространение информации по отделам, обслуживающим близлежащие сопряженные территории (нередки случаи, когда в соседних районных отделах полиции имеется информация о подобном нераскрытом преступлении, схожих приметах по описанию словесного портрета, аналогичном способе совершения преступления); проверка лиц, ранее совершавших преступления данной категории (в первую очередь тех, кто проживает в районе совершения преступления, работает в непосредственной близости или чей путь от дома до работы и обратно пролегает через данный район). Этот способ установления преступника вполне обоснован, поскольку и статистические данные показывают, что «каждое второе (58,7%) расследованное преступление совершено лицами, ранее совершавшими преступления»[6]; проверка следов пальцев рук (если данные следы были обнаружены и изъяты с места происшествия) по системе «Папиллон»; установление контроля за местами возможного сбыта похищенного имущества (это могут быть стихийные вещевые рынки, ювелирные мастерские, комиссионные магазины, ломбарды, коммерческие структуры, специализирующиеся на купле-продаже имущества той категории, под которую попадает похищенное, антикварные магазины, ремонтные мастерские, принимающие лом определенной категории и т.д.). Кроме того, приезжие преступники, именуемые «гастролерами», как правило, сбывают похищенное имущество за пределами района совершения преступления, в других городах и регионах России.

Однако бывают случаи, когда похищенным имуществом являются весьма специфичные вещи, стоимость которых сможет определить лишь специалист (картины, статуэтки и т.д.), а также негромоздкие вещи, которые легко могут быть размещены на теле человека (часы, перстни, иные штучные ювелирные изделия). В таких случаях велика вероятность попытки вывоза похищенного за границу Российской Федерации и последующего сбыта на территориях иных государств. Для перекрытия потенциальных заграничных маршрутов на поиск и идентификацию похищенного имущества ориентируются службы контроля аэропортов, транспортная полиция и пограничная служба ФСБ России.

В целом, традиционные способы решения тактической задачи по поиску преступника, совершившего корыстно-насильственное преступление в условиях неочевидности, достаточно полно раскрыты отечественными учеными-криминалистами [3, 5]. Однако современные

[4] URL: https://мвд.рф/reports/ item/19007735 (дата обращения: 31.05.2020).
[5] URL: https://24.мвд.рф/slujba/Statistika_i_ analitika (дата обращения: 30.05.2020).
[6] URL: https://мвд.рф/reports/ item/19007735 (дата обращения: 31.05.2020).

тенденции нашего общества, безусловно, заставляют всех участников практически любых общественных отношений двигаться в ногу со временем. В условиях постоянно растущего технического прогресса и быстро сменяющих друг друга моделей человеческого поведения в той или иной ситуации, правоохранительным органам не остается ничего, кроме как «догонять» «преступный мир» в плане модернизации. Поэтому помимо контроля за традиционными местами возможного сбыта имущества, нажитого преступным путем, в настоящее время становятся актуальными следующие средства:

– мониторинг сетевых досок частных объявлений («Авито», «Юла» и т.д.). Примером может послужить объявление частного физического лица на популярной доске частных объявлений «Авито», в котором заявлено о продаже лома золотых изделий 585 пробы за 72 тыс. 108 рублей. В ходе осуществления проверочных мероприятий при анализе данного объявления было выявлено, что никаких подтверждающих документов на золотые изделия у продавца нет, в Восточно-Сибирской государственной инспекции пробирного надзора Красноярского края он на учете не состоит, объявление о продаже лома золота находится в одном ряду с его объявлением о продаже автомобильных шин. Безусловно, совокупность этих факторов не является подтверждением незаконного оборота драгоценных металлов и не подтверждает незаконный характер приобретения этих золотых изделий, но это подтверждает, что сбыт похищенного имущества таким способом возможен и эту площадку оперативным сотрудникам необходимо мониторить;

– мониторинг аукциона «AU24.ru»;

– мониторинг администраторов сетевых городских барахолок («Бесплатный Красноярск», «Отдам даром», «Обмен Красноярск» и т.д.);

– мониторинг даркнет-площадок (вход через браузер TOR) (пример: onion-shop — торговая площадка по купле-продаже запрещенных к обороту и ограниченных в обороте в Российской Федерации предметов, а также краденого имущества или реализация имущества, приобретенного за счет похищенных денежных средств, т.е. придание легального вида денежным средствам, добытым преступным путем).

Кроме указанного можно рекомендовать использовать данные о так называемых «очагах» совершения грабежей и разбоев на определенной территории. Идея об использовании этих данных в поисковых целях была высказана много лет назад отечественными учеными-криминалистами [6]. Есть и более поздние разработки этой проблематики [1], позже эта идея легла в основу изучения очагов грабежей и разбойных нападений [3]. Ю.П. Аленин брал за основу работу ученых ГДР, под «очагом» понимающих совокупность преступлений, совершенных преимущественно на определенной территории (город, поселок, район города, жилой массив и т.п.) в конкретный период времени, относящихся к одному виду или группе и предположительно одним и тем же преступником или одной и той же группой преступников. Определяя понятие «очаг преступлений», криминалисты ГДР обозначали его словом «Brennpunkt», что в переводе на русский язык значит «горящая точка» [2]. В отечественной криминалистике существуют такие понятия, как серия, концентрация, скопление однотипных или однородных преступлений, совершенных на одной территории. Для разграничения данных терминов с определением «очага» преступления необходимо указать, что понятие «совокупность преступлений» является более широким, нежели «очаг» [2]. Среди признаков «очага» называют следующие: а) совокупность однородных или однотипных преступлений, б) совершенных на определенной территории, в) за определенный промежуток времени; г) относящихся к одной группе или к одному виду; д) есть предположение, что преступления совершает один и тот же человек или одна преступная группа. То сеть между преступлениями должны присутствовать материально-следовая и территориально-временная связи.

Нами было проведено аналитическое исследование приговоров по грабежам и разбойным нападениям, вынесенных в периоды 2017-2018 и 2018-2019 гг. судами общей юрисдикции г. Красноярска (всего было проанализировано порядка 100 приговоров судов). По результатам

анализа было составлено две карты «очагов» грабежей и разбойных нападений по всем районам города [23-24].

Каждый район имеет свой цвет, а два вида преступления — обозначение (звезда — грабеж, крест — разбойное нападение). Как видно, в каждом из районов г. Красноярска имеется локализация (конкретные улицы) с преобладанием количества изучаемого вида преступлений. Формат документа и масштаб города, к сожалению, не позволяют детально просмотреть каждую улицу города, однако одним из авторов была разработана интерактивная карта, на которой можно посмотреть не только конкретный адрес совершения преступления, но и получить информацию о конкретном приговоре и номере уголовного дела [25].

После анализа вынесенных приговоров стало заметно, что видов и способов совершения грабежей и разбойных нападений не так много, все они типичны, но все же имеют отличительные черты. К примеру, в 2019 г. резко возросли грабежи и разбойные нападения на обыкновенные продуктовые магазины и павильоны, где добычей преступников становились собственно продукты питания и алкогольные напитки. Стоит отметить, что было зарегистрировано несколько случаев нападения на курьеров компаний по доставке еды, где целью была именно еда, а не денежные средства.

Целью второго этапа исследования стало изучение динамики или «дрейфа очагов». Рассматривая динамическое изменение, отмечается, что один из «очагов» преступлений, находящийся в мкр. Солнечный Советского района г. Красноярска, сместился вниз по проспекту 60 Лет Образования СССР [7]. «Очаг» на станции «Красноярск-Северный» сместился вверх по улице 9 Мая и был зарегистрирован около ТРЦ «Комсомольский» [8]. В 2019 г., судя по статистике, был ликвидирован «очаг» в районе ТРЦ «Планета» — там зарегистрирован один грабеж [9]. Говоря о стабильных «очагах» в Советском районе г. Красноярска, стоит отметить местность в районе пересечений улиц Аэровокзальная, Взлетная, Молокова и Партизана Железняка. Данный участок местности представляет собой четырехугольник, внутри и по краям которого на протяжении двух лет стабильно совершаются грабежи и разбойные нападения на жителей города [9]. «Очаг», находившийся по левую сторону проспекта Металлургов, сместился в сторону набережной р. Енисей и теперь находится справа от проспекта, стягиваясь к парку «Гвардейский» [10]. Подводя итог анализа по Советскому району, можно отметить, что в нем зарегистрировано больше преступлений, чем во всех остальных, что находится, конечно же, в прямой зависимости от его территориальных размеров — Советский район — самое крупное муниципальное образование г. Красноярска. Зоной относительной безопасности, в которой не зарегистрировано ни одно из рассматриваемых преступлений, является район ул. Авиаторов ближе к МВДЦ «Сибирь». Зоной абсолютной безопасности в Советском районе стал остров Татышев.

Двигаясь «по часовой стрелке» на карте, переходим в Ленинский район. Достаточно крупным в 2018 г. был «очаг» грабежей и разбойных нападений в районе ТРЦ «МЕГА». В 2019 г. данный «очаг» перестал концентрироваться практически в одной точке и «расплылся» в разные стороны [11]. В 2019 г. на территории Ленинского района было совершено больше грабежей, чем разбойных нападений, и все они разместились вдоль улиц Волжская, Говорова, Тамбовская, которые последовательно переходят одна в другую [12]. Если говорить о ситуации в Ленинском районе в целом, то в 2019 г. сразу же заметен рост грабежей по сравнению с 2018 г.

В Кировском районе г. Красноярска крупным «очагом» в 2018 г. являлся район около одного из гастрономов «Красный Яр» по проспекту имени газеты Красноярский Рабочий. В 2019 г. данный «очаг» не только сохранился, но и существенно вырос в своих размерах [13]. Обратная ситуация прослеживается на участке местности между улицей Грунтовой и улицей Щорса — напротив, уменьшение «очага» в объеме и меньшее количество зарегистрированных преступлений [14]. В целом, в Кировском районе г. Красноярска в 2019 г. произошло больше преступлений, нежели в предыдущем, и, соответственно, руководителями районного отдела

полиции наверняка уже приняты меры, направленные на улучшение ситуации на ответственном участке.

Следующим «по часовой стрелке» на карте города Красноярска является Свердловский район. Полностью ликвидирован «очаг» насильственных корыстных преступлений вблизи Николаевского моста [15]. Около кольцевого движения на съезде с Коммунального моста «очаг» преступлений сместился левее кольца [16]. Как видим, статистика 2018 г. существенно изменилась в лучшую сторону для жителей данного муниципального образования — отмечается снижение регистрации грабежей и разбойных нападений, что скорее всего напрямую зависит от улучшения качества работы сотрудников районного отдела полиции.

В Октябрьском районе города Красноярска статистика показывает прогрессивный рост корыстно-насильственных преступлений. Отчетливо видно, как в 2019 г. разросся «очаг» от ул. Высотная, дойдя до самых крайних границ Железнодорожного района [17]. Ситуация могла быть вызвана как собственным ростом преступности в муниципальном образовании, так и дрейфом «очага» из Железнодорожного района в Октябрьский.

В Железнодорожном районе в 2019 г. был уменьшен «очаг» преступлений по правую сторону от проспекта Свободный [18]. По району в целом отмечается увеличение регистрации сообщений о грабежах и практически полное отсутствие регистрации сообщений о разбойных нападениях [19].

Заключительная территория исследования — это Центральный район города Красноярска. Как это было всегда, в Центральном районе статистика преступности всегда ниже, чем в других районах города. Высокая концентрация зданий органов государственной власти, власти субъекта, городских властей — одна из самых весомых причин этого явления. Однако в 2019 г., по сравнению с предыдущим, ситуация относительно грабежей и разбойных нападений сильно ухудшилась. Небольшая территориальная величина района и относительно низкая концентрация преступлений позволяет рассмотреть динамические изменения по району в целом [20].

Изучив криминогенную ситуацию в Центральном районе и зная общие тенденции по Российской Федерации, можно с уверенностью предполагать, что практически в любом городе нашей страны в его «главном» районе всегда будет меньше преступлений, нежели в других. Значение изучения очагов данных преступлений заключается в том, что «своевременное их распознавание позволяет установить наблюдение в местах вероятного совершения преступления» [21]. Кроме того, определение очага преступления позволяет изучить соотношение между местом совершения преступления и местом жительства потенциальных подозреваемых, определив таким образом круг их поиска, что задает перспективу дальнейшим исследованиям в данном направлении.

Подобное визуальное представление информации поможет правоохранительным органам составлять маршруты патрулирования города, выставлять наряды наблюдения в эпицентры «очагов» преступлений, что свидетельствует о несомненной практической значимости результатов исследования. При условии своевременного пополнения информацией данная карта может стать системной программой, помогающей отследить смещение «очага» конкретного преступления, а также выявить «дрейфующие очаги», которые характеризуются постоянными циклическими перемещениями по одному, по нескольким районам или по городу в целом. Кроме указанного, значение изучения очагов данных преступлений заключается в том, что своевременное их распознавание позволяет установить наблюдение в местах вероятного совершения преступления, то есть своевременно и качественно решать еще одну из тактических задач расследования корыстно-насильственных преступлений — осуществлять их профилактику.

Предлагаемые средства предупреждения, выявления и раскрытия преступлений на примере грабежей и разбойных нападений могут быть использованы в практической деятельности сотрудников правоохранительных органов, поскольку являются целесообразными, доступными в использовании, что может способствовать повышению результативности деятель-

ности по защите жизни, здоровья, имущества граждан в частности, и обеспечения национальной безопасности в целом.

Список литературы

1. Аленин Ю.П. Выявление и расследование очагов преступлений: теория и практика. Одесса: Юрид. ин-т ОГУ, 1996.
2. Аленин Ю.П. Очаги преступлений — самостоятельный объект методики расследования // Криминалистика и судебная экспертиза. Вып. 40. Киев, 1990.
3. Космодемьянская Е.Е. Поиск лиц, совершивших грабежи и разбойные нападения в условиях неочевидности: учебное пособие. Красноярск, 2003.
4. Космодемьянская Е.Е., Межинский Е.А. К вопросу о традиционных и нетрадиционных средствах раскрытия и расследования корыстно-насильственных преступлений // Вестник Сибирского юридического института МВД России. 2020. № 1 (38). С. 99-103.
5. Курс криминалистики. Особенная часть. Т. 1. Методики расследования насильственных и корыстно-насильственных преступлений / отв. ред. В.Е. Корноухов. М., 2001.
6. Постика И.В. Выявление и расследование очага преступления. Одесса, 1981.
7. «Рисунок 2.8. Метки в мкр. Солнечный, 2018 год», «Рисунок 2.9. Метки в мкр. Солнечный 2019 год».
8. «Рисунок 2.10. «Очаг» на станции «Красноярск — Северный» в 2018 году», «Рисунок 2.11. Смещение «очага» к ТРЦ «Комсомольский в 2019 году».
9. «Рисунок 2.12. «Очаг» на ТРЦ «Планета» в 2018 году», «Рисунок 2.13. Ситуация около ТРЦ «Планета» в 2019 году».
10. «Рисунок 2.14. «Очаг в районе «Взлетка — Партизана Железняка в 2018 году», «Рисунок 2.15. «Очаг в районе «Взлетка — Партизана Железняка в 2019 году».
11. «Рисунок 2.16. «Очаг» слева от пр. Металлургов в 2018 году», «Рисунок 2.17. «Очаг» справа от пр. Металлургов в 2019 году».
12. «Рисунок 2.18. «Очаг» около ТРЦ «Мега» в 2018 году», «Рисунок 2.18. «Очаг» около ТРЦ «Мега» в 2018 году».
13. «Рисунок 2.20. «Очаг» в 2018 году», «Рисунок 2.21. Смещение «очага» в 2019 году».
14. «Рисунок 2.22. «Очаг» вблизи гастронома в 2018 году», «Рисунок 2.23. «Очаг» вблизи гастронома в 2019 году».
15. «Рисунок 2.24. Ситуация вокруг ул. Щорса в 2018 году», «Рисунок 2.25. Ситуация вокруг ул. Щорса в 2019 году».
16. «Рисунок 2.26. «Очаг» в 2018 году», «Рисунок 2.27. Ликвидированный «Очаг» в 2019 году».
17. «Рисунок 2.28. «Очаг» около кольца в 2018 году», «Рисунок 2.29. Смещение «Очага» около кольца в 2019 году».
18. «Рисунок 2.30. «Очаг» на ул. Высотная в 2018 году», «Рисунок 2.31. «Очаг» на ул. Высотная в 2019 году».
19. «Рисунок 2.32. 2018 год», «Рисунок 2.33. 2019 год».
20. «Рисунок 2.34. Разбои в 2018 году», «Рисунок 2.35. Грабежи в 2018 году».
21. «Рис. 2.36. Центральный р-н, 2018 г.» «Рис. 2.37. Центральный р-н, 2019 г.».
22. «Рис. 2.36. Центральный р-н, 2018 г.» «Рис. 2.37. Центральный р-н, 2019 г.».
23. «Рисунок 2.5. Общая карта «очагов» грабежей и разбойных нападений, совершенных на территории г. Красноярска за 2018 год».
24. «Рисунок 2.7. Общая карта «очагов» грабежей и разбойных нападений, совершенных на территории г. Красноярска за 2019 год».
25. «Рисунок 2.7. Описание метки с содержанием реквизитов приговора».

А.А. Кузнецов, *к.ю.н., профессор кафедры криминалистики Омской академии МВД России, г. Омск*
Р.А. Макаров, *начальник отдела по расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий следственного управления Управления Министерства внутренних дел Российской Федерации по городу Кургану, г. Курган*

ОСНОВНЫЕ ЭЛЕМЕНТЫ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ХИЩЕНИЙ, СОВЕРШЕННЫХ ДИСТАНЦИОННО С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ

В методике расследования отдельных видов преступлений проблематика понятия и содержания криминалистической характеристики традиционно привлекает внимание криминалистов. Несмотря на продолжающуюся полемику о необходимости ее существования, большинство специалистов сходятся в том, что ее содержание имеет как теоретическое значение так и практическую составляющую ее применения [2]. Значение криминалистической характеристики преступлений состоит прежде всего в том, что на первоначальном этапе расследования преступлений, когда в большинстве случаев существует дефицит исходной информации, за счет устойчивых корреляционных связей между ее отдельными элементами она позволяет выдвинуть обоснованные версии относительно неустановленных обстоятельств [3].

Не вдаваясь в дискуссию по вопросу понятия, в основном придерживаемся мнения А.Г. Филиппова о криминалистической характеристики [6, с. 92], поскольку оно, на наш взгляд, лаконично и максимально отражает сущность данной криминалистической категории. В то же время для понимания существа вопроса обратимся к уже высказанному в этом отношении своего мнения. Криминалистическая характеристика преступления представляет собой систему сведений (информации, данных), проявляющихся при совершении преступлений того или иного вида и имеющих наибольшее значение при выборе применяемых для их раскрытия и расследования криминалистических средств, приемов и методов [1, с. 9]. При этом следует исходить из того, что система сведений проявляется в конкретных элементах криминалистической характеристики, соответственно, в зависимости от вида совершенного преступления количество таких элементов и их значение для методики расследования может быть различным.

Применительно к хищениям, совершенных дистанционно, с использованием средств сотовой связи криминалистическая характеристика может представлять следующую структуру:

– исходную информацию о совершенном преступлении;
– сведения о предмете преступного посягательства;
– сведения о способе совершения преступления (деятельность по подготовке, непосредственному совершению преступления, а также сокрытию его следов);
– сведения о личности преступника;
– сведения о личности потерпевшего.

Представляется, что именно такое сочетание элементов криминалистической характеристики позволяет говорить о основных направлениях расследования дел данной категории, а именно способствует выдвижению типичных версий о характере совершенного преступления, о местах возможного обнаружения следов преступления, о лице (или о группе лиц), участвующих в совершении мошенничества. Зная типичные способы совершения преступления, мы может также предпринять необходимые меры по профилактической деятельности следователя, направленной на устранение причин и условий способствующих данному виду преступлений. В то же время анализ практики свидетельствует, что каждый из названных элементов криминалистической характеристики находится в неразрывной связи друг с другом и основные из них определяют содержание остальных. Поэтому совершенно правы Л.Я. Драпкин,

В.Н. Карагодин, отмечая, что если получена информация об одном из обстоятельств, имеющих значение для дела, то это дает возможность эффективно перебросить версионный информационный мостик к другому, еще не известному обстоятельству [4, с. 351].

Характерной особенностью хищений, совершенных дистанционно с использованием средств сотовой связи, является единая схема, которую используют преступники: на мобильный телефон пострадавшего с незнакомого ему номера поступает телефонный звонок (СМС-сообщение) о том, что его банковская карта заблокирована, либо с банковской карты осуществляется несанкционированная транзакция. Преступник представляется сотрудником банка либо иной организации и, используя соответствующую терминологию, сообщает пострадавшему, что для предотвращения несанкционированных действий, необходимо провести ряд операций, для выполнения которых необходимо сообщить номер банковской карты, дату ее выпуска, срок действия и код с оборотной стороны, а затем сообщить пароль, который поступит в СМС-сообщении, либо проследовать к ближайшему банкомату и выполнить ряд операций для предотвращения несанкционированных действий. Далее пострадавший, действуя указаниям так называемого «сотрудника банка», не подозревая о факте противоправных действий в отношении него, выполняет все действия, о которых ему говорит преступник. В результате пострадавший сам переводит свои денежные средства с лицевого счета своей банковской карты на лицевые счета, подконтрольные преступнику, либо сообщая реквизиты банковской карты и пароли, предоставляет преступнику полный доступ к своим счетам с возможностью подключения услуг «Мобильный банк», «Автоплатеж» на мобильные номера, подконтрольные преступнику.

Такая схема является наиболее распространенной среди хищений, совершаемых дистанционно с использованием средств сотовой связи в Уральском федеральном округе [5]. Анализируя практику расследования дел данной категории, мы приходим к выводу, что наиболее информативными с точки зрения получения доказательственной информации являются следующие элементы криминалистической характеристики:

– сведения о способе преступления (подготовка, совершение, сокрытие преступления);

– сведения о личности потерпевшего;

– сведения о личности преступника (прежде всего имеется поведение таких лиц до, во время и после совершения преступления).

Иные элементы также могут содержать существенные особенности и особенно важны на этапе предварительной (доследственной) проверки материала или на первоначальном этапе расследования, но при условии, если в данный момент информация о названных выше элементах криминалистической характеристики имеется у следователя или оперативного сотрудника.

Поэтому в первую очередь следователя интересует вопрос о том, как действовал преступник и почему выбрал именно данный способ преступления. При анализе материалов расследования дел данной категории можно выделить следующие наиболее распространенные способы хищений, совершаемые дистанционно с использованием средств сотовой связи:

– «Ваш сын попал в ДТП», либо «Ваш сын задержан с наркотическими средствами», либо «Ваш сын стал участником драки, потасовки». От преступника поступает звонок на мобильное устройство пострадавшей стороны. Преступник представляется сотрудником правоохранительных органов (Министерства внутренних дел, Следственного комитета, Прокуратуры, Федеральной службы безопасности), оповещает пострадавшего о негативных обстоятельствах, которые произошли с его родственником, для убедительности передает трубку якобы сыну. Затем преступник предлагает решить вопрос о прекращении всяких

разбирательств за материальное вознаграждение, при этом указывает номера счетов, на которые необходимо перечислить денежные средства, в качестве оплат «решения проблемы».

– Звонки от имени начальника, родственников либо иных знакомых. От преступника на мобильное устройство пострадавшего поступает СМС-сообщение либо телефонный звонок, где преступник представляется родственником, начальником, либо иным знакомым и под надуманным предлогом просит пострадавшего оказать материальное содействие в виде перевода небольшой суммы на предоставляемые лицевые счета банковских карт либо абонентских номеров сотовой связи.

– Выигрыш в лотерею. Механизм совершения аналогичен предыдущему, отличие в легенде, под которой совершается преступление (выигрыш), при этом преступник убеждает пострадавшего о необходимости оплаты несуществующих налогов, услуг доставки и т.п. для получения выигрыша, предоставляя соответствующие счета для оплаты.

– Компенсация за некачественные лекарства, товары услуги, которые ранее были предоставлены. Механизм совершения аналогичен предыдущему, отличие в легенде, под которой совершается преступление (компенсация), при этом преступник убеждает пострадавшего о необходимости оплаты несуществующих налогов, услуг доставки и т.п. для получения компенсации, предоставляя соответствующие счета для оплаты.

– Звонки от имени операторов сотовой связи. Представляясь оператором связи, преступник оповещает пострадавшего о проблемах технического характера (сбои мобильной связи) и убеждает выполнить определенные манипуляции (ввести комбинации цифр) с мобильным устройством, в результате которых с лицевого счета абонентского номера либо банковской карты пострадавшего происходит списание денежных средств.

– Покупка товаров через сеть Интернет. В сети Интернет на соответствующих сайтах продаж товаров и услуг размещаются объявления, злоумышленники указывают номера абонентских телефонов для связи. Не подозревающий о преступных намерениях покупатель связывается с так называемым продавцом (преступником), где пострадавшей стороне предлагают приобрести товар либо услугу по очень выгодной цене. Далее события могут разворачиваться по нескольким сценариям. Первый вариант: введенный в заблуждение покупатель относительно добросовестности намерений так называемого продавца переводит денежные средства на счета, предоставленные преступником, при этом чаще всего продаваемые товар или услуга не существуют. После чего средства связи (абонентские номера), которые были использованы преступником, блокируются, объявление удаляется. Второй вариант: так называемый продавец убеждает свою жертву, что его организация либо он сам работают только по безналичному расчету и для оплаты покупателю необходимо сказать номер своей банковской карты. Далее,преступник сообщает, что покупателю на мобильное устройство поступит СМС-сообщение (цифровой пароль) содержание которого необходимо также сообщить. При этом необходимо отметить, что в таком СМС-сообщении указывается, что цифровой пароль не подлежит огласке, в том числе и сотрудникам банка. После получения всей необходимой информации, преступник похищает (переводит) все имеющиеся на лицевом счете банковской карты пострадавшего денежные средства.

Подготовительные действия мошенников заключаются в приискании (приобретении) мобильных устройств связи (сотовых телефонов), сим-карт, банковских карт, компьютерных устройств (ноутбук, нетбук и т.п.), устройств обеспечивающих доступ к сети Интернет (модемы, вай-фай-роутеры и т.п.), в изучении информации о тарифных планах и специальных предложениях операторов сотовой связи, а также информации о возможностях, которые предоставляют банковские учреждения по безналичным оплатам, по переводам денежных средств с лицевых счетов банковских карт при помощи мобильной связи и т.п. Следует подчеркнуть, что сим-карты и банковские карты приобретаются преступниками через сеть

Интернет, без составления соответствующих документов, которые зачастую оформлены на имена несуществующих, либо третьих лиц. На этапе подготовки к совершению преступления преступники активно применяют меры к его сокрытию: приобретают сим-карты, оформленные на несуществующих лиц, либо приобретают банковские карты, оформленные на имена третьих лиц.

Современное мобильное устройство (сотовый телефон), имеющее доступ в сеть Интернет, позволяет одним нажатием соответствующей клавиши осуществить рассылку 100 СМС-сообщений и более так называемым «веерным» способом, то есть в параметры отправки СМС-сообщений мобильного устройства вводятся значения емкостей абонентских номеров сотовой связи, методом последовательного «перебора» последних 2, 3-х цифр абонентских номеров сотовой связи (в зависимости от количества номерных емкостей на которые отправляются СМС-сообщения), например: 89XXXXXX**18**, 891XXXXXX**19**, 891XXXXXX**20**, и т.д. При этом необходимо отметить, что преступник, который находится в городе Кургане, исходя из анализа уголовных дел, не будет совершать хищения в отношении жителей своего региона, а выберет своими жертвами жителей более отдаленного субъекта Российской Федерации. Кроме того, необходимо также отметить, что в момент совершения преступления (рассылка СМС-сообщений, дача мошеннических указаний) преступники могут передвигаются на автотранспорте из одного района города в другой, либо пересекая границы различных муниципальных образований. Также зачастую с одного абонентского номера (мобильного устройства) осуществляется рассылка СМС-сообщений, при этом для уточнения информации в СМС-сообщении указывается другой абонентский номер, сим-карта которого находится в ином мобильном устройстве. Таким образом, на этапе непосредственного совершения преступления, преступниками также предпринимаются меры к сокрытию преступления — совершение преступлений в отношении жителей других регионов России, что ведет к длительности проведения доследственных проверок, предшествующих возбуждению уголовного дела.

Кроме того, сам факт передвижения преступника в момент совершения преступления приводит к разногласиям между ОВД при установлении места совершения преступления (расположение базовых станций операторов сотовой связи, которыми регистрируются соединения сотовой связи преступника и потерпевшего в момент преступного деяния, места снятия денежных средств), что также значительно увеличивает длительность проведения проверок.

Как правило, мобильные устройства (сотовые телефоны) и сим-карты при совершении преступных действий используются в течение нескольких часов, после чего уничтожаются с целью сокрытия следов преступления.

Более длительное время хранятся компьютерные устройства (ноутбуки, нетбуки, планшеты и т.п.), однако информация в указанных устройствах тщательно маскируется либо удаляется и восстановить ее впоследствии очень сложно.

Не менее важно получить данные о лице, пострадавшем от преступных намерений злоумышленников. Сведения о таких лицах особенно важны при выработке версий и определения направлений профилактической деятельности следователя. Итак, наиболее часто совершаются рассматриваемые преступления в отношении следующей категории лиц:

– женщины в возрасте от 35 лет до 50 лет, имеющие среднюю заработную плату, работающие, как правило, в бюджетной сфере, которые являются держателями зарплатных либо кредитных карт, законопослушные граждане;

– пожилые граждане различного пола (лица пенсионного возраста), которые являются держателями банковских карт;

– иные лица, которые в силу внушаемости или особой подозрительности легко становятся объектами воздействия мошенников.

Все указанные категории лиц в той или иной степени обладают следующим набором личностных характеристик: внушаемость, отсутствие самоконтроля, доверчивость, наивность, инфантилизм, слабая нервная система, сострадание, любопытство, любознательность, отсутствие «трезвого» мышления анализа, критичности и осмотрительности.

Не менее важным элементом криминалистической характеристики являются сведения о личности преступника. Установлено, что 30% подозреваемых, обвиняемых, привлекаемых к уголовной ответственности за совершение хищений, совершенных дистанционно, с использованием средств сотовой связи – это лица, ранее несудимые, возраст от 25 лет до 40 лет. В остальных случаях это:

– лица, ранее судимые за различные виды мошенничеств, в том числе за аналогичные;

– лица, совершившие либо ранее совершавшие преступления указанной категории;

– лица, которые являются родственниками, знакомыми ранее судимых;

– лица, ранее отбывавшие наказания совместно с ранее судимыми за аналогичные преступления;

– лица, ранее несудимые, узнавшие о способе совершения преступления через СМИ либо локальную сеть Интернет.

У преступников рассматриваемой категории не отмечено высокого интеллектуального уровня, качественного образования и других особенностей, отличающих их от других лиц, совершающих преступления. Весомый процент составляют лица, употребляющие наркотические средства, уровень образования которых с трудом дотягивает до среднего. По нашему мнению, так называемый «успех» преступления кроется во владении информацией в области совершения обмана, способе ее передачи (изворотливость и хитрость), кроме того, преступник в момент совершения преступления находится вне поля зрения пострадавшего, тем самым чувствует свое превосходство над пострадавшим и уверенность в безнаказанности, что имеет большое значение при совершении преступного посягательства.

Таким образом, правильное понимание содержания элементов криминалистической характеристики хищений, совершенных дистанционно, с использованием средств сотовой связи, позволит следователю наиболее оптимально и в короткие сроки провести расследование, выявить обстоятельства, способствующие совершению хищений и определить виды эффективной предупредительной деятельности для их устранения.

Список литературы

1. Анешева А.Т., Кузнецов А.А. Первоначальный этап расследования грабежей и разбойных нападений, совершаемых несовершеннолетними: монография. М.: Юрлитинформ, 2013. С. 9.

2. Бессонов А.А. Основы криминалистического учения об исследовании и использовании криминалистической характеристики преступлений: монография. М.: Юрлитинформ, 2016. 256 с.

3. Википедия — свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/ (дата обращения: 12.03.2018).

4. Криминалистика: учебник. 2-е изд., перераб. и доп. М.: Проспект, 2013. 768 с.

5. По специально разработанной анкете было проанализировано более 1000 уголовных дел о хищениях с использованием средств сотовой связи, возбужденных в г. Кургане в 2014-2019 годах.

6. Филиппов А.Г. Проблемы криминалистики. Избранные статьи. М., 2007. С. 92.

А.А. Курин, *к.т.н., доцент кафедры криминалистики Волгоградской академии МВД России, г. Волгоград*

КРИМИНАЛИСТИЧЕСКАЯ РЕГИСТРАЦИЯ КАК ИНТЕГРИРУЮЩЕЕ ЗВЕНО В СИСТЕМЕ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Успешность деятельности полиции во многом зависит от эффективности информационно-аналитического обеспечения выявления, раскрытия и расследования преступлений. В 2019 г. было совершено 2024337 (+1,6) преступлений, из которых остались нераскрытыми 895020 (+6,6%). Основной причиной является неустановление лица, которому может быть предъявлено обвинение (97,8%).

Для получения, обработки и использования необходимых данных субъектами правоприменения используют информационные системы и аппаратно-программные комплексы различного назначения и ведомственной принадлежности. Однако информационное обеспечение в настоящее время имеет преобладающий справочный характер. Это не позволяет в полной мере решать практические задачи, связанные с раскрытием преступлений в дежурные сутки и их успешным расследованием. Согласно статистическим данным, 10% субъектов расследования обращаются к учетам постоянно, остальные 90% обращаются по необходимости или не обращаются вовсе по причине недостаточности знаний в этой области или технической сложности такого обращения. Отсюда следует недостаточная удовлетворенность сотрудников ОВД организацией и результативностью работы учетов (60%). При этом 74% сотрудников не могут оценить полноту использования возможностей криминалистических учетов в своей оперативно-служебной деятельности. Менее 30% сведений, предоставляемых субъектам расследования, являются актуальными. Такова статистика использования информационных ресурсов системы криминалистической регистрации.

Для корректирования работы с информационными ресурсами органов внутренних дел акценты смещаются в область аналитической обработки данных с целью получения актуальной криминалистической и оперативно значимой информации. Концепция создания единой системы информационно-аналитического обеспечения деятельности органов внутренних дел Российской Федерации не решила в полной мере проблемы, связанные с низкой эффективностью информационного обеспечения. Причем сотрудники следственных, оперативных и экспертно-криминалистических подразделений в качестве основных критериев эффективности функционирования системы криминалистической регистрации отметили количество раскрытых преступлений, а также возможность быстрого и полного получения информации. Низкая эффективность обусловлена следующими причинами:

1. Различными подходами к определению перечня источников информации, подлежащих аналитической обработке в рамках оперативной, следственной и экспертно-криминалистической деятельности (6,25%).

2. Слабой разработанностью методик обоснованного выбора рациональных форм представления криминалистической и оперативно значимой информации на основе единой системы свойств, характеристик и признаков объектов, фигурирующих в материалах уголовных дел в качестве вещественных доказательств (6,25%).

3. Отсутствием единых требований к реквизитам, однозначно характеризующим признаки объектов регистрации в учетных документах. Данная проблема входит в круг задач методологического характера, а ее решение лежит в плоскости организационного и научно-методического обеспечения учетно-регистрационной деятельности.

4. Недостаточной обеспеченностью оперативных подразделений мобильными средствами, обеспечивающими дистанционный доступ к необходимым информационным массивам и интерактивный аналитический поиск информации по интегрированным базам и банкам данных. В современных условиях информационный обмен налажен за счет технических каналов связи и телекоммуникаций, обеспечивающих обмен служебной информацией через стационарные автоматизированные рабочие места системы ИСОД МВД России. Порядка 95% информации оперативные уполномоченные получают по каналам телефонной связи, радиосвязи или в результате личного контакта с субъектами информационного взаимодействия (порядка 41,67% анкетируемых).

5. Невозможностью полнофакторной обработки разнородной информации и многоаспектного поиска информации по имеющимся интегрированным базам и банкам данных, в состав которых входят централизованные оперативно-справочные, криминалистические и розыскные, а также экспертно-криминалистические учеты. Данная задача до настоящего времени не решена в полном объеме в силу неурегулированности технических и правовых вопросов о возможности использования специализированных программно-аппаратных средств поиска и анализа информации, что влечет за собой сложности в установлении связей между изучаемыми объектами в ходе производства оперативных аналитических исследований (порядка 20,83% опрошенных).

6. Отсутствием единства в систематике учетов, составляющих систему криминалистической регистрации. Система учетов сегодня формируется по результатам сложившейся практики поступления фактографической информации об обнаруженных и изъятых объектах, направляемых для проверки и последующей постановки на учет. Однако такой подход без прогностической составляющей приводит к ошибочным или абсурдным результатам (4,17%).

7. Отсутствием методологических подходов к аналитической обработке учетно-регистрационных данных. Аналитическая обработка призвана обеспечить получение нового знания о конкретном событии преступления, выделение основных криминалистически значимых элементов его совершения, построение его информационной модели на основе имеющихся и прогнозируемых сведений об обстоятельствах события преступления (2,08%).

8. Отсутствием своевременности, точности и полноты фиксации оперативной и криминалистически значимой информации, направляемой для проверки, постановки на соответствующий учет и аналитической обработки (18,75%).

Учитывая результаты анкетирования сотрудников следственных, оперативных и экспертно-криминалистических подразделений, приведенная совокупность причин низкой эффективности работы системы криминалистической регистрации говорит о комплексности проблемы, которая требует проведения системных мер. Приоритетными направлениями в комплексе мер развития учетно-регистрационной деятельности следует отнести:

1. Совершенствование научных, теоретических и правовых основ информационно-справочного и информационно-аналитического обеспечения выявления, раскрытия и расследования преступлений.

2. Необходимость разработки модели единой телекоммуникационной системы криминалистической регистрации, предусматривающей возможность интеграции учетно-регистрационных массивов различного уровня и ведомственной принадлежности, а также получения аналитической информации с учетом специфики оперативно-служебной деятельности подразделений, выступающих инициаторами запросов.

3. Создание условий для обеспечения полноты и актуальности информационных массивов системы криминалистической регистрации, за счет применения современных средств сбора, обработки, анализа и хранения оперативной и криминалистически значимой

информации, использования эффективных алгоритмов систематизации и поиска необходимой информации посредством программно-аппаратного инструментария.

4. Интеграция ресурсов единой телекоммуникационной системы криминалистической регистрации в глобальные информационные системы международных полицейских организаций и информационных систем (Интерпол, Европол, Африпол, ASEAN[7], МИБ[8]).

Проведенный анализ современного состояния информационного обеспечения раскрытия, расследования и предупреждения преступлений позволяет выдвинуть гипотезу о возможных путях решения поставленной задачи. Использование различных источников информации сопряжено с обработкой значительных объемов информации, которая не представляется возможной без использования средств автоматизации. Аналитическая обработка сведений о конкретных объектах, о видах деятельности физических и юридических лиц открывает возможности установления общности между отдельными событиями, прямо или косвенно связанными с расследуемым преступлением, а также с лицами, причастными к его совершению. Связь события и лица, которому может быть предъявлено обвинение, устанавливается посредством совокупности данных (биометрических, социальных, экономических, территориальных, временных и т.д.). Для этих целей также могут быть использованы ресурсы диспетчерских, геоинформационных, электронных платежных систем, многочисленные базы и банки данных различной ведомственной принадлежности. Формирование и обработка комплекса разнородной информации неизбежно сопровождается существенными организационными и правовыми сложностями, что предусматривает необходимость использования аналитических алгоритмов в отношении учетно-регистрационных данных.

Наиболее рациональным и перспективным способом интеграции криминалистически значимой информации является создание единой телекоммуникационной системы криминалистической регистрации, которая является информационной средой, сосредоточивающей совокупность учетно-регистрационных массивов об объектах и следах, связанных с расследуемыми преступлениями. Доступ к таким ресурсам обеспечивается через метапоисковый сегмент системы. Аналитические сведения предоставляются по единому запросу в реляционные базы данных.

В современных условиях основная часть преступлений раскрывается оперативным путем с использованием системы «Безопасный город». В настоящее время МВД России участвует в разработке Федеральной информационной системы биометрических учетов, которая предназначена для поиска лиц по изображению радужной оболочки глаза, голосу, татуировкам, а в перспективе по походке. Так, обнаруженные на месте преступления следы сканируются и по результатам проверки формируют рекомендательный список лиц, требующих проверки.

Целью информационного обеспечения субъектов расследования является формирование взаимосвязанной структуры достоверных, объективных, полных и актуальных криминалистически значимых фактических данных [1]. Документальные и фактографические данные, используемые для проведения первоначального анализа, могут быть получены правоохранительными органами из гласных или негласных источников, посредством традиционных и современных инновационных средств поиска и регистрации информации. Результативность формирования аналитического продукта находится в прямой зависимости от полноты и достоверности исходной (первичной) информации, а также от оперативности информационного взаимодействия субъектов расследования с использованием телекоммуникационных

[7] ASEAN (***A**ssociation of **S**outh **E**ast **A**sian **N**ations*) — политическая, экономическая и культурная региональная межправительственная организация стран, расположенных в Юго-Восточной Азии.
[8] МИБ — Межгосударственный информационный банк.

возможностей [2], способствующих ее обработке и генерированию новых сведений нового качества и содержания.

В современных условиях причинами недостаточного уровня раскрываемости преступлений (почти каждое второе преступление осталось нераскрытым) [3], являются сложности именно в системе ресурсного обеспечения раскрытия и расследования преступлений [4]. Совокупность существующих информационных массивов позволяет осуществить типизацию первичных данных, среди которых могут быть выделены следующие сведения:

– об инцидентах, которые ранее фиксировались на обслуживаемой территории, они включают сведения, полученные оперативным путем, а также данные об обращениях в полицию, о зарегистрированных преступлениях, о произведенных арестах, о дорожно-транспортных происшествиях и т.д.;

– о зарегистрированных противоправных деяниях на территориях иных региональных (районных) подразделений правоохранительных органов, позволяющих установить факт причастности одних и тех же лиц (объектов) к преступлениям, совершенных в разных местах одним способом;

– о характеристиках криминальных событий на обслуживаемой территории, позволяющих установить причины и осуществить прогнозирование дальнейшего развития событий;

– о физических лицах и осуществляемых ими видах деятельности, что позволяет получить сведения о характеристиках субъектов преступления, их взаимосвязях, характере и специфике их деятельности и т.д.

Совокупность данных, содержащихся в различных информационных массивах, создает дополнительный резерв для информационного обеспечения, дифференцируемого по двум направлениям: информационно-справочному и информационно-аналитическому.

Информационно-справочное обеспечение направлено на поиск данных, формирование рекомендательных списков из собственных ведомственных информационных массивов. Информационно-аналитическое обеспечение представляет собой распределенный сбор разнородных данных из внешних по отношению к поисковой системе ресурсов, анализ, проведение над ними модельных расчетов с целью получения новых знаний и предоставление инициаторам запросов результатов, представленных в наглядной структурированной форме (схема, граф связей, диаграмма).

В целом поиск (получение, сбор), систематизация, аналитическая обработка первичных и вновь поступающих данных позволяют сформировать информационную модель противоправного деяния, способствующую получению субъектами правоприменения нового знания о событии преступления, лицах, причастных к его совершению, а также об используемых ими технических средствах. Аналитическая работа позволяет получить информацию о структуре и иерархии преступных организаций, о товарно-денежных потоках, взаимоотношениях, преступной деятельности, планах, персональных данных участников преступных групп. В результате такой работы формируется профиль преступника или преступной группы с учетом фактических данных о совершенных ранее преступлениях.

Единая телекоммуникационная система криминалистической регистрации нацелена на комплексное использование существующих методов и средств работы с учетно-регистрационными данными совместно со средствами радиоэлектронного мониторинга и радиочастотной идентификации.

Каждый из ранее рассмотренных нами объектов (человек, транспортное средство, документы, предмет преступного посягательства и т.д.) может быть оснащен передающим устройством активного или пассивного действия, которое имеет индивидуальный номер. Объект с присвоенным ему номером обладает определенными свойствами или характеристиками,

информация о которых хранится в системе криминалистической регистрации. За отправную точку при раскрытии преступлений может быть принято любое из установленных фактических данных о лице или объекте преступного посягательства:

– установочные данные лица, полученные из документов, удостоверяющие личность, в том числе электронных;

– сведения о наличии административных правонарушениях и судимости, нахождении в розыске;

– сведения о профессиональных или преступных навыках, полученные из оперативно-справочных, розыскных и оперативных учетов;

– сведения о перемещениях гражданина (оформленные на имя гражданина проездные документы на поезд, самолет, автобус, перемещения личным транспортом, данные из системы «Безопасный город»);

– номерные объекты, зарегистрированные на гражданина (номера мобильных устройств, банковские платежные карты, транспортные средства, гражданское огнестрельное оружие);

– сведения о финансово-хозяйственной деятельности (индивидуальный номер налогоплательщика, СНИЛС, сведения о доходах/расходах из налоговых органов, сведения об имуществе, сведения о банковских операциях, экономической деятельности, предпринимательской деятельности);

– сведения о контактах лица (телефонные переговоры и переписка, обмен информацией через иные средства связи, сведения из социальных сетей, контроль передвижения, получение доступа на охраняемые объекты);

– сведения о механизме преступной деятельности (способ совершения, предмет преступного посягательства, используемые технические и иные средства, способы сокрытия следов преступления).

Представленная совокупность информации требует тщательной аналитической обработки на предмет установления общностей и связей как между собой, так и с событием преступления. Для аналитического исследования информация может быть задана матрицей «объект-признак» или матрицей связи «объект-объект» с возможностью перехода от одной формы к другой. На начальном этапе необходимо решить вопрос о выборе информативной системы признаков, или об определении факторов в системе признаков. Преимущество многомерного поиска заключается в том, что набор исходных признаков заменяется совокупностью взаимосвязанных признаков, которая установлена в ходе неотложных следственных действий и оперативно-розыскных мероприятий [5].

Представленная концепция единой информационной среды, ориентированной на деятельность правоохранительных органов, позволит получить следующие преимущества:

– передавать и документировать данные об объектах в режиме реального времени;

– проводить ситуационный анализ оперативной обстановки на обслуживаемой территории;

– проводить ретроспективный анализ криминалистически значимой информации для установления субъектов преступной деятельности и обстоятельств совершения преступления;

– решать организационные вопросы при подготовке и проведении оперативно-розыскных мероприятий и следственных действий.

Применение указанных технических средств требует проработки правовых, организационных и тактических подходов к использованию радиочастотных систем. В правовом плане требуется решение вопросов о размещении радиочастотных систем непосредственно на объекте или в материале самого объекта [6].

Современный уровень технического развития общества свидетельствует о наличии всех условий для создания единой системы получения аналитической информации при использовании средств телекоммуникации, геоинформационных и навигационных систем, включая технологии защиты информации, технологии искусственного интеллекта. При этом в комплексе следов должно быть выделено достаточное количество признаков, идентифицирующих группу лиц, совершивших преступление.

Таким образом, проверка информации о выявленном преступлении по первичным учетам на предмет единства способа совершения преступления, и других обстоятельств подлежащих доказыванию позволяет получить статистический массив данных, который будет взят за основу в качестве базы знаний о данном виде преступления. Проведенный анализ позволяет установить наиболее вероятную модель совершенного преступления и представить ее в виде матрицы конкретного преступления с известными и неустановленными обстоятельствами. Оперативно-розыскные учеты, использованные совместно с электронными системами контроля в качестве обеспечивающего звена, позволят получить сведения о локализации лиц и объектов. Экспертно-криминалистические учеты позволят получить сведения об общих следовых комплексах, сходстве и различиях в механизме и обстоятельствах совершенного преступления, а также выдвинуть типовые следственные версии расследования или получить основания для объединения уголовных дел в одно производство. Проверка следственных версий на основе сквозной проверки следов и объектов в единой системе криминалистической регистрации позволит комплексно использовать экспертно-криминалистических, централизованных и оперативно-розыскных учетов в раскрытии и расследовании преступлений.

Список литературы

1. Курин А.А., Дронова О.Б. Современные возможности информационного обеспечения процесса выявления и расследования преступлений в сфере потребительского рынка // Всероссийский криминологический журнал. 2017. Т. 11, № 2. С. 318-326.

2. Gentili, Monica et al. (2015) Locating Vehicle Identification Sensors for Travel Time Information. Applications of Location Analysis. Springer International Publishing. P. 307-327.

3. Владимир Путин на расширенном заседании коллегии МВД России. URL: www.putin-today.ru.

4. Соколов Ю.Н. Некоторые виды информационных технологий в уголовном судопроизводстве и ОРД // Материалы НПК. Челябинск, 2009. С. 136.

5. Курин А.А. Совершенствование системы криминалистической регистрации и первичного учета преступлений // Пробелы в российском законодательстве. М., 2014. № 2. С. 7.

6. Курин А.А., Панайоти Д.Н. Направления повышения эффективности раскрытия и расследования преступлений террористического характера на транспорте // Криминалистическое обеспечение антитеррористической деятельности: сборник научных трудов / отв. ред. К.В. Вишневецкий. Краснодар: КрУ МВД России, 2007.

7. Курин А.А., Панайоти Д.Н. Задачи использования навигационного оборудования в раскрытии и расследовании преступлений, связанных с использованием автомобильного транспорта // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: материалы Пятой международной научно-практической конференции. Барнаул: Барнаульский юридический институт МВД России, 2007.

А.М. Лютынский, *к.ю.н., доцент кафедры уголовного процесса и криминалистики Северо-западного института Университета им. О.Е. Кутафина (МГЮА), г. Вологда*
А.В. Селякова, *помощник прокурора г. Вологды, г. Вологда*

ОСОБЕННОСТИ ДОКАЗЫВАНИЯ НЕКОТОРЫХ ОБСТОЯТЕЛЬСТВ ПРИСВОЕНИЯ В СФЕРЕ ЖКХ В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ

Жилищно-коммунальное хозяйство как сфера экономических отношений по обеспечению услугами по водо-, тепло-, электроснабжению жилых и нежилых помещений можно отнести к проблемным в современной российской экономики. Реформа гражданского и жилищного законодательства с 1990-х гг. основана на расширении возможностей собственников жилых помещений эффективно управлять собственностью, контролировать качество коммунальных услуг, выбирать те или иные варианты отношений с ресурсоснабжающими организациями и т.п.

Появление такой правовой формы, как товарищество собственников жилья (ТСЖ) в целом можно оценить как верное правовое решение. Однако практика деятельности ТСЖ особенно связана с проблемами контроля за эффективностью использования средств собственников органами управления ТСЖ. Данные судебной практики позволяют говорить об актуальности изучения правовых и криминалистических особенностей расследования преступлений в сфере ЖКХ, а нарастающая цифровизация всех сфер общественных отношений — о необходимости развития исследований и этого аспекта. Можно говорить о высокой латентности рассматриваемой категории преступлений и сложностях расследования, вызванных, в частности, сложностью отграничения от гражданско-правового деликта, маскировкой под правомерные действия и т.д. [9].

Не претендуя в рамках небольшой статьи на полный охват темы и, тем более, на полный анализ всех видов преступлений в сфере ЖКХ, рассмотрим некоторые особенности, в том числе связанные с цифровизацией общества, которые необходимо учесть, когда мы говорим об одном из видов хищений — присвоении денежных средств ТСЖ председателями правления, ст. 160 УК РФ. Тем более что эти преступления остаются одними из самых распространенных в данной сфере [10].

В соответствии со ст. 291 Гражданского кодекса Российской Федерации и ст. 135 Жилищного кодекса Российской Федерации ТСЖ является некоммерческой организацией, объединением собственников помещений в многоквартирном доме, созданным для совместного управления общим комплексом имущества в многоквартирном доме, обеспечения эксплуатации этого комплекса, владения, пользования и распоряжения общим имуществом.

Опишем достаточно типичный механизм совершения рассматриваемого преступления. Лицо, избранное председателем ТСЖ, получив организационно-распорядительные полномочия, доступ к управлению денежными средствами ТСЖ, самовольно, незаконно, из корыстных побуждений назначает себе повышенные выплаты, премии и т.д., размеры которых не основаны на решении общего собрания собственников, как того требует Жилищный кодекс РФ. Денежные средства незаконно получаются данным лицом на основе его решений, как правило, с помощью банковских операций.

Отметить несколько позиций, на наш взгляд, наиболее важных в контексте доказывания по уголовным делам о подобных преступлениях.

1. Правовая природа вознаграждения председателя правления вызывает споры в судебной практике и юридической науке.

В соответствии с требованиями ст. 147 ЖК РФ председатель правления ТСЖ не может являться лицом, с которым товарищество заключило договор управления многоквартирным домом.

Верховный суд РФ в одном из решений указал, что член правления товарищества собственников жилья (т.е. и председатель правления) не может совмещать свою деятельность в правлении товарищества с работой в товариществе по трудовому договору, а также поручать, доверять другому лицу или иным образом возлагать на него исполнение своих обязанностей члена правления товарищества [4].

Председатель и члены правления ТСЖ товарищества собственников жилья действуют исключительно в интересах собственников жилых помещений, то есть в своих интересах, что делает невозможным вывод о существовании в рассматриваемых отношениях по самоуправлению признаков трудовых отношений. При этом на основании решения общего собрания членов товарищества собственников жилья председателю может быть определен размер вознаграждения за участие в управлении многоквартирным домом.

2. Председатель ТСЖ в силу норм гражданского и жилищного законодательства, обладает административно-хозяйственными и организационно-распорядительными полномочиями в отношении денежных средств ТСЖ, формируемых за счет регулярных платежей собственников и вверяемых председателю для управления и расходования на нужды товарищества. Статус председателя позволяет с точки зрения уголовно-правовой квалификации вменять такой признак, как использование служебного положения.

3. Проблемой является разграничение гражданско-правовых и уголовно-правовых отношений в вопросе неправомерного присвоения денежных средств. С точки зрения гражданского права это в любом случае деликт. На наш взгляд, умысел на хищение необходимо доказывать как с помощью допроса подозреваемого, так и путем установления с помощью иных доказательств фактов знания подозреваемым правового регулирования определения вознаграждения председателя ТСЖ. Например, показания свидетелей — собственников, членов правления, документы ТСЖ (протоколы собраний) из которых можно сделать вывод о сознательном характере действий подозреваемого.

4. Особенности доказывания суммы ущерба связаны с установлением размера денежной компенсации председателю правления и определением момента, с которого необходимо вести отсчет. Ущерб причиняется ТСЖ, а не отдельным собственникам, а сумма похищенного определяется суммированием денежных средств, которые превышают определенный размер и которые подозреваемый регулярно получал [8].

5. Такое социальное явление, как цифровизация не могло не затронуть сферу ЖКХ и, соответственно, породить вопросы, связанные с доказыванием по уголовным делам в рассматриваемой сфере. Многие ТСЖ, используя сеть Интернет и социальные сети, средством текущего общения делают сообщество того или иного ТСЖ, где происходит обмен мнениями, информирование путем объявлений и демонстрации фотоснимков, чаще всего в социальной сети «ВКонтакте».

В случае выявления признаков хищения средств ТСЖ, а особенно когда председатель пользуется возможностью контроля за документацией и предпринимает меры по уничтожению или подделке оригиналов основных документов ТСЖ, актуальными могут стать следующие вопросы:

А) Переписка членов ТСЖ и председателя ТСЖ как источник значимой для доказывания информации.

Правовой статус личной переписки в социальной сети (а также интернет-мессенджерах) и правовые аспекты ее использования в доказывании по уголовному делу неоднозначно понимаются в судебной и следственной практике, как и в юридической науке. Известны случаи, когда участник переписки, допрошенный в качестве свидетеля или потерпевшего по уголовному делу, самостоятельно распечатывает и представляет следователю содержание такой переписки, а следователь заверяет ее и приобщает в качестве иных документов к уголовному делу. Также упоминаются варианты, когда происходит изъятие компьютера или смартфона и переписка вовлекается в уголовное дело путем осмотра носителя.

Позиция Конституционного Суда РФ, высказанная в одном из так называемых «отказных» определений о том, что проведение осмотра с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения специального судебного решения [7], вызвала критику многих юристов-практиков [6].

Мы склонны понимать такую информацию как содержащую охраняемую Конституцией РФ тайну переписки (ст. 23) и в целом поддерживаем позицию о необходимости внесения изменения в УПК РФ, например, в виде ст. 185.1 «Выемка, осмотр электронных переписок и файлов, содержащихся в них» с обязательной процедурой судебного контроля, по аналогии с обыском жилища [5]. Пока такие изменения не внесены, необходимо, на наш взгляд, исходить из смысла важнейших норм и принципов права и применять правила, имеющиеся в УПК РФ для изъятия почтовых отправлений.

Б) Информация на так называемой стене соответствующего сообщества. Ее использование может быть полезным для доказывания некоторых обстоятельств, связанных с расследуемым хищением. Здесь, на наш взгляд, приемлемо производство осмотра как условного предмета страницы сообщества с компьютера, подключенного к сети Интернет. Осмотр зафиксирует наличие тех или иных данных на странице в определенный момент времени. Аналогичный подход можно применить, когда необходимо зафиксировать наличие и изъятие для приобщения к материалам дела документов, размещенных в таком сообществе. В первую очередь, необходимость может возникнуть для протоколов собраний и устава ТСЖ, которые в электронном виде часто размещаются в отдельном разделе такого сообщества.

Конечно, анализ особенностей информации такого рода позволяет говорить о необходимости уточнения законодательства и введения нескольких понятий в УПК РФ, например «электронная информация», «изъятие электронной информации» и т.д., но это тема для отдельного рассмотрения.

Изъятые указанным образом документы могут быть преобразованы в ходе осмотра в печатную форму (о чем делается отметка в протоколе) и приобщены к делу для иллюстрации отдельных фактов. Особенно важно предпринять такие действия, когда подозреваемый пытается представить законность размера своего вознаграждения, подделав или уничтожив оригиналы протоколов собраний ТСЖ. В этом случае точность и подлинность протоколов, исследованных и изъятых в ходе осмотра интернет-страниц сообщества необходимо проверить с помощью допросов членов правления, собственников и иных очевидцев.

Подводя итог, можно резюмировать следующее:

К обстоятельствам, входящим в перечень подлежащих установлению по делам о присвоении средств ТСЖ, необходимо отнести: факт существования ТСЖ; размер вознаграждения председателя правления ТСЖ; зафиксированный в решении общего собрания ТСЖ; размер присвоенных средств в целом (в виде суммы отдельных платежей). Данные интернет-сайтов, электронной переписки отдельных обстоятельств дела важны для доказывания, особенно в ситуации противодействия расследованию. Можно констатировать несовершенство действующего закона в вопросе правового регулирования оборота электронной информации в уголовном судопроизводстве. Однако до внесения необходимых изменений вполне приемлемыми средствами исследования электронно-цифровой информации представляются традиционные осмотры интернет-страниц и в необходимых случаях осмотры и выемки электронной переписки на основе судебного решения.

Список литературы

1. Жилищный кодекс Российской Федерации от 29.12.2004 № 188-ФЗ.
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ.
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ.

4. Кассационное определение Судебной коллегии по административным делам Верховного Суда Российской Федерации от 24.05.2019 № 84-КА19-1.

5. Липский Н.А., Попов Е.М. Проблемы электронной переписки в уголовно-процессуальном доказывании // Ученые записки Санкт-Петербургского имени В.Б. Бобкова филиала Российской таможенной академии. 2017. № 3 (63).

6. Оноприенко О. КС: Для изучения содержимого телефона при его изъятии судебное решение не требуется // Адвокатская газета. URL: https://www.advgazeta.ru/novosti/ks-dlya-izucheniya-soderzhimogo-telefona-pri-ego-izyatii-sudebnoe-reshenie-ne-trebuetsya/

7. Определение Конституционного Суда РФ № 189-О/2018 об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации. URL: http://doc.ksrf.ru/decision/KSRFDecision314926.pdf

8. Приговор Орджоникидзевского районного суда г. Перми от 25.02.2019 г. по делу 1-14/2019 URL: https://sudact.ru/regular/doc/gwXuv2YrKXlt/ (дата обращения: 14.05.2020 г.)

9. Титова К.А. Методика расследования хищений в сфере жилищно-коммунального хозяйства: дисс. ... канд. юрид. наук. Барнаул, 2009.

10. Тюнин В.И., Степанов Ю.И. Преступления, совершаемые в сфере жилищно-коммунального хозяйства (особенности квалификации в связи с механизмом совершения преступлений) // Вестник Санкт-Петербургского университета МВД России. 2014. № 3 (63). С. 63-70.

В.А. Машлякевич, *старший преподаватель Барнаульского юридического института МВД России, г. Барнаул*

НЕКОТОРЫЕ ВОПРОСЫ ВЗАИМОДЕЙСТВИЯ СЛЕДОВАТЕЛЕЙ С ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ НА ЭТАПЕ ПРЕДВАРИТЕЛЬНОЙ ПРОВЕРКИ МАТЕРИАЛОВ ПО ДЕЛАМ О МОШЕННИЧЕСТВАХ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ТЕЛЕФОННОЙ СВЯЗИ

Деятельность по выявлению, расследованию и раскрытию практически любой категории преступлений включает в себя два основных аспекта: оперативно-розыскной и уголовно-процессуальный. Оперативно-розыскной аспект в большинстве случаев подразумевает рассмотрение оперативных материалов органами, осуществляющими оперативно-розыскные функции, до возбуждения уголовного дела, то есть на этапе предварительной проверки материалов.

В этой связи нельзя не согласиться с мнением В.А. Азарова, который полагает, что сравнительный анализ задач уголовного судопроизводства и оперативно-розыскной деятельности приводит к заключению об их общности, так как и та и другая правоприменительная деятельность направлена на «быстрое и полное раскрытие преступлений, выявление, установление и изобличение виновных в их совершении» [1, с. 46]. Реализация такой задачи неминуемо ставит перед следователем и оперативным работником ряд вопросов, основными из которых являются: взаимодействие различных ведомств, служб и подразделений, работающих над раскрытием конкретного преступления, а также использование при расследовании уголовного дела результатов оперативно-розыскной деятельности. На этапе предварительной проверки материалов мошенничеств, совершаемых с использованием средств телефонной связи, в абсолютном большинстве случаев работа сотрудников правоохранительных органов строится на взаимодействии между собой.

При поступлении в орган внутренних дел сообщения о совершенном телефонном мошенничестве (собственно, как и сообщения о практически любом другом преступлении) на место происшествия выезжает следственно-оперативная группа. Ее состав может варьиро-

ваться в зависимости от решения руководителя органа внутренних дел, однако в большинстве случаев в нее будет входить следователь (он же является руководителем данной группы), оперуполномоченный и эксперт-криминалист. Соответственно, процесс расследования данной категории преступлений неминуемо сопровождается взаимодействием сотрудников правоохранительных органов, представляющих различные подразделения.

Одной из наиболее типичных ситуаций такого взаимодействия, по справедливому мнению В.С. Хоршевой, является «совершение неочевидного преступления, когда неизвестно лицо, его совершившее» [2, с. 168]. Изучение эмпирического материала по рассматриваемой категории преступлений показало, что на момент начала этапа предварительной проверки в 94% случаев информация о субъекте преступления отсутствует.

Представляется, что следователь должен включаться в работу не позднее, чем на стадии реализации оперативных материалов в качестве лица, ответственного за своевременное и полное расследование и раскрытие преступления. При этом результаты ОРД, представляемые уполномоченным должностным лицам (органам), должны отвечать предъявляемым к ним требованиям, предусмотренным Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд (далее — Инструкция) [3].

В частности, результаты ОРД, представляемые для решения вопроса о возбуждении уголовного дела, должны содержать достаточные данные, указывающие на признаки преступления. К ним относятся: сведения о том, где, когда, какие признаки и какого именно преступления обнаружены; при каких обстоятельствах имело место их обнаружение; сведения о лице (лицах), его совершившем (если они известны), и очевидцах преступления (если они известны); о местонахождении предметов и документов, которые могут быть признаны вещественными доказательствами по уголовному делу; о любых других фактах и обстоятельствах, имеющих значение для решения вопроса о возбуждении уголовного дела (п. 18 Инструкции).

Таким образом, можно сделать вывод о том, что критериями готовности предоставленных материалов должны являться следующие: наличие достаточных данных, указывающих на признаки преступления, относящегося к компетенции органа предварительного следствия; выявлены ли лица, причастные к совершению преступлений, какова роль каждого из них в содеянном, их имущественное положение; в достаточном ли объеме выявлены и закреплены ли документально эпизоды преступной деятельности лиц, являющиеся объектами документирования; проверены ли данные, которые предполагается использовать при возбуждении уголовного дела и производстве предварительного следствия, нет ли между ними противоречий, свидетельствующих об обстоятельствах, исключающих возбуждение уголовного дела и (или) привлечение разрабатываемых лиц к уголовной ответственности; какие материалы, полученные в результате ОРД, можно использовать в ходе расследования по уголовному делу.

Сказанное выше позволяет говорить о том, что на этапе предварительной проверки мошенничеств, совершаемых с использованием средств телефонной связи, одной из основных задач оперативного работника является (в широком смысле) установление данных, позволяющих решить вопрос о возбуждении уголовного дела.

Как правило, при оперативно-розыскном сопровождении рассматриваемой категории преступлений, на этапе предварительной проверки устанавливается следующая информация:

– сведения о размерах хищения;

– сведения о движении денежных средств;

– результаты оперативно-розыскных и оперативно-технических мероприятий (справки, стенограммы, сводки, аудио- и видеозаписи), подтверждающие причастность фигурантов к совершению преступлений;

– установочные и характеризующие сведения о фигурантах, занимающихся хищением денежных средств посредством совершения мошенничеств с использованием средств телефонной связи;

– сведения о местах ведения преступной деятельности, местах хранения документов и предметов, имеющих значение для дальнейшего расследования и т.д.

В данном контексте считаем целесообразным остановиться на некоторых аспектах оперативно-розыскного сопровождения этапа предварительной проверки материалов по делам о телефонных мошенничествах более подробно.

Исходной информацией, получаемой оперативным работником, является абонентский номер телефона, который использовал преступник при совершении мошенничества. При этом следует отметить, что в случае звонка на мобильный телефон потерпевшего установление абонентского номера преступника не вызовет сложностей — он останется в памяти телефона потерпевшего и в ходе опроса будет установлен.

В случае если телефонный звонок преступника был совершен на стационарный номер телефона, установить абонентский номер звонившего будет несколько сложнее. Рассмотрим данный процесс на примере случаев, где организацией, обслуживающей стационарный номер телефона, является компания «Ростелеком».

Детализация звонков по стационарному телефону может быть получена как путем личного обращения абонента в офис компании, так и запрошена в онлайн-режиме посредством сети Интернет. Личное обращение абонента в офис компании займет довольно продолжительное время, тогда как воспользоваться онлайн-сервисом можно довольно-таки быстро даже при условии, что потерпевший не регистрировал личный кабинет на сайте компании. Итак, для получения детализации через онлайн-сервис необходимо пройти процедуру регистрации на сайте «Ростелеком», после чего в блоке «Расходы и платежи» кликнуть пункт «Детализация вызовов», указать временные рамки проверяемого периода, отметить группы звонков, которые необходимо отобразить, а также ввести свой e-mail. Затем необходимо подтвердить правильность запрашиваемых данных и осуществить запрос. Детализация телефонных звонков будет выслана на указанный при регистрации e-mail.

Получив информацию об абонентском номере, с использованием которого было совершено телефонное мошенничество, оперативный работник, посредством различных онлайн-сервисов (https://www.kody.su/check-tel, https://phonenum.info/ и др.), может установить его принадлежность к субъекту Российской Федерации и оператору связи, обслуживающему данный номер, а значит довольно значительно сузить круг поисков.

Используемые преступниками сим-карты зачастую оформляются на несуществующих лиц либо вовсе не имеют установочных данных. Однако же нередки случаи, когда владелец данной сим-карты действительно существует. Так, с целью совершения мошенничества с использованием средств телефонной связи обвиняемый О. приобрел в личное пользование мобильный телефон и сим-карту с абонентским номером 8-965-…, зарегистрированную на Ф., а также использовал приобретенную ранее сим-карту с абонентским номером 8-950-…, зарегистрированную на П. [4].

Информацию о предполагаемом владельце сим-карты можно узнать с помощью мобильного приложения «Get Contact», которое было зарегистрировано турецкими разработчиками в Лондоне в ноябре 2017 г. Его основной идеей стало определение имени (а зачастую и фамилии) звонящего пользователю абонента даже в том случае, если его нет в списке контактов. Приложение собирает данные о том, каким образом записан тот или иной абонентский номер телефона в книге контактов различных пользователей, у которых оно уже установлено. Учитывая популярность данного приложения (в настоящее время только в России насчитывается более 10 тысяч пользователей, а общая база телефонных номеров превышает 2 млрд), его использование в процессе раскрытия мошенничеств, совершаемых с использованием средств телефонной связи, вполне возможно. Проведя анализ информации, предоставляемой приложением «Get Contact», мы пришли к выводу, что при проверке абонентских номеров в данном

приложении можно получить следующие группы данных о предполагаемых владельцах сим-карты:

– фамилия и имя абонента;
– имя и отчество абонента;
– имя и род деятельности абонента (зачастую в книгах телефонных контактов пользователь может быть записан как «Олег Мебель», «Иван Автослесарь» и т.д.).

Затрагивая вопрос использования продуктов современной цивилизации с целью раскрытия рассматриваемой категории преступлений, следует упомянуть и о банковских мобильных приложениях. В следственной практике встречаются случаи, когда мошенник указывает зачисление на банковскую карту, оформленную на подставного человека и к которой он имеет доступ, в качестве варианта передачи денежных средств потерпевшим. В наиболее распространенном приложении «Сбербанк онлайн» при оформлении перевода денежных средств по номеру телефона отображается информация об имени, отчестве и первой букве фамилии получателя перевода, приводятся первые шесть и последние четыре цифры банковской карты получателя, а также реквизиты (номер и дата) самого перевода. В свою очередь, информация о первых шести цифрах банковской карты может быть использована для определения банка, обслуживающего данную карту. Для этого можно воспользоваться соответствующим онлайн сервисом (например, https://psm7.com/bin-card, https://karta-banka.ru/), на котором необходимо ввести имеющиеся данные. Помимо принадлежности к банку будет предоставлена информация о платежной системе (Visa, MasterCard), типе карты (кредитная, дебетовая) и стране использования.

Таким образом, уже после первоначальной встречи с потерпевшим на этапе предварительной проверки мошенничеств, совершаемых с использованием средств телефонной связи, оперативным путем может быть получена информация о номинальном владельце сим-карты, которой пользовался преступник для совершения преступления, а также регионе, в котором проживает данный человек, и откуда, вероятнее всего, было совершено преступление.

Список литературы

1. Азаров В.А. Уголовно-процессуальные и оперативно-розыскные средства достижения цели раскрытия преступлений // Государство и право. 1997. № 10. С. 46.

2. Хоршева В.С. О некоторых аспектах взаимодействия следователя, дознавателя с оперативными службами органов внутренних дел в ходе расследования преступлений // Вестник Волгоградской академии МВД России. № 1 (48). 2019. С. 168.

3. Приказ от 27 сентября 2013 года Министерства внутренних дел Российской Федерации № 776, Федеральной службы Российской Федерации по контролю за оборотом наркотиков № 398, Следственного комитета Российской Федерации № 68 «Об утверждении, Министерства обороны Российской Федерации № 703, Федеральной служб безопасности Российской Федерации № 509, Федеральной службы охраны Российской Федерации № 507, Федеральной таможенной службы №1820, Службы внешней разведки Российской Федерации № 42, Федеральной службы исполнения наказаний № 535 Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд».

4. Обвинительное заключение по уголовному дел № 11801320067210180 // ГСУ ГУ МВД России по Кемеровской области, 2019.

М.М. Менжега, *к.ю.н., доцент кафедры криминалистики*
Саратовской государственной юридической академии, г. Саратов
Д.С. Хижняк, *д.ю.н., доцент, профессор кафедры криминалистики*
Саратовской государственной юридической академии, г. Саратов

К ВОПРОСУ О КРИМИНАЛИСТИЧЕСКОЙ КЛАССИФИКАЦИИ ТРАНСНАЦИОНАЛЬНЫХ КИБЕРПРЕСТУПЛЕНИЙ

С развитием новых технологий, информационно-техническим перевооружением предприятий, организаций, ростом новых видов преступлений внедрение современных цифровых систем и телекоммуникационных средств в самые широкие сферы деятельности современного общества привело как к развитию положительных тенденций и явлений, так и выявило широкий круг проблем, например, появление новых разновидностей преступлений — в сфере компьютерной информации и целый ряд преступлений, связанных с применением компьютерной техники. Сегодня для многих не является секретом тот факт, что с помощью персонального компьютера можно, например, заблокировать информацию на компьютерах других лиц, получить нужную конфиденциальную информацию, хранящуюся в компьютерах на территории другой страны, в корыстных целях.

В последние десятилетия изменились не только методы совершения преступлений, но и их масштаб. Поскольку правонарушители получили возможность автоматически совершать атаки, количество правонарушений увеличилось. Страны, а также региональные и международные организации предприняли ряд мер, чтобы разрешить усугубляющуюся ситуацию, и сделали борьбу с киберпреступностью своей первоочередной задачей. Сложившаяся в настоящий момент ситуация обусловливает необходимость в исследовании вопросов расследования киберпреступлений и в том числе в рассмотрении вопросов криминалистической классификации транснациональных преступлений в сфере компьютерной информации.

Разработка криминалистической классификации преступлений в российской науке впервые получила свое законодательное закрепление в XIX в., однако основательно начала свое развитие с конца прошлого столетия.

Вопросы криминалистической классификации в своих трудах подробно исследовал И.Ф. Герасимов. Помимо родовой и видовой уголовно-правовой классификации преступлений, он выделял и другие классификации, в частности, объединяя преступления по месту их совершения, в том числе выделяя преступления, место совершения которых не носит однозначного характера, и потому его можно назвать сложным (например, преступления на транспорте, взяточничество, спекуляция и т.п.) [1, с. 151-168].

Сегодня большая часть транснациональных преступлений относится именно к преступлениям неоднозначного характера. В таких преступлениях сложности вызывают определение места совершения преступления (на территории разных стран, в общемировой сети Интернет), способы (телефонное мошенничество, блокирование информации, кража идентичности, пропаганда терроризма), маскировка как способ сокрытия преступления (использование мобильной связи на имя другого лица, использование анонимайзеров [2][9]), преступный опыт лиц, совершающих преступления (в структуру организованной группы входят лица с различным криминальным и профессиональным опытом). Таким образом, основания классификации транснациональных преступлений зачастую имеют смешанный характер.

Профессор Марко Герке отмечает существование проблемы классификации киберпреступлений ввиду того, что их типология не является последовательной, так как не основана на

[9] Анонимайзер — общее название средств для скрытия информации о компьютере, его IP-адресе или пользователе в сети от удаленного сервера.

едином основании для классификации. Им выделяются четыре категории киберпреступлений, в зависимости от объекта правовой защиты:

1. «Преступления против конфиденциальности, целостности и доступность компьютерных данных и систем».
2. «Правонарушения, связанные с цифровым содержанием (контентом)».
3. «Правонарушения, связанные с авторским правом».
4. В четвертую категорию автор включает «преступления с использованием компьютеров», которые, однако, классифицируются не по объекту правовой защиты, а по способу совершения преступления, что приводит к несовпадению оснований классификаций [3].

Кроме того, автор выделяет некоторые преступления, которые имеют смешанный характер и используются для совершения определенных преступных действий (например, «кибертерроризм» или «Фишинг») и охватывают действия, которые подпадают под несколько категорий.

Такая классификация представляется достаточно стройной и логичной, однако, на наш взгляд, есть существенные сходства второй, третьей и четвертой группы преступлений — все они имеют совершенно разный объект, а объединены тем, что могут совершаться с использованием компьютеров и сети Интернет. Так, например, нарушения авторских прав могут совершаться как в сети Интернет, так и без ее использования. Правонарушения, связанные с цифровым контентом, например, распространение детской порнографии, пропаганда нацизма, разжигание религиозной ненависти, также активно совершаются как в сети, так и вне ее. В отличие от преступлений первой группы Интернет в их совершении используется лишь как средство достижения цели. В то время как преступления первой группы совершаются исключительно в сети и объектом выступают общественные отношения в сфере обеспечения безопасности охраняемой законом компьютерной информации, безопасное использование соответствующих технических устройств, их программного обеспечения и информационного содержания.

Кроме того, возникают сомнения корректности фразы «преступления с использованием компьютеров». Компьютеры могут использоваться в совершении множества преступлений, например, для создания в графическом редакторе (с последующей их распечаткой на принтере) поддельных накладных для совершения мошенничества. Вряд ли такое преступление можно отнести к киберпреступлению. Целесообразнее, на наш взгляд, обозначить их как преступления с использованием сети Интернет.

Таким образом, более логичным представляется классифицировать киберпреступления на две группы: «Преступления в сфере компьютерной информации (преступления против конфиденциальности, целостности и доступности компьютерных данных и систем)» и «Преступления с использованием сети Интернет», в которой следует выделить подгруппы преступлений, например, связанные с цифровым контентом; авторским правом и товарными знаками; иные преступления, связанные с использованием сети Интернет.

Таким образом, подводя итог вышесказанному, наиболее целесообразной представляется следующая классификация транснациональных киберпреступлений:

1. Преступления в сфере компьютерной информации:

1.1. Неправомерный доступ к компьютерной информации.

1.2. Создание, использование и распространение вредоносных компьютерных программ.

1.3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

1.4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

2. Преступления с использованием сети Интернет:

2.1. Преступления, связанные с цифровым контентом:

2.1.1. Незаконные изготовление и оборот порнографических материалов.

2.1.2. Возбуждение национальной, расовой или религиозной вражды.

2.1.3. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма.

2.1.4. Организация террористического сообщества и участие в нем, организация деятельности террористической организации

2.1.5. Организация деятельности, направленной на побуждение к совершению самоубийства.

2.1.6. Незаконные организация и проведение азартных игр.

2.2. Преступления связанные с авторским правом и товарными знаками:

2.2.1. Нарушение авторских и смежных прав.

2.2.2. Нарушение изобретательских и патентных прав.

2.2.3. Незаконное использование средств индивидуализации товаров (работ, услуг).

2.2.4. Иные преступления связанные с использованием сети Интернет:

2.2.5. Клевета.

2.2.6. Вымогательство.

2.2.7. Незаконное распространение наркотических средств.

2.2.8. Мошенничество.

2.2.9. Террористический акт, содействие террористической деятельности.

2.2.10. Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем.

Список литературы

1. Герасимов И.Ф. Некоторые проблемы раскрытия преступлений. Свердловск, 1975. С. 151-168.

2. Анонимайзер — общее название средств для скрытия информации о компьютере, его IP-адресе или пользователе в сети от удаленного сервера. URL: https://ru.wikipedia.org/wiki/анонимайзер

3. Prof. Dr. Marco Gercke // Understanding cybercrime: Phenomena, challenges and legal response. URL: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (дата обращения: 02.03.20).

М.А. Лавнов, *к.ю.н., доцент кафедры уголовного процесса*
Саратовской государственной юридической академии, г. Саратов
Н.О. Овчинникова*, к.ю.н., доцент кафедры уголовного процесса*
Саратовской государственной юридической академии, г. Саратов

УГОЛОВНО-ПРОЦЕССУАЛЬНОЕ ДОКАЗЫВАНИЕ ПО ДЕЛАМ О КИБЕРПРЕСТУПЛЕНИЯХ

Повышение доступности цифровых технологий, увеличение скорости передачи данных, анонимность и простота использования Интернета, колоссальное увеличение широты охвата аудитории в последние 20 лет существенным образом изменили все сферы общественной жизни, создали новые возможности для коммуникации, платежных систем, а также ведения бизнеса.

Указанные обстоятельства не остались без внимания со стороны преступного сообщества, вследствие чего сформировалось новое понятие «киберпреступность». Под кибер-

преступностью понимают совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных [1, с. 46-29]. Например, в 2013 г. наблюдался существенный рост преступлений, предусмотренных ст. 159.3 «Мошенничество с использованием электронных средств платежа» (в 2012 г. зарегистрировано 85 преступлений, в 2013 г. — 1297) [2]. По данным исследования, проведенного в 2018 г. частной компанией «Group-IB», специализирующейся на расследовании киберпреступлений, объемы рынка киберпреступности в РФ выглядят следующим образом:

1. *Мошенничество в системах интернет-банкинга — $446 млн:*
   - Обналичивание других нелегальных доходов — $ 89 млн
   - Фишинг — $ 57 млн
   - Хищение электронных денег — $ 23 млн
2. *Спам:*
   - Медикаменты и различная контрафактная продукция — $ 173 млн
   - Поддельное ПО — $ 120 млн
   - Другое (дейтинг, образование, сфера услуг, путешествия и т.д.) — $ 493 млн
3. *Внутренний рынок:*
   - Продажа трафика — $ 167 млн
   - Продажа эксплойтов –$ 52 млн
   - Продажа загрузок — $ 33 млн
   - Анонимизация — $ 9 млн
4. *DDoS-атаки — $ 109,8 млн*
5. *Иное — $ 166 млн* [3].

Назревшие проблемы борьбы с киберпреступностью обусловлены во многом тем обстоятельством, что развитие интернет-технологий опережает создание эффективных механизмов правового регулирования столь быстро, что это неизбежно приводит к образованию пробелов в праве. Кроме того, борьба с преступлениями в сфере компьютерной информации осложняется тем, что данные деяния посягают на охраняемые законом интересы, которые непосредственно связаны с развитием цифровых технологий и находятся в постоянной динамике. С другой стороны, глобальный характер сети Интернет создает широкие возможности для географии преступлений. Угроза киберпреступных посягательств может исходить из любой точки мира. Интернет-трафик маршрутизируется таким образом, что отследить источник его появления становится невозможным, контроль над передачей данных, их объемом и пользователями является невероятно трудной задачей. При этом субъект преступления, потерпевший и технические средства обработки и передачи данных могут находиться в совершенно разных точках земного шара. Указанные обстоятельства свидетельствуют о том, что эффективная борьба с преступлениями в сфере компьютерной информации, их профилактика возможны только совместными усилиями мирового сообщества.

На сегодняшний день существует несколько частных организаций, оказывающих платные услуги по расследованию киберпреступлений и позиционирующих себя как международные компании по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий (например, упомянутая ранее «Group-IB» и «PENTESTIT»). Указанные организации выработали алгоритм расследования киберпреступлений, учитывающий их разновидности, а также протоколы расследования и продукты для мониторинга, выявления и предупреждения киберугроз. Однако вопрос о правовом регули-

ровании деятельности подобных компаний, а также о реальных показателях эффективности их деятельности остается открытым.

На общегосударственном уровне проблемы кибербезопасности были затронуты Президентом РФ В.В. Путиным. Выступая на пленарном заседании Международного конгресса по кибербезопасности, он отметил увеличение числа кибератак на российские ресурсы, указав, что «обеспечение кибербезопасности — это государственная задача, и в ее решении необходимо объединять усилия правоохранительных органов, деловых кругов, общественных организаций и самих граждан». Также были озвучены конкретные меры, которые необходимо предпринять по борьбе с киберпреступлениями.

1. Предстоит выработать новые комплексные решения по предупреждению и пресечению правонарушений против граждан в цифровой среде. Такие решения должны повышать эффективность реагирования оперативных служб на подобные угрозы. Для этого важно создать соответствующие правовые условия, обеспечить удобные формы взаимодействия граждан и государственных структур.

2. Формирование системы автоматизированного обмена информацией об угрозах в цифровом пространстве. При кибератаках эта система позволит лучше координировать действия операторов связи, кредитных организаций, интернет-компаний с правоохранительными органами и тем самым оперативно ликвидировать возникающие угрозы.

3. Стремление к тому, чтобы в России программное обеспечение и инфраструктура связи основывались на отечественных технологиях и решениях, которые прошли соответствующую проверку и сертификацию.

4. Качественное повышение уровня подготовки российских специалистов по противодействию киберпреступности посредством внедрения практико-ориентированных подходов, использования передового зарубежного и российского опыта.

5. Развитие и совершенствование системы международного обмена информацией о киберугрозах [4].

Уголовное судопроизводство в системе мер противодействия преступлениям в сфере компьютерной информации имеет самостоятельную ценность. Как справедливо отмечает В.М. Корнуков, «уголовный процесс был, есть и будет в первую очередь узаконенным способом (средством) борьбы с преступностью и осуществления правосудия по уголовным делам» [5, с. 56]. На современном этапе своего становления и развития уголовный процесс ориентирован не только на борьбу с преступником и совершенным им преступлением, но и на восстановление социальной справедливости путем разрешения возникшего конфликта между личностью, обществом и государством с наименьшими негативными последствиями [6, с. 114].

Расследование уголовных дел в сфере компьютерной информации представляет немалую сложность, что непосредственно влияет на процессуальную деятельность стороны обвинения, позволяя выделить ряд особенностей. Во-первых, усиленный прокурорский надзор на протяжении всего расследования. Во-вторых, организация межведомственного взаимодействия органов прокуратуры, предварительного следствия, оперативных подразделений. В-третьих, необходимость применения специальных знаний. В-четвертых, особенности обстоятельств, подлежащих доказыванию по уголовному делу. Значимость качественного расследования и разрешения уголовных дел о кибепреступлениях предполагает не только изобличение лиц, виновных в совершении преступления, и устранение его последствий, но и уяснение причин и условий, способствовавших совершению преступления. В какой-то степени именно установление обстоятельств, создающих возможность для совершения преступления, является наиболее важной составляющей, так как позволяет изучить преступление с различных

сторон и на основе этой информации разработать рекомендации по улучшению систем информационной безопасности и предотвратить совершение подобных преступлений в будущем.

Действующее уголовно-процессуальное законодательство в части регламентации особенностей доказательственной деятельности практически не учитывает особенности расследования преступлений в сфере компьютерной информации, представляет собой несоизмеримо сложный процесс познания обстоятельств уголовного дела, а также процесс формирования доказательственной базы по уголовному делу.

Основные принципы и механизмы международного сотрудничества в борьбе с преступлениями в киберпространстве были установлены «Конвенцией о преступности в сфере компьютерной информации» (ETS N 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001). Данный международный правовой акт закрепил также границы криминализации, определил вектор развития национального законодательства и международных стандартов противодействия киберпреступности. Следует отметить, что при всей значимости Конвенции вопросам процессуального права посвящено всего две статьи:

– статья 14. Сфера применения процессуальных норм;

– статья 15. Условия и гарантии.

Представляет определенный интерес положение, сформулированное в п. c) ч. 2 ст. 14 Конвенции: «За исключением случаев, когда положениями статьи 21 конкретно предусматривается иное, каждая Сторона применяет полномочия и процедуры, упомянутые в параграфе 1 настоящей статьи, в отношении:

c) сбора доказательств в электронной форме уголовного преступления».

Понятие «электронной формы уголовного преследования» незнакомо российскому уголовно-процессуальному законодательству. С одной стороны, оценить данное положение можно так, что речь идет об «электронных документах», «электронных доказательствах» или «цифровых доказательствах». В таком случае определенные шаги по реализации положений Конвенции в национальном законодательстве можно считать предпринятыми. В УПК РФ появились такие нормы, как:

– статья 164.1. Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий;

– статья 474.1. Порядок использования электронных документов в уголовном судопроизводстве.

Однако официальный перевод рассматриваемого международного правового акта говорит о некой «электронной форме уголовного преследования». Представляется, что это понятие следует отличать от электронного документооборота и рассматривать его как возможность определенной процессуальной деятельности по собиранию доказательств в информационной цифровой среде, признание таких доказательств равнозначными традиционным.

С точки зрения действующего УПК РФ это предполагает проведение ряда специальных судебных экспертиз: информационно-технологической и информационно-технической.

Объектом информационно-технологической экспертизы является установленный порядок обработки информации, осуществляемый по заданным алгоритмам, или информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества.

Информационно-технологическая экспертиза назначается в тех случаях, когда для возникающих в ходе расследования вопросов требуются специальные познания в технологии информационных процессов.

Возможности этой экспертизы достаточно широки. С ее помощью можно определить:

– соответствие существующего технологического процесса компьютерной обработки информации проектной и эксплуатационной документации на конкретную информационную систему либо сеть;

– конкретные отклонения от установленной информационной технологии, а также непосредственных исполнителей, допустивших нарушение установленной информационной технологии;

– надежность организационно-технологических мер защиты компьютерной информации;

– вредные последствия, наступившие из-за неправомерного нарушения установленной технологии компьютерной обработки информации;

– обстоятельства, способствовавшие преступному нарушению технологии электронной обработки информации.

Исследуя обстоятельства совершенного преступления в сфере компьютерной информации, всегда приходится иметь дело с тремя основными группами объектов, а именно:

1. Техническими средствами обработки информации.
2. Электронными носителями информации.
3. Программным обеспечением и базами данных.

Очевидно, что преступления в киберпространстве являются крайне сложными для расследования, они требуют весьма специфических специальных знаний, которые всегда будут соответствовать тенденциям развития информационных технологий. Способы совершения преступлений постоянно адаптируются и развиваются, появляются их совершенно новые формы (к примеру, развитие рынка криптовалют и расширение электронных платежей провоцирует создание ранее неизвестных способов хищения). Кроме того, постоянно изменяются программы-взломщики, вирусы, контент различного содержания, который распространяется через мобильные средства связи, мобильные приложения (CMC или MMC, Bluetooth), электронную почту, веб-доски объявлений, чаты и группы в социальных сетях, NFC-приемники.

Расследование самого простого киберпреступления (рассылка электронных писем с информацией о том, что владельцы денежных средств стали обладателями наследства или победителями акции (лотереи), в результате которого денежные средства владельца переходят на счет злоумышленников, требует целого комплекса процессуальных действий от следователя и дознавателя:

1) получить показания потерпевшего, сотрудников отдела информационной безопасности банка, сотрудников интернет-провайдера;

2) поручить проведение оперативно-розыскных мероприятий, направленных на установление лица, совершившего хищение;

3) получить ответы банка о перечислении денежных средств со счета потерпевшего, снятии денежных средств в банкомате;

4) получить ответы Бюро специальных технических мероприятий (подразделения МВД России) об установлении информации учетных записей в социальных сетях, электронной почтовой службы, информации об администрировании этих данных;

5) при установлении личности хакера произвести его задержание, решить вопрос об избрании меры пресечения, допросить в качестве подозреваемого, произвести обыск, изъять компьютерную технику, которая послужит объектом исследования компьютерно-технической экспертизы [7].

Подводя итоги, следует отметить, что угроза совершения преступлений в киберпространстве становится все более серьезной с развитием информационных технологий,

технологий машинного обучения и искусственного интеллекта. Эффективное противодействие таким вызовам можно осуществлять только путем комплексной адаптации всех сфер общественной жизни, начиная с правил личной «компьютерной гигиены», продолжая созданием правового режима, обеспечивающего компьютерную безопасность и завершая полномасштабным международным сотрудничеством как в сфере уголовного судопроизводства, так и за его пределами. В числе частных способов, направленных на комплексное решение проблемы киберпреступности, можно назвать внедрение спецкурсов о расследовании киберпреступлений еще на этапе получения юридического образования (например, в настоящее время существует общедоступный университетский модуль «Модуль 5. Расследование киберпреступлений», разработанный ООН в 2019 г.) [8]; проведение профильной специализации судей и органов расследования; обеспечение получения ими образования в сфере IT-технологий, позволяющих грамотно и оперативно осуществлять расследование киберпреступлений, правильно ставить вопросы эксперту и оценивать экспертное заключение.

Список литературы

1. Нестерович С.А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов // Вестник науки и образования. № 8 (44). 2018. С. 46-49.

2. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий // Официальный сайт Генеральной прокуратуры РФ. URL: https://genproc.gov.ru/smi/news/genproc/news-1431104/ (дата обращения: 14.10.2019).

3. Исследование о тенденциях высокотехнологичных преступлений и прогнозы Group-IB на следующий год. URL: https://www.group-ib.ru/resources/threat-research.html (дата обращения: 16.10.2019).

4. Пленарное заседание Международного конгресса по кибербезопасности // Официальный сайт Президента РФ. URL: http://www.kremlin.ru/events/president/news/57957 (дата обращения: 14.10.2019).

5. Корнуков В.М. Назначение уголовного судопроизводства и его отражение в регламентации отдельных стадий и институтов // Концептуальные основы реформы уголовного судопроизводства в России: материалы науч. конф. (г. Москва, 22, 23 января 2002 г.). М., 2002. С. 56–59.

6. Михайловская И.Б. Социальное назначение уголовной юстиции // Государство и право. 2005. № 5. С. 111-118.

7. Киберпреступлений становится все больше, однако их раскрываемость уменьшается // Адвокатская газета. Орган Федеральной палаты адвокатов РФ. URL: https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/ (дата обращения: 15.10.2019).

8. Серия университетских модулей. Образование для правосудия. Дохинская декларация: поощрение культуры, соблюдение законности // Модуль 5. Расследование киберпреступлений. URL: https://www.unodc.org/documents/e4j/Cybercrime_ Module_5_Cybercrime_Investigation_RU.pdf (дата обращения: 16.10.2019).

Л.В. Лазарева, *д.ю.н., профессор кафедры уголовно-процессуального права и криминалистики Владимирского юридического института ФСИН России, г. Владимир*

О ДОКАЗЫВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛЬНЫХ ЗНАНИЙ

Среди различных институтов уголовно-процессуального права, которых коснулась глобальная цифровизация, можно выделить институт специальных знаний, имеющий прямое отношение к использованию последних достижений современной науки в процессе расследования преступлений. Как справедливо отмечает В.Д. Зорькин, «сегодня зарождается новое право — «право второго модерна», регулирующее экономические, политические и социальные отношения в контексте мира цифр, больших данных, роботов, искусственного интеллекта» [1].

Мониторинг следственной практики свидетельствует, что информационные технологии используются при совершении самых разных преступлений, например, с использованием электронных средств платежа, мошенничества в сфере компьютерной информации, неправомерный оборот средств платежей, нарушение авторских и смежных прав, преступлений в банковской сфере, распространение наркотических средств, заведомо ложные сообщения о террористических актах и многие др.

Вопросы использования специальных знаний при расследовании преступлений были и остаются сегодня предметом бурных дискуссий, как в научных кругах, так и среди практиков. И в этом нет ничего удивительного. Внедрение в уголовно-процессуальную деятельность информационных технологий способствует более широкому использованию специальных знаний, но в то же время поднимает вопросы о правовом регулировании участия специалиста в следственных действиях, использовании в доказывании заключения и показаний специалиста, возможности привлечения специалиста стороной защиты и многие другие.

Анализ законодательных норм, научной литературы и правоприменительной практики свидетельствует, что до настоящего времени не достигнуто общее понимания по поводу процессуального статуса специалиста и порядка его участия в уголовном деле, а также отсутствие общепризнанности заключения и показаний специалиста как средств доказывания. Поэтому нет ничего удивительного, что в правоприменительной практике наблюдаются серьезные затруднения по привлечению специалиста к участию в уголовном деле, использованию в процессе доказывания его заключения и показаний.

Расследование преступлений в сфере информационных технологий представляет особую сложность, что обусловливается не только их спецификой и неочевидностью, но и присущим им межрегиональным и международным характером [2]. В настоящее время предварительное расследование преступлений указанной категории производится следователями МВД России, а также следователями ФСБ России. Однако следователю бывает тяжело одинаково хорошо расследовать уголовные дела о незаконном обороте наркотиков, квартирной краже и неправомерном доступе к компьютерной информации, несмотря на помощь сотрудников созданного в МВД России Бюро специальных технических мероприятий (Управление «К»). Кроме того, как справедливо отмечает А.Ф. Волынский, и мы с ним солидарны, «техникоемкость деятельности следователя, оперативного работника приобрела к настоящему времени такие масштабы, когда им самим обеспечить эффективное использование имеющихся в их распоряжении средств (компьютерной техники, видеозаписи, фотосъемки и др.) физически невозможно без ущерба для процесса раскрытия и расследования преступлений» [3, с. 120].

Новые требования, методы и подходы в практике борьбы с киберпреступностью требуют систематического пополнения специальных знаний и овладения современными достижениями науки и техники. Рассматривая вопрос использования специальных знаний, следует остановиться на проблеме выбора специалиста. Применительно к конкретному специалисту, как

участнику уголовного процесса, особое значение приобретает его компетентность, т.е. характеристика конкретного человека, получившего квалификацию, которая определяется его профессиональным уровнем. Компетентность, как профессиональная характеристика специалиста, основана на его профессиональных качествах, интеллекте и опыте.

Безусловно, что объем необходимых специальных знаний будет различаться в зависимости от ситуации и решаемых специалистом задач. Так, при производстве таких следственных действий, как осмотр, выемка, обыск, сопровождающиеся изъятием электронных носителей информации и копированием с них информации (ст. 164.1 УПК РФ), требуются специалисты, которые обладают умениями и навыками пользоваться цифровыми технологиями, обладать только цифровой грамотностью уже недостаточно.

Использование специальных знаний в расследовании преступлений является средством познавательной деятельности, поскольку специалист оказывает содействие органам предварительного расследования в установлении обстоятельств, подлежащих доказыванию по уголовному делу. Оставаясь в большинстве случаев техническим помощником следователя, специалист сегодня является еще и посредником в познавательной деятельности субъектов доказывания. Поскольку эта деятельность связана с восприятием объектов материального мира, то субъекты доказывания взаимодействуют с информацией, извлекаемой из сознания специалистов. В свою очередь специалист также выступает субъектом познания, взаимодействуя тем или иным образом с обстоятельствами, подлежащими доказыванию. Деятельность специалиста как участника уголовного судопроизводства основана на использовании при ее выполнении соответствующих знаний. При этом качественные и количественные характеристики зависят от объема знаний, которые имеют историко-бытовой характер и от знаний, приобретаемых в процессе профессионально-практической деятельности, характеризующей специальные знания. Объем таких знаний неограничен и постоянно пополняется не только в процессе образования, но и повышения квалификации, стажировок, практик и т.д.

Поэтому приобретает особо важное значение рекомендация по привлечению специалистов в области информационно-компьютерных технологий уже на этапе планирования и подготовки следственных действий, связанных с поиском, обнаружением и фиксацией следов преступления, с целью получения компетентных разъяснений относительно доступности электронных доказательств и необходимости принятия мер к их сохранности [4, с. 181].

Учитывая существующее множество компьютерных и коммуникационных устройств, имеющих особенности конструкции, принципа работы, технической реализации, считаем привлечение специалиста обязательным условием производства таких следственных действий, как осмотр, выемка, обыск, сопровождающиеся изъятием электронных носителей информации, что значительно увеличивает возможность обнаружения цифровых следов преступления, к которым относят криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе возникновения данной информации, ее обработки, хранения и передачи [5, с. 6-8].

Нам представляется вполне очевидным, что практика производства отдельных следственных действий, в ходе которых осуществляется изъятие электронных носителей информации и копирование с них информации, была бы иной в случае обязательного участия специалиста. Это обстоятельство, на наш взгляд, представляет собой объективную реальность одного из важнейших элементов повышения эффективности расследования преступлений в сфере информационных технологий. При этом, как отмечается, следователь, не будучи специалистом в сфере компьютерных технологий, должен понимать, какими компетенциями должен обладать специалист, привлекаемый к проведению следственных действий, какие технические средства будут им применяться, чтобы обеспечить исчерпывающие меры к обнаружению и фиксации доказательств и исключить их утрату [4, с. 182].

С целью изучения вопроса об эффективности использования специальных знаний в уголовном судопроизводстве нами проведено соответствующее анкетирование среди судей,

прокуроров, следователей и адвокатов. Результаты анкетирования свидетельствуют о том, что большинство участников уголовного процесса положительно оценивают роль специалиста в процессе доказывания.

Между тем несовершенство действующего законодательства, связанное с терминологической неопределенностью, носит не только теоретический характер, но и имеет отражение в практической деятельности.

Из содержания статьи 58 УПК РФ можно предположить, что участие специалиста является не столько его правом, сколько обязанностью, что ставит его реализацию в зависимость от усмотрения лиц, в чьем производстве находится уголовное дело. Вследствие чего у практических работников складывается самое разное представление о круге процессуальных обязанностей специалиста.

Ранее мы предлагали один из вариантов решения проблемы путем получения согласия специалиста [6, с. 129], который, на наш взгляд, будет способствовать не только возможности реализации принципа состязательности в уголовном судопроизводстве, но и обеспечению права специалиста на свободный труд, в случае если выполнение его процессуальных обязанностей выходит за рамки должностных. Однако подобные идеи не получили пока законодательной поддержки.

Еще один вопрос, который не стоит оставлять без внимания — кем определяется, что лицо является специалистом. К сожалению, этот, казалось бы, простой вопрос вызывает сложности на практике. Так, имеют место случаи, когда некоторые правоприменители полагают, что если в законе не закреплен порядок привлечения специалиста, то реализация им своих функций невозможна. Это заблуждение приводит к тому, что следователи отказывают в удовлетворении ходатайства стороны защиты в привлечении специалиста к участию в процессуальных действиях [7, с. 68-72]. Данный вопрос, являясь предметом научных дискуссий, также на протяжении многих лет входил в круг наших научных изысканий и неоднократно освещался нами в специальной литературе. Не видим надобности приводить новые аргументы. По нашему глубокому убеждению, решать вопрос о том, является ли вызванное или приглашенное лицо специалистом, должна исключительно сторона, инициирующая вызов (приглашение) данного лица.

Рассматривая деятельность специалиста как субъекта правоприменительной деятельности, стоит обратить внимание ее на двусторонний характер. Однако сторона защиты ограничена в использовании специальных знаний посредством специалиста.

Специалист, вовлеченный в уголовный процесс по инициативе защитника, может принести существенную пользу в процессе формирования доказательств.

Один из вариантов решения проблемы о признании полученного защитником заключения специалиста доказательством предложен А.А. Тарасовым, который предлагает обязательный допрос такого специалиста следователем и судом [8, с. 156].

Весьма уместно предложение, представляющее не только научный, но и практический интерес, выдвинуто Ф.Г. Аминевым, согласно которому следует «взять все прогрессивное, что имеется в УПК зарубежных стран, адаптировать, закрепить в УПК РФ и применить на практике, а именно, ввести в УПК РФ ст. 204.1 «Заключение специалиста» [9, с. 28]. Подобная позиция высказывалась ранее и нами [10, с. 108-112].

Кстати, подобные идеи уже получили воплощение в некоторых государствах на постсоветском пространстве. В частности, ст. 117 УПК Республики Казахстан называется «Заключение и показания специалиста». И хотя процессуальный порядок получения данного доказательства выглядит поверхностным, по крайней мере, в статье определена его структура и содержание.

В настоящее время в уголовно-процессуальной доктрине существует позиция, заслуживающая внимания, согласно которой заключение специалиста предстает перед следователем в готовом виде и никакому процессуальному формированию не подлежат. В этой связи

отпадает необходимость специальных процессуальных процедур, направленных на формирование этого доказательства. Как справедливо отмечает С.Б. Россинский, речь следует вести о его процессуальной легализации, введении в уголовное дело посредством представления, истребования или изъятия как элемента некоторых следственных действий [11, с. 28-29].

В своих работах мы неоднократно высказывались по этому поводу и предлагали решение этой проблемы посредством включения самостоятельной нормы в УПК РФ, регламентирующей данную процедуру, как более логичной и отвечающей современным подходам к методологии процессуального доказывания [12, с. 185-187]. Полагаем, что с расширением цифровых технологий в уголовном судопроизводстве у правоприменителя могут возникнуть новые трудности в данном направлении.

В заключение отметим необходимость комплексного подхода к вопросам использования специальных знаний в расследовании преступлений цифровой среды, что способствовало бы более широкому внедрению научных и технических возможностей в правоприменительную практику.

Список литературы

1. Зорькин В.Д. Право в цифровом мире. URL: https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html. (дата обращения: 17.03.2020).

2. Расследованием киберпреступлений в СКР займется спецотдел. URL: https://tass.ru/proisshestviya/7889859 (дата обращения: 17.04.2020).

3. Волынский А.Ф. Республика Беларусь реформировала систему судебно-экспертных учреждений. А Россия? // Теория и практика судебной экспертизы в современных условиях: материалы Междунар. науч.-практ. конф. М.: Проспект, 2015. С. 119-124.

4. Семикаленова А.И., Рядовский И.А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6 (103). С. 178-185.

5. Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Междунар. науч.-практ. конференции (19 февраля 2019 г.). Алматы, 2019. С. 6-8.

6. Лазарева Л.В. Концептуальные основы использования специальных знаний в российском уголовном судопроизводстве: дисс. … докт. юрид. наук. Владимир, 2011. 470 с.

7. Галинская А.Е. Использование специальных знаний в судопроизводстве сторонами и их представителями: дисс. …канд. юрид. наук. М., 2017. 158 с.

8. Тарасов А.А. Эксперт и специалист в уголовном процессе России. Уфа: РИЦ БашГУ, 2014. 184 с.

9. Аминев Ф.Г. Теория и практика использования специальных знаний в расследовании преступлений. Уфа: РИЦ БашГУ, 2015. 166 с.

10. Лазарева Л.В. Собирание доказательств посредством использования специальных // Библиотека криминалиста. № 1 (30). 2017. С. 108-112.

11. Россинский С.Б. Следственные действия. М.: Норма, 2018. 240с.

12. Лазарева Л.В. К вопросу о доказательственном значении заключения и показаний специалиста в уголовном процессе // Доказывание и принятие решений в современном уголовном судопроизводстве: сб. научн. трудов. М., 2011. С. 185-187.

М.В. Меркулова, *к.ю.н., старший преподаватель кафедры криминалистики Московского университета МВД России имени В.Я. Кикотя, г. Москва*

О НЕКОТОРЫХ ПРОБЛЕМАХ ОСМОТРА ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

Цифровизация всех сфер жизнедеятельности человека в современных условиях закономерно приводит к активному использованию информационных технологий в преступных целях. Согласно официальным данным МВД России, противоправные деяния в сфере информационно-телекоммуникационных технологий оказывают все большее влияние на структуру преступности. Только за период с января по май 2020 г. их количество выросло на 85,1% (в том числе тяжких и особо тяжких — на 123,7%), а удельный вес возрос до 21,7% от общего числа [1]. Массовый характер получили различные виды мошенничества в сети Интернет, распространение материалов клеветнического и экстремистского характера, неправомерное вмешательство в работу различных автоматизированных систем, хищение денег с банковских счетов граждан и юридических лиц. Так, за указанный период текущего года почти в 6 раз увеличилось количество преступлений, совершенных с использованием расчетных (пластиковых) карт [1].

Органами внутренних дел уделяется повышенное внимание выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий. Для своевременного реагирования на киберпреступления принимаются меры по развитию взаимодействия с кредитными организациями, провайдерами, операторами связи и владельцами интернет-сервисов. Вместе с тем отсутствие единых алгоритмов выявления и раскрытия киберпреступлений, недостаток профессионально подготовленных кадров и современного технического оснащения наряду с масштабами распространения и разнообразием схем и методов совершения преступлений в IT-сфере на сегодняшний день не позволяет добиться кардинального улучшения ситуации [2].

Сказанное не оставляет сомнений в необходимости постоянного совершенствования тактики осмотра персональных компьютеров (далее — ПК) и связанного с ними оборудования. Особую сложность при этом создает специфика объекта осмотра, которая заключается в том, что программная часть ПК, как правило, не может быть осмотрена только путем непосредственного восприятия следователем. Для доступа к интересующим следствие данным требуется масштабное использование специальных знаний и, соответственно, помощь специалиста (иногда нескольких). Однако принимая во внимание возможность защиты указанных данных, ученые и практики отмечают, что преимущественным способом обнаружения интересующей следствие компьютерной информации является компьютерно-техническая экспертиза, в связи с чем актуальной представляется проблема разграничения возможностей осмотра и судебной экспертизы [3, 4].

Отметим, что в качестве объекта осмотра могут выступать: компьютеры, представляющие собой отдельные технические средства обработки информации; компьютеры, входящие в локальную или глобальную сеть; серверы (специализированные компьютеры, выделенные из группы ПК для выполнения сервисных задач без непосредственного участия человека); сетевое оборудование (маршрутизаторы, соединительные кабели и т.д.); периферийные устройства и подключаемые устройства хранения информации (внешние накопители, веб-камеры, принтеры, сканеры и т.д.).

Отдельного рассмотрения требует вопрос привлечения специалистов к участию в осмотре компьютерной техники. Помимо специалиста-криминалиста, целесообразность участия которого в рассматриваемом следственном действии не вызывает сомнений, требуется привлечение и специалистов в иных областях. Чаще всего это лица, компетентные в конкретной области, связанной с компьютерными системами и технологиями: инженер-программист, специалист по сетевым технологиям (администратор вычислительных сетей), системам

электросвязи (в т.ч. слаботочным системам) и др. Требуемый профиль знаний определяется в зависимости от целей и задач осмотра с учетом данных о характере преступления, при этом на практике в качестве специалистов могут выступать не только эксперты, но и сотрудники информационно-аналитических подразделений органов внутренних дел (информационных центров, вычислительных центров). При необходимости в число участников могут быть включены и лица, специализирующиеся в смежных областях знаний, а также работающие с конкретным прикладным программным обеспечением: инженеры-электрики, бухгалтеры, специалисты по автоматизированному проектированию и др.

Если компьютеры объединены в локальную сеть, следует организовать их одновременный осмотр. При этом необходимо установить расположение, назначение и IP-адреса всех компьютеров в сети, наличие сервера, маршрутизаторов (роутеров), места прокладки кабелей, расположение точек подключения к каналам связи (компьютерных розеток). При осмотре сетевого оборудования обращается внимание на целостность кабельных соединений, а также на отсутствие следов подключения посторонней аппаратуры. В случае размещения сетевых кабелей в стенах помещения (так называемой скрытой проводки) магистраль недоступна для непосредственного восприятия, однако проблему позволяет решить использование кабельного тестера (LAN-тестера) — технического устройства, проверяющего состояние кабельной линии. Заметим, что использование тестирующих устройств оправдано и во всех других случаях, когда требуется проверка целостности сетевого кабеля, поскольку зачастую повреждения линии не могут быть определены визуально.

Определенные затруднения на практике могут быть связаны и с описанием персонального компьютера в протоколе осмотра. Нами предлагается следующая схема такого описания.

1. Количество и схема расположения ПК и связанного с ними оборудования, т.е. рабочих мест пользователей (если компьютер входит в локальную сеть).
2. Тип и марка ПК (например: *«объектом осмотра является персональный компьютер IBM PC фирмы Kraftway»*).
3. Характеристики системного блока: наличие и состояние световых индикаторов, аудио- и USB-разъемов, приводов для работы с оптическими компакт-дисками, маркировочных обозначений, пломб, а также наличие загрязнений и механических повреждений.
4. Технические характеристики соединения системного блока с монитором и клавиатурой.
5. Характеристики монитора (марка, модификация, модель, серийный номер, инвентарный номер, цвет и материал корпуса, размер экрана) и клавиатуры (тип, марка, модель, заводской номер).
6. Способ подключения системного блока и монитора к бытовой электросети (например, через сетевой фильтр).
7. Включен или выключен компьютер на момент осмотра.
8. Работоспособность компьютера (если он находится во включенном состоянии, либо после включения в ходе осмотра).
9. Внутренняя спецификация процессорного блока (согласно таблице POST-сведений, выводимой на экран при загрузке компьютера): характеристика системной платы, процессора, жесткого диска, объем оперативной памяти.
10. Характеристики операционной системы, установленной на осматриваемом компьютере (например: *«операционная система Windows 7 SP1 (код программного продукта 00426-OEM-8992662-00010) с пакетом прикладных программ MS OFFICE 2003, Adobe Photoshop CS5, Far Manager версии 2.0 и Norton Internet Security версии 22.17.0.183 фирмы Symantec Corporation»)*.

11. Подключение к компьютеру внешнего накопителя (с участием специалиста) для последующего копирования информации, имеющей отношение к расследуемому делу.

12. Буквенные обозначения имеющихся логических дисков и устройств со съемными носителями.

13. Характеристики логических дисков (например: *«на диске C всего 500 000 Мб места, из них свободно 119 000 Мб; на диске D всего 500 000 Мб места, из них свободно 328 000 Мб»*).

14. Количество каталогов и файлов, находящихся на логических дисках (например: *«на логическом диске C находятся 2200 каталогов и 11267 файлов, из которых 715 скрытых; на логическом диске D находятся 526 каталогов и 3692 файла, из которых 204 скрытых. Сделаны скриншоты №3-7 таблиц каталогов и файлов, находящихся на дисках C и D»*).

15. Запуск находящихся на осматриваемом компьютере программ, осуществляемый специалистом (например: «*специалистом произведена проверка системы компьютера на наличие вредоносных программ для ЭВМ с помощью установленной на осматриваемом компьютере антивирусной программы Norton Internet Security с актуальными базами вирусных сигнатур по состоянию на 11.02.2020 г. В результате проверки было выявлено наличие в памяти компьютера и на системном диске C в директории c:/windows/system32 файла iomem.exe с сигнатурой вируса OneHalf.3544. Сделан скриншот № 8 таблицы результатов сканирования системы»*).

16. Копирование специалистом информации, выведенной на монитор (например: *«с помощью клавиши «Print Screen» сделан скриншот №1 диалогового окна «Свойства: Системный диск (C:)» и скриншот №2 диалогового окна «Свойства: Delta (D:)»»*).

17. Сохранение полученных копий информации на внешнем накопителе (например: *«с использованием портативной версии программы Adobe Photoshop CS5 Portable, установленной на внешнем жестком диске Следственного управления при УМВД г. Н-ска, все сделанные скриншоты последовательно сохранены на данном жестком диске в восьми файлах: 198510scr1.jpg, 198510scr2.jpg, 198510scr3.jpg, 198510scr4.jpg, 198510scr5.jpg, 198510scr6.jpg, 198510scr7.jpg, 198510scr8.jpg — без ретуширования и изменения графических элементов»*).

В ходе осмотра компьютер фотографируется по правилам узловой и детальной фотосъемки; составляется схема проводного соединения системного блока, монитора и клавиатуры между собой и с бытовой электросетью. После осмотра компьютер выключается. Системный блок отключается и опечатывается наклеиванием листа бумаги с подписями следователя и понятых. В дальнейшем осмотренная техника может быть направлена на компьютерно-техническую экспертизу.

На наш взгляд, изложенное еще раз подтверждает, что эффективность производства рассматриваемого следственного действия напрямую связана с организацией подготовки квалифицированных кадров для правоохранительных органов, необходимостью постоянного отслеживания новых технических средств и методов и интеграции их в сферу борьбы с преступлениями, совершаемыми с использованием информационных технологий.

Список литературы

1. Официальный сайт Министерства внутренних дел Российской Федерации: Материалы ФКУ ГИАЦ Состояние преступности в России за январь-май 2020 года. URL: https://мвд.рф/reports/item/20422560.

2. Официальный сайт Министерства внутренних дел Российской Федерации: Выступление Министра внутренних дел Российской Федерации генерала полиции Российской Федерации Владимира Колокольцева на расширенном заседании коллегии Министерства внутренних дел Российской Федерации 26 февраля 2020 г. URL: https://мвд.рф/ document/19639152.

3. Коломинов В.В. Осмотр места происшествия по делам в сфере компьютерной информации // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 145-149.

4. Пропастин С.В. Осмотр или судебная экспертиза: выбор в пограничных ситуациях (на примере обнаружения и исследования компьютерной информации) // Современное право. 2013. № 6. С. 129-132.

Е.А. Моляров, *адъюнкт кафедры оперативно-разыскной деятельности ОВД Барнаульского юридического института МВД России, г. Барнаул*

ОСОБЕННОСТИ ОТОЖДЕСТВЛЕНИЯ ЛИЧНОСТИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ПОИСКОВЫХ СИСТЕМ

Не вдаваясь в дискуссию относительно понятия отождествления личности как оперативно-розыскного мероприятия, обратимся к Модельному закону Содружества Независимых Государств об оперативно-розыскной деятельности (2007), где отождествление личности определяется как установление и идентификация лица по индивидуализирующим статическим и динамическим неизменяемым признакам, а равно и при помощи других способов, позволяющих с достаточной степенью вероятности опознать личность.

Отождествление личности, проводимое с использованием информационно-поисковых систем, созданных для идентификационных задач, имеет свои особенности.

В соответствии со ст. 2 Федерального закона от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации», информационная система представляет собой совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [1]. Что касается информационно-поисковых систем, то они создаются специально для обеспечения поиска и отбора данных, имеющихся в базах данных. В настоящее время каждым субъектом оперативно-розыскной деятельности (далее – ОРД) созданы собственные информационно-поисковые системы, используемые для решения служебных задач. В частности, сотрудниками оперативных подразделений органов внутренних дел при отождествлении личности используются такие ведомственные информационно-поисковые системы, как АДИС, АИПС «Сова», «Портрет-поиск», «Опознание» и др.

Изучение оперативно-розыскной практики показало, что информационно-поисковые системы используются преимущественно как средства (инструменты) отождествления личности, поскольку они (информационные системы) способны выполнять идентификационную задачу. Однако в рассматриваемых системах может содержаться визуальная информация, отражающая внешние признаки человека, поэтому не исключено их использование и в качестве ресурсов, позволяющих получить необходимую для обеспечения отождествления личности идентификационную информацию об опознаваемых объектах.

Акцентируем внимание на новых направлениях развития таких систем, направленных на повышение эффективности проведения исследуемого оперативно-розыскного мероприятия (далее — ОРМ).

Следует подчеркнуть, что посредством информационно-поисковых систем, используемых при отождествлении личности, выполняются исключительно идентификационные задачи, поскольку посредством таких систем возможно осуществлять лишь сравнение (сличение) искомого объекта с объектами, имеющимися в базах данных. При этом диагностические

задачи, направленные на выявление новых признаков искомого объекта, определение его групповой принадлежности посредством рассматриваемых систем не выполняются.

Отметим, что лежащий в основе ОРМ «отождествление личности» оперативно-розыскной метод «оперативное распознание» помимо установления тождества предполагает и определение групповой принадлежности объектов, представляющих оперативный интерес. По результатам проведенного нами анкетирования сотрудников оперативных подразделений 52% респондентов отметили, что проведение ОРМ «отождествление личности» может включать в себя установление групповой принадлежности опознаваемого лица. Вряд ли кто-то не согласится с тем, что путем анализа запечатленных на фото- либо видеоизображении признаков внешности человека оперативным сотрудником могут быть с определенной долей вероятности определены его национальная принадлежность, возраст, профессия, наличие заболеваний, психических отклонений, принадлежность к криминальным структурам и т.д. Такая аналитическая информация может способствовать сужению круга поиска искомого объекта, выбору наиболее эффективных тактических приемов проведения в отношении него последующих мероприятий и, в целом, может использоваться для выдвижения версий и организации раскрытия преступления.

Полагаем, что существующий сегодня потенциал информационных технологий позволяет построить информационные системы, способные в автоматизированном режиме наряду с идентификационными задачами выполнять и диагностические не хуже, чем это может сделать оперативный сотрудник непосредственно.

О наличии потенциальной возможности построения систем с расширенными аналитическими возможностями высказался профессор С.А. Ялышев. Им было отмечено, что создание подобных систем позволит не только перечислить ранее зарегистрированные объекты, но и с некоторой долей вероятности спрогнозировать качества иных неизвестных признаков, а может спрогнозировать и искомый объект, даже если он не зарегистрирован в массиве [2].

Одним из обязательных условий построения таких систем является накопление знаний о внутренних взаимосвязях одних признаков внешности человека (статических и динамических) с другими его признаками, в том числе не относящихся к его внешности. В данной области уже имеются некоторые научные наработки. Например, учеными-психологами выявлены взаимосвязи признаков внешности (статических и динамических) человека с его проявлениями психики. На основе этих знаний разработана методика визуальной психодиагностики [3]. Надо сказать, что данная методика применяется и в ОРД [4].

Представляют интерес и результаты исследования, проведенного П.В. Пинчуком, которые указывают на существование взаимосвязи типов папиллярных узоров на дистальных фалангах пальцев рук, их сочетания с идентификационно-значимыми антропометрическими параметрами головы человека [5]. Как представляется, подобных взаимосвязей существует десятки и сотни, а имеющийся сегодня уровень развития информационных технологий позволяет проводить исследования, направленные на выявление указанных закономерностей.

Другим обязательным условием для построения систем с повышенными аналитическими возможностями является интеграция различных видов оперативно-розыскных и криминалистических учетов с целью объединения всего имеющегося массива информации, а также расширение перечней регистрируемых признаков объектов учета. Это необходимо, собственно, для обеспечения выполнения информационной системой диагностических задач, направленных на получение новых сведений об объекте диагностики, а также для обеспечения исследований, направленных на выявление внутренних взаимосвязей одних признаков объекта с другими. Полагаем, что такая информационная система должна основываться на применении технологий искусственного интеллекта (нейронных сетях). Также искусственный интеллект должен применяться и при проведении вышеупомянутых исследований.

Полагаем, что построение информационных систем, способных в автоматизированном режиме одновременно выполнять идентификационные и диагностические задачи существенно повысят эффективность проведения ОРМ «отождествление личности».

Список литературы

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149 // КонсультантПлюс.

2. Ялышев С.А. Новые направления развития экспертно-криминалистических учетов в контексте повышения эффективности раскры-тия и расследования нераскрытых преступлений прошлых лет // Известия ТулГУ. Экономические и юридические науки. 2016. №1-2. URL: https://cyberleninka.ru/article/n/novye-napravleniya-razvitiya-ekspertnokriminalisticheskih-uchetov-v-kontekste-povysheniya-effektivnosti-raskrytiya-i-rassledovaniya (дата обращения: 03.07.2020).

3. Костина Л.Н. Визуальная психодиагностика как метод познания и предварительной оценки личности в профессиональной дея-тельности психолога // Вестник Московского университета МВД России. 2016. № 6. URL: https://cyberleninka.ru/article/n/vizualnaya-psihodiagnostika-kak-metod-poznaniya-i-predvaritelnoy-otsenki-lichnosti-v-professionalnoy-deyatelnosti-psihologa (дата обращения: 03.07.2020).

4. Яковец Е.Н. Формирование социально-психологического портрета лица, участвующего в осуществлении оперативно-розыскных мероприятий // Труды Академии управления МВД России. 2019. № 2 (50). URL: https://cyberleninka.ru/article/n/formirovanie-sotsialno-psihologicheskogo-portreta-litsa-uchastvuyuschego-v-osuschestvlenii-operativno-rozysknyh-meropriyatii (дата обращения: 03.07.2020).

5. Пинчук П.В. Экспертные возможности решения идентификационных задач на основе взаимосвязи между дактилоскопическими признаками и биологическими характеристиками человека (экспериментальное исследование): автореф. дисс. … канд. мед. наук. М., 2002. С. 22-23.

И.А. Неупокоева, *к.ю.н, доцент кафедры криминалистики Омской академии МВД России, г. Омск*

СОВРЕМЕННЫЙ ПОДХОД К КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКЕ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ

Согласно статистическим данным, в Российской Федерации за январь-декабрь 2019 г. зарегистрировано более 294 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или, что почти на 70% больше, чем за аналогичный период прошлого года. Половина таких преступлений совершается с использованием сети Интернет, а более трети с использованием средств мобильной связи. Свыше 98% таких преступлений выявляется органами внутренних дел [1]. Безусловно, что большую часть преступлений, совершенных таким способом, составляет сбыт сбыта наркотических средств и психотропных веществ.

В этой связи в некоторых территориальных органах МВД России на региональном уровне в структуре управлений по контролю за оборотом наркотиков в настоящее время созданы отделения по противодействию наркоугрозе в сети Интернет, например, в городе Омске создан отдел по расследованию преступлений, совершенных с использованием информационных технологий, средств мобильной связи, сети «Интернет» и вредоносного программного обеспечения СУ УМВД России по г. Омску. Специалисты отмечают, что сбыт наркотических

средств, психотропных веществ и их аналогов с использованием информационно-телекоммуникационных технологий (включая сеть Интернет) существенно способствует наркотизации населения и наркопреступности в целом. Количество преступлений, совершенных данным способом, за последние годы увеличилось в сотни раз [2, с. 126]. Неслучайно законодатель дополнил часть вторую статьи 228.1 Уголовного кодекса Российской Федерации (далее — УК РФ) пунктом «б», устанавливающим уголовную ответственность за сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») [3].

Результаты научных исследований в рассматриваемой сфере используются для формирования криминалистической характеристики преступлений о незаконном сбыте наркотических средств, психотропных веществ и их аналогов по средствам информационно-телекоммуникационной сети «Интернет» которая предназначена как для совершенствования частных методик расследования, так и для непосредственного их использования следователем при организации расследования, в частности для определения в проблемной ситуации эффективных путей решения задач расследования [4, 5]. Анализ учебной и научной литературы по криминалистике, а также практика расследования уголовных дел, материалов, опубликованных в Бюллетене Верховного Суда РФ, а также официальных материалов, размещенных на сайтах судов, позволяет утверждать, что криминалистическая характеристика таких преступлений, должна включать следующие основные элементы:

1) характеристику самого преступного события (объект преступного посягательства; место, время, условия и другие обстоятельства);

2) предмет преступного посягательства (наркотические средства, психотропные вещества и их аналоги);

3) нарушение существующих нормативных правовых актов, связанных с оборотом наркотических средств, психотропных веществ и их аналогов [6-8];

4) корыстные мотивы и цель совершения преступлений (получение материальной выгоды от незаконного сбыта наркотических средств психотропных веществ и их аналогов);

5) механизм следообразования — следы «бесконтактной» преступной деятельности;

6) способы подготовки, совершения и сокрытия преступления («бесконтактный» способ по средствам информационно-телекоммуникационной сети «Интернет»; использование «закладок», тайников; регистрация IP-адресов за пределами Российской Федерации, использование средств телефонной связи).

Следственная практика показывает, что способы совершения бесконтактного сбыта наркотических средств постоянно совершенствуются. Преступниками активно используются не только мессенджеры («Telegram», «Skype», «Jabber», «Viber», «WhatsApp», «Brosix»), но и автоматизированные программы (боты), которые поддаются технической обработке оперативными подразделениями правоохранительных органов в очень усеченном формате. Для оплаты при бесконтактном сбыте наркотических средств и психотропных веществ используются электронные платежные системы «QiwiWallet», «WebMoney», «Yandex-Money», а также криптовалюта Bitcoin и Ethereum. Расследование данных преступлений затрудняет и тот факт, что преступники с целью сокрытия преступления шифруют информацию по совершению преступления путем ананимизации и криптографирования, а именно используют криптоконтейнеры, которые представляют собой виртуальный локальный диск, хранящий в себе зашифрованные данные, доступ к которым возможен при знании пароля либо наличия файл-ключа. Ограничить доступ к данным можно также при помощи защищенных паролем архивов. Защищенные архивы достаточно просто обнаружить при осмотре компьютерной техники, увидеть криптоконтейнеры затруднительно. Так как большинство криптоконтейнеров видны только в момент, когда они смонтированы, т.е. подключены, это очень затрудняет их обнаружение. Наряду с защифрованными виртуальными локальными дисками в роли криптоконтейнера,

может выступать защищенный паролем контейнер (зашифрованный контейнер, архив), имеющий вид файла, ограничивающий доступ к данным и способный маскироваться под файлы любого типа. Так как большинство криптоконтейнеров видны только в момент, когда они смонтированы, т.е. подключены, это очень затрудняет их обнаружение. Практика расследования показывает, что ткриптоконтейнер не всегда представлен в виде файла или виртуального локального диска. В роли зашифрованного контейнера может использоваться неразмеченная (свободная) область носителя данных. Преступники используют криптоконтейнеры и защищенные архивы для хранения в них файлов используемых для осуществления преступной деятельности, например, там могут храниться информация о местах закладок, фотографии мест «закладок» с их описанием и указанием места закладки — тайника, информация о движении денежных средств и др.

Исследование криптоконтейнеров и защищенных архивов затрудняет тот факт, что у экспертов отсутствует их методика исследования. Эксперты судебно-компьютерных лабораторий обладают необходимыми знаниями для исследования защищенных данных, однако основными методами получения доступа к зашифрованным данным является метод подбора пароля по словарю или прямым перебором, которые требуют огромного времени. В опыте экспертных подразделений встречались случаи, когда преступники хранили свои пароли в текстовых файлах на тех же носителях информации. Иногда преступники используют устаревшие методы шифрования, что позволяет применить специальное программное обеспечение для обхода защиты и получения доступа к защищенной информации.

7) состав соучастников организованной группы, преступного сообщества (преступной организации);

8) особенности социального положения преступников;

9) образовательный уровень преступников, в том числе их знания в области компьютерной техники, который позволяет им осуществлять сбыт с использованием информационно-коммуникационных технологий;

10) обстоятельства, подтверждающие, что имущество, подлежащее конфискации, получено в результате совершения преступления или является доходами от этого имущества, либо использовалось или предназначалось для использования в качестве орудия, либо для финансирования организованной группы, преступного сообщества (преступной организации) и т.п.

Анализ судебно-следственной практики показывает, что в качестве способа заключения сделки по покупке наркотиков в основном используются приложения, поддерживаемые операционными системами Android, IOS, WindowsPhon, такие как WhatsApp, Viber, ВКонтакте, Одноклассники, Facebook, Bitcoin, Xabber Telegram, IP-адреса которых находятся за пределами Российской Федерации, что вызывает определенную сложность в привлечении к ответственности преступников и затрудняет процесс расследования. Например, анализ социальных сетей поможет определить объемы сбываемого наркотика, территориальную принадлежность субъекта сбыта, участников преступной группы и лиц, приобретающих и употребляющих наркотические средства. Так, в период времени с марта 2017 г. до 5 июня 2017 г. у Н. возник преступный умысел, направленный на сбыт наркотических средств. С этой целью Н. посредством использования информационно-телекоммуникационной сети Интернет обнаружил сайт, на котором было размещено предложение работы по закладке наркотических средств в тайники за денежное вознаграждение. Н. осознавал, что распространение наркотиков на территории Российской Федерации в немедицинских целях запрещено законодательством страны. Несмотря на это, Н., действуя из корыстных побуждений, согласился оказывать услуги по размещению наркотических средств, психотропных веществ или их аналогов в тайники на территории г. Екатеринбурга. Для общения с неустановленным лицом, которое координировало Н. по направлению преступной деятельности, с целью получения указаний и отчета о выполненной работе скачал на свой мобильный телефон программу «Xabber», предназначенную для мгновенного обмена текстовыми сообщениями. Так, 5 июня 2017 г. около

08 часов неустановленное лицо, используя программу «Xabber» (мобильная программа «Xabber» характеризуется возможностью шифрования сообщений и регистрации по номеру сотового телефона, что позволяет сохранять анонимность лиц, осуществляющих преступную деятельность), сообщил Н. место хранения наркотических средств для последующего его извлечения, расфасовки и размещения в другие тайники. После выполнения указанных действий Н. должен был «заложить» полимерные пакеты с наркотическими средствами в определенные места, о чем в последующем должен был оповестить неустановленное следствием лицо. Довести до конца преступный умысел Н. не смог, так как был задержан сотрудниками полиции [9]. Таким образом, можно констатировать, что содержание криминалистической характеристики таких преступлений, отличается большим объемом, определенной спецификой и различными элементами.

Вместе с тем необходимо отметить, что криминалистика не стоит на месте, поэтому вышеуказанный перечень элементов криминалистической характеристики преступлений о незаконном сбыте наркотических средств, психотропных веществ и их аналогов по средствам информационно-телекоммуникационной сети Интернет, не является «догмой» и может меняться.

Список литературы

1. Краткая *х*арактеристика состояния преступности в Российской Федерации за январь-декабрь 2019 года. URL: http:// www. мвд.рф./mvd/ structure1/ (дата обращения: 10 марта 2020 г.).

2. Земцова С.И. Предмет доказывания при расследовании преступлений, связанных со сбытом наркотических средств, психотропных веществ и их аналогов, совершаемых с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) // Современное право. 2015. № 4. С. 126-133.

3. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 г. № 63-ФЗ // СПС «КонсультантПлюс».

4. Агафонов В.В., Чистова Л.Е. Методика расследования преступлений, связанных с незаконным оборотом наркотических средств, психотропных, сильнодействующих веществ, а также растений, содержащих наркотические средства и психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, совершенные с использованием Интернет и электронных средств связи: учеб.-методическое пособие. М.: ДГСК МВД России, 2011. 144 с.

5. Суров О.А., Земцова С.И., Галушин П.В. Методика расследования незаконного сбыта синтетических наркотических средств, совершенного с использованием интернет-магазинов: учебное пособие. Красноярск: СибЮИ МВД России, 2016. 155 с.

6. Федеральный закон от 8 января 1998 № 3-ФЗ «О наркотических средствах и психотропных веществах» // СПС «КонсультантПлюс».

7. Постановление Правительства Российской Федерации от 30 июня 1998 г. № 681 «Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации» // СПС «КонсультантПлюс».

8. Постановление Правительства Российской Федерации от 1 октября 2012 г. № 1002 «Об утверждении значительного, крупного и особо крупного размеров наркотических средств и психотропных веществ, а также значительного, крупного и особо крупного размеров для растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, для целей статей 228, 228.1, 229 и 229.1 Уголовного кодекса Российской Федерации» // СПС «КонсультантПлюс».

9. Приговор Кировского районного суда г. Екатеринбурга от 6 апреля 2018 по делу № 22–2378/2018. URL: http:// www. sudact.ru/regular.

И.В. Поддубный, *адъюнкт кафедры ОРД ОВД Орловского юридического института МВД России имени В.В. Лукьянова, г. Орел*

НЕКОТОРЫЕ АСПЕКТЫ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ «ОПРОС» ПРИ РАСКРЫТИИ ДИСТАНЦИОННЫХ ХИЩЕНИЙ С БАНКОВСКИХ КАРТ

На сегодняшний день в Российской Федерации широко используются безналичные способы оплаты среди населения, все более актуальным становится использование банковских карт. Согласно данных банка России карточные продукты используют порядка 89% россиян [1].

Необходимо констатировать, что с ежегодным ростом пользователей платежных карт также увеличивается количество случаев хищений. Сегодня хищения с банковских карт приобретают катастрофические масштабы, поскольку преступники используют все новые методы преступной деятельности, разрабатывают эффективные схемы обмана, активно используют информационные технологии. Согласно сведениям Банка России, в 2019 г. восемь из десяти хищений в России осуществлялись с использованием методов социальной инженерии, когда обманом пытаются узнать у клиентов банков конфиденциальные данные или вынуждают совершить перевод в их пользу [2].

Между тем практика раскрытия хищений с банковских карт граждан показывает, что раскрытие зависит от своевременности и качества проведения необходимого комплекса оперативно-розыскных мероприятий, основной задачей которого является задержание фигуранта. Полное раскрытие хищений с банковских карт предполагает установление всех причастных к преступлению лиц, возможно, не только исполнителей, но и организаторов, соучастников.

Одним из первоочередных оперативно-розыскных мероприятий является скрупулезный опрос лица, пострадавшего от противоправного деяния. Качественный опрос дает сотрудникам уголовного розыска максимально ценную информацию по нюансам самого преступления и, возможно, некоторым приметам фигуранта, что, в свою очередь, способствует правильному и быстрому проведению последующих оперативно-розыскных мероприятий и следственных действий. Практика показывает, что опрос граждан — одно из самых распространенных оперативно-розыскных мероприятий.

Отмечая значимость ОРМ «опрос», Н.А. Моисеев и Н.Г. Новоселов говорят о том, что своевременный и тактически правильно проведенный опрос пострадавшего обеспечивает получение исходных данных, позволяющих установить значимые обстоятельства и с их учетом выдвигать и проверять версии по раскрытию преступления [3].

В юридической литературе существует многообразие частных определений понятию «опрос», однако принципиального отличия они не имеют.

В своей работе О.А. Вагин, А.П. Исиченко и Г.Х Шабанов определяют опрос как оперативно-розыскное мероприятие, целью которого является сбор (добывание) информации в процессе непосредственного общения сотрудника оперативного подразделения или по его поручению другого лица с человеком, который осведомлен или может быть осведомлен о лицах, фактах и об обстоятельствах, имеющих значение для решения задач ОРД [4, с. 14]. По мнению Н.А. Трифоновой, опрос — это процесс получения информации в ходе разговора с лицом, представляющим оперативно-розыскной интерес [5]. При этом И.А. Климов говорит об опросе как о специальной беседе, проводимой с гражданами, которым могут быть известны сведения, необходимые для решения конкретных задач ОРД (например, о преступлении, лицах, его совершивших, следах преступной деятельности и т.п.) [6, с. 229]. А.Г. Маркушин под опросом понимает специальную (разведывательную) беседу, проводимую в целях сбора и проверки информации, представляющей оперативный интерес, с лицами, которые располагают или могут располагать необходимыми для решения задач сведениями [7, с. 159].

Таким образом, судя по приведенным определениям правоведов, можно сделать вывод о том, что суть опроса состоит в непосредственном общении субъекта с объектом опроса, целью которого всегда является получение оперативно-значимой информации. Содержательная часть опроса заключается в получении информации, зафиксированной в памяти опрашиваемого лица, путем ее устного воспроизведения [8, с. 230].

В свою очередь, информация, полученная при некачественно проведенном опросе, будет препятствовать быстрому и эффективному проведению комплекса ОРМ, что впоследствии существенно снизит возможность оперативного установления преступников. Вследствие чего у злоумышленников появляется возможность сокрыть следы преступления, уничтожить улики или скрыться, продолжать осуществлять преступную деятельность.

В данном случае уместно указать на мнение В.В. Лысенко, который утверждает, что успешное расследование уголовных дел во многом определяется именно полнотой и качеством материалов, представленных в виде результатов оперативно-розыскной деятельности и доследственной проверки, которые уже в момент поступления должны позволить следователю определиться с кругом лиц, причастных к совершению преступления, и спланировать дальнейшее расследование [9].

Результативность любого вида опроса зависит как от степени осведомленности о личности опрашиваемого, его психологических качествах, отношении к правоохранительным органам, так и от понимания задач проведения опроса, а также осведомленности о надлежащих сведениях, которые необходимо выяснить у опрашиваемого.

Как справедливо отмечают И.В. Ревина и А.Ю. Краснопивцев, правильное формулирование конкретных задач, намеченных для решения путем проведения опроса, во многом обусловливает эффективность этого мероприятия. Без четкого их определения опрос становится стихийным и не гарантирует поступления полной и объективной информации [10].

При опросе необходимо учитывать моральное и физическое состояние заявителя. Недопустимо вслух оценивать и комментировать ответы опрашиваемого. Стоит отметить, что часто жертвами хищений с банковских карт становятся лица пожилого возраста и жители удаленных от административного центра небольших населенных пунктов, чьи познания в области информационных технологий не позволяют им подробно и обстоятельно рассказать о произошедшем. В связи с чем оперативному сотруднику необходимо быть готовым к разъяснению некоторых специфичных терминов и операций.

Например, одной из самых распространенных схем хищения реализуется с помощью абонентских вбросов электронных сообщений с текстом «Ваша карта заблокирована», «Замечена подозрительная транзакция». На абонентский номер жертвы приходит СМС-сообщение, в котором указано, что его банковская карта заблокирована (может быть иная формулировка) и для решения данной проблемы необходимо позвонить по указанному в СМС номере, либо на номер жертвы поступает звонок якобы от службы безопасности банка. И в первом, и во втором случае в ходе общения злоумышленник представляется сотрудником банка и сообщает жертве о каких-либо проблемах с его картой (например, «системой безопасности банка зафиксирована попытка перевода денежных средств с Вашей карты»). После этого под предлогом решения проблемы фигурант для осуществления хищения пытается либо получить конфиденциальную информацию по карте, либо «ведет» жертву к банкомату, где диктует ей набор операций, которые необходимо провести.

При раскрытии хищений, совершаемых перечисленными способами, при опросе сотруднику, уполномоченному проводить опрос необходимо устанавливать следующие данные:

– вводная, характеризующая лицо, информация (ФИО, адрес проживания; с кем проживает; место работы, абонентский номер домашнего или сотового телефона; и т.д.);

– дата и время поступления звонка или СМС, номер, с которого поступил звонок или СМС, номер, который был указан для связи в самом СМС, количество звонков или СМС, абонентский номер телефона, на который поступил звонок или СМС либо который каким-либо образом использовался при совершении преступления;

– сколько человек принимали участие в разговоре, пол фигуранта (мужчина или женщина), возрастные характеристики голоса преступника(ов), описание иных характеристик голоса, характеристика речи, возможные дефекты речи, наличие фона при разговоре, его описание, указание на возможность опознать человека по голосу;

– по возможности дословное изложение разговора со злоумышленником (кем представился, какую проблемную ситуацию назвал, какое решение проблемы предложил, либо какие указания от него поступали). Если осуществлялось несколько звонков, то необходимо выяснить, что говорил преступник каждый раз. В случае если в разговоре участвовало несколько человек, то необходимо выяснить, что говорил каждый и в какой последовательности;

– дата, время, место и способ хищения или перечисления денег от потерпевшего преступнику (установить все реквизиты банковской карты: наименование банка, номер, срок действия, дату и цель оформления, адрес банкомата, все известные данные лица, на чье имя потерпевшим был направлен перевод; были ли звонки после перечисления денег и что говорил преступник);

– когда и при каких обстоятельствах потерпевший обнаружил факт хищения; какие действия предпринял после обнаружения факта хищения и до подачи заявления в полицию получение выписки из кредитной или иной организации (операции по счету, детализация звонков, блокировка счета и т.д.).

В ходе опроса могут возникнуть и другие вопросы, относящиеся к обстоятельствам, подлежащим установлению.

Вышеприведенные рекомендации для проведения опроса заявителя, пострадавшего от хищения с банковской карты, могут заложить основу для проведения дальнейших оперативно-розыскных мероприятий и следственных действий, способствующих быстрому установлению личности преступника.

Список литературы

1. Почему 11% россиян до сих пор не пользуются банковскими картами? Рассказывают эксперты. URL: https://bankstoday.net
2. В 2019 году выросло число жалоб жителей Кузбасса на кибермошенников. URL: https://www.cbr.ru
3. Моисеев Н.А., Новоселов Н.Г. О некоторых первоначальных оперативно-розыскных мероприятиях при раскрытии краж из квартир граждан. URL: https://cyberleninka.ru
4. Вагин О.А., Исиченко А.П., Шабанов Г.Х. Оперативно-розыскные мероприятия и использование их результатов: учебно-практическое пособие. М.: Издательский дом Шумиловой И.И., 2006. С. 14.
5. Трифонова Н.А. О некоторых проблемах проведения опроса в оперативно-розыскной деятельности. URL: https://cyberleninka.ru
6. Оперативно-розыскная деятельность / И.А. Климов, Е.С. Дубоносов, Л.Л. Тузов, Н.А. Кузьмин; ред.: И.А. Климов. 3-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА, 2018. С. 229.
7. Оперативно-розыскная деятельность полиции в раскрытии и расследовании преступлений / А.Г. Маркушин, Н.А. Аменицкая; под ред. А.Г. Маркушина. М.: Юрайт, 2019. С. 159.
8. Оперативно-розыскная деятельность / И.А. Климов, Е.С. Дубоносов, Л.Л. Тузов, Н.А. Кузьмин, ред.: И.А. Климов. 3-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА, 2018. С. 230.
9. Лысенко В.В. Особенности расследования хищений денежных средств с использованием банковских карт в условиях противодействия и его преодоления. URL: https://cyberleninka.ru
10. Ревина И.В., Краснопивцев А.Ю. Опрос как оперативно-розыскное мероприятие: отграничение от допроса как следственного действия. URL: https://www.elibrary.ru

Б.В. Псарева, *к.ю.н., доцент кафедры ГМУ и права Рубцовского института (филиал) Алтайского государственного университета, г. Рубцовск*
С.А. Пирова, *студентка Рубцовского института (филиал) Алтайского государственного университета, г. Рубцовск*

ЮРИСТЫ-БОТЫ И ПРАВОВАЯ ПОМОЩЬ

Машинизация права — это одна из самых обсуждаемых тем в правовом пространстве современности. Несколько десятилетий назад нам сложно было представить, насколько глубоко новые технологии охватят все сферы жизнедеятельности человечества. Суды, федеральные службы и все остальные государственные и коммерческие институты вынуждены оперативно адаптировать под развитие цифрового пространства [1, с. 6; 2, с. 30].

Рассмотрим проблемы автоматизации права на примере использования юристов-ботов в оказании правовой помощи населению, что станет основной целью исследования. Теоретические (анализ, синтез) и практические (социологический опрос) методы исследования позволят наиболее полно раскрыть тему.

Чат-бот — это диалоговая система на основе текстовых данных, то есть программа, которая симулирует письменную беседу с пользователей и отвечает на его вопросы. Польза юристов-ботов для компаний колоссальна: бот способен консультировать в диалоговом режиме сотни пользователей одновременно, экономя время и средства [3]. Согласитесь, даже опытный юрист не способен воспроизвести такую скорость. Поиск информации для бота составит секунды, бот не требует оплаты труда, отпуск, больничный, работоспособен круглосуточно.

Боты, способные к обучению, имеют в основе искусственный интеллект и нейронные сети. Подобный чат-бот не использует шаблоны подготовленных ответов, а строит его из адекватных соответствующих предложений по теме вопроса. Кроме этого, ведется сбор и анализ всех запросов и слов, сказанных роботу [4]. Для правового помощника более эффективен чат-бот на основе искусственного интеллекта. Использование чат-ботов на сайтах поможет улучшить связь с клиентом, при этом сократив его ожидание ответа от поддержки. Поселив чат-бот на сайте интернет-магазина, можно обеспечить оперативное получение ответов на часто задаваемые вопросы новых клиентов.

Рынок правовых услуг диктует свои условия, любой современный сайт юридических консультаций предлагает для бесплатной первичной консультации помощь чат-бота. Подобную помощь предлагают не только гражданам, не имеющих специальных знаний в области права, но и самим юристам. Многие чат-боты способствуют созданию документов, анализируют контракты. Среди популярных чат-ботов лидируют: Docubot, LawBot, Lexi [5].

Машинизация предполагает подчинение права правилам логики. Создание любого чат-бота состоит в создании алгоритма: последовательных действий, подходящих под определенные ситуации. Существуют сайты, позволяющие любому юристу создать чат-бота в виде диалогового окна на официальном сайте компании без специального знания программирования, например, на сайте «Form.One». Активная фаза развития инновационных технологий во всех сферах жизни общества создает уникальные по эффективности средства взаимодействия с точки зрения удобства их применения и сроков исполнения. Но, как и в любых процессах, в данной сфере существуют свои недостатки. Суть их сводится к тому, что законодательство не поспевает за развитием этого огромного кластера [6, с. 211].

Здесь возникает первая проблема автоматизации права — можно ли подчинить право законам логики полностью. Для успешного внедрения чат-ботов в правовую реальность необходимо создать формальный логический язык для описания законов и других юридических документов, описать возможные типы легальных выражений этого языка и легальных

логических переходов между этими выражениями, переписать законодательство на этом языке. Нагромождение правовых актов, постоянно внесение изменений в законы, сложности кодификации, неоднозначность толкования права специалистами, многозначность юридических терминов — эти особенности в совокупности создают непреодолимое препятствие для изобретения формального юридического языка, подчиняющегося не просто логике права, но и математической логике алгоритма, не допускающей появления заранее непредусмотренного исключения.

А.А. Иванов в статье о глубине машинизации права выдвинул тезис о нелогичности права: «Те, кто начинал как юрист или хотя бы как гуманитарий, меня поймут: они воспринимают право не как инертный механизм, но как субъективное явление, если не сказать больше, одушевлённое существо. Праву присуща воля, которая стремится достичь свободно избранной цели, не считаясь с правилами формальной логики. У права есть такие сущностные свойства, которые нельзя игнорировать… Нелогичность права — это такое его свойство, которое лежит на поверхности. Гораздо более важной, внутренней причиной, которая препятствует машинизации права, является, как ни странно, свободная воля человека» [7, с. 32].

Человек по своей природе творец, он наделен свободой воли и стремится выразить свою волю. Безусловно, каждый слышал о так называемых «пробелах» и «лазейках» в законе. Многие обнаруживают подобные явления и используют в своих интересах. Закон придуман человеком и им же может быть «разорван», как и любой шаблон поведения. Шаблоны теряют свою актуальность, закон изменяется вместе с потребностями человека. В связи с этим абсолютная машинизация права и свободная воля человека несовместимы. При этом право — достаточно гибкое явление, и эксперты в области права обсуждают роботизацию в правовой сфере автоматизацию юридических функций и возможные изменения юридической профессии в той мере, насколько это необходимо самому человеку [8, с. 20].

Но вернемся к теме юристов-ботов и их роли в оказании правовых услуг.

Выяснив, что создание единой информативной базы для юристов-ботов проблематично, остановимся на изучении юристов-ботов, созданных отдельными юристами. Юристов-ботов на данный момент сложно признать автономными техническими средствами [9, с. 76]. Использование ботов не просто в режиме взаимодействия (решение всегда остается за человеком), а в режиме сосуществования (автономность технического средства) представляется возможным после решения множества проблем неэффективности чат-ботов [10, с. 87].

В поисках необходимой информации на просторах Интернета подобных чат-ботов встречали все. Бот способен не просто дать консультацию по интересующему вопросу, но и подготовить пакет документов: составить жалобу, заявление или иск в суд [11]. Не стоит забывать — последовательность действий и ответов бота составляет юрист, поэтому результативность бота напрямую зависит от уровня квалификации его создателя.

Некоторые авторы выдвигают тезисы, согласно которым полученные искусственным интеллектом результаты следует признавать охраняемыми объектами интеллектуальной собственности, на которые отсутствует право авторства; каждый такой объект должен иметь автоматически присваиваемый идентификационный номер, позволяющий, во-первых, определить, каким искусственным интеллектом он создан, во-вторых, установить разработчика саморазвивающейся программы, обладающего исключительным правом не только на эту программу, но и на объект, ею созданный [12, с. 320].

Юристы-боты созданы для оказания правовой помощи рядовым гражданам, поэтому авторы провели опрос среди студентов и молодых специалистов разных сфер и отдельно для представителей юридической сферы, в целом количество опрашиваемых составило 86 человек. Целью опроса явилось выявление уровня спроса у населения на подобное предложение юридических компаний. Важным показателем опроса стало мнение населения о результа-

тивности юристов-ботов. Перед респондентами были поставлены вопросы с возможностью выбора нескольких вариантов ответа.

Результаты опроса показали низкую заинтересованность населения в использовании чат-ботов: 42% опрошенных отметили назойливость диалоговых окон, что мешает просмотру основного контента сайта, 25% респондентов предпочитают вести поиск информации самостоятельно. Примечательно, что 16% не использовали чат-боты и заочно считают их бесполезными. Всего лишь 7% использовали чат-боты и этого им хватило для решения правового вопроса. Столько же процентов пришлось на пользователей, которые также использовали ботов, но это не принесло ожидаемого результата (рис. 1). Тот же опрос среди юристов дал подобные результаты, однако юристы активнее используют ботов в качестве помощника. Наиболее низкий процент получил ответ, согласно которому консультации хватило для решения вопроса (рис. 2).

Главной проблемой во внедрении чат-ботов, отталкиваясь от результатов опроса, можно назвать их назойливость, всплывающее окно вызывает раздражение среди пользователей сайта. Поэтому разработчикам сайтов следует пересмотреть варианты предложения такой услуги. Нежелание использовать новые технологии и предвзятое отношение к ботам охватывает большую часть опрошенных. Это можно объяснить недоверием населения к новым технологиям, неосведомленность пользователей о принципе работы чат-ботов, поэтому население предпочитает обращаться к юристам очно. Возможно, нежелание пользоваться ботами отразилось в редком выборе последнего варианта ответа, предполагающего, что бот в полной мере выполнил поставленную задачу.

Опрос юристов позволил поставить тезис о низкой продуктивности чат-ботов именно для представителей правовой сферы, причиной тому может являться высокая сложность и глубина вопроса, поставленного специалистом в области права. Следует сделать общий вывод из опроса: чат-боты, в большинстве случаев, способны выполнить только типовые задачи и ответить на общие вопросы клиента.

О высокой эффективности чат-ботов не придется говорить пока не будет создан единый формальный язык права, что, по мнению автора, невозможно в связи с необходимостью всецелого пересмотра законодательной базы не только РФ, но и зарубежных стран. Внедрение новых технологий всегда сопровождается обсуждением терминологического аспекта темы [13, с. 14]. Применение юристов-ботов в современных реалиях наиболее продуктивно в варианте первоначального сбора информации ботом об индивидуальной ситуации клиента с дальнейшим привлечением специалиста к работе.

Искусственный интеллект не способен в полной мере заменить человека, поскольку не рассчитан на решение нестандартных ситуаций с учетом сугубо человеческих свойств — таких как совесть, справедливость [14, с. 24].

Юриспруденция, как и всякая область деятельности человека, обладает своими особенностями и требует творческого подхода, в том числе поиск выходов из коллизионных ситуаций, которых достаточно в практике среди судебных дел. Чат-боты на данном этапе способны произвести анализ документов и источников среди всех доступных ему баз данных, но решить нестандартную задачу они не способны на данном уровне их развития. Еще боты не оказывают юридические консультации в контексте местного профессионального законодательства.

Важной проблемой для чат-ботов является актуальность информации в диалогах. За нее, как правило, отвечают «отцы» ботов (обычно специалисты по управлению знаниями). За каждый ответ в базе программы отвечает конкретный сотрудник (носитель этой информации). Этот сотрудник регулярно получает автоматический запрос проверить актуальность и обновить ее при необходимости. Боты-юристы экономят компаниям деньги, но контролируют при этом качество обслуживания.

В последнее время мы можем увидеть успешность применения чат-ботов на западе в решении типовых ситуаций. Чатбот DoNotPay получил известность в 2016 г. после того, как за первый 21 месяц своего существования рассмотрел 250 тысяч дел, из которых 160 тысяч оспорил. Проект запустил студент Стэнфордского университета Джошуа Бродер. Изначально DoNotPay обрабатывал только штрафы за парковку, но затем сервис начал помогать людям, которым грозит выселение или лишение недвижимой собственности. Также чатбот стал решать вопросы, связанные с компенсацией за задержку авиарейсов и поездов и со страхованием на случай неплатежеспособности. Сервис поможет решить вопросы с декретным отпуском, оспорить покупку, совершенную мошенниками по кредитной карте истца, и даже подать иск на компании, которые досаждают рекламными звонками. В 2017 г. бот освоил тысячу отраслей права [15].

На примере внедрения юристов-ботов для оказания правовой помощи населению можно вывести следующий тезис: машинизация права в полной мере неосуществима в силу субъективности права и индивидуального подхода к праву каждого человека в целом. Учитывая уровень развития искусственного интеллекта и широкую область распространения, следует ожидать в ближайшем будущем его использование не только в виде правовой помощи населению, но и непосредственно при свершении правосудия. Профессия юриста не исчезнет в силу машинизации права и повсеместного внедрения искусственного интеллекта, она трансформируется и предложит специалистам широкий круг узких направлений деятельности, связанных с использованием информационных технологий.

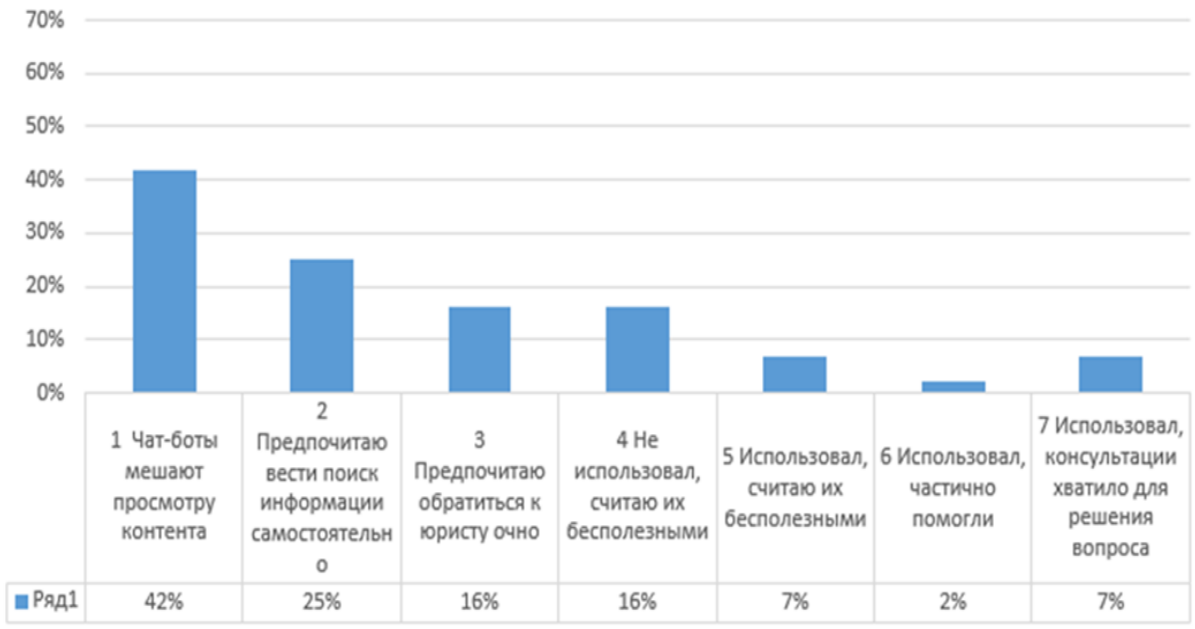


Рис. 1. Опрос студентов и молодых специалистов вне юридической деятельности (рисунок авторов)

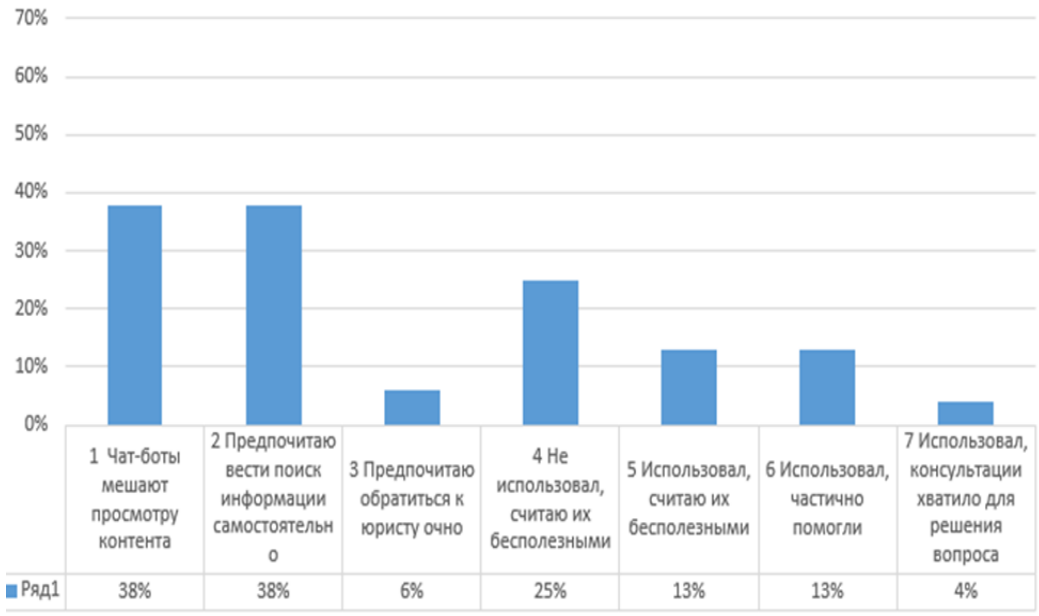


Рис. 2. Опрос студентов и молодых специалистов в сфере права (рисунок авторов)

Список литературы

1. Голомолзин А.Н. В цифровой сфере ограничений традиционного мира не существует и это необходимо учитывать // Закон. 2017. № 12. С. 6-15.

2. Булгакова Е.В. Методы анализа и принципы систематизации данных, используемых при подготовке и принятии юридических решений // Информационное право. 2016. № 04. С. 29-33.

3. Инновации в юридическом бизнесе. URL: http://www.anglolex.org/Life/Legaltech.html / (дата обращения: 28.05.2020).

4. Чат-боты — за ними будущее. URL: https://livesurf.ru/chat-boty/6042-chat-botyza-nimi-budushhee.html#kak-oni-rabotayut_2 (дата обращения: 02.05.2020).

5. Эти 5 чат-ботов помогут вам в работе по всему миру. URL: https://platforma-online.ru/media/detail/5-poleznykh-chat-botov-dlya-yuristov/ (дата обращения: 12.04.2020).

6. Закиров Р.Ф. Использование современных IT-технологий как средство достижения основных задач судопроизводства // Вестник гражданского процесса. 2018. № 1. С. 211-219.

7. Иванов А.А. О глубине машинизации права // Закон. 2018. № 5. С. 31-41.

8. Кондрашов И., Иванов А., Цшайге Х., Пронин А. и др. LegalTech и юристы будущего // Закон. 2017. № 11. С. 20-36.

9. Кутейников Д.Л., Ижаев О.А., Лебедев В.А., Зенин С.С. Регулирование взаимодействия человека с автономными техническими средствами: дискуссия о правовых режимах // Российское право: образование, практика, наука. 2019. № 3. С. 75-79.

10. Кутейников Д.Л., Ижаев О.А., Лебедев В.А., Зенин С.С. Киберфизические, кибербиологические и искусственные когнитивные системы: сущность и юридические свойства // Lex russica. 2019. № 9. С. 85-90.

11. Как искусственный интеллект меняет юридическую профессию и чем это грозит юристам. URL: https://forbes.kz/process/technologies/ kak_iskusstvennyiy_intellekt_menyaet_yuridicheskuyu_professiyu_i_chem_eto_grozit_yuristam/ (дата обращения: 04.05.2020).

12. Синельникова В.Н. Правовой режим результатов интеллектуальной деятельности, созданных саморазвивающимися программами // Пермский юридический альманах. 2019. № 1. С. 320-328.

13. Незнамов А.В. К вопросу о применении технологий искусственного интеллекта в правосудии: терминологический аспект // Арбитражный и гражданский процесс. 2019. № 10. С. 14-18.

14. Васильев А.А., Шпопер Д.Искусственный интеллект: правовые аспекты // Известия АлтГУ. Юридические науки. 2018. № 6 (104). С. 23-25.

15. Бот-юрист DoNotPay освоил 1000 отраслей права. URL: https://hightech-fm.turbopages.org/s/hightech.fm/2017/07/12/donotpay-2 (дата обращения: 03.05.2020).

М.Е. Репин, *судебный пристав специализированного отдела оперативного дежурства Управления ФССП России по Нижегородской области, г. Нижний Новгород*

УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ ПРОБЛЕМЫ ДОКАЗЫВАНИЯ ОТДЕЛЬНЫХ ВИДОВ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Стремительное вовлечение Российской Федерации в мировое информационное пространство в конце XX — начале XXI вв. придало мощнейший импульс развитию IT-технологий. В этот период происходит активное становление и совершенствование глобальных телекоммуникационных и компьютерных сетей, разработка программного и аппаратного обеспечения электронно-вычислительных машин, поголовная и повсеместная цифровизация и компьютеризация всех без исключения сфер общественно-политической и экономической сфер жизни практически каждого индивида.

Бурное развитие информационных технологий приводит к повышению уровня комфорта как для каждого отдельного взятого индивида, так и к общим положительным изменениям во всех сферах жизнедеятельности общества. Привычные для всех сегодня виды услуг — медицинское и социальное обслуживание, образование, финансовые инструменты и сервисы переходят на цифровой формат и становятся более удобными, качественными и доступными для населения [1, с. 36–40]. В настоящее время за Российской Федерацией прочно закрепилась репутация ведущей IT-страны в мировом информационном сообществе.

Но в современных реалиях имеющая место глобальная цифровизация и экономическая интеграция отдельно взятых государств в единое мировое пространство подразумевает собой не только положительные, но и отрицательные моменты.

В период с 2015 по 2019 г. мы все чаще были вынуждены наблюдать рост и повсеместную распространенность такого вида преступной деятельности в сфере информационных технологий, как фишинговые атаки. Фишинг — это интернет-мошенничество с использованием платежных банковских карт, взломом логинов и паролей, распространением материалов порнографического характера. Его целью является получение доступа к конфиденциальным данным клиентов банков и платежных систем. Иными словами, фишинг — это метод, который доставляет вредоносное программное обеспечение в корпоративную сеть финансово-кредитной организации [2, с. 147-152]. Фишинговые атаки представляют собой некую разновидность социальной инженерии, основанную на незнании самими пользователями элементарных основ информационной безопасности: в частности, большинство людей попросту не знают очевидных фактов: электронные службы и сервисы никогда не осуществляют рассылку сообщений с просьбами сообщить свои персональные данные, учетные записи, логины, пароли и т.д.

С целью стабилизации ситуации в стране в мае 2017 г. Президентом России Владимиром Путиным утверждена Стратегия развития информационного общества в Российской Федерации на 2017-2030 гг. В ней впервые было употреблено понятие «критическая информационная инфраструктура Российской Федерации» и подчеркнута важность ее защиты «с использо-

ванием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы». Информационная безопасность России в этом документе трактуется как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства». Сама же система обеспечения информационной безопасности признана неотъемлемой частью системы обеспечения национальной безопасности страны [3].

Вместе с тем на сегодняшний день выявленных фактов преступной деятельности с использованием глобальной сети Интернет остается по-прежнему крайне мало. Это мы можем объяснить тем, что киберпреступность — большой и хорошо организованный бизнес, который ежегодно оперирует миллиардами долларов по всему миру [4, с. 12-15]. Мошенники, преследуя цель хищения чужого имущества, регулярно обогащают свои теоретические знания, совершенствуют имеющиеся умения и навыки для более полного использования возможностей глобального цифрового пространства и сети Интернет. Основная проблема в настоящее время состоит в том, что финансирование киберпреступности гораздо выше, чем финансирование компаний и организаций, которые противостоят и борются с ней [5, с. 7-15].

Несмотря на некоторые особенности и специфичность раскрытия нового вида мошенничества в следственно-судебной практике имеются конкретные примеры успешного выявления и расследования рассматриваемой категории дел, по которым уже были вынесены судами обвинительные приговоры.

Более детально рассмотреть схему преступления фишинг-мошенничества нам поможет официальная информация, предоставленная пресс-службой Следственного департамента МВД России, где идет речь об успешном выявлении и раскрытии первого в нашей стране уголовного дела о компьютерном «фишинге». Главными «героями» это громкого уголовного дела стали два родных брата из Санкт-Петербурга. Братья детально изучили имеющуюся в свободном доступе на специализированных интернет-ресурсах и форумах информацию, успешно освоили основные правила и принципы работы системы дистанционного банковского обслуживания. После этого они разработали действенный план хищения денег со счетов клиентов крупнейшего российского банка ПАО «ВТБ» [6].

Тем не менее собственными силами реализовать свой преступный план братьям было явно не под силу. Для этих целей они привлекли к себе в сообщники весьма преуспевающего студента одного из ведущих отечественных вузов. Именно этот студент и разработал программное обеспечение, представляющее собой копию оригинальной веб-страницы дистанционного банковского обслуживания клиентов. На поддельной веб-странице, размещенной в информационно-телекоммуникационной сети Интернет, компьютерные преступники в качестве контактов службы технической поддержки разместили арендуемые ими абонентские номера и специально созданные для этого адреса электронной почты.

Впоследствии киберпреступники для реализации своих противоправных действий активно использовали возможности вредоносного программного обеспечения типа «троян». В настоящее время это один из многочисленных и распространенных типов вредоносных программ, маскирующийся под легитимное программное обеспечение [7].

Этот вирус после активации на зараженном компьютере захватывал отдельные файлы и злонамеренно изменял конкретные параметры, задействованные в функционале «клиент-банк». Как следствие этого, любые из обращений клиентов банка к официальному интернет-сайту ПАО «ВТБ» автоматически переадресовывались на специально разработанные для целей преступной деятельности серверы, принадлежащие компьютерным мошенникам, на которых и были размещены заранее созданные ими поддельные веб-страницы.

Как и предполагали злоумышленники, клиенты ПАО «ВТБ» попадали на дубликат интернет-страницы официального сайта банка. Далее, ничего не подозревая и не испытывая каких-либо сомнений в юридической чистоте проводимых финансовых операций, они вводили свои персональные данные: пароль, уникальный номер, переменный код и др. Совокупность перечисленных сведений предоставляет возможность для разового направления распоряжения о проведении банковских операций с денежными средствами. Данная информация сохранялась специально разработанным для преступных целей вирусным программным обеспечением, обрабатывалась и передавалась кибермошенникам.

С целью получения новых переменных кодов мошенники отправляли клиентам смс-сообщения или звонили им, представляясь сотрудниками собственной безопасности или работниками службы технической поддержки банка. Далее злоумышленники заявляли о необходимости незамедлительного повторного введения переменного кода, объясняя этот факт тем, что случился программный сбой и возможности наступления по этой причине неблагоприятных финансовых последствий.

Получив необходимые идентификационные данные (логины, пароли и коды), мошенники от имени легальных клиентов направляли дистанционные распоряжения на перевод денежных средств с клиентских банковских счетов на счета третьих лиц, подконтрольные им самим, после чего различными способами обналичивали похищенные деньги [8, с. 58–64].

В период с мая 2010 г. по февраль 2011 г. два родных брата из Санкт-Петербурга совместно со студентом калининградского вуза обманули более 140 граждан из 46 регионов нашей страны и присвоили себе около 13 млн рублей [9].

Для расследования, доказывания и раскрытия первого уголовного дела по интернет-фишингу были привлечены:

– сотрудники Управления «К» МВД России;

– сотрудники Следственного департамента МВД России;

– сотрудники центра информационной безопасности ФСБ России;

– компьютерные криминалисты из компании Group-IB;

– сотрудники отдела расследования компьютерных инцидентов ЗАО «Лаборатория Касперского».

При расследовании рассматриваемой категории дел подлежат установлению и доказыванию следующие обстоятельства:

– имел ли место сам факт совершения преступления;

– способ совершения преступления, место совершения, период времени совершения, средства сокрытия следов, орудие совершения мошенничества;

– установление факта использования вредоносных программ, заражения ими компьютеров жертв;

– определение потерпевших в результате мошенничества;

– установление личности виновного(-ых), сбор характеризующего материала, определение ролей каждого из участников фишинга;

– размер вреда, причиненного преступлением;

– определение местонахождения похищенных денежных средств, подлежащих конфискации в порядке ст. 104.1 «Конфискация имущества» Уголовного кодекса Российской Федерации [10, с. 179–186].

В июле 2010 г. сотрудники службы безопасности ПАО «ВТБ» одновременно обратились в Лабораторию Касперского и правоохранительные органы. Там они сообщили о возникшей проблеме — продолжающейся серии хищений со счетов физических лиц, являющихся их клиентами.

Как показывает следственно-судебная практика, интернет-мошенники тщательно стараются «замести следы» своей противоправной деятельности и используют различные приемы, способы и средства анонимизации для того, чтобы субъекты расследования не смогли найти какую-либо связь между конкретными личностями и вредоносным программным обеспечением.

На персональных компьютерах жертв были прописаны IP-адреса серверов, находящихся за пределами Российской Федерации. По результатам проведенных исследований было установлено, что на них находились украинские либо отечественные не отвечающие на запросы правоохранительных структур данные, которые занимались арендой IP-адресов за рубежом и последующей сдачей их в субаренду отечественным пользователям. Обращение к таким арендодателям с запросами о предоставлении интересующих сведений об арендаторах в абсолютном большинстве случаев редко имело шансы на положительный итог. Однако троянская программа постоянно активно обменивается данными с серверами, которыми успешно управляют кибермошенники. При грамотном профессиональном подходе субъектам расследования практически всегда удается установить какую-либо хотя бы косвенную связь между этими серверами и персоналиями, участвующими в инциденте [11].

По соответствующим запросам правоохранительных органов, осуществляющих расследование данного уголовного дела, специалисты проводили сбор и анализ данных — IP-адресов серверов, использовавшихся кибермошенниками, время и даты их регистрации, даты атак, суть и даты любых изменений на серверах: все, что было связано с ними и имеется в открытом доступе. В результате тщательно проведенного анализа специалисты приходили к определенным умозаключениям и выводам, выявляли конкретные контактные данные злоумышленников или указания на то, где эти контактные данные можно получить. Субъекты расследования, в свою очередь, проверяли сделанные ими выводы и сообщали вновь добываемую информацию и сведения, которые способствовали сужению области проводимых исследований и анализов соответствующими специалистами.

Таким образом, только пройдя несколько уровней подобного системно-структурного анализа механизма модели преступной деятельности данного вида, правоохранителям совместно со специалистами «Лаборатории Касперского» удалось вычислить тех, кто стоит за организацией серверной инфраструктуры, с которой когда-либо взаимодействовал вирус. После чего у правоохранительных органов появились относительно четкие и достоверные сведения о кибермошенниках.

Перед тем как непосредственно начать похищать чужие денежные средства, мошенникам необходимо осуществить ряд рутинных процедур, при совершении которых они могут оставлять различного рода следовые картины. Конкретные навыки сокрытия таких следовых картин преступлений в сфере высоких технологий напрямую зависят от интеллекта и уровня квалификации преступника. На одном из таких этапов преступной деятельности технических умений и навыков братьям-хакерам не хватило. Именно это и позволило стражам закона и компьютерным специалистам пойти по следу и, познав его, выйти на конкретных людей.

До ареста подозреваемого следователям Следственного департамента МВД России необходимо было возбудить уголовное дело, для чего нужны основания. К нашему сожалению, предоставить просто техническое описание мошеннической инфраструктуры и схемы действий нарушителей закона недостаточно. Необходимо изложить факты и дать определения терминам на понятном для не технического специалиста языке. Например, следователь должен объяснить суду, почему именно эти данные принадлежат конкретному подозреваемому именно таким образом, чтобы его доводы были приняты [12, с. 122-124]. Эта, на первый взгляд, простая задача требует вовлечения квалифицированных технических специалистов и тесного взаимодействия со следствием на протяжении всего длительного процесса выявления и расследования преступной деятельности в IT-сфере [13, с. 77-81].

В максимально короткий срок, установленный действующим законодательством Российской Федерации, специалистам «Лаборатории Касперского» необходимо было предоставить следователю максимум аналитической информации, а также подготовить соответствующие обзорные справки и необходимые отчеты для приобщения к делу.

После проведения целого комплекса проверочных мероприятий Следственным департаментом МВД России в январе 2011 г. было возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 1 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ч. 3 ст. 30 «Приготовление к преступлению и покушение на преступление» и ч. 4 ст. 159 «Мошенничество» Уголовного кодекса Российской Федерации по факту использования и распространения вредоносного программного обеспечения, а также хищения денежных средств организованной группой со счетов клиентов ПАО «ВТБ» в системе дистанционного банковского обслуживания «Телебанк».

Особый интерес у всех вызывает тот факт, что сотрудники правоохранительных органов полагали практически до самого момента ареста, что имеют дело с одним, а не с несколькими подозреваемыми. В глобальной сети Интернет — на закрытых хакерских форумах — преступники умышленно действовали под одним псевдонимом. Уже в процессе следствия и проведения допросов соучастников данной преступной деятельности была получена достоверная информация о непосредственной причастности двух лиц. Как стало ясно после ареста, выдавая себя за одного человека, братья-близнецы общались в сети поочередно. Таким способом злоумышленниками обеспечивалась практически круглосуточная бесперебойная работоспособность преступного механизма. Работу «в паре» кибермошенники в своей схеме использовали и для того, чтобы совершить максимальное количество хищений денежных средств.

После ареста подозреваемых по рассматриваемому уголовному делу по соответствующему запросу Следственного департамента МВД России, в качестве второй экспертной организации к раскрытию IT-мошенничества подключились компьютерные специалисты-криминалисты из компании Group-IB, которая занимается расследованием киберпреступлений. Эксперты компании проводили криминалистическое исследование как самих компьютеров, так и прочих носителей и накопителей информации, обнаруженных в квартире преступников в ходе задержания.

Непростая задача специалистов компании Group-IB состояла в том, чтобы ответить на интересующий следствие вопрос: использовалась ли данная вредоносная программа для осуществления преступной деятельности, в том числе связанной со ст. 272 Уголовного кодекса Российской Федерации, а именно получение неправомерного доступа к компьютерной информации. Это удалось доказать, сравнив экземпляры программ, обнаруженных на компьютерах жертв мошенников, с экземплярами, обнаруженными непосредственно на компьютерах задержанных.

На одном из изъятых у задержанных ноутбуков эксперт Group-IB нашел некоторые следы, которые в своей совокупности прямо указывали на то, что пользователь данного компьютера активно занимался противоправной деятельностью. А именно, несмотря на тщательные меры конспирации, предпринятые всеми соучастниками расследуемого преступления, в журнале браузера одной из виртуальных машин все-таки сохранились фактические данные о посещении фишинговых страниц. Данные посещения осуществлялись, предположительно, с целью проверки их работоспособности, а также работоспособности функционала непосредственно самой вредоносной программы.

После нескольких проведенных исследований и экспертиз компьютерными криминалистами Group-IB были подготовлены соответствующие заключения экспертов, в которых полностью подтверждались выводы специалистов «Лаборатории Касперского» относительно функционала вредоносной программы. В дополнение к этому отчетливо обосновывалась причастность арестованных к совершению хищений денежных средств у клиентов банка.

Для того чтобы довести предварительное следствие до своего логического завершения, следователям Следственного департамента МВД России предстояло оформить и подготовить надлежащим образом все необходимые материалы для передачи уголовного дела в суд.

На данном этапе следствия технические эксперты и специалисты «Лаборатории Касперского» давали разъяснения по показаниям обвиняемых, а также помогали переводить специфические компьютерные термины и выражения на юридический язык, который бы был понятен судье.

Известные нам братья-хакеры из Санкт-Петербурга 11 сентября 2012 г. Чертановским районным судом города Москвы были признаны виновными в совершении преступлений по ч. 2 ст. 272, ч. 1 ст. 273 и ч. 4 ст. 159 УК РФ (неправомерный доступ к охраняемой законом компьютерной информации, использование и распространение вредоносных программ для электронно-вычислительной техники, а также мошенничество, совершенное группой лиц по предварительному сговору с причинением ущерба в особо крупном размере) и приговорены к шести годам лишения свободы «условно» с испытательным сроком 5 лет и штрафу по 450 тыс. рублей в пользу государства с каждого. Их соучастник — студент одного из калининградских вузов — признан виновным тем же судом в пособничестве в совершении мошенничества (ч. 5 ст. 33 и ч. 4 ст. 159 УК РФ) и приговорен к 4 годам «условно» и штрафу в 200 тыс. рублей [14].

Список литературы

1. Потехина И.П. Развитие информационно-коммуникационных технологий в условиях глобализации // Вестник Саратовского государственного социально-экономического университета. Экономика и бизнес. 2012. № 2. С. 36-40.
2. Задохина Н.С. Информационные технологии в банковской деятельности и безопасность их использования // Тенденции и перспективы развития банковской системы в современных экономических условиях: материалы II международной научно-практической конференции (Брянск, 17-18 декабря 2019 года). Брянск: Брянский государственный университет имени академика И.Г. Петровского, 2020. С. 147-152.
3. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы: утверждена Указом Президента РФ от 9 мая 2017 г. № 203 // КонсультантПлюс (дата обращения: 30.03.2020).
4. Афанасьев А.Ю., Репин М.Е. Уголовно-процессуальные и криминалистические особенности расследования киберпреступлений // Криминалистическое обеспечение раскрытия и расследования преступлений: материалы X Всероссийского научно-практического круглого стола (Ставрополь, 26 февраля 2016 г.). Ставрополь: Ставропольский филиал Краснодарского университета МВД России, 2016. С. 12-15.
5. Шаталов А.С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции // Вестник Сибирского юридического института МВД России. 2018. № 3 (32). С. 7-15.
6. Обокрали виртуально: хакеры похитили 60 миллионов рублей // Российская газета. 2012. 22 марта. № 61(5734) URL: https://rg.ru/2012/03/20/moshenniki-site.html (дата обращения: 02.04.2020).
7. Как не стать жертвой троянца? Держать шлюзы закрытыми // URL: https://www.kaspersky.ru/resource-center/preemptive-safety/avoiding-a-trojan-virus (дата обращения: 03.04.2020).
8. Ефремова О.В. Розыск и доказывание мошенничества — фишинга // Теория и практика выявления и расследования экономических и иных преступлений: материалы Международной научно-практической интернет-конференции (Нижний Новгород, 20 мая 2013 г.) / под ред. доктора юридических наук, профессора А.Ф. Лубина. Н. Новгород: Нижегородская академия МВД России, 2014. С. 58-64.

9. Фишеров поймали за руку. URL: http://www.iksmedia.ru/news/4235557s20121.html (дата обращения: 02.04.2020).
10. Ларичев В.Д. Методика построения криминалистической характеристики экономических преступлений // Общество и право. 2012. № 5 (42). С. 179-186.
11. Дело о фишинге: как ловили хакеров-близнецов из Санкт-Петербурга. URL: https://ria.ru/20121221/915789715.html (дата обращения: 05.04.2020).
12. Подшивалов А.П., Малахов А.С. Некоторые аспекты оперативно-розыскной характеристики мошенничеств, совершаемых дистанционным способом // Правопорядок: история, теория, практика. 2019. № 2 (21). С. 77-81.
13. Никитина И.А. Финансовое мошенничество в сети Интернет // Вестник Томского государственного университета. Право. 2010. № 337. С. 122-124.
14. Случаи задержания российских хакеров. URL: https://ria.ru/20130809/955384955.html (дата обращения: 20.02.2020).

Я.П. Ряполова, *к.ю.н., доцент кафедры уголовного процесса и криминалистики Юго-Западного государственного университета, г. Курск*

ПРАВОВОЙ РЕЖИМ ИСПОЛЬЗОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ И ТЕХНОЛОГИЙ В ДОКАЗАТЕЛЬСТВЕННОЙ ДЕЯТЕЛЬНОСТИ НА ЭТАПЕ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА*

Специфика расследования преступлений, совершенных с использованием информационных технологий, позволяет отметить, что основная часть доказательственной информации формируется на этапе приема сообщения о преступлении и реагирования на него. На сегодняшний день специалистами выработаны обстоятельные криминалистические характеристики преступлений указанной категории, подготовлены многочисленные рекомендации по их квалификации, проведению доследственных проверок и отдельных следственных действий [1-3].

Очевидно, пристального внимания законодателя в плане соответствующей разработки и модернизации требуют уголовно-процессуальные нормы, регламентирующие использование технических средств и технологий в доказательственной деятельности на начальном этапе досудебного производства.

Справедливо считать, что изменения уголовно-процессуального законодательства не отражают темпа развития современных телекоммуникационных отношений [4], только отдельные последние изменения законодательства (ФЕДЕРАЛЬНЫЕ ЗАКОНЫ ОТ 04.03.2013 г. № 23-ФЗ, ОТ 03.07.2016 Г. № 323-ФЗ, от 27.12.2018 г. № 533-ФЗ и др.) направлены на восполнение известного пробела. Как полагают многие исследователи, цифровизация досудебного уголовного судопроизводства происходит фрагментарно, непоследовательно и неоперативно, законодатель медлит с интегрированием в уголовный процесс предлагаемых «электронных новинок», не обращая внимания даже на тот факт, что Уголовно-процессуальный кодекс РФ в этом вопросе заметно отстает от других российских процессуальных законов [5].

Последние изменения УПК РФ несправедливо обошли вниманием правовую регламентацию отношений в сфере использования технических средств и современных информационных технологий на этапе возбуждения уголовных дела. Если обратиться к правовым положениям, налицо рассогласованность отдельных предписаний ст. 164.1 УПК РФ, в обновленном

* *Исследование выполнено за счет гранта Российского научного фонда (проект № 19-78-00088).*

виде закрепившей порядок изъятия (копирования) электронных носителей информации. Расположение ст. 164.1 УПК РФ среди общих положений о производстве следственных действий, а не в специальных — о производстве конкретных следственных действий (выемки, обыска) — свидетельствует о возможности производства изъятия (копирования) электронных носителей информации в ходе производства практически любого следственного действия, в рамках которого будет обнаружен электронный носитель информации, имеющий значение для уголовного дела. Представляется, данное правило применимо при производстве допустимых следственных действий в стадии возбуждения уголовного дела (осмотр места происшествия, осмотр трупа, предметов и документов, освидетельствование).

Однако часть 1 ст. 164.1 вводит особые ограничения, связанные с производством вышеуказанных действий при производстве по уголовным делам о преступлениях в сфере предпринимательской деятельности в контексте уже возбужденного дела, что говорит как минимум о непоследовательности в логике построения частей названной статьи. В данном контексте вывод о распространении рассматриваемых правил на перечень следственных действий, проводимых в стадии возбуждения уголовного дела, может оказаться не столь очевидным. Отдельные авторы обращают внимание на то, что в соответствии с пояснительной запиской к проекту федерального закона от 27.12.2018 № 533-ФЗ целью нового порядка являются дальнейшее формирование благоприятного делового климата в стране, сокращение рисков ведения предпринимательской деятельности, а также создание дополнительных гарантий защиты предпринимателей от необоснованного уголовного преследования. В связи с чем последовательность изложения частей нормы (ст. 164.1 УПК РФ) может навести на мысль, что ч. 2 и 3 указанной статьи применимы по уголовным делам, расследуемым в связи с совершением ограниченного перечня преступлений [6].

По-прежнему не закреплена процессуальная форма «изъятия» электронных носителей в ходе иных процессуальных и проверочных действий (истребование и представление предметов, проведение документальных проверок и ревизий). На практике распространены случаи, когда заявитель, очевидец либо пострадавшее лицо при подаче заявления, оформления явки с повинной, в ходе дачи объяснений добровольно предоставляет электронный носитель (карту памяти телефона либо видеорегистратора, например), а следователь копирует электронную информацию на свой компьютер. На данном этапе органы дознания и предварительного следствия еще не могут использовать весь предоставленный им арсенал процессуальных средств, в частности, провести полноценный обыск или выемку. В то же время современный порядок проведения доследственной проверки предполагает возможность «изъятия документов и предметов, в порядке, установленном настоящим Кодексом» (ч. 1 ст. 144 УПК РФ) [7].

На основании изложенного в целях реализации принципа правовой определенности предлагается закрепить в ст. 144 УПК РФ указания на возможность изъятия, истребования, осмотра, копирования обнаруженных электронных носителей информации при производстве следственных и иных процессуальных действий на этапе проверки сообщения о преступлении.

Дискуссионным является вопрос о возможности осмотра информации, содержащейся в памяти мобильного телефона, планшета, ноутбука и пр., изъятых в ходе проводимых следственных действий в отсутствие согласия их законных владельцев. На практике данный вопрос не вызывает ожидаемых затруднений: с помощью современных технических средств возможно извлечение большого объема информации, хранимой на мобильном телефоне, в том числе и защищенной. В законности подобного осмотра нет сомнений в тех случаях, когда на корпусе либо чехле телефона есть следы преступления (отпечатки пальцев, биологические следы и т.д.) Осмотр телефона до возбуждения уголовного дела проводится безотлагательно в случаях, когда необходимо уточнить его IMEI либо серийный номер сим-карты, который находится на обороте этой сим-карты. С другой стороны, поиск, изъятие и копирование содержащейся в телефонах электронной информации (журнал звонков, заметки, переписка

в мессенджерах, sms-сообщения, фото, видео, интернет-история) часто способствуют оперативному изобличению участников преступного события, розыску и задержанию последних, поиску трупов, похищенного имущества и т.п. и в целом обеспечению надежной доказательственной базы для органов следствия [8].

Суды все чаще признают допустимым доказательством протоколы осмотра мобильного телефона, «протоколы осмотра содержимого памяти телефона», «протоколы осмотра сведений, извлеченных из памяти планшета», «протокол осмотра детализаций телефонных и интернет-соединений абонентских номеров» и пр. [9-11]. Следует учитывать сформулированную Конституционным судом РФ позицию в определениях от 25 января 2018 г. № 189-О и от 17 июля 2018 г. № 1955-О, от 28.11.2019 № 3205-О, согласно которой «проведение осмотра с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств (а равно иных технических средств), изъятых в установленном законом порядке, не предполагает вынесения об этом специального судебного решения». Некоторую сбалансированность озвученного подхода обеспечивает, по всей видимости, указание на то, что «лица, полагающие, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения способны причинить ущерб их конституционным правам, в том числе праву на тайну переписки, почтовых, телеграфных и иных сообщений, могут оспорить данные процессуальные решения и следственные действия в суд в порядке, предусмотренном ст. 125 УПК РФ» [12]. Несложно догадаться, что общая тенденция разрешения таких обращений будет складываться именно в пользу следственных органов. По озвученным причинам отдельными авторами обосновывается также, что для осмотра информационной среды сотового телефона (связанной с просмотром имеющихся СМС-сообщений, сведений, содержащихся в переписке посредством социальных сетей, мессенджеров и т.д.) не требуется согласия лица [13].

В то же время получение с помощью технических средств доступа к переписке, содержащейся на мобильном телефоне, по содержанию идентично другому следственному действию — «осмотр и выемка электронных сообщений или иных передаваемых по сетям электросвязи сообщений», которое согласно требованию ч. 7 ст. 185 УПК РФ может быть произведено следователем только по решению суда, отличие лишь в том, что сотовый телефон физически изъят в ходе ранее проведенного следственного действия и находится на момент осмотра во владении следователя или дознавателя. Налицо системное противоречие в подходах к определению процессуальных оснований для ограничения конституционных прав лиц, вовлекаемых в уголовных процесс на этапе доследственной проверки, когда признаки преступления только устанавливаются. Опасность кроется в возможных злоупотреблениях со стороны сотрудников органов предварительного расследования, чреватых неконтролируемым вторжением в частную жизнь участников проверки: вместо осмотра места происшествия либо освидетельствования с изъятием предметов, либо на этапе фактического задержания будет проведен личный обыск и у законного владельца изъят мобильный телефон. В ряде случаев осмотр телефона и содержимого программ электронной переписки в практике органов, осуществляющих оперативно-розыскную деятельность, оформляется таким «суррогатным» действием, как личный досмотр. Мы солидарны с точкой зрения С.В. Зуева в этом вопросе: в связи с неоднозначной правовой оценкой действий, связанных с осмотром мобильных телефонов, представляется необходимым в УПК РФ определить основания ограничения конституционных прав физических лиц в конкретных случаях [14].

В настоящее время в ст. 164 УПК РФ закреплена возможность применения технических средства и способов обнаружения, фиксации и изъятия следов преступления и вещественных доказательств в отношении производства следственных действий, остается неурегулированным вопрос использования технических средств при производстве иных процессуальных

действий (получение объяснений, особенно по случаям, когда опрашиваемое лицо находится в опасном для жизни состоянии; проведение исследований, особенно в случаях, когда существует вероятность утраты (израсходования) объектов исследования [15], представление предметов и документов в электронном виде, задержание подозреваемого, видео- и фотофиксация момента доставления задержанного лица, получение устного заявления о преступлении и пр.).

Представляется очевидной необходимость расширения возможностей использования технических средств фиксации доказательственной информации и документирования процессуальных решений, явно недостаточно частичного отказа от института понятых в пользу фото- и видеоудостоверения результатов отдельных следственных действий (ч. 1.1 ст. 170 УПК РФ) [16]. Также в ч. 1.1 ст. 144 УПК РФ следовало бы предусмотреть право участников проверки ходатайствовать о применении тех или иных технических или электронных средств.

Таким образом, рациональное использование технических средств и современных технологий в ходе производства процессуальных действий по собиранию доказательств в стадии возбуждения уголовного дела — та область правового регулирования, на которой должны «стать на якорь» субъекты законодательной инициативы в обозримом будущем.

Список литературы

1. Вехов В.Б. Особенности проведения доследственной проверки по делам о преступлениях в сфере компьютерной информации // Эксперт-криминалист. 2013. № 4. С. 2-4.
2. Поляков В.В. Особенности производства осмотра по компьютерным преступлениям // Российский следователь. 2017. № 21. С. 14-17.
3. Алымов Д.В. Эвристические методы в следственной деятельности // Российский следователь. 2013. № 19. С. 2-3.
4. Зуев С.В., Овсянников Д.В., Копирование электронной информации в теории и практике уголовного процесса // Вестник СамГУ. 2014. № 11-2 (122). С. 168-173.
5. Добровлянина О.В. Некоторые аспекты о процессуальном изъятии (копировании) электронных носителей информации / под ред. О.А. Кузнецовой, В.Г. Голубцова, Г.Я. Борисевич, Л.В. Боровых, Ю.В. Васильевой, С.Г. Михайлова, С.Б. Полякова, А.С. Телегина, Т.В. Шершень // Пермский юридический альманах. 2019. № 1. С. 641-649.
6. Бондаренко А.А. Изъятие электронных носителей информации при расследовании уголовных дел экономической и общеуголовной направленности, а также по соединенным уголовным делам // Законодательство и практика. 2019. № 1. С. 36-40.
7. Россинский С.Б. Выемка: следственное действие или процессуальная форма изъятия? // Российский следователь. 2017. № 19. С. 28-32.
8. Багмет А.М., Скобелин С.Ю. Пределы ограничения конституционных прав граждан в ходе осмотра сотовых телефонов участников уголовного судопроизводства // Уголовное право. 2017. № 6. С. 97-103.
9. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 13.08.2019 № 66-АПУ19-16.
10. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 24.10.2019 № 34-АПУ19-3.
11. Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 12.03.2019 № 203-АПУ19-3).
12. Определение Конституционного Суда РФ от 28.11.2019 г. № 3205-О «Об отказе в принятии к рассмотрению жалобы гражданина Габашвили Игоря Сергеевича на нарушение его конституционных прав частью первой статьи 176 и частью второй статьи 177 Уголовно-процессуального кодекса Российской Федерации».

13. Табаков С.А. Производство предварительной проверки и дознания по факту мелкого коммерческого подкупа // Законодательство и практика. 2018. № 1. С. 18-23.

14. Зуев С.В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. 2018. № 4. С. 58-60.

15. Ряполова Я.П. Исследования предметов и документов как новая форма использования специальных познаний в стадии возбуждения уголовного дела // Российский следователь. 2010. № 24. С. 2-5.

16. Жариков Ю.С. Современная стратегия развития уголовного судопроизводства в России // Современное право. 2018. № 7-8. С. 86-91.

А.А. Смирнов, *аспирант кафедры криминалистики Московской академии СК РФ, руководитель отдела криминалистики СУ СК РФ по Липецкой области, полковник юстиции, г. Липецк*

АСПЕКТЫ ГЕНЕЗИСА КРИМИНАЛИСТИЧЕСКИХ ЗНАНИЙ ОБ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ

Информационная эра, или эра информационных технологий, начала зарождаться в 1980-х г. и продолжается до сих пор, она ознаменовала собой повсеместный переход от аналоговых технологий к цифровым.

Информационная эра (англ. Information Age, также известная как эра компьютеров или «информационная эпоха — электронная эпоха») — продолжающийся период в истории человечества с глобальным сдвигом от традиционной индустрии, установленной индустриальной революцией, к цифровой, компьютеризованной индустрии, основанной на трансфере информации. Также эта эра характеризуется широкими возможностями для отдельных лиц, особенно для преступников, свободно передавать и принимать информацию мгновенным доступом, как к освоенным знаниям, так и к любой информации о планах, поставленных человечеством [2].

В современном мире человек, все больше и больше в своей жизни использует цифровые устройства и, в частности, такие как:

- персональные компьютеры;
- ноутбуки;
- планшеты;
- мобильные телефоны;
- смарт-часы и многие другие.

Все эти устройства объединяются в единую сеть, по средствам глобальной сети Интернет, используя как проводные каналы связи (оптоволоконные), так и беспроводные каналы связи (мобильные, спутниковые каналы связи) — которые называются нейросети.

Все это не могло отложить свой отпечаток и на преступность. Поэтому в последнее время происходит рост преступлений совершаемых в сети Интернет или с использованием цифровых устройств. Вот далеко не полный перечень этих преступлений, которые входят в отдельную криминалистическую группу:

- распространение вредоносных программ, взлом паролей, кражу номеров банковских карт;
- распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду;
- вмешательство через компьютерные сети в работу различных систем.

Кроме того, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием Интернета, является мошенничество. Так, в письме Федеральной комиссии по рынку ценных бумаг от 20 января 2000 г. № ИБ-02/229 указывается, что инвестирование денежных средств на иностранных фондовых рынках с использованием сети Интернет сопряжено с риском быть вовлеченными в различного рода мошеннические схемы.

Другой пример мошенничества — интернет-аукционы, в которых сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара.

В различных государствах, в частности США, получили распространение аферы, связанные с продажей доменных имен: производится массовая рассылка электронных сообщений, в которых, например, сообщают о попытках неизвестных лиц зарегистрировать доменные имена, похожие на адреса принадлежавших адресатам сайтов, и владельцам сайтов предлагается зарегистрировать ненужное им доменное имя, чтобы опередить этих лиц. Так, вскоре после 11 сентября 2001 г. Федеральная торговая комиссия США отметила факт массовой продажи доменных имен зоны «usa».

В это же время в криминалистике, как в науке, начинается зарождение знаний о преступлениях, совершаемых с применением информационных технологий. Накапливается опыт по выявлению и раскрытию данных преступлений, нарабатывается материально-техническая база [2].

Современные преступления совершаются де-факто в двух мирах, один из которых привычный нам мир материальных объектов, а другой — виртуальный. Мы погружены в этот виртуальный мир различными способами. Например, опосредованно — попадая в объективы систем видеонаблюдения, перенося мобильные телефоны, регистрируемые базовыми станциями сетей сотовой связи, используя карты накопления бонусных баллов в магазинах или устанавливая в автомобиль систему сигнализации с GSM-модулем и функцией трекинга маршрута [1].

В связи с тем, что цифровой мир является де-факто виртуальным, здесь появляется больше возможностей по скрытию следов преступлений.

Преступники при совершении преступлений через сеть Интернет начинают использовать различные анонимайзеры, VPN и другое.

Анонимайзер — общее название средств для скрытия информации о компьютере, его IP-адресе или пользователе в сети от удаленного сервера. Анонимайзеры применяются не только для обеспечения конфиденциальности, но и в качестве возможности посещать заблокированные в стране сайты, получения доступа к чатам и форумам, если ваш IP-адрес там заблокирован, обхода ограничений файлообменников и др.

VPN (англ. Virtual Private Network «виртуальная частная сеть») — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например Интернет).

Для поиска возможных цифровых улик криминалисты вынуждены проделывать большую аналитическую работу, работать в команде со смежными службами, а также анализировать большой объем информации от сотовых и интернет-провайдеров. Но как бы ни старались злоумышленники, уничтожить все следы даже в виртуальном мире невозможно, и криминалистические службы, накопив уже достаточный багаж знаний, активно выявляют и раскрывают преступления, совершенные с применением цифровых (информационных) технологий. Но, как говорится, мир не стоит на месте, преступники придумывают новые методы и способы совершения преступлений, IT-компании изобретают способы защиты от подобных преступлений, а криминалисты внедряют новые методики, материально-техническую базу и другое, чтобы быть впереди в этой «борьбе».

Преступники в XXI в. для совершения атак в информационном пространстве начали объединяться в группы, так называемые хакерские сообщества, а кроме того, совершать преступления за пределами своей страны, что значительно усложняет расследование подобную категорию преступлений и существенно увеличивает сроки расследования дел. В этом случае действовать приходится по международным каналам. Это дает преступникам время замести следы преступлений, а также выехать за пределы территории (страны), в которой данное преступление совершалось. Для увеличения качества расследования и сокращения сроков необходимо разрабатывать нормативно-правовые акты в международных организациях, а также подобные акты заключать между странами. Чтобы юридические лазейки не позволяли преступникам длительные время оставаться на свободе, если вообще не затеряться на территории третьих стран.

Сама главная отличительная особенность преступлений, совершаемых с применением информационных технологий, может быть их неочевидность, последствия таких преступлений могут проявиться через достаточно большой промежуток времени. Например, произведена кража персональных данных, а через год, используя эти данные с применениям мошеннических схем, получают кредиты. Или выпускают цифровую подпись и перепродают недвижимость или другое имущество.

Схемы, по которым совершаются преступления, с каждым годом становятся все более изощренными, особенно с внедрением большого количества информационных систем, которые, с одной стороны, должны помогать гражданам, но с другой — позволяют зачастую совершать в отношении их правонарушения. При создании подобных систем просчитать все возможные риски часто не представляется возможным.

Сейчас можно выделить следующие основные способы совершения преступлений, совершаемых с применением информационных технологий:

– применение социальной инженерии преступники входят в доверие, завладевают паролем от интернет-банков и дальше уже контролируют счета своих жертв, выводят оттуда деньги;

– внедрение специального программного обеспечения посредством рассылки по электронной почте, сообщений в мессенджерах и другие, получают доступ к компьютерам, телефонам и другим устройствам и уже имеют полный к данным хранящимся на устройстве совершают преступления, это может быть доступ к информационным ресурсам, интернет-банкам, получение личной и персональной информации;

– применение технических устройств для считывания данных с банковских карт, всевозможные накладки на банкоматы, применение поддельных копий банкоматов и другие.

Как видим, поле этой криминальной деятельности преступников очень обширное. В настоящее время накоплен большой багаж знаний о преступлениях, совершаемых с применением информационных технологий, разработаны соответствующие методики, налажено взаимодействие с государственными и частными организациями, операторами и провайдерами. В раскрытии подобных дел в настоящее время стоит проблема — сроки раскрытия преступлений, в связи с тем, что приходится обрабатывать большой массив информации, полученный от различных структур, распутывать все цепочки транзакций при переводе денежных средств с применением счетов различных банков. Зачастую приходится устанавливать всю цепочку сервера, в случаях применения преступниками программного обеспечения, способного имитировать выход в сеть из других точек мира или подмены IP-адресов. Решение всех этих задач требует большого количества времени.

В качестве положительного примера раскрытия преступлений в рассматриваемой сфере следует отметить дело об организации и осуществлении компьютерных DDoS-атак 3 на

ведущие букмекерские сайты Армении. В ходе предварительного следствия по данному 3 DDoS — хакерская атака на вычислительную систему с целью довести ее до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системам. В результате оперативного сотрудничества и взаимодействия Главного следственного управления по расследованию особо важных дел следственного комитета и отдела по киберпреступлениям при ГУБОП Полиции Республики Армения не только было раскрыто данное уголовное дело, но также были выявлены и другие преступные деяния, совершенные разными лицами, в том числе и лицами, находящимися за пределами Республики Армения. По данным уголовного дела, атаки производились хакерами, которые находились на территории Украины, которые постоянно изменяли IP-адреса. В ходе расследования уголовного дела об организации компьютерного саботажа и незаконного присвоения компьютерных данных, совершенного группой лиц по предварительному сговору, установлены виновные, одно лицо объявлено в международный розыск. Ведутся также оперативно-розыскные мероприятия для выявления и привлечения к уголовной ответственности лиц, непосредственно осуществивших DDoS-атаки на сайты [3].

Кроме того, на территории Липецкой области было возбуждено уголовное дело по признакам преступления, предусмотренного ч. 4 ст. 132 УК РФ «Насильственные действия сексуального характера, совершенные в отношении лица, не достигшего четырнадцатилетнего возраста». Преступник познакомился с потерпевшей через Интернет, достоверно знал о ее малолетнем возрасте, так как потерпевшая сама ему говорила об этом и это следует из полученных в ходе следствия, при осмотре телефона потерпевшей, «скринах» переписки преступника и потерпевшей. Используя определенные психологические приемы, преступник заставлял малолетнюю потерпевшую фотографировать и пересылать ему свои интимные фото, осуществляя соответственно аналогичные действия. Информация о противоправных действиях в правоохранительные органы поступила от матери потерпевшей, случайно обнаружившей переписку своей дочери с неизвестным мужчиной. Раскрытие данного преступления затруднялось тем, что при выходе в Интернет преступник каждый раз использовал различные IP-адреса. Сотрудниками правоохранительных органов была проделана кропотливая работа по сбору доказательственной базы. Преступление было раскрыто при отработке с потерпевшей с фотомассива лиц, ранее привлекаемых за совершение аналогичных преступлений.

Таким образом, очень много задач в эпоху цифровизации ставится перед криминалистическими подразделениями СК РФ, которым надо развиваться в ногу со временем. В настоящее время криминалисты уверенно справляются с поставленными перед ними задачами, а именно сотрудниками ведомства постоянно обобщается опыт раскрытия и расследования данных преступления. Созданы экспертные подразделения, основной целью которых является исследование цифровых объектов. На вооружении следователей находятся новейшие технические средства, позволяющие извлекать и анализировать информацию, содержащуюся в компьютерах и сотовых телефонах, в большинстве случаев даже удаленную, которую преступник пытался скрыть «от посторонних глаз». Работа в этом направлении продолжается и будет совершенствоваться в соответствии с техническим прогрессом.

Список литературы

1. Баев О.Я. Основы криминалистики: курс лекций. М.: Экзамен, 2003.
2. URL: https://ru.wikipedia.org/wiki/Информационная_эра.
3. Новые способы совершения преступлений в сфере информационных технологий на территории государств — участников СНГ. Аналитический обзор / И.Б. Колчевский, В.М. Журавлев, А.Г. Кузнецов, О.В. Демковец, Д.А. Брехов. М.: ФГКУ «ВНИИ МВД России», 2018. 76 с.

А.Б. Соколов, *к.ю.н., доцент кафедры криминалистики Омской академии МВД России, г. Омск*

ПОНЯТИЕ И СТРУКТУРА КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Современность характеризуется широким применением средств компьютерной техники практически во всех областях жизнедеятельности человека. К сожалению, такая тенденция имеет не только положительные, но и отрицательные стороны. Примером этого является совершение преступлений в сфере компьютерной информации. Анализ статистических данных показывает неуклонный рост таких преступлений. Так, уже за январь-май 2020 г. было зарегистрировано 180498 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в том числе 1326 — неправомерный доступ к компьютерной информации (ст. 272 УК РФ) из них всего 195 преступлений было раскрыто [1].

Низкая раскрываемость исследуемых противоправных деяний связана с различными причинами. К некоторым из них возможно отнести сложность в определении места, времени, конкретных лиц, а иногда и способа совершения преступления, своевременной фиксации следов преступления. Кроме того, негативное воздействие оказывает допущение в ходе рассмотрения сообщений о неправомерном доступе к компьютерной информации ошибок процессуального и криминалистического (тактического) характера. В последующем они могут приводить к неправильной квалификации преступного деяния, безвозвратной утрате доказательств, определению ошибочного направления в расследовании.

Минимизировать степень допущения просчетов в стадии возбуждения уголовного дела и создать информационную основу для раскрытия и расследования рассматриваемого вида противоправного деяния позволит криминалистическая характеристика преступлений.

Анализ позиций ученых, высказанных относительно понятия и сущности указанной категории, позволяет заключить, что она представляет собой систему описания криминалистически значимых признаков преступления, проявляющихся в сведениях об обстановке и способе совершения преступления, личности преступника и потерпевшего, механизме следообразования, предмете преступного посягательства и иных обстоятельствах, имеющих значение для раскрытия, расследования и предупреждения преступлений [2-6].

Тем не менее продолжающееся исследование криминалистической характеристики преступлений, высказывание дополнительных аргументов в пользу обоснования ее практической значимости требует, на наш взгляд, уточнения ее структуры и содержания применительно отдельных видов преступлений, что исключает единый подход к решению указанного вопроса.

Существуют разнообразные суждения относительно структуры криминалистической характеристики преступлений.

По мнению А.Н. Колесниченко, криминалистическая характеристика включает в себя следующие элементы: способ приготовления, совершения и сокрытия преступления; место, время, обстановка, орудия и средства совершения преступления; предмет посягательства; личность потерпевшего; личность преступника; следы преступления [7].

По мнению В.Г. Танасевича, к элементам криминалистической характеристики следует отнести: «способ совершения преступления; обстановку совершения преступления, непосредственный предмет преступного посягательства, условия охраны его от посягательства, личность субъекта преступления; маскировка, направленная на сокрытие преступного деяния и виновных лиц, осуществляемая как в процессе совершения преступления, так и после него» [8]. Дискуссионным является отнесение к самостоятельному элементу криминалистической характеристики преступлений маскировки, направленной на сокрытие преступного деяния и виновных лиц. Разделяем мнения Г.Г. Зуйкова и Р.С. Белкина, что это не более чем один из способов сокрытия преступления и, соответственно, являющийся структурным элементом

способа совершения преступления [9, 10]. Условия охраны также не могут быть признаны в качестве самостоятельного элемента криминалистической характеристики, поскольку в большей части отражают характеристику обстановки совершения преступления.

Интересной представляется позиция Р.С. Белкина относительно того, что криминалистическая характеристика отдельного вида преступлений должна включать характеристику исходной информации, системы данных о способе совершения и сокрытия преступления и типичных последствиях его применения, личности предполагаемого преступника и мотивах и целях преступления, личности вероятной жертвы преступления, о некоторых обстоятельствах совершения преступления (место, время, обстановка) [10]. Полагаем, что мотивы и цели преступной деятельности относятся больше к элементам состава преступления (субъекту преступления), т.е. речь идет об уголовно-правовой характеристике.

А.Г. Филиппов в качестве элементов криминалистической характеристики выделяет: предмет преступного посягательства; способ совершения и сокрытия преступления; обстоятельства подготовки и совершения преступления (время, место, условия охраны объекта и т.д.); особенности оставляемых преступниками следов (механизм следообразования); личность преступника и потерпевшего [11].

Предлагаемые учеными структурные элементы криминалистической характеристики преступлений в основном отражают ее типичную структуру, имеющую единство и взаимосвязь элементов. Однако криминалистическая характеристика неправомерного доступа к компьютерной информации имеет свои отличительные черты по сравнению с иными противоправными деяниями.

Элементный состав криминалистической характеристики рассматриваемого противоправного деяния определяется содержанием диспозиции ст. 272 Уголовного кодекса Российской Федерации. Считаем, что под неправомерным следует понимать доступ лица к конфиденциальной информации или информации, составляющей государственную или иную охраняемую законом тайну, не обладающего на то полномочиями, при соблюдении условий обеспечения ее защиты. Состав рассматриваемого преступления является материальным, что предполагает обязательное наступление хотя бы одного из перечисленных в уголовном законе последствий — уничтожение, блокирование, модификацию либо копирование компьютерной информации. Неправомерный доступ к компьютерной информации считается оконченным с момента наступления хотя бы одного из указанных результатов.

С учетом сказанного не вызывает сомнений, что сведения об **обстановке совершения преступления** является элементом криминалистической характеристики неправомерного доступа к компьютерной информации. Относящиеся к структуре указанного элемента место и время совершения преступления являются обстоятельствами, подлежащими доказыванию. При этом их точное определение порой вызывает значительную сложность.

Следует разграничивать место совершения и место обнаружения признаков преступления, которые, как правило, не совпадают. Это обусловлено особенностями функционирования информационно-телекоммуникационных технологий с учетом возможностей глобальной сети Интернет. Местами совершения преступлений могут выступать участок местности или помещение, где были выполнены действия по неправомерному доступу к компьютерной информации. Они могут осуществляться непосредственным либо удаленным доступом.

Временем совершения неправомерного доступа к компьютерной информации следует считать момент окончания осуществления общественно опасного действия при наступлении хотя бы одного из последствий — уничтожения, блокирования, модификации либо копирования компьютерной информации.

Центральным элементом криминалистической характеристики рассматриваемого вида преступлений является **способ совершения преступления**, под которым мы понимаем действия лица (группы лиц) по подготовке, непосредственному совершению и сокрытию следов и своего участия в неправомерном доступе к компьютерной информации.

Определение способа совершения исследуемого вида преступления зависит, с одной стороны, от используемых средств компьютерной техники, программного обеспечения, с другой — предмета преступного посягательства (местонахождение компьютерной информации, способы и средства ее защиты и др.).

Способ совершения неправомерного доступа к компьютерной информации находит свое отражение в таком элементе криминалистической характеристики, как **механизм следообразования**. Следовая картина рассматриваемого противоправного деяния является особенной и может содержать как идеальные, так и материальные следы. Разделяем позицию ученых, указывающих на материальную природу компьютерной информации и, соответственно, электронно-цифровых следов [12]. Не вступая в полемику с отдельными учеными, отметим, что придерживаемся позиции В.Б. Вехова, который определяет электронно-цифровой след как «любую криминалистически значимую компьютерную информацию, т.е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов» [13].

Наибольшую ценность будут представлять следы, указывающие на то, каким образом осуществлялся неправомерный доступ к компьютерной информации; каким образом были преодолены способы и средства защиты информации; какие знания и умения были (могли быть) использованы; были ли попытки скрыть (уничтожить) следы совершенного преступления.

С другой стороны, данные о способе неправомерного доступа к компьютерной информации позволяют высказать суждение о виде и местонахождении следов преступного деяния и целенаправленно организовать их поиск, определить уровень знаний и умений лиц, совершивших преступление, прогнозировать их поведение после совершения преступления.

Предметом преступного посягательства выступает компьютерная информация. Федеральный закон «Об информации, информационных технологиях и защите информации» определяет ее как сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [14].

Особенности рассматриваемого вида преступлений заключаются в том, что установление конкретной компьютерной информации, подвергнутой уничтожению, блокированию, модификации либо копированию, позволяют следователю выдвинуть версию относительно личности вероятного преступника.

Учитывая сказанное, сведения о предмете преступного посягательства являются элементом криминалистической характеристики неправомерного доступа к компьютерной информации.

Неотъемлемым элементом криминалистической характеристики преступлений рассматриваемого вида является **личность вероятного преступника**.

К сведениям о личности вероятного преступника следует отнести социальный статус, род занятий, наличие преступного опыта, уровень профессиональной подготовки; возможности доступа к средствам компьютерной техники; свойства характера и др.

Установление указанных данных позволит правильно выбрать оптимальное направление поиска преступника, определить места хранения скопированной информации и др.

При этом осуществление конкретным лицом действий до, во время и после совершения неправомерного доступа к компьютерной информации влияет на степень детализации обстоятельств, подлежащих установлению, а также на алгоритм действия следователя по расследованию преступления.

Как следствие, изучение связи особенностей личности вероятного преступника с выявленными сведениями о способе, обстановке совершения преступления и механизме следообразования образуют новые данные, позволяющие определить ход дальнейшего расследования.

Учитывая сказанное, отметим, что криминалистическая характеристика неправомерного доступа к компьютерной информации является системой сведений о присущих данному виду преступлений признаках и свойств, находящих свое проявление в следующих элементах:

– обстановка совершения преступления;
– способ совершения преступления;
– механизм следообразования;
– предмет преступного посягательства;
– личность вероятного преступника.

Рассматривая проблему содержания криминалистической характеристики преступлений, В.К. Гавло указал, что «нельзя слишком широко толковать это понятие — начиная от отличительных черт, свойств и признаков того или иного вида преступления и наиболее типичных доказательств, а также обстоятельств, способствующих его совершению» [15]. Поэтому в содержание следует включать только те компоненты, которые характеризуют преступление с криминалистической стороны. Криминалистическая характеристика является информационной основой расследования преступлений.

Список литературы

1. Официальный сайт Министерства внутренних дел Российской Федерации. Состояние преступности в Российской Федерации за январь-май 2020 года. URL: https://мвд.рф/reports/item/20422560/ (дата обращения: 11.07.2020).
2. Шурухнов Н.Г. Криминалистическая характеристика преступлений. Криминалистика (актуальные проблемы) / под ред. Е.И. Зуева. М., 1998. С. 119.
3. Криминалистика: учебник / отв. ред. Н.П. Яблоков. М., 1999. С. 36–37.
4. Криминалистика: учебник / Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. 3-е изд., перераб. и доп. М. 2000. С. 656-658.
5. Криминалистика: учебник для прикладного бакалавриата / под ред. А.Г. Филиппова. 3-е изд., перераб. и доп. М., 2017. С. 330-332.
6. Криминалистика: учебник для бакалавров / отв. ред. Е.П. Ищенко. М., 2019. С. 273.
7. Методика расследования отдельных видов преступлений: программированные задания: учебное пособие / под ред. В.П. Бахина. Киев, 1985. С. 33-34.
8. Танасевич В.Г. Теоретические основы методики расследования преступлений // Сов. гос-во и право. 1977. № 6. С. 92.
9. Зуйков Г.Г. Поиск преступников по признакам способов совершения преступлений: учебное пособие. М., 1970. С. 76.
10. Белкин Р.С. Курс криминалистики: в 3 т. М., 1997. Т. 3: Криминалистические средства, приемы и рекомендации С. 366-367.
11. Филиппов А.Г. Криминалистика: учебник. М., 2007. С. 310.
12. Поляков В.В., Шебалин А.В. К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: материалы Одиннадцатой международной научно-практической конференции. Барнаул: 2013, Ч. 1. С. 123-125.
13. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. Волгоград, 2008. С. 94.
14. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // КонсультантПлюс.
15. Гавло В.К. К вопросу об актуальных направлениях развития криминалистической методики и тактики расследования // Актуальные направления развития криминалистической методики и тактики расследования. М., 1978. С. 31.

А.Р. Сысенко, *к.ю.н., доцент кафедры криминалистики Омской академии МВД России, г. Омск*
Н.И. Герасименко, *к.ю.н., старший преподаватель кафедры криминалистики Омской академии МВД России, г. Омск*

ОСОБЕННОСТИ ПОДГОТОВИТЕЛЬНОГО ЭТАПА ОСМОТРА ИНФОРМАЦИОННОЙ СРЕДЫ В СЕТИ ИНТЕРНЕТ

Для качественного производства осмотра информации в сети Интернет важно понимание общих целей данного следственного действия, которые, по мнению О.Б. Дронова, состоят в следующем:

– фиксация факта наличия и активности интересуемого интернет-домена;

– обнаружение и фиксация данных, имеющих значение для расследования уголовного дела (самого факта и способа реализации запрещенной продукции, контактные данные организации и др.);

– установление физического расположения домена (сведений о хостинг-провайдере);

– получение сведений о регистраторе доменного имени.

Подготовительный этап следственного осмотра информационной среды сети Интернет состоит из следующих компонентов:

1. Уяснение характера предполагаемой к осмотру информации: является ли она общедоступной или представляет собой конфиденциальную информацию, имеющую закрытый характер.

2. Подпадает ли указанная информация под действие конституционных норм о тайне переписки, предусмотренных ст. 23 Конституции РФ, и, следовательно, необходимо ли судебное решение на ограничение конституционных прав конкретных лиц, которое является неизбежным при проведении следственного осмотра.

3. Определение круга участвующих лиц и обеспечения их присутствия.

4. Решение вопроса о необходимости использования специальных технико-криминалистических средств и программного обеспечения, подготовки специальных бланков процессуальных документов.

5. Определение иных способов фиксации информации в сети Интернет в ходе осмотра (за исключением протоколирования).

6. Определение места совершения преступления, что справедливо для производства осмотра места происшествия [1, с. 143].

Изучение юридической литературы по настоящему вопросу, а равно анализ следственной практики, позволяет нам утверждать, что для осмотра информации в сети Интернет следователю следует привлекать следующих лиц:

1. Понятых как лиц в соответствии с УПК РФ, привлекаемых для удостоверения хода и результатов следственного действия. При этом в литературе отмечают, что у понятых, привлекаемых для участия в следственных действиях подобного рода, должно иметься хотя бы общее представление об информационных технологиях (на уровне простого пользователя) для понимания характера совершаемых следователем действий.

В научном мире справедливо отмечается, что в качестве понятых следует приглашать людей, сведущих в компьютерной технике [3, с. 172]. Лицо, которое не понимает сути происходящего, в дальнейшем при допросе может подставить под сомнение достоверность полученных в результате следственного действия доказательств. В исключительных случаях в качестве понятых могут быть работники предприятия, фирмы, учреждения, компании, где проводится осмотр, если они не заинтересованы.

2. Собственника информационного ресурса (если это возможно и представляется необходимым), а также правообладателя информации конфиденциального характера. Указанные лица призваны дать в ходе осмотра информацию ориентирующего для следователя характера о том, в каком разделе информационного ресурса, на какой вкладке имеется та или иная информация, а также для преодоления средств защиты в виде идентификации, ввода паролей и тому подобное.

3. Специалиста, то есть лица, обладающего специальными знаниями в области информационных технологий и способного помощь следователю в наиболее полном и достоверном отражении в протоколе информации, имеющей доказательственное значение.

После определения круга участвующих лиц следователю необходимо определить перечень необходимых технико-криминалистических средств, необходимых для осмотра информации в сети Интернет. Сюда относится подготовка необходимой компьютерной техники и программного обеспечения, необходимого для считывания, изъятия и хранения обнаруженной информации. Указанными средствами может быть персональный компьютер, исполненный в переносном варианте «Notebook», кабель и программное обеспечение, позволяющее осуществить копирование.

Для качественного копирования информации необходимы объемы используемых жестких дисков (у переносного компьютера этот объем должен быть не меньше, а в идеальном случае равен объему диска осматриваемого компьютера). Также можно использовать носители информации, обладающие большой емкостью: лазерные и DVD-диски, внешние жесткие диски и тому подобное.

На подготовительном этапе большое значение имеет инструктаж всех участников осмотра, в ходе которого следователь обозначает задачи предстоящего следственного действия, особенности его производства и предполагаемого изымаемого объекта. Инструктаж целесообразнее проводить вместе со специалистом, который разъяснит технические моменты предстоящего осмотра. При этом необходим категорический запрет кому бы то ни было из лиц, работающих на объекте осмотра, или находящихся на нем по иным причинам, соприкасаться с ЭВМ, выключать без специального указания со стороны следователя энергоснабжение объекта, самостоятельно производить какие-либо манипуляции со средствами компьютерной техники, если результат этих манипуляций заранее неизвестен.

Важным является определение места совершения преступления. Как полагает Т.П. Ишмаева, при совершении одного преступления, например, неправомерного доступа к компьютерной информации, может быть несколько мест происшествия:

1. Рабочее место, рабочая станция — место обработки информации, ставшей предметом преступного посягательства.

2. Место постоянного хранения или резервирования информации — сервер или стример.

3. Место использования технических средств для неправомерного доступа к компьютерной информации, находящейся в другом месте, при этом место использования может совпадать с рабочим местом, но находиться вне организации, например, при стороннем взломе путем внешнего удаленного сетевого доступа.

4. Место подготовки преступления (разработки вирусов, программ взлома, подбора паролей) или место непосредственного использования информации (копирование, распространение, искажение) [2, с. 84].

Следует справедливо заметить, что местом происшествия может быть одно помещение, где установлен компьютер и хранится информация, ряд помещений, в том числе в разных зданиях, расположенных на различных территориях, либо участок местности, с которого проводится дистанционный электромагнитный или аудиоперехват.

На современном этапе также выделяется новое для современной практики место совершения преступления, а именно информационное пространство (киберпространство), где не действуют географические, юридические законы и понятия. И вполне справедливо выделяется ряд вопросов о специфических особенностях при проведении осмотра места происшествия. Ввиду специфики компьютерных преступлений для обнаружения следов преступлений в процессе осмотра места происшествия необходимо наличие специальных знаний в области компьютерных технологий [4, с. 123].

Особенности осмотра информации в сети Интернет и в целом — осмотра компьютерной техники обязывают обращать большое внимание на подготовительную стадию, так как высока вероятность утраты информации, имеющей доказательственной значение.

Список литературы

1. Дронов О.Б. Осмотр интернет-ресурса как следственное действие, направленное на противодействие распространению товаров, не соответствующих установленным требованиям // Вестник Волгоградской Академии МВД России. 2016. № 2.
2. Ишмаева Т.П. К вопросу об особенностях осмотра места происшествия по делам о компьютерных преступлениях // Правопорядок: история, теория, практика. 2015. № 4.
3. Романенко М.А. Следственный осмотр по делам о преступных нарушениях авторских прав в сфере программного обеспечения // Вестник Омского университета. 2008. № 1.
4. Хомколов В.П. Организационно-правовые аспекты расследования и предупреждения преступлений в сфере компьютерной информации: дис. ... канд. юрид. наук. Иркутск, 2004. 184 с.

А.В. Цахуев, *старший преподаватель кафедры уголовного процесса и криминалистики Юридического института Дагестанского государственного университета, эксперт отдела криминалистики следственного управления Следственного комитета Российской Федерации по Республике Дагестан, г. Махачкала*

ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПРИГОТОВЛЕНИЯ К УЧАСТИЮ В НЕЗАКОННЫХ ВООРУЖЕННЫХ ФОРМИРОВАНИЯХ И МЕЖДУНАРОДНЫХ ТЕРРОРИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ ЗА ПРЕДЕЛАМИ РОССИЙСКОЙ ФЕДЕРАЦИИ

На сегодняшний день наибольшую угрозу национальной безопасности и целостности Российской Федерации представляют преступления террористической направленности. Одним из наиболее опасных проявлений терроризма является деятельность незаконных вооруженных формирований (далее — НВФ) и международных террористических организаций (далее — МТО), в том числе и за пределами Российской Федерации [3, с. 292]. Согласно статическим данным, в последние годы заметно увеличились случаи участия граждан России в НВФ и МТО на территории иностранных государств. В качестве примера — вооруженные конфликты в Сирии, Ираке, Йемене, Египте, Афганистане и др., на территории которых действуют многочисленные НВФ и МТО [5, с. 7, 8].

Проведенный анализ следственной и судебной практики свидетельствует о проблемах, допускаемых при выявлении, расследовании и доказывании фактов участия в НВФ и МТО за пределами России, пресеченных на этапе приготовления, и ошибках, допускаемых в привлечении к уголовной ответственности за совершение преступлений, предусмотренных ч. 1 ст. 30 и ч. 2 ст. 205.5 или ч. 2 ст. 208 Уголовного кодекса Российской Федерации (далее — УК РФ).

В ряде случаев не были своевременно реализованы материалы оперативно-розыскной деятельности, содержащие признаки рассматриваемых преступлений.

Основной сложностью доказывания таких преступлений, пресеченных на этапе приготовления, является опровержение доводов обвиняемых об отсутствии умысла на их совершение. В этой связи собранные по делу доказательства должны позволять опровергнуть версию следовании в государства, приграничные с зонами вооруженных конфликтов, с иными целями.

В последние годы сотрудники правоохранительных органов задержали в аэропортах при попытке регистрации на рейс в государства, приграничные с территориями, подконтрольными НВФ и МТО, сотни лиц, намеревавшихся выехать из Российской Федерации для дальнейшего вступления в НВФ и МТО. Десятки будущих боевиков были остановлены при попытке выезда из России через контрольно-пропускные пункты автомобильным транспортом. Имеются факты успешного привлечения к уголовной ответственности радикалов, задержанных на этапе приискания способов проникновения на территорию Ирака, Сирии и Афганистана и других стран, на территории которых действуют НВФ и МТО.

В качестве примера: в 2018 г. осуждены М. и А., задержанные на этапе приискания денежных средств на транспортное средство и установлении возможного маршрута следования на территории, подконтрольные НВФ и МТО в Сирии [1].

В большинстве случаев подсудимые по таким уголовным делам в судебном заседании отказывались от ранее данных признательных показаний и выдвигали версию о выезде из России с туристическими целями либо прохождения обучения или трудоустройства.

Поскольку у России и приграничных стран отсутствует прямое регулярное авиасообщение с Сирией, Ираком и Афганистаном, в которых базируются МТО и НВФ, проникновение на их территорию возможно лишь через территорию сопредельных государств. Как правило, транзитной страной для лиц, намеревавшихся вступить в НВФ и МТО в вышеуказанных странах, является Турецкая Республика, при этом самым популярным является авиаперелет в Турцию, а затем следование на автомобильном транспорте к границе.

Проведенный анализ следственной и судебной практики показал, что доказательствами приготовления лица к вступлению в НВФ и МТО на территории иностранного государства являются:

– переписка о маршруте следования из России в Сирию, Ирак и другие страны и способах незаконного пересечения границы с этими государствами;

– телефонные соединения и переписка (в том числе мультимедийные файлы) с приверженцами радикальных течений ислама, а также с лицами-боевиками, уже состоявшими в НВФ и МТО;

– показания свидетелей о ставших им известными намерениях и предпринятых действиях осужденных к вступлению в НВФ и МТО;

– показания сотрудников оперативно-розыскных подразделений об обстоятельствах, ставших им известными при проведении оперативно-розыскных мероприятий;

– обнаружение в ходе личного обыска предметов одежды и вещей, приготовленных для выезда за пределы территории Российской Федерации.

Кроме того, проведенный анализ позволил нам выделить основные обстоятельства, свидетельствующие об умысле на вступлении в НВФ и МТО на территории иностранного государства:

– увлечение радикально-экстремистскими течениями ислама;

– заключение мусульманского брака с лицом, находящимся на территории приграничного с зоной вооруженного конфликта иностранного государства;

– интерес к различным сайтам и страницам в социальных сетях с экстремистско-террористическим подтекстом;

– обращение в УФМС за получением заграничного паспорта при отсутствии сведений о посещении других иностранных государств в туристических целях;

– факт реализации имущества, увольнения с работы без намерения трудоустройства;
– создание условий для выезда за пределы России (поиск денежных средств, изучение арабского языка, культуры, обычаев, приобретение необходимых предметов одежды и пр.);
– изучение навыков обращения с оружием, взрывного дела, медицины и др.;
– поиск контактов с участниками МТО и НВФ;
– приобретение авиабилета в одну сторону.

Следует учитывать, что приведенные признаки в отдельности не являются свидетельством приготовления лиц к совершению рассматриваемых преступлений, об умысле на вступление в НВФ и МТО можно судить лишь при наличии совокупности доказательств.

Важные доказательства могут быть получены при осмотре электронных носителей информации (телефоны, смартфоны, планшеты и др.), в памяти которых хранятся так называемые цифровые следы (переписка в мессенджерах, социальных сетях и др.). Так, по делам рассматриваемой категории посредством таких носителей информации может приниматься присяга лидерам НВФ и МТО, осуществляться поиск маршрутов следования к иностранному государству, на территории которого действуют такие НВФ и МТО, поиск проводников и лиц, имеющих намерение вступить в НВФ и МТО и т.д.

Так, в 2019 г. А. осужден за приготовление к участию в деятельности МТО на территории Сирии. В ходе расследования у А. был изъят мобильный телефон «iPhone 6S», при осмотре которого была обнаружена видеозапись, на которой А. на фоне флага МТО «ИГИЛ» принимает присягу на верность ее лидеру. Кроме того, в памяти телефона была обнаружена переписка с другими лицами на различные темы: необходимая сумма для выезда из России, необходимые предметы одежды, методы конспирации и др. [2]

Для опровержения доводов лица, задержанного при попытке вылета в страну, приграничную с зоной влияния боевиков, или транзитное государство, о том, что он следует туда с туристическими целями, важную роль играет содержимое его багажа. Как правило, будущие боевики НВФ и МТО берут с собой предметы военной экипировки, спортивную одежду, медикаменты и пр., и в их багаже отсутствует одежда, присущая гардеробу обычного туриста. В этой связи в протоколе осмотра должны быть тщательно описаны все предметы, приготовленные для вылета. Содержимое багажа необходимо отразить в фототаблице.

В ряде случаев обвиняемые не отрицали намерение выехать на территорию зоны влияния боевиков, указывая, что они ехали туда для оказания помощи жителям страны, страдающим от войны. Однако такая версия подсудимых была опровергнута совокупностью доказательств, свидетельствующих о приверженности обвиняемых радикально-экстремистским взглядам, поддержании ими террористической идеологии и подготовке к участию в силовых акциях боевиков.

Нередко в ходе судебного заседания подсудимые высказывают версию о том, что якобы сами намеревались сообщить в правоохранительные органы о подготовке к выезду в другие государства для последующего вступления в НВФ и МТО и добровольно прекратили преступные действия, в связи с чем заявляли ходатайства о прекращении уголовного преследования и об освобождении их от уголовной ответственности на основании примечаний к ст. 208 и 205.5 УК РФ.

В целях опровержения таких доводов необходимо тщательно документировать процедуру задержания подозреваемых с указанием всех обстоятельств. При задержании лиц в аэропорту целесообразно проводить допрос сотрудников пограничной службы и органов внутренних дел на транспорте и иных свидетелей, при этом особое внимание следует уделить поведению подозреваемого перед вылетом и при нахождении в здании аэропорта [4, с. 170-172].

Следует отметить, что в последние годы проводимая правоохранительными органами работа позволила на ранних этапах выявлять и устанавливать факты приготовления граждан России к выезду для осуществления террористической деятельности на территории иностранных государств.

Таким образом, применение изложенных нами рекомендаций существенно повлияет на своевременное раскрытие, расследование и доказывания приготовления к участию в незаконных вооруженных формированиях и международных террористических организациях за пределами Российской Федерации.

Список литературы

1. Дело № 1-189/2018. Архив Северо-Кавказского окружного военного суда за 2018 год.
2. Дело № 1-78/2019. Архив Северо-Кавказского окружного военного суда за 2019 год.
3. Меркурьев В.В., Агапов П.В. Уголовная политика в сфере противодействия преступлениям, связанным с участием российских граждан в незаконных вооруженных формированиях на территориях иностранных государств // Вестник Нижегородской академии МВД России. 2016. № 4 (36). С. 292-295.
4. Цахуев А.В. Вопросы квалификации преступлений, связанных с участием граждан Российской Федерации в незаконных вооруженных формированиях и международных террористических организациях на территории иностранного государства // Закон и право. 2020. № 6. С. 170-172.
5. Цахуев А.В. Типичные следственные ситуации первоначального этапа расследования участия граждан Российской Федерации в незаконных вооруженных формированиях на территории иностранного государства // Российский следователь. 2019. № 8. С. 7-10.

А.В. Ширяев, *аспирант кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*

КЛАССИФИКАЦИЯ СЛЕДОВ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Следы преступления традиционно принято разделять на материальные и идеальные. В частности, еще в 1977 г. Р.С. Белкин писал, что под следами преступлений понимаются остаточные явления в виде материально-фиксированных отображений одного объекта на другом, а равно и идеальные, мысленные образы, зафиксированные в памяти человека [1]. Несмотря на то, что компьютерные технологии во время издания указанной работы уже существовали, криминалисты не оперировали понятием «виртуальный след».

Постепенно развитие компьютерных технологий привело к пониманию необходимости выделения новых следов преступных деяний — виртуальных следов. В.А. Мещеряков пишет, что виртуальный след представляет собой любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации. Данные следы занимают условно промежуточную позицию между материальными и идеальными следами.

По мнению указанного автора, с одной стороны, «виртуальные следы» можно относить к материальным, поскольку они существуют реально на материальном носителе, их обнаружение и изъятие возможно только с применением программно-технических средств и непосредственно восприниматься не могут. Однако включать данные следы в состав материальных следов нецелесообразно, так как они зависят от способа считывания, не имеют неразрывной связи с устройством, с помощью которого осуществлялась запись информации, и являются неустойчивыми, что сближает их с идеальными следами. Следует указать, что отнесение виртуальных следов к идеальным было бы ошибочным, поскольку они хранятся не в памяти человека, а на материальных объектах [2].

Ряд авторов, например, Е.Р. Россинская, полагают, что виртуальные следы преступления — это разновидность материальных следов. «Виртуальные следы являются исключительно материальными следами, так как были зафиксированы на материальных носителях путем изменения свойств или состояния отдельных их элементов и отмечает, что данный вид информации не отделим от материального носителя, поэтому к материалам дела приобщается именно носитель» [3].

Анализ материалов уголовных дел, возбужденных по признакам преступлений, предусмотренных ст. 159.6 УК РФ, а также главой 28 УК РФ (в данном случае с учетом специфики следовой картины данные преступления можно рассматривать в совокупности), позволил сделать вывод о том, что во всех уголовных делах в качестве вещественных доказательств осмотрены и приобщены к материалам дела материальные носители (флеш-накопители, компакт-диски), содержащие виртуальные следы преступлений. Однако здесь не следует путать «след преступления» и «вещественное доказательство».

По сути, второе как раз и является средой отображения (хранения) первого. Это справедливо в отношении как материальных следов преступления, так и виртуальных. Например, точно также к материалам уголовного дела приобщается гипсовый слепок следа обуви, и именно слепок выступает вещественным доказательством, хотя по сути первоначальным следом преступления является именно отпечаток подошвы обуви (на грунте, в снегу и т.д.).

Здесь по сути материальный след зафиксирован посредством материального объекта, в случае же виртуальных следов на материальном объекте фиксируются именно виртуальные следы, и общность способа фиксации и приобщения к материалам уголовного дела еще не говорит о том, что виртуальный след — это разновидность материальных следов. В любом случае в обвинительных заключениях, приводя список доказательств, подтверждающих вину обвиняемого, следователи указывают не материальный носитель, а приводят описание именно виртуального следа как информационного объекта.

Очевидно, что виртуальные следы не могут существовать обособленно от материального носителя, вместе с тем их специфика заключается в том, что такие следы могут быть без ущерба для их сущности и содержания перемещены на иной носитель, отличный от того, на котором они отобразились изначально. Например, какая-либо информация с сервера банковской организации, содержащая следы несанкционированного доступа из внешней киберсреды, может быть скопирована на иной носитель (флеш-накопитель, компакт-диск и т.д.) и в таком виде представлена на экспертное исследование, а в дальнейшем приобщена к материалам уголовного дела. При этом по сути такой материальный носитель будет выступать лишь хранилищем виртуального следа, но никак не средой его возникновения (отображения).

Иными словами, сам факт того, что виртуальные следы исследуются и хранятся, будучи размещенными на материальном носителе, еще не говорит о том, что такие следы в целом носят материальный характер. В.В. Поляков пишет, что «характерное для типичных следов их подразделение в зависимости от механизма следообразования для виртуальных следов также не актуально, так как нет характерных традиционных следов от удара, нажима, разреза и пр. Очевидно, что эти следы не обладают физическими и химическими характеристиками (массой, цветом, геометрической формой, запахом и т.д.)» [4]. Иными словами, виртуальным следам не присущи свойства и характеристики материальной вещи, в связи с чем их отнесение к материальным следам в качестве одной из их разновидности представляется ошибочным.

Иными словами, здесь поднимается проблема самостоятельности виртуальных следов как обособленного вида следов преступлений. Такие следы имеют общие черты с материальными, хотя бы потому, что в любом случае киберпространство в конечном итоге основано на материальных носителях. Информационно-телекоммуникационная сеть Интернет, несмотря на ее внешнюю «неосязаемость», обеспечивается непрерывной работой дата-центров, которые представляют собой материальные объекты, обеспечивающие существование информации. И в конечном итоге любое действие пользователя находит свое отражение на материальном носителе.

Однако со всей очевидностью между, например, следом орудия взлома на определенном элементе входной двери, гаражных ворот, оконного проема и следом операции в сети Интернет или на компьютерном устройстве, существующем на материальном носителе (хранилище информации в дата-центре, жесткий диск компьютера и т.д.), существуют различия. Первые в любом случае представляют собой овеществленный объект, который, как правило, доступен для непосредственного наблюдения, вторые же, несмотря на определенную связь с материальными носителями, не имеют овеществленного характера и, по сути, представляют собой часть информационной среды, для непосредственного наблюдения недоступной.

Следовательно, несмотря на определенное сходство с точки зрения наличия материального носителя, материальные и виртуальные следы представляют собой обособленные и самостоятельные виды криминалистических следов.

Как раз неовеществленный характер роднит виртуальные следы преступления с идеальными, т.е. следами, отобразившимися в сознании человека. По сути, и визуальный образ внешности преступника, сохранившийся в сознании потерпевшего, и данные о том, что в ту или иную компьютерную сеть было совершено несанкционированное проникновение из внешней киберсреды, представляют собой информацию, которая, как уже отмечалось выше, не овеществлена.

Однако отличие идеальных следов от виртуальных заключается, во-первых, объектом их «хранения», во-вторых, способами извлечения. Если идеальные следы извлекаются в рамках следственных действий вербального характера (допрос), то для извлечения виртуальных следов необходимы определенные специальные операции с материальными носителями таких следов. Следовательно, идеальные и виртуальные следы преступлений, несмотря на определенные общие черты, также представляют собой обособленные виды следов. Таким образом, виртуальные следы преступления представляют собой обособленный вид следов преступных деяний, наряду с материальными и идеальными следами.

В.Б. Вехов пишет, что термин «виртуальный» происходит от латинского virtualis, что означает «не имеющий физического воплощения или воспринимаемый иначе, чем реализован в действительности» [5]. Иными словами, основополагающая сущностная характеристика виртуального следа — это его невещественность, хотя, безусловно, такой след имеет связь с материальными объектами, поскольку они выступают его носителями. Но сами по себе носители «следом преступления» не являются, представляя собой лишь среду существования и хранения данного следа.

Безусловно, что именно виртуальные следы обусловливают проблематику следовой картины кибермошенничества. Для работы с ними следователю со всей очевидностью необходимы специальные навыки, позволяющие отыскать такие следы, изъять их и обеспечить сохранность. Поскольку именно виртуальные следы играют первостепенное доказательственное значение при расследовании кибермошенничества, их утрата может существенно осложнить или вовсе сделать невозможным доказывание вины обвиняемого.

Вместе с тем при расследовании кибермошенничества не следует игнорировать и иные виды следов — идеальные и материальные. В этом заключается существенное отличие мошенничества в сфере компьютерной информации от преступлений в сфере компьютерной информации (глава 28 УК РФ). Если в последнем случае виртуальные следы, как правило, занимают собой практически все «доказательственное пространство», то при кибермошенничествах не менее важную роль играют идеальные и материальные следы преступления. Даже само по себе то, что мошенничество в сфере компьютерной информации отнесено законодателем к так называемым «общеуголовным» преступлениям, указывает на то, что отождествлять данное преступление с виртуальной средой и предлагать отыскивать следы преступления исключительно в ней было бы ошибочным.

Под идеальными следами преступления понимают отображение события или его элементов в сознании человека, мысленный образ воспринятого. Характер идеальных следов и их сохранность во многом зависят от состояния органов чувств лица, воспринявшего эти следы,

его памяти, уровня интеллекта и т.д. Поэтому такие следы носят в значительной мере субъективный характер. Идеальные следы на сегодняшний день играют вспомогательную роль, а именно они служат орудием для обнаружения материальных следов [6].

Если в целом с приведенным определением можно согласиться, то суждение о том, что идеальные следы играют вспомогательную роль, выступая средством обнаружения материальных следов, представляется ошибочным. Действительно, материальные следы преступления, представляющие собой результаты материального отражения свойств взаимодействующих в ходе преступной деятельности материальных объектов, исследование которых позволяет формировать доказательственную информацию об отдельных обстоятельствах совершенного преступления [7], с точки зрения доказательственного значения носят более объективный характер, поскольку не деформированы субъективными элементами, связанными с состоянием органов чувств и памяти лица, сознание которого отобразило идеальные следы.

С этой позиции материальный след, безусловно, «предпочтительнее» идеального, однако не совсем верно говорить о том, что идеальный след — это всего лишь этап на пути отыскания материальных следов. Идеальные и материальные следы — это обособленные элементы следовой картины преступления, безусловно, в конечном итоге идеальный след преступления может способствовать отысканию материального (как, впрочем, и наоборот), но и в целом это совершенно самостоятельные элементы, каждый из которых имеет свое особое значение. При этом, как уже отмечалось выше, первоочередное значение при расследовании кибермошенничества имеют виртуальные следы.

Так, в производстве СЧ СУ при УМВД России по г. Барнаулу находилось уголовное дело в отношении Д., в рамках расследования которого установлено, что Д., действуя умышленно, незаконно, из корыстных побуждений, с целью личного незаконного обогащения и обращения чужого имущества в свою пользу, путем ввода, модификации компьютерной информации и вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации, будучи осведомленным о порядке и правилах доступа к автоматизированной услуге «мобильный банк» ПАО «Сбербанк» и возможности перевода с ее помощью денежных средств без использования банковской карты владельца счета, используя имеющуюся в его распоряжении сим-карту оператора сотовой связи ПАО «Мегафон» отправил компьютерную информацию в форме электронного текстового «СМС-сообщения» на абонентский номер, используемый ранее незнакомым ему М. следующего содержания: «ваша банковская карта заблокирована». Тем самым сообщил М. заведомо ложные сведения о блокировании его банковских карт, привязанных к лицевым счетам, открытым на его имя и обслуживаемым в ПАО «Сбербанк».

Далее М., будучи введенным в заблуждение сообщением, поступившим на его абонентский номер и содержащим заведомо ложные сведения о блокировании его банковской карты, перезвонил на указанный абонентский номер, используемый Д., который принял входящий звонок от потерпевшего и, представившись сотрудником ПАО «Сбербанк», при этом таковым в действительности не являясь, действуя из корыстных побуждений, в ходе разговора ввел М. в заблуждение относительно необходимости взятия на контроль сотрудниками ПАО «Сбербанк» клиентов указанного банка, у которых на расчетных счетах имеется сумма, превышающая 500000,0 рублей, при этом выяснив у М. номер его банковской карты и кодовое слово, указанное в договоре при оформлении банковского лицевого счета.

Продолжая свои преступные действия в рамках единого умысла, Д. в течение определенного периода времени, используя мобильный телефон, имеющий доступ в сеть Интернет, произвел действия по вводу, модификации компьютерной информации и вмешательству в функционирование средств хранения, обработки и передачи компьютерной информации, введя сообщенные М. данные на интернет-сайте «Сбербанк Онлайн», получил прямой доступ к распоряжению денежными средствами, находящимися на лицевом счете М., похитил указанные денежные средства за несколько тождественных операций [8].

В данном случае присутствуют все виды следов — виртуальные (следы ввода и модификации компьютерной информации и вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации), идеальные (показания потерпевшего относительно обстоятельств совершенного преступления) и материальные (в частности, у Д. был изъят мобильный телефон, посредством которого он осуществлял доступ в сеть Интернет, на корпусе телефона обнаружены следы пальцев рук Д.). И каждый из видов таких следов играл самостоятельную доказательственную роль, дополняя друг друга, а не являясь «прикладным способом» в цепочке отыскания, например, материальных следов.

Все указанные виды следов, безусловно, дополняют друг друга — например, совершенно недостаточно доказать факт ввода и модификации компьютерной информации и вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации — требуется также увязать данные действия непосредственно с Д., чему способствовало отыскание материальных следов (следов пальцев рук) на устройстве (мобильном телефоне), посредством которого был осуществлен доступ в сеть Интернет.

Вышеизложенное позволяет сделать определенные выводы. Традиционное деление следов преступления на материальные и идеальные претерпело существенные изменения в свете стремительного развития сферы компьютерной преступности, и в настоящее время следует выделять третий вид — виртуальные следы.

Несмотря на то, что такие следы имеют определенные сходные черты с материальными и идеальными, было бы ошибочным отказывать им в самостоятельности. Виртуальные следы, представляющие собой любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации, выступают обособленным видом криминалистических следов, выявление, исследование и обеспечение сохранности которых требует от следователя особых навыков. Безусловно, именно виртуальные следы играют важнейшую роль при расследовании кибермошенничества, однако в силу того, что данное преступление сочетает в себе действия в киберпространстве и физической среде, а так же взаимодействие (общение) обвиняемого и потерпевшего, виртуальные следы здесь должны дополняться материальными и идеальными.

Список литературы

1. Белкин Р.С. Курс советской криминалистики. М., 1977. С. 65.
2. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. … докт. юрид. наук. Воронеж, 2001. С. 15.
3. Россинская Е.Р. Криминалистическое исследование компьютерных средств и систем как новый раздел криминалистической техники // Байкальский исследовательский журнал. 2017. № 4. С. 102.
4. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дисс. ... канд. юрид. наук. Барнаул, 2008. С. 70.
5. Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: автореф. дисс. ... докт. юрид. наук. Волгоград, 2008. С. 11.
6. Алиев М.Б. Идеальные следы в криминалистике и их значение в расследовании преступлений // Закон и право. 2020. № 1. С. 16.
7. Мороз А.В. Понятие «материальные следы преступления» // Общество и право. 2016. № 2. С. 108.
8. Материалы уголовного дела № 125004-22/19 в отношении Д. по ч. 2 ст. 159.6 УК РФ // СЧ СУ при УМВД России по г. Барнаулу. 2019 год.

В.В. Шишов, *к.ю.н., преподаватель кафедры уголовного процесса Московского университета МВД России им. В.Я. Кикотя, г. Москва*

О НЕОБХОДИМОСТИ СОВЕРШЕНСТВОВАНИЯ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ УДАЛЕННОЙ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ СОТРУДНИКАМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Современный мир стремительно развивается за счет внедрения во многие сферы жизнедеятельности современных компьютерных технологий, направленных на упрощение доступа к информации, управлению ресурсами.

В настоящее время постепенно внедряются технологии удаленной биометрической идентификации, основу которой представляют биометрические персональные данные, предусмотренные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Стоит отметить, что удаленная биометрическая идентификация строится преимущественно на принципах добровольности предоставления биометрических персональных данных.

Федеральным законом от 31 декабря 2017 г. № 482-ФЗ внесены изменения в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в том числе в части введения механизма удаленной биометрической идентификации клиента кредитной организации, который разработан Банком России в рамках реализации программы развития технологий финансовых услуг. Таким образом, развитие финансовых технологий с использованием инструментов удаленной идентификации и аутентификации позволит клиентам обращаться в финансовые учреждения, даже не предоставляя документы, удостоверяющие личность. Система видеонаблюдения распознает их и позволит оказать услугу.

Постановлением Правительства РФ от 30 июня 2018 г. № 772 определен состав сведений, размещаемых в единой информационной системе персональных данных: биометрические персональные данные физического лица — гражданина РФ: данные изображения лица, данные голоса; идентификатор сведений в соответствующем регистре Единой системы идентификации и аутентификации (далее — ЕСИА); идентификатор сведений об уполномоченном сотруднике уполномоченной организации в регистре органов и организаций ЕСИА, идентификатор сведений о физическом лице в регистре физических лиц ЕСИА, биометрические персональные данные которого размещаются в единой биометрической системе; контактные данные физического лица (номер абонентского устройства подвижной радиотелефонной связи, электронной почты).

Распоряжением Правительства РФ от 22 февраля 2018 г. № 293-р. Оператором единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (далее — Оператор единой информационной системы персональных данных), определено ПАО «Ростелеком».

Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ от 25 июня 2018 г. № 321 определен порядок обработки этих данных.

Порядок взаимодействия правоохранительных органов с Оператор единой информационной системы персональных данных определен Постановлением Правительства РФ от 28 декабря 2018 г. № 1703. Для этого сотрудникам правоохранительных органов необходимо обратиться в ПАО «Ростелеком» с запросом, например, о получении данных изображения лица конкретного человека, а оператор направляет данные изображения, полученные в результате поиска в единой биометрической системе, которые относятся к направляемому в запросе изображению лица в соответствии с методикой определения степени схожести, утверждаемой Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации.

Инструменты удаленной идентификации показывают достаточную эффективность не только в сфере оказания финансовых услуг, но и в раскрытии преступлений, задержании лиц их совершивших. Так, несмотря на использование такой идентификации в тестовом режиме, установленных только в метрополитенах и в отдельных районах крупных городов, ежемесячно удается задержать от 5 до 10 преступников [1].

Конечно, указанные цифры могут показаться незначительными, поскольку в 2019 г. только судами приостановлено 7611 уголовных дел в связи с розыском подсудимых [2]. Сравнительно небольшое количество установленных лиц вызвано несовершенством систем распознавания лиц.

Стоит отметить, что успешному раскрытию и расследованию преступлений способствует и дактилоскопирование участников уголовного судопроизводства. В соответствии с Федеральным законом от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» обязательной дактилоскопической регистрации подлежат подозреваемые в совершении преступления, обвиняемые в совершении преступления, осужденные за совершение преступления, подвергнутые административному аресту. Получение иных биометрических персональных данных осуществляется крайне редко, при этом отсутствует общая система для их внесения и обработки. Например, в соответствии с Федеральным законом от 07 февраля 2011 г. № 3-ФЗ «О полиции» предусмотрено право сотрудников полиции производить фотографирование, аудио-, видеосъемку лиц, задержанных по подозрению в совершении преступления, заключенных под стражу, обвиняемых в совершении преступления, подвергнутых административному наказанию в виде административного ареста, иных задержанных, если в течение установленного срока задержания достоверно установить их личность не представилось возможным. Согласно Приказу МВД России от 31 декабря 2015 г. № 1266, осуществляется фотографирование подозреваемых и обвиняемых, содержащихся в изоляторах временного содержания.

Введение для подозреваемых, обвиняемых, осужденных, лиц, подвергнутых административному аресту, обязанности предоставления биометрических персональных данных — изображения лица в значительной степени повысит эффективность установления и проверки на причастность к совершенному преступлению лиц, ранее привлекаемых к уголовной ответственности, дисциплинирует лиц, содержащихся под домашним арестом либо в отношении которых избрана мера пресечения в виде запрета определенных действий, позволит упростить процедуру идентификации лица в случае предоставления им заведомо ложных анкетных данных при задержании.

Перспективным представляется и введение обязанности предоставления биометрических персональных данных несовершеннолетними, склонными к систематическому самовольному уходу из дома, лицами, имеющими психические отклонения и склонными к бродяжничеству, иностранным гражданам, прибывающим на территорию Российской Федерации.

Технологии удаленной идентификации применяются и в зарубежных странах. Например, в Великобритании используется технология идентификации для определения возраста лица, которому осуществляется продажа алкогольной продукции, в США эти же технологии применяются для ограничения допуска лиц на территорию школ и детских лагерей, популярные социальные сети и смартфоны внедряют технологии распознавания для разблокировки доступа к отдельным приложениям. Для оперативной проверки задержанных лиц сотрудники полиции Лондона оснащены смартфонами с установленными приложениями по идентификации личности [3]. Внедряются и системы аутентификации по уникальному рисунку кровеносных сосудов глазного дна посредством сканирования инфракрасным излучением через зрачок к задней стенке глаза, которые уже используются в аэропортах Объединенных Арабских Эмиратов.

Таким образом, внедрение технологии удаленной идентификации личности, несмотря на высокую стоимость, оправдана, прежде всего, оперативностью решения задач по обеспечению безопасности, однако требует дальнейшего нормативного регулирования. Представляется

целесообразным наделение органов внутренних дел полномочиями Оператора единой информационной системы персональных данных, а также в установлении обязанности для подозреваемых, обвиняемых, осужденных, лиц, подвергнутых административному аресту, обязанности предоставления биометрических персональных данных — изображения лица. Непосредственными исполнителями сбора персональных биометрических данных могут стать эксперты-криминалисты, обладающие навыками составления фотокомпозиционных портретов. Положительный опыт использования технологии удаленной идентификации и аутентификации правоохранительными органами зарубежных государств позволяет сделать вывод о необходимости оснащения сотрудников правоохранительных органов специальными смартфонами с установленными специальными приложениями по проверке задержанных лиц.

Список литературы

1. МВД подвело итоги тестовой работы систем распознавания лиц в Москве // Газета «Ведомости». URL: https://www.vedomosti.ru/technology/articles/2019/06/26/805163-mvd-podvelo (дата обращения: 20.06.2020 г.).

2. Отчет о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции за 12 месяцев 2019 г. URL: http://www.cdep.ru/index.php?id=79&item=5258 (дата обращения: 20.06.2020).

3. Западные страны начинают применять технологии распознавания лиц. URL: https://www.vedomosti.ru/technology/articles/2019/08/02/807944-tehnologiyu-raspoznavaniya-lits (дата обращения: 20.06.2020 г.).

Е.Н. Яковец, *д.ю.н., заслуженный юрист РФ, в/ч 2462, ведущий научный сотрудник, г. Москва*

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ГОСУДАРСТВЕННОЙ ГРАНИЦЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Из открытых источников можно получить сведения относительно геоинформационной системы (ГИС) «Граница», разработанной АО Конструкторское бюро «Панорама» — ведущей российской компанией в области создания геоинформационных систем и технологий. Целью создания указанной ГИС является оперативный мониторинг обстановки и принятия обоснованных и своевременных решений по охране Государственной границы Российской Федерации. К числу ее основных аналитических задач относятся:

– сбор, обработка, хранение, оценка и отображение в 3D-режиме пространственной информации вокруг интересующих пограничные органы объектов;

– получение, обработка и визуализация событий и происшествий, сведения о которых поступают из следующих источников: от информационных систем по управлению техническими средствами наблюдения и контроля периметров объектов; от переносных средств наблюдения; от беспилотных летательных аппаратов; от вспомогательных сил;

– формирование и визуализация маршрутов движения пограничных нарядов;

– мониторинг движения собственных транспортных средств, а также автотранспорта нарушителей, контроль их скорости, мест и времени стоянок, отклонения от заданных маршрутов;

– получение, обработка и визуализация сведений о возможных маршрутах перемещения нарушителей госграницы и предполагаемых преступников, визуализация этих данных с учетом особенностей местности;

– подготовка информации для оптимального размещения застав, вышек, иных объектов пограничной инфраструктуры;

– построение зон огневого поражения из выбранных точек;

– расчет позиций средств оптической и радиолокационной разведки зоны доступности радиосигнала на уровне 10 м от земли и др.;

– формирование отчетов, справок, сводок.

Для реализации этих задач ГИС «Граница» включает в свой состав следующие необходимые элементы:

– ситуационный центр для общего управления всей системой охраны государственной границы, оперативного мониторинга обстановки на границе и приграничной полосе во всей стране и принятия обоснованных и своевременных решений в случае руководства операциями по слежению, разработке и задержанию нарушителей, преступников;

– банк пространственных данных для сбора, хранения и выдачи пользователям пространственной информации;

– интернет-портал для предоставления доступа к ГИС «Граница» через Интернет;

– ГИС-заставы для управления системой охраны государственной границы на отведенном участке пограничного отделения, оперативного мониторинга обстановки на границе и в приграничной полосе — в зоне ответственности заставы, а также принятия обоснованных и своевременных решений при управлении операциями по слежению, разработке и задержанию нарушителей, и предполагаемых преступников [1].

Для решения поставленных задач ГИС «Граница» выполняет следующие функции:

– использование, отображение и преобразование пространственных данных различных проекций о выбранном объекте;

– построение и автоматическая загрузка карты 3D-модели участка местности (двухмерная карта с теневым отображением матрицы высот рельефа), отображение ее оптимальной детализации при изменении соответствующего масштаба;

– применение технологии «атлас-работа» с набором перекрывающих друг друга топографических карт на один и тот же район, с различным масштабом и уровнем детализации;

– использование пространственных данных с геопорталов и других источников;

– ведение банка данных цифровых карт (материалы космической и воздушной съемки местности, включая данные с беспилотных летательных аппаратов (БПЛА), данные оптической, мультиспектральной, радиолокационной и лазерной съемки местности).

Геоинформационной системой более высокого уровня представляется ГИС «Интегра 4D-Планета Земля». Сведений об этой системе в открытом доступе немного. Можно лишь сделать вывод о том, что это единственная в мире система, в которой все объекты, датчики, устройства и даже видеоизображения привязаны к географическим координатам и времени. Здесь реализовано 4D-моделирование, позволяющее еще более точно воспроизводить объективную реальность. Данная система была продемонстрирована президентом консорциума «Интегра-С» В.А. Куделькиным на Международном военно-техническом форуме «Армия-2018», проходившем с 21 по 26 августа 2018 г., в рамках доклада на тему «Современное состояние, перспективы разработки, создания и сопровождения высокотехнологичных пограничных комплексов и систем в интересах пограничных органов федеральной службы безопасности» [2].

Безусловно, эти и другие геоинформационные системы должны активно внедряться в деятельность пограничных органов (ГИС ПО). Вместе с тем подобные ГИС — это всего лишь дополнительный инструментарий для аналитической обработки информации, который помогает визуализировать криминальные события и выявлять лиц, к ним причастных, на Государственной границе РФ, в пограничной зоне и в пунктах пропуска через Государственную границу РФ. Однако использование подобных систем автономно от других средств получения аналитически значимой информации, как показывает практика, эффективно в меньшей степени.

Решение даже тех аналитических задач, которые перечислены выше, не всегда возможно без использования иных средств проведения криминального анализа.

Основным элементом ситуационного центра, связанного с анализом оперативной обстановки на приграничной территории, призвана стать автоматизированная логико-аналитическая система (АЛАС), которая позволяют интегрировать и обрабатывать «большие данные», интересующие пограничные органы, с помощью искусственного интеллекта (ИИ). К этим «большим данным», в частности, относятся и те сведения, которые могут быть получены и визуализированы с помощью ГИС ПО.

В нашей стране, к сожалению, правоохранительная система в своих ответных действиях на технологизацию криминального мира явно запаздывает. Большинство российских специалистов начали активно обсуждать проблемы применения ИИ лишь около трех лет назад, хотя автор данной статьи вместе со своими единомышленниками активно обсуждали необходимость его внедрения в оперативно-служебную деятельность правоохранительных органов более 15 лет назад. Уже тогда среди узкого круга специалистов решались проблемы интеграции геоинформационных систем с АЛАС [3, 4].

Для эффективного решения задач по контролю за оперативной обстановкой на приграничной территории в АЛАС помимо потоковой информации необходима также обработка телефонных биллингов, получаемых в режиме реального времени при осуществлении радиолокационной разведки. Это позволяет оперативно выявлять лиц из числа злоумышленников, использующих беспроводные средства связи для установления взаимодействия со своими соучастниками, и устанавливать их местонахождение с помощью геолокации.

Кроме этого, для выявления, предупреждения и раскрытия преступлений, совершаемых на приграничной территории, весьма важным является использование зарекомендовавшего себя с положительной стороны автоматизированного банка данных (БД) «Записная книжка», позволяющего эффективно выявлять связи абонентов в криминальной среде на основе анализа их телефонных номеров [5].

Однако телефонные номера абонентов, представляющих оперативный интерес, — это лишь один из видов учетно-регистрационной информации, которой должны располагать пограничные органы. Она должна систематически накапливаться в оперативно-розыскном учете пограничных органов в ходе регистрации криминогенно активных лиц, имеющих притяжение к приграничной территории. Основу этого учета должны составлять биометрические персональные данные физических лиц (результаты опознавательной фотографии, дактокарты, словесные портреты, по возможности, — образцы почерка и ДНК-коды), имеющих отношение к совершению правонарушений в пограничной сфере, а также характеризующие последних дополнительные сведения фактографического характера (сводки, сообщения, справки и др.).

С учетом всего сказанного можно представить следующую модель аналитической обработки оперативно значимой информации. Получаемая с помощью ГИС ПО визуальная информация, поступающая от информационных систем по управлению техническими средствами наблюдения и контроля периметров объектов, переносных средств наблюдения, БПЛА и из других источников в режиме реального времени, с привязкой к координатам и рельефу конкретного участка местности поступает в АЛАС.

В том случае, если речь идет о пресечении пограничного правонарушения либо о преследовании нарушителя Государственной границы РФ, одновременно должны задействоваться возможности по установлению абонентов номеров телефонов и других средств связи, выходивших в эфир в изучаемом районе с геопривязкой этих абонентов к соответствующей территории.

Задействование в рамках АЛАС БД «Записная книжка» способствует установлению на основании телефонных биллингов конкретных абонентов, выходящих на связь в пределах приграничной территории, и получение на них необходимых биометрических данных из оперативно-розыскного учета. Эти данные могут быть использованы в ходе идентификации фигурантов после их задержания.

Кроме этого, при интеграции с АЛАС современных идентификационно-диагностических систем появляется возможность выявления потенциальных правонарушителей (т.е. выделения их из общего потока законопослушных граждан, следующих через пункты пропуска) и отождествления их личности в дистанционном режиме реального времени с привязкой к конкретным координатам местности.

В настоящее время к идентификационным системам подобного рода предъявляется ряд повышенных требований. Они должны обеспечивать отождествление личности, как в режиме стационарного опознания объекта, так и в процессе его перемещения в пространстве. Подобные системы позволяют реализовывать следующие возможности:

– предъявление фотографий последовательно в четырёх ракурсах (первый снимок — анфас, второй снимок — правый профиль, третий снимок — ¾ анфас слева, на четвертом — лицо должно быть изображено в полный рост: это необходимо для отображения максимального количества идентификационных признаков физического лица);

– ввод в систему наряду с фотографиями наиболее пригодных для идентификации видеофайлов, в том числе — получаемых с камер видеонаблюдения;

– работу с объектами, относящимися к различным типажам (европейцы, кавказцы, азиаты и т.д.);

– предварительный поиск фигурантов по признакам словесного и субъективного портрета, особым приметам или полям регистрационных данных;

– учет варьирования возрастного интервала объектов отождествления в пределах 15-20 лет;

– учет отклонения изображения лица по вертикальной и горизонтальной оси не менее чем на 12–14°;

– программную оптимизацию качества исходного фотоматериала;

– устойчивость системы к появлению дополнительных атрибутов внешности объекта (очки, усы, борода и т.д.);

– автоматическую оцифровку изображений.

Таким образом, в случае интеграции с АЛАС ГИС ПО приобретает роль одного из основных функциональных элементов последней, связанных не только с получением визуальной оперативно значимой информации, но и ее анализом на основе оперативного распознания и идентификации криминогенно активных лиц.

В этом случае в качестве ситуационного центра (СЦ), «предназначенного для общего управления всей системой охраны государственной границы, оперативного мониторинга обстановки на границе и приграничной полосе на всем ее протяжении и принятия обоснованных и своевременных решений в случае руководства операциями по слежению, разработке и задержанию нарушителей, преступников», о котором говорилось в начале данной статьи в контексте разработки ГИС «Граница», логичнее рассматривать СЦ, основанный на АЛАС.

В заключение хотелось бы порассуждать о наиболее совершенной модели СЦ, позволяющей поднять работу пограничных органов на новый организационный уровень, которая позволит не только консолидировать всю представляющую интерес информацию, но и обрабатывать ее в любом режиме, включая режим реального времени. Новые подходы к автоматизации работы пограничных органов в данном случае базируются на разработанной системе корреляционных связей различных объектов анализа, в первую очередь — отдельных элементов оперативно-розыскной характеристики преступлений. С помощью подобных методик возможно осуществление многомерного анализа данных для обеспечения поддержки принятия различного рода оперативно-тактических решений в сфере пограничной деятельности.

Подобный СЦ может представлять собой многоуровневый комплекс, обеспечивающий сбор, обработку и хранение учетно-регистрационной информации на естественном языке. В особой мере это актуально в тех случаях, когда приходится интегрировать сведения,

получаемые из внешних источников, которые насыщены различной нестандартной терминологией. Безусловно, в этом комплексе предусмотрено место и для геоинформационных систем. К данным СЦ предъявляется ряд специфических требований, в частности:

1) для обеспечения функционирования системы в целом:

– каждый объект или отдельно взятый его признак должны быть одинаково доступны для исследования в ходе использования любых форм и видов анализа;

– необходимо обеспечивать совместимость признаков всех изучаемых объектов;

– должен осуществляться выбор наиболее оптимальных (рациональных) цепочек связей между объектами, однако, «лишние» и «нерациональные» взаимосвязи также должны отображаться в процессе визуализации результатов анализа;

– следует обеспечивать целенаправленное получение дополнительной информации о самих объектах и окраске их связей;

2) для визуализации результатов анализа:

– необходимо располагать возможностью просмотра исходного документа, явившегося источником той или иной информации, без выхода из заданного режима;

– предпочтение должно отдаваться наглядному отображению результатов анализа в виде соответствующих графов, позволяющих фиксировать различные признаки объектов и характер связей между ними;

– в информационной системе следует предусмотреть средства навигации по графу связей (либо иному другому средству визуализации результатов анализа);

– необходимо обеспечить возможность представления результатов анализа не только в виде графов, но и в виде таблиц, матриц, графиков, текстовых описаний, а также в виде геоинформационных изображений;

3) для сохранения и выдачи результатов аналитического поиска:

– его результаты должны фиксироваться в таком виде, чтобы при необходимости в любой момент их можно было бы востребовать и оценить;

– необходимо иметь генератор отчетов, обеспечивающий выдачу стандартных отчетных форм с учетом возможности их корректировки в соответствии с предъявляемыми требованиями;

– сведения обо всех выявляемых в ходе анализа объектах, их признаках и связях следует заносить в соответствующую базу знаний.

Подобным образом наиболее эффективно может быть решена проблема информационного взаимодействия различных подразделений пограничных органов. Используемые современные телекоммуникационные технологии, позволяющие объединять различные банки данных в единый комплекс на базе общего информационного пространства, дают возможность комплексного изучения информации как «внутреннего», так и «внешнего» свойства. Это крайне важно для диагностического анализа преступлений «по горячим следам», контроля в режиме реального времени за состоянием оперативной обстановки и ее прогнозирования, определения криминогенной активности корпоративных объектов и отдельных лиц, отождествления личности и т.д.

Используемое для достижения указанных целей функциональное ядро АЛАС позволяет сотруднику, осуществляющему анализ, избавиться от переизбытка неструктурированной информации, которую при обычных условиях он не в состоянии эффективно применять. Система в автоматическом режиме может производить смысловой разбор и классификацию входящего потока информации, устанавливая обстоятельства, объективно присущие любому факту, событию или явлению.

Внешняя информация, как известно, может иметь дефинитивный (точно установленный) и латентный (неявный) характер. В последнем случае предполагается получение уточняющих

сведений через дополнительные источники информации (включая криминалистические, криминологические и административные учеты).

Для обеспечения связи программных компонентов распределенной информационной системы между собой средства электронно-вычислительной техники, отвечающие за их функционирование, объединены в единую сеть.

В алгоритмическую составляющую системы вводятся необходимые терминология и понятия, структурированные по уровням общности и по семантическим взаимосвязям, которые формируют смысловое пространство системы и отражают представление о содержании анализируемых объектов. На начальном этапе внедрения системы эти представления являются априорными. Однако на базе результатов анализа по мере накопления определенных объемов информации система формирует об этих объектах более определенные представления. В ходе функционирования АЛАС корректировка данных представлений должна обеспечиваться автоматически, без перерывов в ее эксплуатации. Вместе с тем при использовании системы в актуальном состоянии должно поддерживаться не только информационное отображение текущей ситуации в отслеживаемой области, но и результаты анализа прошлых событий. Это обеспечивает идущий в системе постоянно возобновляемый (циклический) процесс качественного преобразования исходных данных в знания, отражающие реальное содержание проблемы. Исходная информация выводится из оперативной памяти и архивируется, резко уменьшаясь в объеме, что позволяет решить одну из самых острых проблем для любой компьютерной системы — проблему содержания так называемого дорогостоящего «информационного кладбища».

Таким образом, данные, поступающие на вход системы, отслеживающей ту или иную ситуацию, анализируются, сопоставляются с уже имеющейся информацией, оцениваются и обобщаются на различных этапах обработки, а затем переходят в архив, оставляя после себя определенный след в виде знаний различной категории сложности. При необходимости архивные данные могут быть вновь востребованы для сравнительного и диагностического анализа в сочетании с новой информацией. Результаты обработки латентной и дефинитивной информации, дополняя и уточняя друг друга, позволяют добиться качественно нового результата при проведении анализа, в первую очередь, — за счет изучения правонарушений, сходных по фабуле совершения.

Наряду с этим СЦ должен включать в свой состав еще целый ряд элементов компьютерного компонента (так называемые функциональные компоненты):

1) дежурный компонент: первичная обработка исходной информации, оперативная реакция на требования информационной поддержки в нештатных ситуациях;

2) аналитический компонент: полный цикл обработки информации (сопоставление вновь поступивших сведений с уже имеющимися, их анализ, формирование выводов), создание табельных, отчетных и аналитических документов, формулирование требований по повышению уровня полноты и достоверности поступающей информации, а также по устранению возникающих противоречий.

Этот компонент должен предусматривать возможность подключения к АЛАС мощных автоматизированных систем, использующих для осуществления идентификации и диагностики массивы сведений, концентрирующихся в оперативно-розыскном и криминалистическом учетах (дактоучеты, банки геномной информации, образцы почерка, изображения, аудиозаписи, описания и др.);

3) обратная связь с источниками информации: оценка степени достоверности исходной поступающей информации; оценка инициаторами качества и оперативности исполнения заданий;

4) оперативное использование информации: ее анализ, формирование результатов анализа на выходе; конкретизация выводов требуемого уровня сложности;

5) администратор комплекса: выполнение всех текущих технологических операций, а также операций по настройке, модернизации и расширению системы.

Одной из важнейших проблем при создании АЛАС является формирование и поддержание в актуальном состоянии информационного отображения проблемы, то есть решение задачи, связанной с функционированием системы слежения, которая должна обеспечивать:

– постоянное (в реальном масштабе времени) поддержание достоверного, полного и непротиворечивого информационного отображения отслеживаемой проблемы;

– выявление событий, влияющих на изменение текущей ситуации;

– накопление знаний о причинах возникновения этих изменений и их последствиях;

– оперативное представление необходимой информации требуемого уровня детализации и полноты в удобной для восприятия форме с целью выработки обоснованных оперативно-тактических решений.

Таким образом, многопользовательская сетевая модель АЛАС, основанная на использовании ИИ, является наиболее перспективной для последующего создания на ее базе полномасштабной версии, обеспечивающей функционирование как отдельно взятого федерального органа исполнительной власти (в данном случае — пограничных органов), так и нескольких взаимодействующих между собой правоохранительных ведомств или спецслужб.

Список литературы

1. Геоинформационная система «Граница» // КБ Панорама. URL: https://gisinfo.ru/products/granica.htm (дата обращения: 24.04.2020).

2. Делегация консорциума «Интегра-С» приняла участие в Международном военно-техническом форуме «Армия-2018» // Консорциум «Интегра-С» — Цифровые интеллектуальные системы безопасности. URL: https://integra-s.com/news/delegatsiia-konsortsiuma-integra-s-priniala-uchastie-v-mezhdunarodnom-voenno-tekhnicheskom-forume-armiia-2018/ (дата обращения: 24.04.2020).

3. Губин А.В., Хлуднев П.Н., Яковец Е.Н. Современные подходы к информационно-аналитическому обеспечению оперативно-розыскной деятельности органов внутренних дел // Информатизация и информационная безопасность правоохранительных органов. М.: Академия управления МВД России, 2003. С. 188-192.

4. Губин А.В., Яковец Е.Н. Вопросы построения логико-аналитического комплекса ситуационного центра ГУВД Москвы // Информатизация, информационная безопасность и математическое моделирование деятельности органов внутренних дел: сборник научных статей. М.: Академия управления МВД России, 2004. С. 78-94.

5. Букейханов П.Е. Информационные технологии в сфере розыскной работы органов внутренних дел // Информатизация и информационная безопасность правоохранительных органов. М.: Академия управления МВД России, 2002. С. 249-255.

РАЗДЕЛ 3. УГОЛОВНО-ПРОЦЕССУАЛЬНАЯ ДЕЯТЕЛЬНОСТЬ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Я.А. Климова, *к.ю.н., старший преподаватель кафедры административной деятельности и охраны общественного порядка Волгоградской академии МВД России, г. Волгоград*

ОСОБЕННОСТИ ОСУЩЕСТВЛЕНИЯ ПРОКУРОРОМ НАДЗОРА ЗА РАССЛЕДОВАНИЕМ УГОЛОВНЫХ ДЕЛ В СФЕРЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

В настоящее время современные технологии проникли практически во все сферы нашей жизни, что обусловливает тенденцию к увеличению количества преступлений, совершенных в сфере компьютерной информации.

Согласно статистическим данным Генеральной прокуратуры РФ, в 2018 г. правоохранительные органы Российской Федерации зарегистрировали 174674 преступления, совершенных в сфере компьютерной информации, из них предварительно расследовано 43362 преступления. За период с января по декабрь 2019 г. правоохранительные органы Российской Федерации зарегистрировали 294409 преступлений, совершенных с использованием информационно-телекоммуникационных технологий. По сравнению с аналогичным периодом предыдущего года наблюдаются значительный прирост +68,5%. Также в 2019 г. было предварительно расследовано — 65238 преступлений, прирост составил +50,4%. В период с января по март 2020 г. правоохранительные органы Российской Федерации зарегистрировали 101537 (+83,9%) преступлений, совершенных в сфере компьютерной информации, предварительно расследовано — 21343 (+60,2%) [1].

Данные статистики свидетельствуют о более чем значительном увеличении количества преступлений в сфере компьютерной информации. Следует отметить, что в силу как объективных, так и субъективных причин существует большая степень вероятности низкого уровня расследования таких дел.

В условиях продолжающегося реформирования уголовного судопроизводства все более актуальной становится проблема обеспечения эффективного и качественного прокурорского надзора за расследованием уголовных дел рассматриваемой категории. Поскольку в силу специфики расследования таких дел возможно допущение нарушения прав и свобод участников уголовного судопроизводства. В этой связи прокурор должен особенно тщательно осуществлять надзор на всех стадиях расследования уголовных дел в сфере компьютерных преступлений.

Так, на стадии возбуждения уголовного дела прокурор должен помимо постановления о возбуждении уголовного дела проверить все материалы, полученные в ходе предварительной проверки, с целью анализа их полноты и достаточности для принятия решения о наличии в деянии признаков преступления, а также их легитимности и допустимости. Учитывая специфику объекта преступлений, материалы могут содержать оперативно-служебные документы, в которых отражены результаты осуществления оперативно-розыскной деятельности (протокол оперативного наблюдения, протокол контрольной закупки, протокол и стенограмма просушивания телефонных переговоров), протоколы следственных действий (протокол осмотра места происшествия, в ходе которого проводилось изъятие компьютерной техники, носителей информации, финансовых документов), различные справки специалистов об исследованиях.

Следует отметить, что на практике нередкими являются случаи, когда прокурор вместо текущего надзора за ходом расследования осуществляет последующий надзор уже на завершающем этапе досудебного производства при поступлении уголовного дела с обвинительным заключением. Полагаем, что прокурорский надзор за предварительным расследованием такой категории дел должен осуществляться постоянно, на всех этапах производства по уголовному делу.

О справедливости нашего мнения свидетельствует многочисленная судебная и правоприменительная практика.

Так, согласно постановлению Останкинского районного суда г. Москвы о прекращении уголовного дела, уголовного преследования, в связи с отказом государственного обвинителя от обвинения в судебном заседании были рассмотрены материалы уголовного дела по обвинению Евдокимова А.Е., в совершении преступления предусмотренного п. «в» ч. 2 ст. 273 УК РФ. Однако государственным обвинителем было заявлено об отказе от обвинения, предъявленного А.Е. Евдокимову, в связи с отсутствием в его деянии состава преступления. Свой отказ обвинитель мотивировал тем, что в ходе судебного разбирательства было установлено отсутствие у оперативных служб достаточной информации свидетельствующей о том, что Евдокимов А.Е. занимается установкой нелицензионного программного обеспечения. Соответственно, поскольку до проведения ОРМ — «проверочная закупка» в отношении Евдокимова А.Е., какими-либо сведениями о совершении им преступлений, или о готовящемся с его участием преступлениях в том числе и следственные органы не располагали, то умысел у Евдокимова А.Е. на совершение вмененных ему в ходе следствия действий, был сформирован под влиянием и в результате уговоров оперативных сотрудников [2].

Данный пример подтверждает, что при осуществлении качественного прокурорского надзора на досудебных стадиях уголовного судопроизводства выявить наличие в материалах дела оснований для прекращения уголовного преследования возможно было до направления уголовного дела в суд.

Здесь стоить отметить, что эффективность надзора напрямую зависит от имеющихся у него полномочий. Поскольку попытка разделить функции предварительного следствия и прокурорского надзора привела к кардинальному усечению полномочий прокурора: прокурор перестал выполнять функцию процессуального руководства следствием, то есть фактически прокурор был лишен эффективных надзорных инструментов в отношении предварительного следствия. В настоящее время об осуществлении прокурором функции процессуального руководства можно говорить только по отношению к расследованию в форме дознания; следователи же обладают процессуальной самостоятельностью. Необходимо уточнить, что следователь обладает процессуальной самостоятельностью по отношению к прокурору, поскольку у прокурора нет специальных полномочий по осуществлению процессуального надзора.

Таким образом, возрастание роли прокурора при реализации надзорных полномочий за органами предварительного расследования при производстве по уголовным дел по преступлениям в сфере компьютерной информации обуславливается существенным увеличением количества таких преступлений. Необходимость расширения полномочий прокурора с целью эффективной реализации возложенных на него функций, укрепления его статуса как гаранта законности проведения предварительного расследования является сегодня актуальной проблемой и требует законодательного разрешения.

Список литературы

1. Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/analytics (дата обращения: 21.05.2020).

2. Постановление Останкинского районного суда гор. Москвы о прекращении уголовного дела, уголовного преследования, в связи с отказом государственного обвинителя от обвинения по ч. 2 ст. 273 УК РФ № 1-12/2013 (1-554/2012) от 23 апреля 2016 г. URL: http://www.sud-praktika.ru/precedent/83691.html (дата обращения: 18.05.2020).

Ю.С. Латынская, *помощник мирового судьи Вологодской области по судебному участку № 59, г. Харовск*

ВОЗБУЖДЕНИЕ УГОЛОВНОГО ДЕЛА ЧАСТНОГО ОБВИНЕНИЯ В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ

Действующий Уголовно-процессуальный кодекс Российской Федерации (далее — УПК РФ) в ст. 20 определяет категорию дел, которые возбуждаются в порядке частного обвинения. К ним относятся: 1) умышленное причинение легкого вреда здоровью (ч. 1 ст. 115 УК РФ); 2) нанесение побоев лицом, подвергнутым административному наказанию (ст. 116.1 УК РФ); 3) клевета (ч. 1 ст. 128.1 УК РФ). Глава 11 УПК РФ регламентирует порядок производства указанных уголовных дел.

В ст. 318 УПК РФ указано единственное основание для возбуждения дел частного обвинения — заявление потерпевшего или его законного представителя мировому судье [5]. Данное правило основано на принципе диспозитивности и имеет своей целью создание условий для разрешения конфликтных ситуаций без участия государственных органов. Однако в некоторых ситуациях присутствуют различные субъективные факторы, оказывающие влияние на потерпевшего. К таким факторам можно отнести: оказание давления на потерпевшего, угроза жизни и здоровью, уверенность в безнаказанности преступника, основанное на недоверии органам и другие. Также к субъективным факторам можно отнести и мнение судьи, рассматривающего заявление, так как именно он оценивает достаточность данных, содержащихся в заявлении, опираясь на свое внутреннее убеждение [2, с. 239].

Хочется отметить, что в ч. 4 ст. 20 УПК РФ закреплена обязанность органов, осуществляющих расследование, возбудить уголовное дело даже при отсутствии заявления потерпевшего или его законного представителя, в случае если преступление было совершено в отношении лица, которое в силу своего зависимого или беспомощного состояния, или по иным причинам не может защищать свои права и законные интересы.

Согласно ст. 318 УПК РФ, заявление потерпевшего по делам частного обвинения должно подаваться в суд только в письменной форме и отвечать установленным в законе требованиям. В данном заявлении должны содержаться следующие данные: наименование суда, в который оно подается; описание преступления, места и времени его совершения, а также обстоятельство его совершения; ходатайство, направленное суду, для принятия уголовного дела к производству; сведения о потерпевшем, данные его документов, удостоверяющие личность; информация о лице, привлекаемом к уголовной ответственности; список свидетелей, которых необходимо вызвать в суд; подпись лица, подавшего данное заявление.

В настоящее время с совершенствованием цифровых технологий одним из направлений развития уголовного судопроизводства можно выделить расширение возможности обращения с заявлением о преступлении как в правоохранительные органы, так и в суд с помощью цифровых технологий. Отметим, что с 1 января 2017 г. вступили в силу дополнения в УПК РФ, которые ввели в действие ст. 474.1, предусматривающую возможность подачи ходатайства, заявления, жалобы, представления в суд в порядке и сроки, которые установлены УПК РФ, в форме электронного документа, подписанного лицом, направившим такой документ, электронной подписью в соответствии с законодательством Российской Федерации, посредством заполнения формы, размещенной на официальном сайте суда в информационно-телекоммуникационной сети Интернет. Материалы, приложенные к ходатайству, заявлению, жалобе, представлению, также подаются в форме электронных документов. Однако законодатель не упоминает, какие именно заявления подлежат подаче в форме электронного документа. Если опираться на вышеуказанную статью УПК, то препятствий для подачи заявления частного обвинения в электронной форме нет. Между тем криминологическая характеристика лиц, пострадавших от такого рода преступлений, свидетельствует о реальной невозможности

воспользоваться указанными лицами данным правом, т.к. большинство не имеет электронной подписи [1, с. 59].

В соответствии с ч. 1 ст. 319 УПК РФ, если поданное заявление не соответствует требованиям, содержащимся в УПК РФ или имеет некоторые недостатки, то мировой судья выносит постановление о возвращении заявления, в котором предлагает лицу, его подавшему, привести заявление в соответствие с указанными требованиями и устанавливает для этого определенный срок. Если указанные недостатки не были устранены в установленный срок, судья отказывает в принятии заявления к своему производству и уведомляет об этом лицо, его подавшее. Когда заявление соответствует всем установленным в УПК РФ требованиям, мировой судья выносит постановление о принятии его к производству.

К причинам, по которым суд может отказать в принятии заявления, относятся:

– несоблюдение указаний судьи к требованиям, представляемых к заявлению;

– недостаток у потерпевшего по делу частного обвинения данных о лице, привлекаемого к уголовной ответственности.

В случае если данные о лице, совершившем преступление, отсутствуют и неизвестны потерпевшему, то мировой судья отказывает в принятии заявления к своему производству и направляет его руководителю следственного органа или начальнику органа дознания для решения вопроса о возбуждении уголовного дела.

Данные действия занимают много времени, в связи с чем рассмотрение уголовного дела растягивается на длительный период. Для того чтобы процесс принятия заявления к своему производству и возбуждение уголовного дела частного обвинения ускорился, на наш взгляд, необходимо создать электронные бланки (формы) образцов заявлений о преступлениях по делам частного обвинения, которые соответствуют требованиям УПК РФ, содержат в себе разъяснения, примеры, ссылки на правовые акты, а также процессуальные гарантии защиты прав и законных интересов участников уголовного судопроизводства. Данные бланки (формы) необходимо разместить на официальном сайте суда, где граждане смогут самостоятельно их заполнить и направить в суд посредством сети Интернет на проверку. Согласно Приказу Судебного департамента при Верховном Суде РФ от 11 сентября 2017 г. № 168 «Об утверждении Порядка подачи мировым судьям документов в электронном виде, в том числе в форме электронного документа» просмотр документов, поданных в суд в электронном виде, осуществляется работником аппарата суда, ответственным за прием документов в электронном виде. Данное лицо должно убедиться в том, что документы, поступившие в информационную систему, адресованы суду, доступны для прочтения, оформлены в соответствии с Порядком подачи документов, включая соблюдение требования о наличии графической подписи лица в электронном образе обращения в суд, требований к электронной подписи (п. 4.4). Если названные условия не соблюдены, отправителю направляется уведомление о том, что документы не могут быть признаны поступившими в суд [4]. Тут опять же возникает вопрос о наличии электронной подписи у лица, подающего заявление, что требует тщательного изучения.

В случае если данное внедрение электронных бланков положительно отразится на развитии судопроизводства, поднимется вопрос об электронном ведении уголовного дела частного обвинения. Так, ст. 8.1 УПК Литовской Республики предусматривает ведение уголовных дел в электронной форме и использование Интегрированной системы уголовно-процессуальной информации учреждений досудебного следствия [1, с. 60].

После того как мировой судья примет заявление к своему производству, потерпевший приобретает статус частного обвинителя, а лицо, в отношении которого подано заявление, обвиняемого.

При проверке заявления судья определяет, указаны ли в заявлении деяния, которые можно квалифицировать по ч. 1 ст. 115, ст. 116.1 и ч. 1 ст. 128.1 УК РФ. Если выяснится недостаточность и отсутствие данных, то он выносит постановление об отказе в приеме заявления

к производству. Кроме этого, необходимо проверить отсутствие обстоятельств, исключающих производство по делу, перечень которых указан в ч. 1 ст. 24 УПК РФ.

Таким образом, уголовное дело частного обвинения считается возбужденным с момента принятия мировым судьей надлежаще оформленного заявления и вынесения постановления.

Однако часто возникают некоторые проблемы еще на стадии возбуждения уголовных дел частного обвинения, которые влияют на дальнейшую возможность рассмотрения дела.

Как мы уже упомянули, в соответствии с законодательством после получения заявления от потерпевшего мировой судья должен убедиться, что оно соответствует требованиям ст. 318 УПК РФ, в случае несоответствия, судья выносит постановления о возвращении и устанавливает сроки для устранения недостатков. Одновременно уголовное дело частного обвинения может оказаться неподсудным данному суду (например, если преступление совершено на территории другого судебного участка).

Недостатком процедуры возбуждения уголовного дела частного обвинения является то, что судья, несмотря на неподсудность ему уголовного дела, обязан принять заявление к производству. В соответствии со ст. 227 УПК РФ разрешение вопроса о подсудности судьей осуществляется на этапе назначения судебного заседания, т.е. после принятия заявления к своему производству. Ю.Ю. Денисова, проанализировав практику, отмечает, что существуют случаи, когда заявление, подаваемое судье не только не подсудно этому мировому судье, но и не соответствует требованиям УПК РФ. В результате, судья после устранения недостатков, возбуждает уголовное дело частного обвинения и после этого принимает решение о направлении уголовного дела по подсудности [3, с. 22].

Таким образом, создание электронных бланков (форм) приобретет огромную значимость при составлении наиболее сложных обращений для непрофессиональных участников, к форме и содержанию которых закон предъявляет жесткие требования, и позволит минимизировать случаи возвращения таких заявлений для устранения замечаний, а также ускорить принятие по ним решений. При создании электронных бланк (форм) законодатель должен определить четкий алгоритм их заполнения, основанный на уголовно-процессуальном законодательстве и обеспечить процессуальными гарантиями для защиты от всевозможных рисов. Однако этот процесс представляется достаточно трудоемким и включает в себя внедрение автоматизированных систем электронного документооборота, изучение вопроса об электронной подписи. Следует отметить, что цифровизация уголовного судопроизводства должна быть направлена не на облегчение деятельности государственных органов, а именно на обеспечение демократизации, гуманизации, справедливости уголовного судопроизводства.

Список литературы

1. Андреева О.И., Зайцев О.А. Перспективы ведения российского уголовного судопроизводства в электронном формате // Уголовная юстиция. 2018. № 12. С. 57-61.

2. Дамбаева Д.Р. Особенности возбуждения уголовных дел частного обвинения // Приоритетные направления развития науки и образования. 2016. № 4-2 (11). С. 238-242.

3. Денисова Ю.Ю. Актуальные проблемы возбуждения уголовных дел частного обвинения у мирового судья, пути их решения // Мир народов. Серия: Наука и практика. 2018. № 2 (7). С. 19-23.

4. Приказ Судебного департамента при Верховном Суде РФ от 11 сентября 2017 г. № 168 «Об утверждении Порядка подачи мировым судьям документов в электронном виде, в том числе в форме электронного документа».

5. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 24.04.2020).

И.П. Попова, *к.ю.н., доцент кафедры уголовного процесса Восточно-Сибирского института МВД России, председатель Усть-Илимского городского суда Иркутской области в почетной отставке, г. Иркутск*

К ВОПРОСУ ДОКАЗЫВАНИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ В АСПЕКТЕ ЦИФРОВИЗАЦИИ И ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Значение института доказывания в уголовном судопроизводстве можно сравнить с некоей жизненно важной функцией организма, которая сопровождает человека на протяжении всей его жизни. Процесс доказывания осуществляется еще на стадии возбуждения уголовного дела и завершается на стадии исполнения состоявшегося судебного решения. В этой связи все изменения, происходящие в общественных отношениях, не могут не затрагивать и ключевую «артерию» уголовного процесса — доказывание.

В последние годы в тренде научного сообщества высказываться о масштабных реформах уголовного судопроизводства, обусловленных цифровизацией государства и экономики. Термины «цифровизация уголовного судопроизводства», «электронное правосудие» вошли в лексикон в рамках научных дискурсов и сопровождают не только пояснительные записки законопроектов, но и нормативные источники. Между тем в настоящее время толкование этих терминов каждым автором проходит через призму его взглядов на указанные процессы и отраженные в его правосознании современные тенденции развития отечественного уголовного процесса.

В этой связи, предваряя раскрытие обозначенной в названии тематики, уместно раскрыть авторское содержание исследуемых категорий. Представляется, что цифровизация уголовного судопроизводства нацелена на максимальное технологическое оснащение органов, осуществляющих производство по уголовному делу, судебную систему, использование различных информационных технологий в целях соблюдения разумного срока судопроизводства, транспарентность судебной системы, обеспечение доступа к правосудию и оптимизацию деятельности всех участников уголовно-процессуальных правоотношений. Тогда как под термином «электронное правосудие» вовсе не следует рассматривать осуществление правосудия посредством замены судьи искусственным интеллектом либо иными каким-либо иными техническими средствами или устройствами.

Вместе с тем нельзя отрицать активное влияние цифровой среды на состояние преступности, поскольку совершение преступлений сопровождается использованием различных технических средств, что требует обработки большого массива данных и в конечном итоге обусловливает и изменение процесса доказывания не только по такого рода, но и по иным преступлениям. Как верно отмечает Е.А. Карякин, «окружающая нас действительность становится информационной, необходимо только обнаружить искомую информацию и зафиксировать ее для дальнейшего использования» [1, с. 191].

Понятие информационных технологий как процессов, методов поиска, сбора, хранения, обработки, предоставления, распространения информации и способов осуществления таких процессов и методов дано в Федеральном законе от 27.07.2006 г. № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации» [2].

Применительно к уголовному судопроизводству следует данное понятие конкретизировать указанием на то, что данные процессы и методы направлены в отношении информации, имеющей значение для уголовного дела, в целях получениях доказательств, на основе которых устанавливаются обстоятельства, подлежащие доказыванию в пределах, установленных ст. 73 УПК РФ. Соответственно, указанные методы и способы должны базироваться на стандартах доказывания, используемых в уголовном процессе с учетом правовых положений уголовно-процессуального закона.

В условиях доступности электронно-цифровой среды для всех участников уголовного судопроизводства ключевыми вопросами являются два момента: 1) вопросы допустимости

полученных результатов, 2) оценка полученных с помощью информационных технологий доказательств.

Разрешение вопроса оценки доказательств, вне зависимости от способа их получения и вида, — исключительная прерогатива субъекта доказывания, правомочного принимать процессуальное решение на той или иной стадии производства по уголовному делу.

Принцип свободы оценки доказательств (ст. 17 УПК РФ) базируется на внутреннем убеждении субъекта доказывания, на определенных нравственных категориях и ценностях, потому представляется, что их наличие не только чуждо, но и претит технологиям, позволяющим использование юнитов искусственного интеллекта в доказывании по уголовным делам.

Вопрос виновности, как основной вопрос уголовного правосудия, может быть разрешен только судьей на основе итоговой оценки собранных и исследованных доказательств, тогда как современные и появляющиеся новые информационные технологии могут лишь служить средством, если так корректно высказаться, технологизации (усовершенствования) процедуры разрешения дела по существу, но не автоматизации уголовного правосудия, его цифровизации в аспекте использования формальных доказательств и шаблонизации действий и решений правоприменителей.

Несмотря на прогрессивные исследования когнитивных функций в рамках внедрения в современные реалии искусственного интеллекта, существует твердая убежденность в том, что тонкая материя уголовного процесса оказывает столь жесткое влияние на всех, кто в него вовлечен, что исключает замену судьи машиной, пусть даже самой совершенной, с точки зрения ее разарботчиков.

Думается, что предложенные отдельными авторами так называемые «компромиссные варианты» разработки специальных программ по математическому моделированию и алгоритмизации принятия судебных решений с целью предложить «судье «оптимальный» с учетом заложенных критериев приговор, который будет иметь для него рекомендательное и ориентирующее значение» [3, с. 592], являются дискуссионными, противоречащими базисным ценностям уголовного правосудия. Судейское усмотрение лежит в основе судебного познания и правового мышления, без которых индивидуализировать правовые нормы к конкретному уголовному делу не представляется возможным. Предложения таким образом «освободить судью при вынесении приговора от усмотрения», применить математические подходы к судьбе человека подрывают те нравственные устои правосудия, что составляют его сущностные характеристики.

Задача законодателя заключается в создании надлежащего механизма отправления правосудия, позволяющего обеспечить подлинную независимость судебной власти, минимизации судебных ошибок и максимальных средств судебной защиты как тех, чьи права интересы затронуты преступлением, так и всех тех, кто вовлечен в уголовное судопроизводство в целях справедливого правосудия. Варианты решения этих задач зависят и от целевых ориентиров уголовного судопроизводства, поэтому парадигмальные изменения должны находить отражение и в нормативном регулировании порядка производства по уголовному делу.

Провозглашая защиту прав и законных интересов потерпевших от преступления, законодатель в назначении уголовного судопроизводства, содержание которого отражено в ст. 6 УПК РФ, не указал на необходимость охраны публичных интересов общества и государства. Впрочем, публичное начало российского уголовного процесса пронизывает весь уголовно-процессуальный закон, а частные интересы потерпевших и иных участников уголовного судопроизводства не противопоставлены публичным интересам.

Таким образом, данный ключевой момент оценки полученных с помощью информационных технологий доказательств не требует ни корректировки подхода к нему, ни реформирования законодательства.

Тогда как вопросы допустимости, полученных с помощью информационных технологий результатов, и составляют тот вектор исследований института доказывания, который на базе научных дискурсов может привести к изменениям в УПК РФ. Как справедливо отмечают

отдельные авторы, в «уголовно-правовой сфере электронная информация стала объектом, предметом и орудием совершения преступления, а выявление и раскрытие компьютерных киберпреступлений нельзя себе представить без использования «электронных доказательств», применения информационных технологий в производстве расследования» [4, с. 42].

Следует констатировать, что в процессе доказывания и по другим категориям дел довольно широко применяются различные информационные технологии и технические средства для получения информации, имеющей значение в доказывании.

Учитывая разнообразие как самой информации, так и технологий ее получения, следует солидаризироваться с предложением Е.А. Карякина о разработке совокупности условий, соответствие которым влияет на допустимость использования в доказывании информации, как полученной с помощью конкретных технических устройств, так и снятой с носителей информации сетевых систем. В качестве условий получения сторонами потенциальной доказательственной информации Е.А. Карякин предлагает рассматривать следующие:

– научно подтвержденная возможность получения информации;
– законность, безопасность и этичность получения информации;
– возможность верификации (декодирования и проверки), в том числе силами привлеченного специалиста (эксперта) [1, с. 193].

Сохраняет актуальность при оценке допустимости доказательств, полученных на основе различных информационных технологий, оценка соблюдения таких требований, как законность источника доказательств, и законность метода их получения, на что обращает внимание Е.Н. Петухов [5, с. 92].

Уместно привести примеры, иллюстрирующие данные моменты. Например, технические сведения о времени и скорости движения транспортного средства с помощью глобальной навигационной системы ГЛОНАСС в доказывании по уголовным делам о преступлениях в области безопасности дорожного движения и эксплуатации транспорта используются в виде справок, как иных документов, и в виде показаний свидетелей.

Так, по уголовному делу в отношении Х. по обвинению в совершении преступления, предусмотренного ч. 3 ст. 264 УК РФ, суд первой инстанции сослался на такое доказательство, как справка. Как отмечено судом апелляционной инстанции, в приговоре суд «отверг доводы защиты о том, что пешеходы переходили дорогу не по пешеходному переходу, так как место ДТП — 22,5 метра от пешеходного перехода, поскольку опровергаются показаниями свидетелей И., О., а также справкой ООО «Транс-Глонасс», согласно которой в 03 часа 36 минут 23 секунды автомобиль проезжал пешеходный переход и через 4 секунды полностью остановился, со слов свидетеля О. последний звук тормозов не слышал» [6].

По уголовному делу в отношении А. по обвинению в совершении преступления, предусмотренного ч. 3 ст. 264 УК РФ, в доказывании при постановлении обвинительного приговора были использованы также сведения системы «ГЛОНАСС», но путем допроса свидетеля. Так, из показаний свидетеля обвинения Ф. следует, что «он работает в организации, которая занимается системой мониторинга транспортных средств, на которых установлена система «ГЛОНАСС». Программа зарегистрирована в Росреестре. В рамках данного уголовного дела он делал маршрут автомобиля «Рено-Логан» (регистрационный знак №) в виде графика. Скорость движения данного автомобиля на участке дороги, где произошло ДТП, была 121 км/час и после стало 0 км/час» [7].

Представляется, что в данном случае одна и та же информация о фиксации скорости и времени движения транспортного средства в ходе следствия была получена путем снятия информации с технических носителей и представлена в доказывании с помощью тех источников, что предусмотрены законом, каждый из которых является законным. Вопрос о том, требовалось ли допрашивать в качестве свидетеля лицо, оформившее справку о снятии информации, может возникать при оценке допустимости данного доказательства, как иного документа. Во всяком случае, данные, полученные с технических устройств, стали предметом

исследования эксперта в каждом приведенном случае в рамках судебной автотехнической экспертизы и использованы в доказывании в совокупности с иными доказательствами.

Подводя итог исследованию вопросов доказывания в уголовном судопроизводстве в аспекте цифровизации и информационных технологий, следует резюмировать, что все новеллы законодательства в этой сфере возможны лишь на основе системного изучения проблематики и действующих принципов уголовного правосудия и, без поспешно формулируемых решений, учитывая интенсивность воздействия норм уголовно-процессуального закона на всех участников уголовно-правового конфликта, обусловленного преступлением.

Список литературы

1. Карякин Е.А. К вопросу об информационном подходе к объективизации доказывания в современном уголовном процессе // Вестник университета имени О.Е. Кутафина. 2018. № 2. С. 188-193.
2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 18.03.2019) // Собрание законодательства РФ. 2006. № 31. Ст. 3448.
3. Зуев С.В., Никитин Е.В. Информационные технологии в решении уголовно-процессуальных проблем // Всероссийский криминологический журнал. 2017. Т. 11, № 3. С. 587-595.
4. Зайцев О.А., Пастухов П.С. использование информационных технологий в российском уголовном судопроизводстве // Вестник экономической безопасности. 2016. № 5. С. 40-43.
5. Петухов Е.Н. Критерии допустимости доказательств и их источников в уголовном процессе России // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2004. № 4. С. 91-92.
6. Апелляционное Постановление Верховного суда Республики Татарстана от 13 декабря 2019 г. № 22-9222/2019. URL: https://sudact.ru/regular/doc /GeIH2cxpRbdJ/.
7. Апелляционное Постановление Самарского областного суда от 16 августа 2019 г. № 2-4829/2019. URL: https://sudact.ru/regular/doc/s5rJFYqJZFbR/?

А.В. Смолин, *преподаватель кафедры криминалистики Нижегородской академии МВД России, г. Нижний Новгород*

УГОЛОВНО-ПРОЦЕССУАЛЬНАЯ ПРИРОДА ЭЛЕКТРОННОГО ДОКАЗАТЕЛЬСТВА

В середине прошлого века начался процесс интеграции информационных технологий в различные сферы деятельности человека, который достиг своего апогея в последнее десятилетие. Современный мир трудно представить без различного рода технических устройств, принципы работы которых построены на процессах передачи и обработки цифровой информации. Вовлекаясь в механизм преступной деятельности, данные устройства запечатлевают в себе ее отражения, что позволяет им принимать участие в процессе воссоздания картины совершенного преступления, то есть становиться элементом доказывания. В связи с этим в науке уголовного процесса появился термин «электронное доказательство».

Данное понятие отсутствует в действующем Уголовно-процессуальном кодексе РФ, хотя он содержит другие понятия, смежные с ним. Например, электронные носители информации. Отсутствие нормативно-правового закрепления электронного доказательства привело к многочисленным исследованиям процессуалистов и криминалистов по вопросам его содержания и использования в процессе доказывания, в особенности существует много подходов

к раскрытию его понятия. Так, по мнению М.В. Горелова, электронным доказательством являются сведения об имеющих значение для расследования обстоятельствах, выраженные в цифровой, звуковой форме или видеозаписи, а также различные протоколы, зафиксированные с помощью электронно-вычислительных средств [1, с. 8]. В.Б. Вехов, по сути, взяв за основу общее понятие доказательств, зафиксированное в ч. 1 ст. 74 УПК РФ, также акцентировал внимание на отличие формы выражения электронных доказательств [2, с. 47].

Таким образом, авторы сходятся в точке зрения, что основной особенностью электронного доказательства является его форма. И в данном случае речь идет не об уголовно-процессуальной форме, а форме его выражения. М.П. Поляков и А.Ю. Смолин в своей работе также отметили данную тенденцию, а именно, что многочисленные исследования о понятии и сущности электронного доказательства скатились в техническую сторону, забывая при этом о его процессуальной природе [3].

Несомненно, многих практических работников пугает содержание цифровой информации, поскольку в отличие от привычного выражения она представляет собой лишь код, состоящий из нулей и единиц. Непосредственно для человека данная информация не познаваема. Им она может быть воспринята только опосредовано, через различные технические устройства, которые смогут ее преобразовать в сведения, понятные для него. В данном случае речь идет о нашем восприятии действительности, и готовности встречи и доверия такой информации. Настолько обыденные и понятные для каждого субъекта доказывания сейчас — следы пальцев рук, в свое время также с трудом воспринимались в качестве доказательств. Один из таких примеров был описан Ю. Торвальдом о расследовании дела об убийстве в Дептфорде в 1905 г. [4, с.77-84]. Безусловно, такие же проблемы были и, возможно, сейчас присутствуют при восприятии судом и другими участниками уголовного судопроизводства доказательств в цифровом виде. Но с течением времени вопросов к понятию формы его закрепления и выражения становится все меньше.

Соответственно, в данном случае необходимо говорить не о технической форме электронных доказательств, а уголовно-процессуальной — том законном выражении, в форме которого они смогут существовать при уголовном деле. По данному вопросу существует три основных позиции: выделение их как самостоятельного вида доказательств; отнесение их к иным документам; признание вещественными доказательствами.

Сторонниками первого подхода являлись Н.А. Зигура и А.В. Кудрявцева, полагавшие, что компьютерная информация должна выступать в качестве самостоятельного вида доказательства [5, с. 30]. В обоснование своей позиции они фактически подчеркивали особенности технической формы электронного доказательства: ее специфичность, механизм формирования и среду обитания. Любое доказательство — единство процессуальной формы и содержания, которое извлекается посредством законных средств из источника, содержащего в себе отражение преступной деятельности. Техническая же форма — это оболочка содержания доказательства, то, каким образом она отображается и существует на объекте-носителе. Цифровая информация сама по себе закодирована. В основе ее образования и существования лежат процессы, понятные далеко не каждому человеку. Это признал и законодатель, когда ввел изменения, закрепленные Федеральным законом от 27.12.2018 № 533-ФЗ «О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации», обязывающие субъектов расследования привлекать специалистов для работы с электронными носителями информации. Но цифровая среда не единственная, в которой есть свои особенности отображения и хранения информации. Почему тогда не возникает аналогичного вопроса об особенностях запечатления информации человеком? В основе этого лежат нейронные процессы, происходящие в нервной системе человека, в особенности в головном мозге. В данном случае ответ лежит, вероятно, в том, что показания лиц не одно столетие признаются доказательством по делу и давно воспринимаются всеми участниками процесса обыденно.

Рано или поздно и цифровые технологии станут такой же неотъемлемой частью не только всего общества, но и уголовного процесса. А за исключением технической формы, электронная информация не отличается от каких-либо других процессов и отражений преступной деятельности. Она также несет в себе содержание — сведения, которые могут иметь значение для доказывания. Данные сведения должны быть восприняты и понятны субъектом расследования и иными участниками уголовного процесса. Для этого применяются различные технические устройства, которые перекодируют цифровой сигнал в понятное для человека его выражение. По сути, этот процесс не отличается от химического исследования наркотического средства — без применения техники обнаруженное вещество не может быть идентифицировано, а значит, не может быть познано и воспринято. Все это говорит о том, что по своему процессуальному содержанию электронное доказательство не слишком отличается от более привычных видов доказательств. Данную точку зрения разделяли И.А. Зинченко и А.П. Попов, отмечая, что для субъекта расследования не имеет значения, каким образом выполнена информация, важно ее значение для доказывания [6].

Тем самым видится необоснованной идея В.А. Мещерякова и В.В. Трухачева о введении в УПК РФ новой категории доказательств, в основу которой должна быть положена цифровая информация, а также формировании нового следственного действия, представляющего возможность получения такого доказательства [7, с. 110]. Действующий УПК РФ закрепляет достаточно широкий перечень уголовно-процессуальных форм и средств получения доказательств, и добавление нового только лишь на том основании, что цифровая информация имеет иное техническое закрепление, нецелесообразно. Необходимо только определиться с единообразием механизма данного уголовно-процессуального преобразования.

Так, в ходе расследования уголовного дела следователем в компании сотовой связи получен компакт-диск с содержащейся на нем информацией о соединениях между абонентами и абонентскими устройствами. С точки зрения доказывания значение имеет исключительно содержащаяся на диске информация о времени, месте соединения, номерах абонентов, с которыми они происходили. То есть доказательством должны выступать сведения о телефонных соединениях. Но при этом только одна цифровая информация без носителя существовать не может. В связи с этим для приобщения к уголовному делу и ей, и носителю необходимо придать процессуальную форму. Возникает вопрос — как это сделать? В научной литературе на данный вопрос нет единого ответа.

Большинство авторов разделились на две группы: одни утверждали, что электронное доказательство должно существовать в качестве вещественного доказательства, другие приписывали ему свойства иного документа. Например А.А. Тушев и Н.А. Назаров в качестве критерия такого разграничения выделяли первостепенность либо формы, либо содержания. Так, если для доказывания важна информация, выраженная в фактических свойствах или качествах объекта материального мира, то такое доказательство необходимо признавать вещественным, если же важно содержание объекта, то необходимо признавать его иным документом [8, с. 196-197].

Подобный двойственный подход к процессуальной форме электронного доказательства обусловлен отсутствием прямой регламентацией данного вопроса в УПК РФ. Оно же порождает принятие ошибочных решений практическими сотрудниками. Законодатель же, хоть прямо в тексте закона и не указал на необходимость отнесения электронных доказательств к вещественным, но данный вывод вытекает из положений ч. 4 ст. 81 и ч. 1 ст. 81.1 УПК РФ. Таким образом, разделяя позицию авторов [9], придерживающихся аналогичного подхода, сделаем вывод, что любое электронное доказательство, вне зависимости от того, что представляет первостепенное значение для доказывания — форма или содержание, должно признаваться вещественным доказательством.

Понимая, что обилие дискуссий об электронных доказательствах в первую очередь связано с отсутствием их процессуальной регламентации, необходимо ответить на вопрос — стоит ли закреплять в УПК РФ его понятие? Как уже отмечалось ранее, ряд авторов дает

утвердительный ответ. Но есть и те авторы, кто не видит в закреплении понятия «электронное доказательство» никакой принципиальной роли для уголовного процесса. Интересной представляется позиция П.С. Пастухова, который отмечает, что вопросы включения в нормы УПК РФ понятия «электронное доказательство» должны решаться не созданием нового источника доказательств, а системы состязательного уголовно-процессуального доказывания [10, с. 192]. Так, в доказательственном праве США не ведутся дискуссии, в отличие от отечественного процесса, о самостоятельности электронного доказательства как отдельного вида. Американских юристов интересуют преимущественно вопросы нарушения прав и законных интересов граждан при изъятии у них компьютерной информации, а с понятийным аппаратом они обходятся более свободно [11, с. 43].

Вероятно, и нам не стоит так тщательно вдаваться в этимологию понятия электронного доказательства и придумывать новые способы его получения и закрепления. Для правоприменителя куда важнее знать и понимать критерии законности обнаружения, получения и оперирования доказательствами, нежели неуловимые для него тонкости различия их видов. Уголовно-процессуальное законодательство должно давать пространство для «маневра» каждой из сторон процесса, чтобы в равных условиях они могли либо убедить суд в выдвинутой им версии, или же убедиться в ее несостоятельности.

Все вышесказанное дает основание полагать, что электронное доказательство имеет существенное отличие от других видов доказательств лишь в своей технической форме. Итак, процесс его «рождения» и использования в доказывании не требует дополнительного нормативно-правового регулирования.

Список литературы

1. Горелов М.В. Электронные доказательства в гражданском судопроизводстве России: вопросы теории и практики: дисс. ... канд. юрид. наук. Екатеринбург, 2005. 185 с.
2. Вехов В.Б. Электронные доказательства: проблемы теории и практики // Правопорядок: История, теория, практика. 2016. № 4. С. 46-50.
3. Поляков М.П., Смолин А.Ю. Концептологический анализ феномена электронных доказательств // Вестник Нижегородской академии МВД России. 2019. № 2 (46) С. 135-145.
4. Торвальд Ю. Век криминалистики / пер. с нем. И.С. Власова, Л.А. Пэк. М.: РГ-Пресс, 2018. 368 с.
5. Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательств в уголовном процессе России: монография. М.: Юрлитинформ, 2011. 176 с.
6. Зинченко И.А., Попов А.П. Институт электронных носителей информации в уголовно-процессуальном праве. URL: https://www.iuaj.net/node/2814 (дата обращения: 20.03.2020).
7. Мещеряков В.А., Трухачев В.В. Формирование доказательств на основе электронной цифровой информации // Вестник Воронежского института МВД России. 2012. № 2. С. 108-110.
8. Тушев А.А., Назаров Н.А. Информация как основа всех видов доказательств в уголовном процессе // Общество и право. 2012. № 3. С. 195-197.
9. Краснова Л.Б. Электронные носители информации как вещественные доказательства // Известия Тульского гос. ун-та. Экономические и юридические науки. 2013. № 4-2. С. 254-259.
10. Пастухов П.С. «Электронные доказательства» в состязательной системе уголовно-процессуальных доказательств // Общество и право. 2015. № 1 (51). С. 192-196.
11. Окоменко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис. … канд. юрид. наук. М., 2016.

А.С. Соколов, *старший преподаватель кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*
А.Ю. Поволотцкий, *преподаватель кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*
Р.А. Мухортов, *магистрант Алтайского государственного университета, г. Барнаул*

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШЕННЫХ С УЧАСТИЕМ НЕСОВЕРШЕННОЛЕТНИХ

Современное развитие информационных технологий затронуло многие важные области жизнедеятельности государства: банковскую систему, добычу и хранение стратегически важных ресурсов, оборону, связь, системы жизнеобеспечения населения, структуры обеспечения устойчивой работы государственного аппарата, транспорт, энергетика.

Под преступлениями в сфере компьютерной информации в самом общем виде следует понимать виновно опасные деяния, которые совершены в сферах информационных технологий, воздействуя на определенные сведения, которые представляются в электронной форме, могут храниться, обрабатываться и передаваться [1].

Расследование рассматриваемых преступлений невозможно без понимания их причин и принципов организации. Рассмотрим некоторые особенности совершения преступления в сфере компьютерной информации.

Фишинг — это практика отправки мошеннических электронных писем в попытке обмануть получателя, как правило, с целью получения денег. Пожилые люди особенно уязвимы перед такими видами компьютерных преступлений, но ни в коем случае не являются единственными жертвами. Распространенным примером фишинговой схемы является так называемая афера «испанский заключенный», в которой кто-то отправляет сообщение с просьбой получателю обналичить чек для них, сохранить часть выручки и отправить остаток обратно отправителю.

Конечно, чек, который они вам прислали, в конце концов аннулируется, скорее всего, после того как вы отправите им деньги. Мошенники часто также используют информацию о вашем банковском счете либо из аннулированного чека, либо из любого чека, который вы им посылаете, чтобы создать новые чеки с вашей информацией на нем и продолжить свою мошенническую схему с какой-то новой несчастной жертвой.

Хакеры проникают в онлайн-сети, чтобы незаконно загружать конфиденциальную информацию, манипулировать функциями системы и в некоторых случаях красть идентификационные данные, которые могут быть использованы для мошеннической покупки товаров в Интернете.

Это часто достигается путем прямых атак на веб-сайты, обманом заставляя отдельных пользователей загружать вредоносные программы, замаскированные под другие материалы, или скрывая код в электронных письмах.

Часто смысл взлома заключается не в том, чтобы взять информацию из компьютера, а в том, чтобы использовать ее как часть сети компьютеров, используемых для атаки на более ценные цели, такие как банки или правительственные учреждения, со взломом и получением.

Уголовный кодекс (глава 28) содержит составы преступлений рассматриваемой категории. Одновременно они зачастую представляют собой способ совершения других преступлений. Так, по статистике МВД о состоянии преступности за 2019 г., 9,2% всех зарегистрированных преступлений за отчетный период совершены с использованием компьютерных и телекоммуникационных технологий [2].

На основе обобщенного анализа можно сделать вывод, что среднестатистический преступник — это молодой человек, получивший высшее или среднее специальное образование,

причем чаще всего техническое. Данная выше характерная черта может быть присуща почти половине представителей современного молодого поколения, поэтому актуально сосредоточить пристальное внимание на изучении психологических аспектов, характеризующих личность.

При расследовании уголовных дел с участием несовершеннолетних обязателен учет присущих данным категориям дел особенностей. Началу следственных действий присуща стандартная тактика расследования уголовных дел данной направленности. Основой при построении общих и частных криминалистических версий выступает роль и значение следственных ситуаций.

На первоначальном этапе, прежде всего, следует провести осмотр места происшествия с целью выявления и фиксации данных, позволяющих сделать вывод об обстоятельствах, имеющих значение для уголовного дела, а именно о наличии виртуальных следов, трасологических следов, особенностей доступа, организации, функционирования и устройства различных видов сетей.

По прибытии на место происшествия следователь должен обеспечить неприкосновенность предполагаемых носителей следов преступления, т.е. исключить до окончания следственного действия контакт потерпевшего и иных лиц с электронными устройствами и каналами связи, общение и выход за пределы осматриваемой территории (помещения) всех присутствующих лиц [3].

Самостоятельные манипуляции с техникой при отсутствии конкретно известного результата категорически воспрещены. Немаловажным является проведение осмотра любой доступной документации, которая находится около осматриваемого устройства [4].

Обязательное участие специалиста в области компьютерной техники при осмотре места преступления сегодня не предусмотрено уголовно-процессуальным законодательством, при этом его участие требуется в иных случаях изъятия электронных носителей информации. К примеру, оно обязательно при проведении обыска. Так как изъятие электронных носителей информации зачастую сопровождает осмотр места происшествия, целесообразно привлечение специалиста в ходе осмотра.

Отдельно стоит остановиться на привлечении понятых. Общие принципы уголовного судопроизводства предписывают им необходимость обладания определенным объемом знаний, которого было бы достаточно, чтобы понять суть следственного действия, к которому они привлечены.

В случае объективной невозможности этого возможна фиксация хода следственного действия при помощи технических средств. Дополнительно обязанностью следователя является заблаговременная подготовка специализированных средств изъятия виртуальных следов посредством копирования — портативные криминалистические накопители, стандартные паспортизированные программы, целью которых является копирование данных [5].

Главенствующая роль в производстве расследования зачастую присуща заключению судебной компьютерно-технической экспертизы.

Особенности расследования преступлений, совершаемых несовершеннолетними, в том числе в сфере компьютерной информации, закреплены в общей части УПК РФ, а также в нормах главы 50 УПК РФ.

При расследовании преступлений, совершенных несовершеннолетними, следователь в первоочередном порядке выявляет условия, которые способствовали совершению преступления, круг общения несовершеннолетнего, его поведение, образование, моральные устои, образ жизни, а также иные, важные для расследования условия [6].

Процесс расследования преступлений носит уголовно-процессуальный характер, который является общим для всех категорий лиц, совершивших преступления. В нашем случае

имеются определенные исключения, которые относятся только к несовершеннолетним преступникам и которые закреплены в гл. 50 УПК РФ [7].

Законодатель в указанной главе установил дополнительные обстоятельства, входящие в предмет доказывания по уголовным делам о преступлениях несовершеннолетних. К ним относится необходимость установления возраста несовершеннолетнего подозреваемого и обвиняемого, условий воспитания и жизни несовершеннолетнего подозреваемого и обвиняемого, уровня психического развития несовершеннолетнего подозреваемого и обвиняемого, а также других его личностных особенностей.

Что же касается задержания и заключения под стражу несовершеннолетнего, то данная мера пресечения является самой жесткой и может применяться к несовершеннолетнему подозреваемому (обвиняемому) в исключительных случаях, когда исключена возможность применения более мягкой меры пресечения и имеются на то законодательные основания (ст. 423 УПК РФ) [8].

Немаловажным обстоятельством для следствия по уголовным делам о преступлениях, совершенных несовершеннолетними, является обязательное участие защитника (ст. 51 УПК РФ).

Кроме того, приоритетными особенностями при проведении допроса несовершеннолетнего подозреваемого (обвиняемого), являются присутствие законного представителя несовершеннолетнего и временные ограничения, но этим их круг не ограничивается (более подробно в ст. 425 УПК РФ).

Резюмируя, можно отметить необходимость отнесения компьютерных преступлений к категории сложных, а использование компьютерной информации в преступных целях угрожает интересам как отдельных личностей, так и в целом государству и обществу.

Грамотное и четкое расследование указанной категорий дел обязательно при расследовании преступлений, совершенных несовершеннолетними. Расследование преступлений в сфере компьютерной информации, совершенных несовершеннолетними, проводится по общей методике, но ему присущи свои особенности.

К ним можно, например, отнести необходимость установления дополнительных сведений и условий; обязательное участие защитника, особенности при проведении допроса (участие законных представителей и его сокращенное время), а также выделение уголовного дела в отдельное производство и особый порядок избрания меры пресечения под стражу и задержания.

Таким образом, при расследовании преступлений, совершенных несовершеннолетними в рассматриваемой сфере, важно иметь в виду особенности данной возрастной группы, и в зависимости от этого выявлять возможные мотивы и цели совершения преступлений.

Список литературы

1. Зеленкина О.Ю. Особенности расследования преступлений в сфере компьютерной информации // Сибирские уголовно-процессуальные и криминалистические чтения. № 2 (24). С. 92-100.

2. Состояние преступности в России за январь-ноябрь 2018 года Министерство Внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр». URL: https://мвд.рф (дата обращения: 26.06.2020).

3. Чуб В.С. Компьютерные преступления. Криминалистические особенности расследования // Вестник современных исследований. 2018. С. 411-412.

4. Коломинов В.В. Осмотр места происшествия по делам в сфере компьютерной информации // Сибирские уголовно-правовые и криминалистические чтения. 2017. № 3. С. 145-149.

5. Соколов А.С. Особенности расследования преступлений в сфере компьютерной информации // Аллея науки. 2018. С. 331-336.

6. Кучмезов Р.А. О некоторых особенностях расследования преступлений с участием несовершеннолетних лиц // Успех современной науки. 2019. С. 254-256.

7. Леснова К.И. Особенности производства предварительного расследования в отношении несовершеннолетних // Проблемы правоохранительной деятельности. 2018. С. 74-76.

8. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ / ред. от (ред. от 07.04.2020) // СЗ РФ. 17.06.1996. № 25. Ст. 2954.

9. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // СЗ РФ. 04.08.2014. № 31. Ст. 4398.

Ю.А. Умнягина, *адъюнкт Нижегородской академии МВД России, г. Н. Новгород*

ПРОБЛЕМЫ СОБЛЮДЕНИЯ ПРАВ УЧАСТНИКОВ УГОЛОВНОГО СУДОПРОИЗВОДСТВА ПРИ ПОЛУЧЕНИИ СВЕДЕНИЙ С ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

В настоящее время происходит процесс активного развития информации и носителей электронной информации. Роль информационных устройств и содержащихся на них данных, специфика их формирования и сохранения на носителях свидетельствует о необходимости совершенствования законодательства в рассматриваемой области.

Уполномоченный по правам человека в Российской Федерации Т.Н. Москалькова в качестве приоритетных направлений деятельности выделяет содействие выстраиванию единой государственной системы, направленной на защиту прав и свобод человека, акцентирует внимание на увеличении доли граждан, указывающих на значимость соблюдения основных прав, касающихся личной и семейной тайны, свободы и личной неприкосновенности [1].

Уполномоченный Российской Федерации при Европейском суде М.Л. Гальперин отмечает, что Россия нацелена на поиск и воплощение общих консенсусных подходов к защите и реализации конвенционных прав человека. М.Л. Гальперин заостряет внимание на таких сферах, как уголовное преследование, проверка сообщений о преступлениях, сбор и поиск доказательств, обеспечение прав участников уголовного судопроизводства, в том числе при производстве следственных действий и оперативно-розыскных мероприятий [2]. Однако уголовно-процессуальное законодательство не во всех случаях может защитить права граждан, данные им Основным законом нашей страны, что свидетельствует о недостаточной динамичности закона по сравнению с изменениями в обществе и в мире в целом.

Федеральным законом от 27.12.2018 г. № 533-ФЗ «О внесении изменений в ст. 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» [3] введена специальная норма, предусматривающая особенности изъятия электронных носителей информации. Изменения, вступившие в силу с 8 января 2019 г., устраняют изъяны предыдущей редакции закона, более детально регламентируют порядок изъятия электронных носителей информации и нацелены на дополнительные гарантии защиты и обеспечения прав граждан, однако в рассматриваемой области еще остается много нерешенных законодателем вопросов.

Мобильный телефон в настоящий момент является самым доступным и распространенным средством совершения преступления, и в таких случаях значимым является не сам предмет, а информация, находящееся в нем. Т.Н. Москалькова отметила, что по данным социологических опросов, 70% населения страны пользуются услугами связи и Интернетом, прослеживается постоянное увеличения числа пользователей мобильной связью. Времяпровождение человека в сети составляет около 6 часов в день и данный показатель продолжает расти [4]. В связи с этим нельзя обходить стороной значимость и пренебрегать ценностью информации, хранящейся в средствах сотовой связи.

Информация, хранимая на электронных устройствах, достаточна разнообразна и ввиду своей значимости может иметь доказательственное значение по уголовным делам. На электронных носителях может находится информация, затрагивающая тайну личной переписки, сведения о финансовых операциях, сведения о загрузке документов и посещения сайтов, аудио, видео и фото различного характера, который снимал владелец устройства, и другие данные, позволяющие узнать о его привычках и предпочтениях.

Личные права граждан, гарантируемые основным законом нашей страны, являются высшей ценностью и охраняются государством. Ст. 18 Конституции Российской Федерации устанавливает, что деятельность исполнительной и законодательной власти базируется на основных правах и свободах человека и гражданина, которые в свою очередь обеспечиваются правосудием.

В соответствии с Конституцией РФ гарантом обеспечения права на защиту телефонных переговоров, переписки, почтовых телеграфных и иных сообщений выступает судебная власть (ст. 23) Однако в настоящее время в уголовно-процессуальном законодательстве нет прямого указания на необходимость получения судебного разрешения на изъятие и последующий осмотр содержимого мобильного телефона.

К примеру, гражданка Сандакова И.С. обратилась с жалобой в Конституционный суд Российской Федерации с просьбой признать противоречащими статье 23 Конституции Российской Федерации положения статей 29 и 182 УПК РФ, которые, по ее мнению, позволяют органам предварительного расследования на основании постановления о производстве обыска в жилище изымать у лиц, которые не являются участниками уголовного судопроизводства, предметы и документы, содержащие охраняемую законом тайну, в том числе мобильный телефон с последующим осмотром содержащийся в нем информации без дополнительного получения на то разрешения суда. Изъятие мобильного телефона у Сандаковой И.С. произошло в рамках обыска в жилище и лишь с наличием судебного разрешения на производства конкретного следственного действия, ограничивающего права граждан. Конституционный суд Российской Федерации отказал в принятии к рассмотрению жалобы, сославшись на то, что нормы статей 29 и 182 УПК РФ нарушены не были, а получения дополнительного судебного разрешения на изъятие сотового телефона не требуется в соответствии с уголовно-процессуальным законодательством Российской Федерации [5].

Во избежание процессуальных неразберих и в целях обеспечения конституционных прав гражда, Федеральным законом от 6 июля 2016 г. № 375 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» [6] законодатель закрепил обязанность следователя получать судебное разрешение при необходимости осмотра и изъятия электронных сообщений или иных передаваемых по сетям электросвязи сообщениям. Данное положение нашло свое закрепление в ч. 7 ст. 185 Уголовного кодекса Российской Федерации «Наложение ареста на почтово-телеграфные сообщения, их осмотр и выемка». Следует обратить внимание и на то, что хранящаяся в мобильных устройствах информация может находится не только в форме текстовых

сообщений, но и в видео-, аудио- и фотоформатах, которые не поступали извне на электронное устройство, а создавались и в последующем хранились на нем.

В соответствии с п. 35 ст. 2 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» [7] электросвязь понимается как любой прием, передача, излучение сигналов, письменного текста, голосовой информации, звуков, изображений или сообщений любого рода по радиосистеме, оптической, проводной и другим электромагнитным системам. Одним из основных первичных сигналов электросвязи является телефонный сигнал. Следовательно, положения ч. 7 ст. 185 УПК РФ в части сообщений, передаваемых по сетям электросвязи, должны включать в себя выемку и осмотр информации с мобильных телефонов, однако в настоящее время этого не происходит.

Суд апелляционной инстанции судебной коллегии по уголовным делам Ставропольского краевого суда отказал в удовлетворении жалобы гражданина Д. о признании незаконным постановления следователя о производстве выемки мобильного телефона, обосновывая это тем, что следователем при производстве следственного действия не было допущено нарушений процессуального законодательства. Также в определении суда указано, что выемка сотового телефона происходила в присутствии специалиста в рамках расследуемого уголовного дела, по которому гражданин Д. был допрошен в качестве свидетеля, а мобильный телефон, изъятый у гражданина Д., не является предметом, содержащим государственную или личную тайну, и поэтому судебного разрешения на его изъятие не требуется [8].

Вместе с тем в некоторых случаях Конституционный суд Российской Федерации, отказывая в принятии жалобы к рассмотрению, аргументирует это тем, что гражданин сам добровольно разблокировал телефон, предоставил пароль и не возражал его изъятию и последующему осмотру. Если отталкиваться от представленных выше тезисов, получается, что в тех случаях, если лицо отказалось предоставить пароль от мобильного телефона и выразило свое несогласие на его изъятие и последующий осмотр, то данные следственные действия должны производится по решению суда. Однако это далеко не так.

Гражданин Попов А.Н. обратился в Конституционный Суд Российской Федерации на нарушение его конституционных прав. При обыске у Попова А.Н. был изъят сотовый телефон, который позже был осмотрен на предмет наличия в нем сведений о телефонных соединениях и входящих/исходящих сообщениях. Однако, по мнению Конституционного Суда РФ, если в ходе осмотра принадлежащего заявителю сотового телефона он сообщил установленный в нем пароль и в последующем не препятствовал исследованию портативного электронного устройства, то нет оснований полагать, что оспариваемыми законоположениями были нарушены конституционные права Попова А.Н. [9].

Представленная выше ситуация не исключает возможности оказания на лицо психологического давления со стороны правоохранительных органов в момент дачи согласия на изъятие мобильного телефона и сообщения пароля. В рассматриваемом вопросе остается много пробелов и недоработок.

В уголовно-процессуальном законодательстве отсутствует четкое регулирование вопросов изъятия средств сотовой связи. Процессуальное законодательство Российской Федерации не успевает за интенсивным развитием общественных отношений и на данный момент не может в полной мере обеспечить защиту прав и свобод человека и гражданина. Все это вызывает значительные трудности в применении правовых норм в практической деятельности. Рассматриваемые положения требуют значительной доработки с целью обеспечения процессуальных гарантий личных прав граждан.

Список литературы

1. Доклад Уполномоченного по правам человека в РФ «Доклад о деятельности Уполномоченного по правам человека в Российской Федерации за 2018 год» // Российская газета. 2019. № 125.

2. Круглый стол «Институт следственных судей в уголовном процессе»: Тезисы к вступительному докладу Уполномоченного Российской Федерации при Европейском суде по правам человека — заместителя Министра юстиции М.Л. Гальперина 1 февраля 2018 г. // Бюллетень Европейского суда по правам человека. Российское издание. 2018. № 2. С. 9-13.

3. Федеральный закон от 27 декабря 2018 г. № 533-ФЗ «О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2018. № 295.

4. Доклад Уполномоченного по правам человека при Европейском суде «Доклад о деятельности Уполномоченного по правам человека в Российской Федерации за 2019 год» // Российская газета. 2019. № 234.

5. Определение Конституционного суда РФ от 26 января 2017 г. № 204-О «Об отказе в принятии к рассмотрению жалобы гражданки Сандаковой Ирины Сергеевны на нарушение ее конституционных прав пунктом 5 части второй статьи 29 и частью третьей статьи 182 Уголовно-процессуального кодекса Российской Федерации». URL: https://base.garant.ru/71612136/

6. Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Российская газета. 2016. № 150.

7. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (с изм. и доп. от 06.06.2019) // Собрание законодательства РФ. 2003. № 28. Ст. 2895.

8. Апелляционное определение Ставропольского краевого суда № 22К-3966/2017 от 19.02.2017 г. // КонсультантПлюс. URL: http://www.consultant.ru/

9. Определение от 28 февраля 2017 г. № 338-О «Об отказе в принятии к рассмотрению жалобы гражданина Попова Анатолия Николаевича на нарушение его конституционных прав статьями 176 и 177 Уголовно-процессуального кодекса Российской Федерации» // КонсультантПлюс.

РАЗДЕЛ 4. ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ

М.О. Баев, *д.ю.н., заведующий кафедрой криминалистики Воронежского государственного университета, г. Воронеж*

К ВОПРОСУ О ВИДАХ РИСКА В ДЕЯТЕЛЬНОСТИ ЗАЩИТНИКА ПО УГОЛОВНОМ ДЕЛАМ

В деятельности защитника можно выделить несколько видов риска.

Начать следует с риска самого решения стать членом корпорации, решение рискованное, влекущее добровольное принятие на себя дополнительных обязательств и перед собой, и перед доверителями, и перед обществом, и перед государством, и перед корпорацией. Печальный опыт последних лет, имеются в виду факты привлечения адвокатов-криминалистов к уголовной ответственности, позволяют сделать неутешительный вывод о том, что в абсолютном большинстве случаев это люди случайные, стаж в профессии от нескольких месяцев до нескольких лет, как правило, выходцы из оппонирующих структур. В этой связи невольно напрашивается неутешительный вывод: 1) ошибка в целеполагании; 2) недооценка рисков, в то время как вся адвокатура не просто под пристальным вниманием системы правоохраны, а когда профессиональная деятельность каждого конкретного адвоката рассматривается чуть ли ни через лупу!

Резюмируя этот тезис, отметим: чем осознаннее принимается данное решение, чем больше и глубже претендент разобрался и в идеологических, и в профессиональных основах деятельности, и в существовании корпорации и конкретного адвоката внутри сословия — тем меньше риск и четче понимание специфики принятия решений при обсуждении конкретных профессиональных задач.

Следующим видом риска выступает принятия решения поручения на ведение конкретной уголовной защиты:

а) потенциальный либо реальный (либо могущий быть расцененный как таковой) конфликт интересов, как следствие:

– невозможность (в рамках требований) осуществить эффективную защиту;

– риск отвода от участия в деле.

б) идеологическая составляющая конкретного уголовного дела:

– дела о террористических актах;

– риск попадания в ситуации субъективной невозможности продолжения защиты, например, защита лица, совершившего насильственное преступление в отношении ребенка;

в) чрезмерная занятость по иным делам, не позволяющая осуществить эффективную защиту;

г) осведомленность адвоката о реальных обстоятельствах инкриминируемых деяний при обозначенной при заключении соглашения позиции доверителя, отрицающего их. Законодательный запрет отсутствует, более того, адвокат — не субъект оценки доказательств по внутреннему убеждению, но когнитивный диссонанс при потенциальной защите очевиден.

Выводом выступает то, что рисковых факторов при принятии решения о защите по конкретному делу, касающихся как самого адвоката, так и эффективности потенциальной защиты, множество, но они могут быть выявлены (определены) и учтены при принятии соответствующего решения.

Но если вы все-таки приняли решение и взялись за осуществление конкретной защиты, необходимо, на наш взгляд, учитывать следующее:

Деятельность защитника по уголовному делу должна гарантировать непривлечение к уголовной ответственности невиновного подзащитного, выявление всех оправдывающих и исключающих или смягчающих ответственность подзащитного обстоятельств и назначение последнему при признании его виновным справедливого наказания, независимо от деятельности лиц, осуществляющих уголовное преследование. Именно такой обеспеченный защитником исход — судопроизводства позволяет считать, что защитник с честью выполнил свою процессуальную функцию, даже если не достиг оптимальной цели своего участия.

Очевидным риском в деятельности защитника выступают действия адвоката в условиях информационной неопределенности, постоянно сталкивается с необходимостью принятия решений и совершения действий в ситуациях, когда планируемый результат не только не предопределен однозначно, но порой и вообще труднопредсказуем.

В такой ситуации следует обратиться к нескольким принципиальным положениям теории игр, в силу своей специфики и направленности уделяющей повышенное внимание принятию решений в условиях риска. В соответствии с ее основными постулатами условия риска имеют место, когда лицо, принимающее решение, не может быть уверено в конкретном результате его реализации, а потому должно быть готово, что осуществится худший из возможных прогнозируемых вариантов (например — привлечение к уголовной ответственности без достаточных на то доказательств, либо за деяние, не содержащее в себе состава преступления). Однако совершенно очевидно, что избежать риска возможно, лишь ничего не предпринимая для достижения целей защиты даже в ситуациях, когда принятие решения и, как следствие, совершение определенных целеполагающих действий объективно необходимо. Поэтому в современных условиях, когда законодатель предусмотрел использование всех не запрещенных уголовно-процессуальным кодексом средств и способов защиты в виде права защитника, а не в качестве его непреложной профессиональной обязанности, как было предусмотрено УПК РСФСР (и что по нашему категорическому убеждению в значительно большей степени соответствовало основополагающим принципам защитной деятельности), подобная «позиция» защитника была бы фактически равна отказу от защиты, абсолютно недопустимому ни в нормативном, ни в этическом плане.

Чем выше информационная неопределенность при принятии решения — тем выше риск его отрицательных последствий, поэтому с самого начала защиты адвокат должен объективно проанализировать всю доступную информацию по делу, выдвинуть все возможные предположения о развитии ситуации а, в дальнейшем — постоянно воспринимать информацию о текущем состоянии защиты и анализировать ее на предмет значимости для защиты.

Одним из видов риска безусловно выступает тактический риск. Относительно данного риска целесообразно сформулировать принцип максимина: **минимизация тактического риска при принятии тактически значимых решений и совершении соответствующих действий в целях обеспечения максимально гарантированного объективно и (или) субъективно выгодного результата защитной деятельности.**

Встречаются рисковые ситуации, для принятия решений в которых опыта самого адвоката зачастую недостаточно.

Приведем пример из адвокатской практики.

Гражданину, неоднократно судимому, в том числе и за умышленное убийство, было предъявлено обвинение в совершении преступления (предусмотренного ч. 4 ст. 111 УК РФ) при следующих обстоятельствах: сожительница данного гражданина пришла к нему домой в состоянии алкогольного опьянения. По этой причине между ними возникла ссора, в ходе которой он на почве возникших неприязненных отношений с целью причинения тяжкого вреда здоровью нанес ей руками и ногами более 220 ударов, в том числе не менее 15 ударов в

область головы, не менее 68 ударов в область шеи и живота. От полученных телесных повреждений потерпевшая скончалась на месте. Судебно-медицинская экспертиза трупа потерпевшей также установила наличие в ее половых органов спермы, происхождение которой от подозреваемого исключается.

Изучение адвокатом материалов поступившего в суд уголовного дела показало следующее. Сожительница характеризовалась крайне отрицательно: многие годы употребляла наркотики и занималась проституцией. Днем 11 октября она вместе с подозреваемым и своим знакомым (личность его в ходе расследования не была установлена) распивала спиртные напитки. Затем ушла вместе со знакомым; возвратилась через сутки, после чего между ней и подозреваемым произошли указанные выше события, повлекшие гибель потерпевшей.

После нанесения телесных повреждений и наступления смерти подозреваемый сообщил об этом матери потерпевшей и попросил вызвать полицию; до прибытия представителей правоохранительных с места происшествия не скрывался, попыток скрыть труп и (или) другие следы совершенного преступления не предпринимал. Будучи доставленным в отдел внутренних дел, написал «явку с повинной», где указал, что пишет ее без физического или психического насилия. Тут же с участием назначенного ему защитника он был допрошен в качестве подозреваемого, полностью признал себя виновным в смерти при изложенных выше обстоятельствах, отметив лишь, что до случившегося потерпевшая «его довела» своим пьянством, употреблением наркотиков и занятием проституцией». При участии защитника с Суховым была осуществлена проверка показаний на месте, в ходе которой он свои «признательные» показания подтвердил. Через несколько дней ему было предъявлено указанное выше обвинение; в протоколе допроса он собственноручно отметил, что виновным себя признает полностью, однако от дачи показаний отказался на основании ст. 51 Конституции РФ. Остальные имеющиеся в материалах дела доказательства, подтверждая факт нанесения телесных повреждений и смерти потерпевшей на месте обнаружения ее трупа, не свидетельствовали о том, что преступление совершено именно обвиняемым.

При подготовке к суду в беседе наедине с защитником, вступившим в дело после окончания предварительного расследования, он высказал желание отказаться от предыдущих «признательных» показаний и в судебном заседании показать, что после распития спиртных напитков с потерпевшей и ее знакомым он ушел, а возвратившись на следующий день, обнаружил потерпевшую избитой и мертвой и спросил мнение своего защитника о целесообразности занятия в суде такой защитной позиции.

Для защитника возникла типичная ситуация принятия решения в условиях риска (здесь мы условно абстрагируемся от морально-этических проблем, связанных с корректировкой защитником позиции подзащитного). Обычно в подобных ситуациях, как уже говорилось, защитник принимает решение, основываясь лишь на своем профессиональном опыте и интуиции.

В данном же случае адвокат решил использовать для принятия столь ответственного для судьбы подзащитного решения ряд достаточно несложных методов теории статистических решений (раздела теории игр, изучающего принятие решений в условиях риска). Из ряда возможных моделей, описывающих степени определенности возможных исходов или последствий различных действий, к ситуации, в которой адвокат должен принять решение о рациональной защитной позиции, наиболее применима модель, формулируемая следующим образом: «Выбор решения при риске, если каждое действие приводит к одному из множества возможных частных исходов, причем каждый исход имеет вычисляемую или экспертно оцениваемую вероятность появления. Предполагается, что ЛПР (лицу, принимающему решение) эти вероятности известны или их можно определить путем экспертных оценок». С учетом этого возможные исходы (в виде грозящего наказания) принятия того или иного решения и степень вероятности наступления одного из них в первую очередь было предложено оценить экспертам.

Здесь следует оговориться, что возможные защитные позиции диаметрально противоположны с точки зрения адвоката:

– если в суде виновным себя не признает, его защитник обязан обосновывать лишь эту позицию, и, следовательно, не сможет активно апеллировать к смягчающим обстоятельствам совершения подсудимым преступления;

– если придерживается в суде своих первоначальных показаний, защита достаточно обоснованно может ставить вопрос о нахождении подсудимого в момент совершения преступления в состоянии аффекта либо, как минимум, признания факта аморального поведения потерпевшей как обстоятельства, смягчающего наказание в соответствии с п. 3 ч. 1 ст. 61 УК РФ.

В данном случае предлагаемые исходы в виде грозящего подзащитному наказания определялись на основе их усредненной оценки пятью судьями, четырьмя следователями и пятью адвокатами, причем экспертам было предложено учитывать как обстоятельства дела, доказанность, так и сведения о личностях обвиняемого и потерпевшей. При заполнении опросного листа умышленно в целях объективизации выводов не указывалось и не учитывалось должностное положение автора мнения. Полученные результаты рассматривались как усредненные.

В зависимости от того, какую линию защиты в суде изберет подсудимый, оценки распределились следующим образом:

1. Не признает себя виновным.

Вероятность исходов по наказанию:

а) 0 лет — вероятность до 10% (оправдание Сухова — оптимальный для защиты исход);

б) 12-13 лет — до 10%;

в) 15 лет (максимальное наказание по данной статье УК) — до 80%.

2. Виновным себя признает, поясняя, что преступление им совершено в состоянии аффекта.

Вероятность исходов по наказанию:

а) 2 года (максимальное наказание, предусмотренное ст. 113 УК; с учетом личности подсудимого — оптимальный для защиты исход) — до 10%;

б) 12-13 лет — до 80%;

в) 15 лет — до 10%.

Затем для оценки большей или меньшей полезности для обвиняемого выбора одной из названных выше его позиций по делу (в теории игр позиции именуют стратегиями) была использована также достаточно несложная модель решения задачи отыскания «математического ожидания выигрыша», которая рассчитывается как сумма произведений полученных величин.

Таким образом, при выборе первой стратегии в суде получаем следующее прогнозируемое наказание:

$f_1 = 0{,}1*0 + 0{,}1*13 + 0{,}8*15 = 13{,}3$ года;

при выборе второй стратегии:

$f_2 = 0{,}1*2 + 0{,}8*13 + 0{,}1*15 = 11{,}8$ года.

Следовательно, изменение подсудимым показаний в суде и отрицание им своей виновности в совершении инкриминируемого ему деяния с весьма высокой степенью вероятности повлечет назначение ему наказания как минимум на 1,5 года большего, чем грозящее ему наказание, рассчитанное по принципу минимакса.

С учетом данных предположений защитник не рекомендовал ему отрицать в суде его виновность, в то же время посоветовал ему акцентировать в своих показаниях обстоятельства, которые можно расценить как нахождение его в момент совершения преступления в состоянии аффекта, вызванного аморальным поведением потерпевшей. Подсудимый с рекомендациями своего защитника согласился.

Судом подзащитный признан виновным в совершении преступления, предусмотренного ч. 4 ст. 111 УК РФ, и приговорен к 10 годам лишения свободы. Осужденный был субъективно удовлетворен назначенным ему наказанием. Приговор не обжаловался.

Таким образом, алгоритм реализации предлагаемого метода принятия стратегического решения защитником состоит в следующем:

1) формулирование всех возможных стратегий поведения подзащитного в данных условиях риска;

2) определение (в усредненном виде) возможных реакций (исходов) на каждую стратегию подзащитного со стороны обвинения и суда и вероятности каждой из таких реакций с использованием метода экспертных оценок;

3) расчет минимального и максимального значений ожидаемой величины выигрыша в зависимости от использования подзащитным всех возможных стратегий и вероятностей всех возможных на них реакций.

Очевидно, что реализации подлежит та стратегия подзащитного, которая предполагает наибольшую величину выигрыша (в рассмотренном выше случае — наименьшая величина наказания, которое может быть назначено судом или хотя бы субъективно удовлетворительный для него в этом отношении результат).

Рассмотренный пример достаточно убедительно иллюстрирует надежность (хотя и не безусловность) и возможности использования данного метода для разрешения и других задач при принятии защитником решений в условиях риска, когда действия и решения противостоящей ему стороны можно лишь прогнозировать с большей или меньшей степенью вероятности.

С.В. Власова, *к.ю.н., профессор кафедры уголовного процесса Нижегородской академии МВД России, г. Нижний Новгород*

К ВОПРОСУ О МОДЕРНИЗАЦИИ ПОЛНОМОЧИЙ ПРОКУРОРА В КОНТЕКСТЕ ОБВИНИТЕЛЬНОЙ ВЛАСТИ

Понятие «обвинительная власть» тесно взаимосвязано с обвинением и уголовным преследованием и дает правильное представление о характере отношений между субъектами публичного уголовного преследования, в том числе к «субъективному публичному праву» на уголовный иск.

Одним из основателей учения о прокуратуре как обвинительной власти был Н.В. Муравьев, который на принадлежность прокуратуре власти обвинительной, которая находит свое проявление в уголовном преследовании и конкретно — в обвинении на суде [1, 2].

Концепция обвинительной власти нашла официальное признание в правительственных кругах царской России [3]. В Особых предписаниях уголовному судопроизводству, а именно в статье 4 указывалось, что обвинительная власть принадлежит прокурорам [4].

Об обвинительной власти писали виднейшие представители уголовно-процессуальной науки того времени: И.Я. Фойницкий, Н.А. Буцковский, А. Квачевский [5-7]. В наше время ее приверженцами выступили С.А. Шейфер[10], А.С. Александров, С.Д. Белов, Г.Н. Королев, М.П. Поляков, А.Д. Марчук и др. [8-16].

Профессор А.С. Александров обвинительную власть определяет как некую часть исполнительной власти, уполномоченную законодательством осуществлять противодействие

[10] У профессора С.А. Шейфера был специфический взгляд на организацию обвинительно-следственной власти, в которой равновелики величинами он считал прокурора и следователя. В целом он тяготел к следственной трактовке как обвинения, так и власти, уполномоченной на выполнение функции обвинения и осуществление уголовного преследования.

преступности в конкретной правовой форме и именно обвинительная власть наделяется правом на постановку вопроса перед властью судебной о применении уголовного закона к лицам, которые его нарушают. Он акцентирует внимание на уникальности обвинительной власти, указывая на ее феноменальность и факт того, что право ею распоряжаться принадлежит исключительно только прокурору [17]. Компетентные государственные органы, наделенные властью обвинительной, предъявляют требование суду о применении уголовного закона в форме наказания или иных мер уголовной ответственности, что суд в свою очередь и делает.

Ряд авторов об обвинительной власти говорят как о совокупности правоохранительных органов, их полномочиях по осуществлению уголовного преследования, деятельности, которую они осуществляют в рамках расследования и раскрытия преступлений, изобличения преступников, обоснования перед судом утверждения об их виновности и постановке вопроса о необходимости привлечения преступников к уголовной ответственности и возмещения причиненного вреда [18].

Н.А. Аменицкая говорит об обвинительной власти как о некоей структуре, выдвигающей и предъявляющей обвинение и впоследствии поддерживающей обвинение в суде [19].

Профессор В.А. Лазарева под обвинительной властью определяет права и возможности, которые принадлежат специальным государственным органам и должностным лицам по осуществлению уголовного преследования лиц, которыми были совершены преступления, с целью привлечь их к законной уголовной ответственности [20-21].

В отличие от профессора В.А. Лазаревой, Н.В. Буланова резко сужает круг государственных органов и должностных лиц, представляющих обвинительную власть до прокуратуры и Следственного комитета РФ [23]. Профессором А.С. Александровым круг государственных органов и должностных лиц, представляющих обвинительную власть, обозначается определением «агенты обвинительной власти» [24].

Профессор А.П. Кругликов говорит об исключительной принадлежности обвинительной власти прокурору [25]. З. Гатауллин и ряд других авторов отмечают, что прокурор выступает олицетворением обвинительной власти [26-28]. Т.В. Трубникова также отмечает, что обвинительная власть принадлежит исключительно прокурору [29]. Н.А. Колоколов отмечает тенденцию усиления обвинительной власти прокурора [30].

Но есть и другая — следственная трактовка обвинительной власти. Так, В.В. Пушкарев отмечает факт наделения следователя обвинительной властью [31]. В.В. Руновский говорит о превращении следователя в орган обвинительной власти [33]. Е.В. Тарибо обвинительную власть видит как некую резервную (дублирующую) систему, в том случае когда в объективности иных структур возникают обоснованные сомнения [33].

В.А. Середнев категорически возражает против наделения следователя статусом «обвинительной власти» [34]. Мы полностью разделяем эту точку зрения. Одним из важнейших шагов по перестройке правовой системы противодействия преступности состоит в лишении следователя обвинительной власти и вместе с тем власти применять уголовный закон.

Верным является только исковой подход к определению главенства обвинительной властью: только прокурор может выступать в суде с требованием вначале (1) об обоснованности предъявления обвинения, а затем (2) об удовлетворении уголовного иска (признании обвинения обоснованным) — это прокурор.

И.В. Круглов пишет: «Субъектом права на конкретный уголовный иск является прокурор в процессе; обвинительная же власть принадлежит в целом прокуратуре; прокуратуре должно принадлежать и право на наказание; отказ прокурора от преследования в целях экономии энергии и средств обвинения не ставит под сомнение желательность уголовного преследования самого по себе, но только в конкретном случае и только по причинам, указанным в законе; с вынесением приговора право на иск прокурора исчерпывается» [35].

Как пишет Е.Г. Васильева, уголовный материальный истец есть владелец пришедшего в ажитацию субъективного материального права на наказание, то есть государство. Уголовный процессуальный истец есть лицо, вчинившее формальное исковое прошение в пользу

субъективного материального права государства на наказание, находящегося в состоянии ажитации. Представитель уголовного процессуального истца — лицо, осуществляющее на основании договора или в силу закона права процессуального истца [36].

Значит, призванием обвинительной власти посредством обращения в суд выступает обязанность добиться в ходе своей деятельности реализации уголовной репрессии при помощи уголовно-правовых средств.

Обвинительная власть специфична в силу ее комплексного характера и распространения на уголовный процесс и ОРД, и права на ее осуществление принадлежат, как правило, правоохранительным органам, которые объединены под эгидой борьбы с преступностью и выполняют функцию по осуществлению уголовного преследования.

Аналогичного с мнением автора придерживается коллектив исследователей во главе с Н.А. Колоколовым, которые указывают на основное направление функционала обвинительной власти — добиваться реализации уголовной репрессии, поддержания упорядоченности общественной структуры уголовно-правовыми средствами [37].

В.А. Расчетов указывает, что представители органов обвинительной власти выступают в качестве субъектов уголовного преследования [38].

Сотрудники органа дознания, предварительного следствия и органов, осуществляющих ОРД, — все они выступают в качестве агентов обвинительной власти и уполномочены на уголовное преследование, главным образом в том, что касается выявления, расследования преступления, изобличения подозреваемого посредством получении обвинительных доказательств против него.

Публичные органы уголовного преследования должны выступать в качестве процессуального инструментария, посредством которого будут получены основания для предъявления обвинения, поддержания его в суде. Право же на предъявление обвинения перед судом и на поддержание государственного обвинения должно принадлежать только прокурору — субъекту дискреционных (диспозитивных) полномочий на обвинение.

По мнению автора, прокурор должен и может говорить свое окончательное слово по итогам проводимых проверок заявлений потерпевшего и оценки законности, а также он должен делать вывод о целесообразности начала публичного уголовного преследования субъекта предпринимательской деятельности.

Список литературы

1. Муравьев Н.В. Прокурорский надзор в его устройстве и деятельности: пособие для прокурорской службы. М., 1899. Т. 1. С. 26, 11.
2. Муравьев Н.В. Общие основания устройства и уголовной деятельности прокурорского надзора (1891–1892 г.) / Из прошлой деятельности. СПб., 1900. Т. 1. С. 534.
3. Сборник решений Правительствующего Сената по вопросам о привлечении к ответственности должностных лиц судебного ведомства за неправильные действия по службе / сост. Н. Рычков. СПб., 1879. С. 75.
4. Рамазанов Т.Б. Концепция судебно-правовой реформы в Российской Федерации: результаты и перспективы реализации // Вестник Дагестанского государственного университета. Серия 3: Общественные науки. 2014. № 2. С. 18-25.
5. Фойницкий И.Я. Курс уголовного судопроизводства: в 2 томах. 1912. Т. 2. С. 33.
6. Буцковский Н.А. О деятельности прокурорского надзора вследствие отделения обвинительной власти от судебной. СПб., 1867. С. 8.
7. Квачевский А. Об уголовном преследовании, дознании и предварительном исследовании преступлений по судебным уставам 1864 года: Теоретическое и практическое руководство. Ч. 3. Вып. 1-2. СПб., 1869. С. 12-15, 399.
8. Шейфер С.А. Досудебное производство в России. Этапы развития следственной, судебной и прокурорской власти. М.: Норма; ИНФРА-М,2014. С. 111-136.

9. Королев Г.Н. О возможностях влияния прокурора на формирование государственного обвинения в ходе досудебного производства // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия Право. 2018. № 4. С. 126-130.

10. Марчук А.Д. Обвинительная власть в современной России // Вестник Волжской государственной академии водного транспорта. 2014. № 40. С. 18-21.

11. Александров А.С. К вопросу о создании единого Следственного комитета. Россия — родина слонов? // Вестник СГАП. 2010. № 6. С. 17-21.

12. Александров А.С. К вопросу о реформировании следственного аппарата и правовой формы досудебного производства по уголовному делу // Вестник Сибирского юридического института МВД России. 2011. № 1 (9). С.12-19.

13. Горюнов В.Ю., Шерстнев В.Б. Учение об обвинительной (следственной) власти: Самарский и Нижегородский варианты // Юридический вестник Самарского университета. 2017. №4. С. 110-112.

14. Александров А.С., Кухта А.А., Марчук А.Д. Обвинительная власть. Уголовный иск // Уголовный процесс: Проблемные лекции / под ред. В.Т. Томина, И.А. Зинченко. М.: Юрайт, 2013. С. 227.

15. Ковтун Н.Н. Формирование государственного обвинения как самостоятельная стадия уголовного судопроизводства России // Журнал российского права. 2019. № 9. С. 123-137.

16. Королев Г.Н. Прокурорское уголовное преследование в российском уголовном процессе. М., 2006. С. 35-36.

17. Александров А.С. Забыть Фойницкого? // Стратегии уголовного судопроизводства: сб. материалов Научной конференции к 160-й годовщине со дня рождения И.Я. Фойницкого. М.: РАП, 2008. С. 23.

18. Уголовный процесс. Проблемные лекции / под ред. В.Т. Томина, И.А. Зинченко. М.: Юрайт, 2013. С. 82.

19. Аменицкая Н.А. Организация и деятельность обвинительной власти в правовом государстве // Реформы 1864 года в теории и практике российского конституционализма: история и современность (к 150-летию Земской и Судебной реформ 1864 г.): материалы Международной научно-практической конференции, 10–12 апреля 2014 г. / отв. ред. В.Н. Корнев, Н.А. Петухов, В.Е. Сафонов. М.: РГУП, 2014. С. 31-36.

20. Лазарева В.А. Обвинительная власть: понятие, субъекты, формы реализации // Уголовное судопроизводство. 2012. № 1. С. 14-18.

21. Лазарева В.А. Понятие обвинительной власти // Теория уголовного процесса: состязательность. М.: Юрлитинформ, 2013. Ч. 1. С. 137-146.

22. Бедняков И.Л. Досудебное производство: между прошлым и будущим // Уголовное судопроизводство. 2018. № 4. С. 24-30.

23. Буланова Н.В. Прокурор в уголовном судопроизводстве: пути совершенствования процессуального статуса прокурора // Уголовное право. 2017. № 4. С. 33-36.

24. Александров А.С. Институт следственной власти в России: краткая история возникновения, развития и дегенерации // Вестник Нижегородской академии МВД России. Юридическая наука и практика. 2016. № 2 (34). С. 407.

25. Кругликов А.П., Бирюкова И.А. Процессуальное руководство прокурором уголовным преследованием от имени государства – принцип уголовного судопроизводства // Законность. 2019. № 2. С. 38-42.

26. Гатауллин З. Выработка позиции по уголовному делу и организация государственного обвинения // Законность. 2008. №11. С. 18-22.

27. Федяков Н.Н. Особенности участия группы прокуроров в прениях сторон // Российский судья. 2018. № 11. С. 22-25.

28. Крюков В.Ф. Уголовное преследование в судебном производстве: уголовно-процессуальные и надзорные аспекты деятельности прокурора. Курск, 2010. С. 138.

29. Трубникова Т.В. Пределы упрощения уголовного процесса // Актуальные проблемы российского права. 2015. № 12 (61). С. 131-139.

30. Колоколов Н.А. Последние новеллы УПК РФ баланс обвинительной власти стабилизируется // Уголовное судопроизводство. 2009. № 2. С. 25-33.

31. Пушкарев В.В. Толкование функции уголовного преследования (обвинения) в решениях Европейского суда по правам человека, европейской комиссии по правам человека, Конституционного Суда Российской Федерации как предпосылка ее нормативного выражения в процессуальном статусе следователя // Международное уголовное право и международная юстиция. 2016. № 4. С. 15-17.

32. Руновский А.В. Процессуальная роль следователя в уголовном суде // Российский следователь. 2012. № 2. С. 13-16.

33. Тарибо Е.В. Судебный конституционный нормоконтроль: осмысление российского опыта: монография. М.: Норма, 2018. С. 136.

34. Середнев В.А. К вопросу о роли и статусе следователя в российском уголовном процессе // Российский следователь. 2017. № 1. С. 7-10.

35. Круглов И.В. Уголовный иск и механизм его доказывания: дис. ... канд. юрид. наук. Н. Новгород, 2001. С. 116.

36. Васильева Е.Г. Уголовный процесс: догматико-аксиологическое исследование: монография. М.: Юрлитинформ, 2013. С. 71, 511, 512.

37. Уголовное судопроизводство: теория и практика / под ред. Н.А. Колоколова. Том. 3. М.: Юрайт, 2018. С. 152.

38. Расчётов В.А. Об органах обвинительной власти в системе государственного механизма // Полицейская и следственная деятельность. 2016. № 4. С. 71-80.

О.А. Грачёва, *к.ю.н., доцент кафедры прокурорского надзора и криминологии Саратовской государственной юридической академии, г. Саратов*

К ВОПРОСУ ОБ УНИФИКАЦИИ ПОВОДОВ К ПРОВЕДЕНИЮ ПРОКУРОРОМ ПРОВЕРКИ В ДОСУДЕБНОМ ПРОИЗВОДСТВЕ ПО УГОЛОВНЫМ ДЕЛАМ

Федеральный закон «О прокуратуре Российской Федерации» и Уголовно-процессуальный кодекс РФ не содержат детерминации как понятия прокурорская проверка исполнения закона органами предварительного расследования, так и перечень поводов для ее проведения. Так, под поводом в его общем смысле следует понимать обстоятельство, используемое с какой-нибудь целью, причина, предлог [1].

Поводом именно для осуществления прокурором проверки, как правило, является поступившая в органы прокуратуры информация о фактах нарушения закона [2]. Подобную информацию могут содержать поступившие в органы прокуратуры письменные заявления, а именно жалобы, запросы, обращения, или переданные устно на личном приеме (п.п. 1.9, 2.1 Инструкции № 45) [3]. Такая информация может быть самостоятельно обнаружена прокурорами в Интернете, газетах, журналах и других средствах массовой информации [4].

Что касается проверок, проводимых прокурором в порядке общего надзора, Конституционный Суд РФ в своем Постановлении № 2-П от 17.02.2015 изложил дополнительные требования к поводам проведения прокурорских проверок: эти сведения должны указывать на признаки нарушений законов, которые нельзя подтвердить или опровергнуть в ходе межведомственного взаимодействия с соответствующим надзирающим государственным органом, причем расширение пределов проверки допустимо в случаях, когда в ходе ее проведения выявляются признаки новых нарушений, оценка которых также не может быть дана вне мероприятий собственно прокурорского надзора. В связи с этим проверка прокурора может быть

признана незаконной, если прокуратура не докажет наличие достаточности поводов для проведения проверки и не обоснует невозможность проведения проверки контролирующими органами.

По большей части, в уголовном процессе осуществление прокурором проверки исполнения закона связано с совершением должностными лицами органов дознания и предварительного следствия процессуально значимых действий либо принятия решений (например, прием заявления о совершенном или готовящемся преступлении, вынесение постановления о возбуждении, либо отказе в возбуждении уголовного дела и т.д.).

Поводы же к проведению прокурором проверок в досудебном производстве имеют определенную специфику, вытекающую из того, что: 1) прокурорский надзор в сфере уголовного судопроизводства должен осуществляться вне зависимости от наличия информации о фактах нарушения закона в деятельности следователя либо дознавателя; 2) прокурор является непосредственным участником уголовно-процессуальной деятельности [5, 6].

Возлагая на прокурора функцию надзора за исполнение законов органами предварительного расследования, уголовно-процессуальный закон подразумевает, что осуществление прокурорских проверок исполнения закона органами расследования должно являться постоянным. В приказах Генеральной прокуратуры РФ прямо предписывается осуществлять прокурорские проверки исполнения закона в ходе предварительного расследования систематически.

Исходя из этого, можно сказать, что для проведения прокурором проверок в сфере уголовного судопроизводства существует особый повод — требования закона о непрерывном осуществлении надзора прокурора за процессуальной деятельностью следователя и дознавателя.

Разумеется, это не умаляет наличия иных поводов для проведения прокурорских проверок в досудебном производстве. Прокурорская проверка при осуществлении досудебного производства может быть связана с совершением должностными лицами органов дознания и предварительного следствия процессуально значимых действий либо принятием решений.

Анализ действующего законодательства позволяет выделить следующие поводы к проведению прокурором проверок в досудебном производстве по уголовным делам:

– направление прокурору органами дознания и следствия копий постановлений о возбуждении уголовного дела, отказе в возбуждении уголовного дела; приостановлении и прекращении уголовных дел, копий иных решений, принимаемых в ходе предварительного расследования;

– осуществление дознавателем процессуально значимых действий и решений, требующих согласия прокурора (п. 4, 5, 6 ч. 2 ст. 37 УПК РФ);

– требования закона о систематическом проведении проверок законности процессуальной деятельности следователя и дознавателя (п. 1, 3, 4, 6, 10 ч. 1 ст. 37 УПК РФ);

– данные о нарушениях уголовно-процессуального законодательства, допущенных в ходе предварительного расследования, полученные прокурором из иных источников;

– принесение жалобы участниками процесса и иными лицами на действия (бездействие) и решения дознавателя, начальника подразделения дознания, начальника органа дознания, следователя, руководителя следственного органа и нижестоящего прокурора;

– поступление прокурору ходатайства подозреваемого (обвиняемого) и постановления следователя о заключении досудебного соглашения о сотрудничестве (ст. 317.2 УПК РФ);

– поступление к прокурору уголовного дела с обвинительным заключением, актом, постановлением.

Исходя из вышесказанного, поводом для проведения прокурорской проверки в досудебном производстве следует считать требования закона либо информацию, поступившую прокурору, которые служат обязательной предпосылкой для осуществления прокурорами проверок соблюдения законодательства органами предварительного расследования.

Представляется необходимым закрепить в уголовно-процессуальном законодательстве унифицированные поводы к осуществлению прокурором проверок в досудебных стадиях уголовного судопроизводства.

Соответствующая система поводов для проведения прокурором проверок в сфере уголовного судопроизводства будет одновременно выступать в качестве системы гарантий прав личности и гарантий для органов предварительного расследования от необоснованного вмешательства в их деятельность.

Список литературы

1. Ушаков Д.Н. Толковый словарь русского языка. М.: Альта-Принт, 2005. URL: http://dic.academic.ru/dic.nsf/ushakov/940962 (дата обращения: 12.11.2019).
2. Приказ Генеральной прокуратуры РФ от 07.12.2007 г. № 195 (ред. от 21.06.2016) «Об организации прокурорского надзора за исполнением законов, соблюдением прав и свобод человека и гражданина» // Законность. 2008. № 3.
3. Приказ Генеральной прокуратуры РФ от 30.01.2013 № 45 (ред. от 21.09.2018) «Об утверждении и введении в действие Инструкции о порядке рассмотрения обращений и приема граждан в органах прокуратуры Российской Федерации» // Законность. 2013. № 4.
4. Приказ Генеральной прокуратуры РФ от 18.07.2013 № 295 (ред. от 30.06.2014) «Об утверждении и введении в действие Временной инструкции по учету работы прокуроров в органах прокуратуры Российской Федерации» // Законность. 2013. № 5.
5. Приказ Генеральной прокуратуры РФ от 26.12.2017 № 33 «Об организации прокурорского надзора за процессуальной деятельностью органов дознания» // Законность. 2017. № 5.
6. Приказ Генеральной прокуратуры РФ от 28.12.2016 № 826 «Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия» // Законность. 2017. № 3.

Н.Н. Ильин, *к.ю.н., заведующий кафедрой судебно-экспертной и оперативно-разыскной деятельности Московской академии Следственного комитета Российской Федерации, г. Москва*

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАБОТЕ С ЭЛЕКТРОННЫМ ОБОРУДОВАНИЕМ ТРАНСПОРТНЫХ СРЕДСТВ

Осмотр места происшествия по делам о нарушениях правил безопасности движения и эксплуатации транспорта является первоначальным следственным действием, общие положения которого довольно детально описаны в специальной литературе.

Для того чтобы провести качественно осмотр места происшествия по делам о транспортных происшествиях, необходимо сформировать расширенную следственную группу с включением в нее нескольких следователей (с определением старшего группы), следователя-криминалиста, специалиста-криминалиста экспертно-криминалистического подразделения МВД России, судебно-медицинского эксперта, сотрудников полиции (для обеспечения охраны места происшествия), представителей Межгосударственного авиационного комитета (по делам об авиационных происшествиях зарегистрированных воздушных судов), представителей Ространснадзора Минтранса России (по делам о происшествиях на железнодорожном, внутреннем водном и морском транспорте), спасателей МЧС России, специалистов в сфере определенного вида транспорта (из научно-исследовательских институтов или образовательных учреждений в сфере транспорта).

В связи с тем, что характер повреждений, положение транспортных средств и объектов транспортной инфраструктуры, следы, образовавшиеся в результате происшествия, трудно

поддаются описанию, целесообразно в ходе осмотра места происшествия привлекать специалистов и применять технические средства фотосъемки, видеозаписи с составлением подробных схем происшествия и осматриваемой территории.

В соответствии с действующим уголовно-процессуальным законодательством участие специалиста обязательно лишь при осмотре трупа (ч. 1 ст. 178 УПК России). В остальных случаях, как отмечает С. А. Вазюлин, привлечение специалиста для участия в производстве следственного действия является правом следователя, а не его обязанностью [1, с. 69-81]. Ввиду того, что осмотр места происшествия по делам о нарушении правил безопасности движения и эксплуатации железнодорожного, воздушного, морского и внутреннего водного транспорта и метрополитена требует специальных знаний в различных областях техники, представляется, что участие специалиста является обязательным. Это, в свою очередь, будет способствовать качественному проведению осмотра места происшествия, своевременному назначению и эффективному производству соответствующей транспортно-технической судебной экспертизы.

Цели привлечения специалиста определены в ч. 1 ст. 58 УПК России, а его роль в процессуальных действиях довольно подробно описана в различных источниках [2, 3]. Применительно к рассматриваемой теме участие специалистов при производстве осмотра места происшествия по делам о нарушениях правил безопасности движения и эксплуатации транспорта должно разграничиваться в зависимости от решаемых ими задач.

Специалисты в сфере транспорта оказывают следователю содействие для обнаружения, закрепления и изъятия информации с технических средств управления транспортным средством, объективного контроля (например, бортовых самописцев и радиоактивных датчиков по делам об авиапроисшествиях), а также различных документов по технической эксплуатации транспортного средства (приказы, инструкции, правила, регламенты и т. д.), содержащие сведения о техническом состоянии транспортного средства (диагностические карты, акты проверок и т.д.), сведения о лице, управляющем транспортным средством (летная книжка пилота, судовая роль и т.д.), дополнительные сведения об обстоятельствах транспортного происшествия (например, метеорологическая документация).

Уровень развития науки и техники на сегодняшний день позволяет автоматизировать многие процессы управления судном. В частности, с помощью морской электронной картографической навигационной информационной системы (ЭКНИС) возможно осуществлять отображение карт и места судна, вести судовой журнал, прокладку трассы движения и осуществлять контроль отклонений от заданного маршрута в электронном формате [4, с. 74-79].

Определение местоположения и курса судна является исключительно важным при проверке сообщения о преступлении на водном транспорте. Помимо традиционных для судоходства способов фиксации местоположения и курса судна, на сегодняшний день существует возможность высокоточного определения данных параметров с помощью спутниковых систем. К широко используемой глобальной американской спутниковой системе навигации GPS в настоящее время присоединились российская навигационная система ГЛОНАСС, европейская Galileo, китайская BeiDou и французская DORIS. Установка на судне систем спутникового слежения является общемировой практикой, одобренной Международной морской организацией. В 2008 году Постановлением Правительства Российской Федерации № 641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS» для судов морского, внутреннего речного и смешанного плавания введено обязательное оснащение аппаратурой спутниковой навигации, позволяющей непрерывно отслеживать и анализировать данные, включающие временные и пространственные координаты судна, его курс как сведения, необходимые для обеспечения безопасности судоходства.

При расследовании преступлений, связанных с нарушением правил дорожного движения и эксплуатации транспортных средств, обязательному выяснению подлежит причинно-следственная связь между нарушением правил дорожного движения или эксплуатации транспортных средств и причинением тяжкого вреда здоровью, либо смерти по неосторожности.

Важную роль в изучении обстоятельств аварии и реконструкции происшедшего события способны сыграть сведения, которые возможно получить в результате исследования блоков управления подушками безопасности с функцией памяти (ими сегодня оснащено большинство современных автомобилей) [5, с. 165-170; 6, с. 160-164]. Блок управления подушками безопасности оснащен устройством, называемым «регистратор данных о событии» (EDR), которое фиксирует данные, поступающие на него перед столкновением (опрокидыванием) и непосредственно в процессе аварии. EDR при аварии или при условиях, приближенных к аварии, может записывать (в зависимости от производителя устройства) до 60 аналоговых и 30 дискретных («включено/выключено») параметров движущегося транспортного средства, многие из которых являются криминалистически значимыми. Среди таких параметров в течение некоторого временного интервала до столкновения (опрокидывания) могут фиксироваться:

– состояние защелки замка ремней безопасности водителя и пассажира, находившегося на переднем сиденье;

- положение рычага переключения передач;
- степень нажатия педали акселератора, тормоза;
- обороты двигателя;
- показания спидометра;
- повороты рулевого колеса;
- время включения систем экстренного торможения;
- сигналы от датчиков света и дождя [7, с. 169-174].

В момент столкновения (опрокидывания) может фиксироваться время выдачи команды на срабатывание подушек безопасности.

Информация в электронной памяти EDR непрерывно обновляется. При этом объем памяти некоторых моделей EDR позволяет сохранить посекундно регистрируемые данные за период времени, охватывающий 5 секунд до момента столкновения (опрокидывания), и заканчивая 1-й секундой после него.

В связи с изложенным Главным управлением криминалистики Следственного комитета Российской Федерации рекомендуется при осмотре места происшествия и автомобилей участников ДТП необходимо незамедлительно изымать блок управления подушками безопасности для последующего его технического исследования с целью установления указанных выше данных об автомобиле [8].

Таким образом, при работе с новейшим электронным оборудованием транспортных средств необходимо придерживаться статьи 164.1 УПК России, предусматривающей обязательное участие специалиста при осмотре и изъятии информации с электронных носителей.

Список литературы

1. Вазюлин С.А. Актуальные вопросы производства осмотра места происшествия по уголовным делам о нарушении правил безопасности движения и эксплуатации железнодорожного транспорта // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: материалы Всероссийской научно-практической конференции (27 мая 2016 года). Орел: Изд-во Орловского юридического института МВД России имени В.В. Лукьянова, 2016. С. 69-81.

2. Участие специалиста-криминалиста в следственных действиях: курс лекций / Р.Ю. Трубицын, В.Н. Хрусталев. Саратов: Изд-во Сарат. юрид. ин-та МВД России, 2002. 212 с.

3. Участие специалиста в процессуальных действиях: учебник / А.М. Зинин, А.И. Семикаленова, Е.В. Иванова; под общ. ред. А.М. Зинина. М.: Проспект, 2016. 288 с. URL: http://www.studentlibrary.ru/book/ISBN9785392203772.html (дата обращения: 03.02.2020).

4. Вовченко Н.В. Роль электронных информационных систем в развитии средств навигации // Научные труды Дальневосточного государственного технического рыбохозяйственного университета. Т. 35. 2015. С. 74-79.

5. Головчанский А.В. Использование данных электронных систем безопасности и управления транспортных средств при расследовании дорожно-транспортных преступлений // Вестник Воронежского института МВД России. 2014. № 3. С. 165-170.

6. Кривицкий А.М., Залужный Г.И., Залужная О.Г., Засимович Е.А. Диагностирование электронных систем автомобиля // Вопросы криминологии, криминалистики и судебной экспертизы. 2017. № 1 (41). С. 160-164.

7. Бессонов А.А. Информация о типичных следах преступления как элемент его криминалистической характеристики // Гуманитарные исследования. № 4 (52). 2014. С. 169-174.

8. О проведении компьютерно-технических исследований при расследовании дорожно-транспортных происшествий с человеческими жертвами (методические рекомендации). М.: Главное управление криминалистики (Криминалистический центр), 2014.

В.П. Корж, *д.ю.н., профессор кафедры уголовного процесса, криминалистики и экспертологии Харьковского национального университета внутренних дел МВД Украины, почетный работник прокуратуры Украины, г. Харьков*

КОРРУПЦИОННЫЕ ТЕХНОЛОГИИ ОРГАНИЗОВАННОЙ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ЭКОНОМИКИ

Организованная экономическая преступность проникла во все базисные отрасли и сферы экономики, приобрела масштабы, представляющие угрозу национальной безопасности Украины. Наиболее криминализированными, пораженными коррупцией являются финансовая, банковская, внешнеэкономическая сфера, энергообеспечения, предприятия металлургической, нефтеперерабатывающей, химической промышленности, агропромышленного комплекса и сфера земельных правоотношений. Организаторы теневого бизнеса, как правило, лидеры организованной преступной деятельности, посредством коррупции, политического лоббизма незаконно присвоили значительную часть государственной собственности, проникли в политические, государственные институты, средства массовой информации, оказывают влияние на формирование законодательной, исполнительной и судебной власти. Они владеют огромным криминальным капиталом, многие — и депутатским мандатом, лоббируют принятие законов в своих корыстных интересах. В частности, принятие Закона № 4025 от 15.11.2011 о декриминализации 26 составов экономических преступлений в Уголовном кодексе Украины, Закона № 221–VII от 18.04.2013 о декриминализации взяточничества, Закона № 101-IX от 21.09.2019 о декриминализации фиктивного предпринимательства, также других законов, в том числе об упразднении контрольно-ревизионной службы, надзорных функций прокурора, спецподразделений по борьбе с организованной преступностью, подразделений по борьбе с экономическими преступлениями, органов дознания.

Полагаем, что лидеры организованных преступных групп (организаций), используя технологию коррупционного лоббирования, ликвидировали в Украине не только правовую базу противодействия экономической преступности и коррупции, но и государственные органы, призванные ей противодействовать.

Негативное влияние на экономику, политику, управление, социальную и правовую сферы, международные отношения и гражданское правосознание оказывает коррупция. К сожалению, антикоррупционная политика, антикоррупционное законодательство Украины неадекватно размерам и темпам роста коррупции в стране. В уголовном законодательстве отсутствует понятие коррупционного преступления. Декриминализация взяточничества является серьезной ошибкой законодателя и это негативно влияет на реальное противодействие коррупции в высших органах государственной власти, практику расследования коррупционных преступлений. Большинство украинских исследователей в своих работах верно указывают

на то, что получение взятки, дача взятки относятся к коррупционным преступлениям [1, с. 28; 2, с. 168]. Полагаем, что в уголовном законодательстве Украины необходимо криминализировать наиболее распространенные коррупционные преступления — дачу взятки и получение взятки.

В юридической литературе представлено несколько научных подходов к определению уголовно-правового понятия коррупции, видам коррупционных преступлений. Так, П.Н. Панченко рассматривает коррупцию как систематически совершаемое организованное взяточничество [3, с. 64], тогда как А.А. Аслаханов, В.С. Комиссаров и другие исследователи отмечают, что взяточничество — это распространенный и опасный вид коррупции [4, с. 81; 5, с. 4]. Коррупцию в широком аспекте рассматривает А.И. Мизерий как социальное явление [6, с. 13]. Можно согласиться с мнением А.И. Гурова в том, что коррупция является обязательным признаком организованной преступности. Под коррупцией он понимает не просто дачу и получение взятки за предоставление любой услуги, постоянную связь должностных лиц с организованными преступниками [7, с. 205]. Эту позицию разделяет О.В. Филимонов, который указывает, что в ряде случаев организованная преступность и коррупция связаны настолько тесно, что это дает основание ученым выделять коррупцию как один из признаков организованной преступности [8, с. 36].

По данным правовой статистики органов прокуратуры Украины, каждое шестое преступление в сфере экономики связано с коррупцией, поэтому она является основным признаком организованной преступной деятельности. Следует согласиться с Н.П. Яблоковым в том, что «сведения о механизме преступления в криминалистической характеристике представляют собой систему данных, описывающих главным образом временной, последовательный, динамический порядок связи отдельных этапов, обстоятельств, факторов подготовки, совершения и сокрытия следов преступления, позволяющих воссоздать технологическую картину процесса его совершения» [9, с. 17]. Организаторы преступного бизнеса заранее продумывают: выбор сферы, предмета преступного посягательства, изощренные коррупционные технологии, способы совершения экономических преступлений и способы сокрытия их следов, способы обеспечения безопасности преступной деятельности с помощью коррупционных связей. Они стремятся иметь «своих» чиновников, как в органах государственной власти, управления, так и прикрытие («крышу») в правоохранительных органах.

Системный анализ материалов оперативно-розыскной деятельности и следственной практики позволил сделать вывод о том, что при совершении экономических преступлений лидеры организованных групп делают ставку на подкуп должностных лиц разных уровней государственной власти и управления, местного самоуправления, финансовых, контрольных, правоохранительных органов. Коррупционные связи с политическими деятелями, руководством «скамеечных», «заказных» (бизнесом) партий, должностными лицами высших органов государственного управления, полиции, прокуратуры, таможни, службы безопасности, государственной фискальной службы обеспечивают им коррупционные услуги в процессе реализации преступных планов на приоритетных направлениях экономики. Коррумпированные должностные лица обеспечивают:

– *коррупционное содействие членам ОПГ в выборе* сферы, предмета преступного посягательства;

– *коррупционное покровительство* при подготовке, совершении преступления и сокрытии его следов;

– *коррупционное обеспечение* эффективности и безопасности организованной преступной деятельности, легализации криминальных доходов;

– *коррупционный протекционизм* при создании фиктивных фирм, получении кредитов, льгот, других преимуществ;

– *коррупционное вмешательство* в деятельность подчиненных должностных лиц, предприятий, организаций с целью оказания содействия преступному бизнесу, в том числе *«келейному проведению приватизации, акционирования и залоговых аукционов»* [10, с. 77];

– *коррупционное лоббирование* интересов коммерческих криминальных структур, теневого производства при принятии законов, управленческих решений, иных нормативных актов;

– *коррупционное противодействие* выявлению оперативными органами признаков экономического преступления, расследованию преступной деятельности организованных групп — «быстрое срабатывание защитных средств, характерных именно для преступной организации, имеющей коррупционные связи, группы безопасности, своих адвокатов (угрозы следователю и его близким, давление на следствие разных влиятельных лиц; подключение к участию в расследовании наиболее подготовленных адвокатов, опережающие расследование действия организованного преступного формирования и пр.)» [11, с. 26].

Таким образом, коррупционная технология позволяет организаторам преступного бизнеса планировать и успешно реализовывать преступные планы на приоритетных направлениях экономики. Организаторы преступного бизнеса с целью получения *коррупционных услуг* устанавливают *коррупционные связи* с должностными лицами властных, управленческих, фискальных, таможенных органов, полиции, прокуратуры, СБУ, которые за *коррупционное вознаграждение* («откат») обеспечивают реализацию *коррупционных схем* в интересах организованной группы, эффективность и безопасность совершаемой преступной акции в сфере экономики. Следует отметить, что лидеры организованных групп с коррупционными связями совместно с коррумпированными чиновниками разрабатывают коррупционные схемы: *инвестирования* коммерческих структур за бюджетные средства; *присвоения* бюджетных средств, имущества государственных, коммунальных предприятий; *криминального банкротства* государственных предприятий с целью их приватизации; *незаконной приватизации* имущества государственных, коммунальных предприятий*; незаконных внешнеэкономических* операций с целью последующего получения бюджетных средств за налог на добавленную стоимость; *незаконных* финансовых, хозяйственных, банковских операций с бюджетными средствами*; неправомерного размещения* ценных бумаг без регистрации их выпуска*; легализации* преступных доходов путем введения их в законную экономику, политические институты, средства массовой информации; *неправомерного получения* дотаций, субвенций, кредитов, льгот и других преимуществ.

Структурным компонентом коррупционных технологий экономических преступлений являются *коррупционные «откаты»* (вознаграждения). В практической деятельности субъектов предпринимательства «откат» рассматривается как форма вознаграждения коррумпированным должностным лицам, то есть разновидность взятки чиновнику, который обеспечивает безопасность преступной акции и полное и успешное ее завершение. Размер «отката» устанавливается по договоренности сторон (7-50%). Изучение следственной практики позволяет сделать вывод о том, что члены ОПГ коррупционные «откаты» выплачивают коррумпированным должностным лицам органов государственной фискальной службы за безопасность преступных акций, неприкосновенность членов ОПГ, предотвращение проведения налоговых проверок или содействие их благоприятному завершению. Организаторы преступного бизнеса предоставляли *коррупционные «откаты»* должностным лицам банковских учреждений за выдачу банковских кредитов по фиктивным документам. *Коррупционное содействие* должностных лиц банковских учреждений (при наличии правильно оформленных кредитных документов) состоит в рекомендации на заседании кредитного совета банка выдать кредит, если перед заседанием совета была оговорена сумма «отката». Она может составлять от 1 до 20% запрашиваемой суммы, с учетом цели получения кредита, условий кредитования, процентной ставки, легальности бизнеса, использования фиктивных структур и т.д. Организаторы преступного бизнеса выплачивают коррупционные «откаты» политическим деятелям, должностным лицам министерств, ведомств, департаментов, управлений, чиновникам всех уровней исполнительной власти за реализацию коррупционных схем, содействие развитию и расширению преступного бизнеса, обеспечение безопасности преступной деятельности. Некоторые коррумпированные должностные лица министерств, ведомств, члены правительства при проведении приватизации, продажи государственной собственности иностранным компаниям

завуалировано устанавливали суммы коррупционного «отката» в договорах. Так, при продаже завода «Криворожсталь» сумма коррупционного отката составила 20% от стоимости завода (240 млн долл. США).

Таким образом, в условиях рыночных основ хозяйствования организованные группы с *коррупционными связями* получают *коррупционные услуги,* используют *коррупционные* схемы и беспрепятственно совершают экономические преступления. Организаторы ОПГ выплачивают *коррупционное вознаграждение* (откат) коррумпированным должностным лицам государственных органов за реализацию *коррупционных схем*, оказание *коррупционных услуг,* полное и успешное завершение преступных финансовых и хозяйственных акций на приоритетных направлениях экономики, обеспечение безопасности организованной преступной деятельности.

Вышеизложенное позволяет рассматривать коррупционную технологию экономического преступления как совокупность действий, операций, приемов, методов организаторов преступного бизнеса, направленных на установление *коррупционных связей* с должностными лицами государственных органов власти и управления, разработку *коррупционных схем* с целью реализации преступных акций и *сокрытии* их следов, *оплаты* коррупционных вознаграждений («откатов») за *коррупционное содействие или бездействие, коррупционное лоббирование, коррупционный протекционизм, коррупционное противодействие, коррупционное вмешательство, коррупционное покровительство* и другие неправомерные преимущества.

Криминалистические знания коррупционной технологии организованной преступной деятельности в сфере экономики необходимы следователю, прокурору, оперативному работнику для решения задач выявления, раскрытия и расследования экономического преступления, совершенного организованной группой с коррупционными связями.

Список литературы

1. Мельник М.И. Корупція: сутність, поняття, заходи протидії: монографія. К.: Атіка. 2001. С. 304.
2. Лукомський В.С. Кримінальна відповідальність за дачу хабара та посредництіо в хабарництві: афтореф. дис…. канд. юрид. наук:12.00.08./ Інстит. Держ. І права АН України К., 1996. С. 28.
3. Панченко П.Н. Да не дрогнет рука... Практические советы тем, кто дает и берет взятки. Книга для людей деловых и просто думающих. Нижний Новгород,1995. С. 65.
4. Аслаханов А.А. Проблемы уголовно-правовой борьбы со взяточничеством // Государство и право. 1993. № 4. С. 81-88.
5. Комиссаров В. С. Уголовно-правовые аспекты борьбы с коррупцией // Вест. Моск. ун-та. Сер. 11. Право. 1993. № 1. С. 28.
6. Мизерий А.И Уголовно-правовые и криминологические аспекты борьбы с коррупцией в органах власти: автореф. дисс… канд. юрид. наук: 12.00.08. Нижнегород. юрид. ин-т МВД РФ, 2000. С. 29.
7. Гуров А.И. Профессиональная преступность: прошлое и современность. М.: Юридическая литература, 1990. С. 304.
8. Филимонов О.В. Социально-правовой контроль — направление борьбы с коррупцией // Коррупция в России: состояние и проблемы: материалы научно-практической конференции. М.: Московский институт МВД России, 1996. С. 36-43.
9. Яблоков Н.П. Криминалистика: учеб. для вузов. М.: Норма, 2000. С. 371.
10. Лунеев В.В. О проблемах уголовной политики и криминальных реалий в России // Вестник Акдемии следственного комитета РФ. 2015. № 3. С. 71-83.
11. Основы борьбы с организованной преступностью: монография / под ред. В.С. Овчинского, В.Е. Эминова, Н.П. Яблокова. М., 1996. С. 267.

Н.А. Куркова, *к.ю.н, доцент кафедры уголовного процесса, криминалистики и правовой информатики Балтийского федерального университета им. И. Канта, г. Калининград*
О.А. Макарова, *к.ю.н., доцент кафедры уголовного процесса, криминалистики и правовой информатики Балтийского федерального университета им. И. Канта, г. Калининград*

ПРОБЛЕМА ОЦЕНКИ ПОКАЗАНИЙ СВИДЕТЕЛЕЙ В СУДЕБНОМ СЛЕДСТВИИ

На сегодняшний день определенный интерес среди ученых и практиков вызывают вопросы участия свидетеля в расследовании преступлений. Как отмечает О.А. Славгородская, обращение к проблемам изучения личности свидетеля связано с отсутствием единого, научно разработанного криминалистического учения о личности свидетеля [1, с. 316]. С другой стороны, на практике возникают сложности тактического и методического характера, связанные с получением достоверных свидетельских показаний.

Как показал анализ уголовных дел, один из недостатков следственной практики — это бессистемное изучение личности свидетеля, что приводит к односторонности и неполноте его исследования. В связи с этим некоторые обстоятельства уголовного дела остаются невыясненными. Восполнить недостатки предварительного расследования в какой-то степени можно в судебном разбирательстве.

Иногда свидетель в суде дает информацию, которую он не сообщил следователю в ходе допроса. Поэтому государственный обвинитель или защитник могут упрекнуть его во лжи. Однако это может быть следственная ошибка, так как на предварительном расследовании были упущены данные сведения, следователь не выяснил подробности. Этот пример свидетельствует о важности изучения личности свидетеля, как в теории, так и на практике.

Весьма интересна статистика по участию свидетелей в уголовном судопроизводстве. Каждый пятый свидетель в судебном заседании изменяет первоначально данные показания в сторону, которая благоприятствует обвиняемому [2, с. 90]. Каждый четвертый свидетель по тем или иным причинам отказывается от своих показаний в ходе судебного разбирательства или не является в суд вовсе. По результатам социологического опроса только 14% граждан согласны содействовать правосудию при условии обеспечения им защиты [3, с. 16]. Ежегодно в России свидетелями тяжких и особо тяжких преступлений становятся более 11 млн человек. Из них 2,5 млн в ходе судебных заседаний из-за боязни мести со стороны обвиняемых, подсудимых изменяют показания, именно страх мести является главным препятствием для оказания содействия правосудию [4, с. 6].

Нестабильное эмоциональное состояние также является зачастую причиной наличия расхождений в показаниях свидетеля. Кроме того, что допрашиваемое лицо пережило стресс, став очевидцем преступления, это же лицо переживает и тяжелое эмоциональное потрясение от нахождения в зале суда, необходимости дачи объяснений и, следовательно, необходимости повторного припоминания неприятной информации. Давая показания, лицо мысленно возвращается в негативную обстановку происшествия и вновь переживает неприятные события [5].

Р.А. Адельханян и Д.И. Аминов в качестве причин дачи ложных показаний свидетелем рассматривают страх мести со стороны обвиняемого, подсудимого; наличие взаимной или односторонней неприязни по отношению к обвиняемому (подсудимому), в связи с чем возникает желание ухудшить его положение; нежелание принимать участие в следственных и судебных действиях [6, с. 126].

Наиболее частыми случаями дачи ложных показаний свидетелями является желание освободить обвиняемого (подсудимого) от уголовной ответственности или добиться смягчения наказания. Также нередки случаи, когда свидетели дают ложные показания при допросе по причине оказания на них давления заинтересованными лицами. Свидетелями, которые дают ложные показания чаще всего оказываются лица, которые непосредственно либо косвенно связаны с обвиняемым или потерпевшим. Сокрытие правды при допросе осуществляется по разным мотивам в зависимости от того, какие отношения сложились у свидетеля

с обвиняемым или потерпевшим. Например, мотив мести, желание защитить родственника, желание скрыть свою причастность к преступлению, избежать мести со стороны обвиняемого, подсудимого [7].

Как показывает анализ уголовных дел по делам о преступлениях, совершенных организованной преступной группой, показания свидетелей часто напрямую влияют на результат рассмотрения уголовного дела судом.

22 июля 2014 года в подмосковном городе Одинцово был убит 43-летний Алексей Захаров — ключевой свидетель по уголовному делу в отношении одного из лидеров ореховской преступной группировки Дмитрия Белкина (Белок). Утром, когда А. Захаров вышел из дома своих родственников, преступник произвел в него восемь выстрелов. Свидетель находился под государственной защитой, так как в ходе следствия ему угрожали расправой, требуя изменения показаний.

Федеральный закон от 20.08.2004 (ред. 07.02.2017) «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» предусмотрел возможность применения в отношении свидетеля, его близких родственников и близких лиц мер безопасности при наличии достаточных данных о том, что им угрожают убийством, применением насилия, уничтожением или повреждением имущества либо иными противоправными деяниями. Только 2% опрошенных следователей считают предпринимаемые в отношении свидетелей меры безопасности достаточными.

Одна из главных свидетельниц обвинения по делу казанской организованной преступной группы «Хади Такташ» Юлия Гаврилова, находящаяся под защитой государства, не дожила до судебного заседания. В канун 2002 года она была найдена мертвой в собственной квартире, смерть наступила от отравления угарным газом.

Ежегодно в отношении 3000 свидетелей и их родственников осуществляются такие меры безопасности, как личная охрана, охрана жилища и имущества, выдача специальных средств индивидуальной защиты, связи и оповещения об опасности, обеспечение конфиденциальности сведений о защищаемом лице, переселение в безопасное место, изменение внешности с помощью грима. Защита одного человека ежемесячно обходится федеральному бюджету в среднем в 200 тысяч рублей, а охрана предоставляется на год-два.

Допрос свидетеля, находящегося под государственной защитой, в судебном заседании проводится в условиях, исключающих его визуальное наблюдение другими участниками судебного разбирательства с учетом имеющегося технического оборудования. Например, используется отдельное помещение в здании суда для передачи голоса свидетеля в искаженном виде в зал судебного заседания путем проводной или видеосвязи. Наиболее правильным представляется допрос свидетеля путем использования средств виде-оконференц-связи[11] с обязательным применением программного обеспечения, изменяющего голос свидетеля в целях сохранения его анонимности, либо при помощи веб-камер и мониторов компьютеров, находящихся на столе судьи в зале судебного заседания и в засекреченной комнате, где находится свидетель. Ведь судья должен визуально наблюдать свидетеля, в том числе с помощью технических средств видеонаблюдения. Очевидно, что нахождение свидетеля в зале суда в переодетом виде или в соседнем помещении без изменения вида и голоса не могут способствовать целям обеспечения его безопасности.

Работу видео-конференц-связи обеспечивают секретари судебного заседания и помощники судей [8]. Однако технические проблемы возникают довольно часто. Даже в ходе одного заседания приходится прерываться для возобновления трансляции в связи с потерей звука или изображения. Участники судебного заседания в случае необходимости должны повторить уже озвученные ранее позиции по уголовному делу. Нередки ситуации, когда качество видео-конференц-связи совсем низкое, что не позволяет лицу в полной мере донести до суда свою

[11] К началу 2018 года системами видео-конференц-связи оснащено 100% областных, краевых судов, 63% районных и гарнизонных военных судов. На оборудование судов в 2017 году было затрачено 635 млн руб.

позицию, а судье правильно воспринять и дать надлежащую оценку показаниям свидетеля. Несмотря на удобство системы видео-конференц-связи, она не может заменить живое общение в суде. К сожалению, современная видеосвязь очень сильно искажает коммуникацию со свидетелями, а значит, важные фрагменты их показаний могут быть потеряны либо неверно интерпретированы, невозможно отследить невербальные сигналы.

Учитывая искажения и помехи при изменении голоса свидетеля под псевдонимом, технические возможности оборудования, судья дублирует свидетелю вопросы, задаваемые сторонами, ответ поступает в зал судебного заседания при помощи установленных динамиков. Такую особенность следует учитывать государственному обвинителю и защитнику при формулировании вопросов свидетелю, которые должны быть краткими и содержательными одновременно.

При поступлении провокационных вопросов со стороны защиты, направленных на установление личности свидетеля, не связанных с обстоятельствами дела (например, где проживает свидетель, при каких условиях познакомился с подсудимым и т.п.), государственный обвинитель должен незамедлительно ходатайствовать перед судом об их снятии, мотивируя это тем, что ответы на поставленные вопросы приведут к рассекречиванию свидетеля, что может отрицательно сказаться на его безопасности.

Очевидно, что допрос анонимного свидетеля в суде требует тщательной к нему подготовки. Должны быть изучены материалы уголовного дела, проанализированы показания свидетеля под псевдонимом, учтены разногласия показаний свидетеля с показаниями других допрошенных лиц по делу и др. При необходимости выяснения тех или иных обстоятельств может потребоваться проведение дополнительных допросов и повторных с целью устранения противоречий с показаниями других лиц и результатами исследования вещественных доказательств и т.п. При допросе свидетелей в ходе судебного заседания особое значение для сторон имеет установление психологического контакта с допрашиваемым лицом, правильно подготовленные вопросы, учет особенностей личности свидетеля и умение распознавать ложные показания посредством применения тактических приемов. Конкретное их применение зависит от сложившейся ситуации [9].

Весьма эффективным, на наш взгляд, является использование метода ситуационного моделирования для разрешения ситуаций, когда нужно распознать и оценить достоверность показаний свидетеля. По мнению Т.С. Волчецкой, участниками допроса осуществляется деятельность, представляющая собой мыслительный процесс, целью которого является выстраивание перспективной модели предстоящего допроса и прогнозирование различных тактик его проведения в зависимости от различных ситуаций и многовариантных возможностей развития событий [10, с. 12].

В ходе реализации основной стадии допроса свидетелей можно выделить ключевые проблемы, определяющие следующие психологические задачи:

1) диагностика и оценка состояния психофизиологических, познавательных процессов, памяти, уровня и характерных особенностей мышления;

2) выбор и применение психологических способов активизации памяти, стимулирования мышления, восстановления ассоциативных связей;

3) психологический анализ поведения свидетеля до, в момент и после совершения преступления;

4) психологическая диагностика личностных особенностей свидетеля: социальной направленности, убеждений и т.д.;

5) диагностика отношений свидетеля к событию преступления, лицам, его совершившим, наступившим последствиям;

6) оперативный анализ и оценка невербальных реакций свидетеля, особенно при диалоговом этапе допроса;

7) оперативное изменение тактики допроса на основании перечисленных факторов;

8) применение специальных психологических приемов распознавания и преодоления умышленного искажения фактов.

Значение указанных моментов может существенно различаться в зависимости от каждой конкретной ситуации.

Представляется, что можно выделить несколько распространенных судебных ситуаций, которые могут возникнуть при проведении допроса свидетеля:

1. Свидетель дает правдивую и достоверную информацию. Как правило, данная категория свидетелей не заинтересована в исходе дела.

2. Свидетель говорит правду, но насколько достоверна эта информация неизвестно, так как допрашиваемое лицо добросовестно заблуждается или забыло некоторые факты. Следует помнить, что правдивые показания не всегда бывают объективными (достоверными).

Так, 19 августа 2014 года в Калининграде на пересечении Московского проспекта и улицы Кутаисской переходил дорогу мужчина. При этом машины в крайнем и среднем ряду, несмотря на разрешающий сигнал светофора, движения не начинали, а пропускали гражданина К. Когда мужчина подошел к крайней полосе, его сбил автомобиль золотистого цвета марки «Ауди-100». Водитель автомобиля двигался на разрешающий сигнал светофора, но из-за стоявших автомобилей в двух соседних полосах поздно заметил переходящего дорогу пешехода и сбил его. Пешеход получил травмы средней степени тяжести.

По делу в суде был допрошен свидетель. В частности, судья задал вопрос свидетелю-пешеходу: «Поясните, видели ли вы, на какой свет светофора (для пешеходов) начал переходить дорогу пешеход, которого сбили?». Свидетелем дан следующий ответ: «Я не видел, на какой свет светофора для пешеходов начал движение данный пешеход, возможно, что на зеленый. Но в тот момент, когда его сбил автомобиль, свет светофора для пешеходов был красным» [11].

3. Свидетель дает заведомо ложные показания, так как он заинтересован в исходе дела. В большинстве случаев такие свидетели прямо или косвенно связаны с событием преступления и возможно причастны к нему.

Так, свидетель по уголовному делу был оштрафован на 20 тыс. рублей за дачу ложных показаний. Мужчина дал заведомо ложные показания, обеспечив алиби своему знакомому, который являлся обвиняемым по делу о грабеже. Несмотря на то, что суд предупредил мужчину об ответственности за дачу ложных показаний, свидетель все же решил помочь своему знакомому. В результате суд Центрального района г. Калининграда признал лжесвидетеля виновным по ч. 1 ст. 307 УК РФ [12].

Для того чтобы максимально точно и объективно оценить показания свидетелей, необходимо провести их анализ с позиций наличия в них логики и согласованности, учитывать условия воспроизводства показаний и интенсивность процесса припоминания; проверить источники полученной информации; обратить внимание на новые факты, а также сопоставить показания между собой и иными доказательствами, имеющимися в деле. Важно помнить, что со временем процесс припоминания замедляется и по истечении определенного времени свидетелю достаточно сложно вспомнить некоторые детали происшествия или точную хронологию событий.

После пережитой психотравмирующей ситуации допрашиваемые лица часто излагают факты необъективно, преувеличивая или излишне детализируя одни обстоятельства и обобщая другие. Поэтому их показания могут быть признаны недостоверными не только по причине умышленного искажения фактов, но и вследствие воздействия физиологических особенностей восприятия, наличия помех для наблюдения [13, с. 204]. В связи с этим важным является единообразие показаний свидетелей, особенно если нет вещественных доказательств.

Например, вечером 4 ноября 2012 года в районе зоопарка в г. Калининграде нетрезвый молодой человек приставил острый предмет к горлу незнакомой ему девушки и стал спрашивать, сколько стоит ее жизнь. В этот момент у нее зазвонил телефон. Потерпевшая держала его в руке. Молодой человек отобрал у нее телефон и отключил. Она стала звать на

помощь, вскоре подъехали работники полиции. Молодой человек, увидев их, убежал, однако был задержан позже при патрулировании улицы. При нем были обнаружены ключи, но телефона не было. В связи с этим встал вопрос о том, достоверны ли показания потерпевшей. Было опрошено более 10 друзей потерпевшей, и все они заявили, что она честный человек, не склонный к фантазиям. Показания были признаны судом достоверными [14].

Таким образом, изучение личности свидетеля как в криминалистике, так и в уголовном процессе тесно взаимосвязано и представляет собой комплекс свойств лица, который является участником уголовного судопроизводства. Так, комплекс свойств свидетеля имеет решающее значение для вынесения законного и обоснованного приговора в отношении подсудимого. Таким образом, весь спектр сведений о личности свидетеля приобретает криминалистическое значение и используется судом для решения тактических задач.

Представляется, что сфера применения криминалистического учения о личности свидетеля в процессе его допроса в суде может не только ограничиваться вопросами тактики судебного следствия, но и носить комплексный характер. Проблема криминалистического изучения личности свидетеля в суде, на наш взгляд, должна рассматриваться в нескольких плоскостях: в сфере уголовного судопроизводства, общей теории криминалистики, криминалистической техники, тактики, криминалистической методики расследования отдельных видов преступлений. И в том числе с учетом основ предмета криминалистики [1, с. 318].

Во-первых, закономерностей механизма преступления — с целью изучения поведения и действий свидетеля в суде (как составной элемент динамической системы механизма преступления: субъект преступления — отношение субъекта преступления к своим действиям и последствиям преступной деятельности и соучастникам — предмет преступного посягательства-способ совершения преступления — преступный результат — обстановка преступления (время, место, условия) — поведение и действия лиц, оказавшихся случайными участниками события и т.д.). Действия, движения и поступки лиц, случайно или косвенно связанные с событием преступления, как элемент механизма преступления [15, с. 179; 16, с. 4].

Во-вторых, закономерностей, связанных с информационной составляющей события преступления и личности свидетеля, как носителя идеальных следов преступления.

В-третьих, закономерностей работы с доказательственной информацией и рекомендациями по актуализации памяти свидетеля и установления психологического контакта.

Подводя итог исследованию вопроса об использовании криминалистического изучения личности свидетеля в процессе судебного допроса, можно отметить, что судебное следствие крайне сложно представить без участия свидетеля. Представляется, что тактические и методические рекомендации судебного допроса должны обеспечить единство линии поведения свидетеля, как на стадии предварительного расследования, так и на стадии судебного разбирательства, а также в целях обеспечения безопасности участия свидетелей в процессе рассмотрения дела в суде.

Список литературы

1. Славгородская О.А. Криминалистическое изучение личности свидетеля // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия Право. 2015. № 5-6. С. 315-321.

2. Волчецкая Т.С., Бедризов А.Г. Криминалистическое изучение личности свидетеля: основные методы // Вестник Балтийского федерального университета им. Канта. 2012. № 9. С. 90-97.

3. Зайцев Е.О. Государственная защита анонимного свидетеля в сфере уголовного судопроизводства РФ и зарубежных стран: сравнительно-правовое исследование: автореф. дис. … канд. юрид. наук. М., 2016. 32 с.

4. Богданов В. Говорите, вас защищают // Российская газета. 2014. № 6372 (100).

5. Помаз Г.С. Использование возможностей психологической науки при производстве допроса подозреваемых, обвиняемых и потерпевших // Философия права. 2016. № 2 (75). С. 79-83.

6. Криминалистика: учебное пособие. М.: Юнити-Дана, 2015. 615 с.
7. Рычкалова Л.А. Проблемные аспекты тактики допроса свидетелей // Общество и право. 2013. № 4. С. 167-169.
8. Регламент организации применения видеоконференц-связи в федеральных судах общей юрисдикции, утв. приказом Судебного департамента при Верховном Суде РФ от 28.12.2015 № 401.
9. Гавло В.К., Курчеев В.С., Удовиченко В.С. Ситуационный подход в разрешении следственных ситуаций, возникающих при допросе подозреваемых и обвиняемых по делам о незаконном обороте наркотических средств и психотропных веществ // Известия Алтайского государственного университета. Серия Право. 2014. № 2 (28). С. 122-128.
10. Волчецкая Т.С. Ситуационное моделирование в расследовании преступлений: автореф. дис. … канд. юрид. наук. М., 1991. 23 с.
11. Архив Калининградского гарнизонного военного суда за 2014 г. Уголовное дело № 20/12/0043-14Д.
12. За ложные показания свидетель оштрафован на 20 тыс. рублей. URL: https://www.newkaliningrad.ru/news/incidents/1293357-za-lozhnye-pokazaniya-svidetel-osh-trafovan-na-20-tys-rubley-.html.
13. Аминов Н.И., Давыдов Н.А., Кокурин А.В. Юридическая психология. М., 2015. 304 с.
14. Архив Калининградского гарнизонного военного суда за 2012 г. Уголовное дело № 20/14/0055-12Д.
15. Белкин Р.С. Криминалистика: учебник для вузов / под ред. Р.С. Белкина. М.: Норма, 2001. 990 с.
16. Кустов А.М. Моделирование механизма совершённого преступления при производстве следственного осмотра // Информационный бюллетень Московской государственной академии приборостроения и информатики. М., 2003. № 4. С. 4-11.

Л.Г. Лифанова, *к.ю.н., доцент, профессор кафедры криминалистики Ставропольского филиала Краснодарского университета МВД России, г. Ставрополь*

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ С УЧАСТИЕМ НЕСОВЕРШЕННОЛЕТНИХ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ

Особенности производства следственных действий с участием несовершеннолетних участников уголовно-процессуальных отношений продиктованы необходимостью обеспечения дополнительных мер юридической защиты для данной категории граждан. В юридической литературе справедливо подмечено, что «…у несовершеннолетних в процессе их взросления складывается определенный уровень общественного и правового сознания, отношение к закону, к вопросам морали и нравственности, к окружающим людям, степень ответственности и самостоятельности в своем поведении…» [1, с. 426]. Именно личностные характеристики подростков, выражающиеся в отсутствии надлежащего уровня сформированности правосознания, непонимания в должной мере характера и последствий своего участия в противоправной деятельности, неосознания важности и серьезности проводимых с их участием следственных действий, побудили законодателя предусмотреть особый порядок проведения уголовно-процессуальных мероприятий с участием лиц, не достигших 18-летнего возраста.

Однако ни глава 50 УПК РФ, регламентирующая производство по уголовным делам в отношении несовершеннолетних, ни отдельные нормы, содержащиеся в иных главах уголовно-

процессуального кодекса (например, ст. 191 «Особенности проведения допроса, очной ставки, опознания и проверки показаний с участием несовершеннолетнего»), не позволяют говорить об отсутствии законодательных пробелов при производстве следственных и процессуальных действий с участием несовершеннолетних. Особенно это касается этапа проверки сообщений о преступлении.

Так, в рамках доследственного производства, согласно ч. 1 ст. 144 УПК РФ, следователь (дознаватель) вправе получать объяснения. Процессуальный порядок производства данного процессуального действия законодателем не определен. Закон допускает, что сведения, содержащиеся в объяснении, могут быть использованы в качестве доказательств (ч. 1.2 ст. 144 и ч. 3 ст. 226.5 УПК РФ). Полагаем, что в этом случае они должны обладать юридической силой информации, полученной при допросе. То есть порядок получения объяснения должен соответствовать процедуре допроса. Это означает, что при получении объяснения у несовершеннолетнего, обязательно присутствие законного представителя и педагога (психолога). Сложности правоприменительного характера в данном случае следующие. Законодателем предусмотрено участие законного представителя:

– несовершеннолетнего подозреваемого (обвиняемого) — с момента первого допроса на основании постановления следователя (дознавателя) — ч. 1 ст. 426 УПК РФ;

– несовершеннолетнего потерпевшего (ч. 2 ст. 45) — момент и порядок вступления в дело не определены;

– несовершеннолетнего свидетеля (ст. 166, 191 и др.) — момент и порядок вступления в дело не определены.

Как правило, о допуске в качестве законного представителя несовершеннолетнего потерпевшего или свидетеля, следователь, по аналогии с требованиями ч. 1 ст. 426 УПК РФ, выносит постановление. Полагаем целесообразным унифицировать в УПК РФ порядок допуска законного представителя несовершеннолетнего потерпевшего, свидетеля либо лица, участвующего в рамках доследственной проверки, посредством внесения изменения в УПК РФ:

часть 2 статьи 45 УПК РФ дополнить словами «Законный представитель несовершеннолетнего потерпевшего допускается к участию в уголовном деле на основании постановления следователя, дознавателя с момента наделения несовершеннолетнего статусом потерпевшего»;

дополнить статью 56 УПК РФ частью 10 следующего содержания: «Если свидетель является несовершеннолетним или по своему физическому или психическому состоянию лишенным возможности самостоятельно представлять свои права и законные интересы, к обязательному участию в следственных действиях с данным свидетелем привлекается его законный представитель, о допуске которого следователем (дознавателем) выносится постановление»;

дополнить часть 1.1 статьи 144 УПК РФ словами «При получении объяснения от несовершеннолетнего или лица, по своему физическому или психическому состоянию лишенным возможности самостоятельно представлять свои права и законные интересы, участие законного представителя является обязательным, о чем делается отметка в бланке объяснения».

При получении объяснения у несовершеннолетнего участника доследственного производства вправе присутствовать адвокат. Это следует из ч. 1.1 ст. 144 УПК РФ. Полагаем, если несовершеннолетний — это лицо, в отношении которого проводится доследственная проверка, то условием правомерности использования сведений, изложенных в объяснении, в качестве доказательства является непременное участие адвоката. В ином случае, даже при условии присутствия законного представителя в рассматриваемом процессуальном действии информация, содержащаяся в объяснении, не может иметь доказательственного значения.

В случае если несовершеннолетний не достиг 16-летнего возраста, то получение от него объяснения должно предусматривать присутствие педагога или психолога. Нормативная регламентация процессуального статуса данных субъектов, порядок их участия в следственных

действиях в юридической литературе обоснованно подвергается обсуждению и критике [2, с. 135]. В то же время практически все авторы едины в том, что функциональное назначение участия педагога и психолога в следственных действиях — установление и поддержание психологического контакта следователя с несовершеннолетним [3, с. 165]. Участие обозначенных субъектов при получении объяснения у несовершеннолетнего должно преследовать те же цели.

На практике зачастую у следователя отсутствует возможность обеспечить порядок получения объяснения у несовершеннолетнего, аналогичный порядку производства допроса. Это может быть вызвано потребностью незамедлительного получения сведений о совершенном преступлении для обеспечения раскрытия его по горячим следам. Нарушения уголовно-процессуального закона в этом случае нет (порядок получения объяснения в УПК РФ не предусмотрен), однако сведения, содержащиеся в объяснении, могут иметь ориентирующее значение, а использование их качестве доказательств должно стать недопустимым.

После возбуждения уголовного дела несовершеннолетнего следует допросить в порядке, обусловленном его правовым статусом. При этом следует учитывать, что в соответствии с ч. 5 ст. 191 УПК РФ при допросе несовершеннолетнего потерпевшего или свидетеля обязательно применение видеозаписи или киносъемки (если нет возражений со стороны несовершеннолетнего или его законного представителя). Отметим, что законодатель не регламентирует должным образом порядок применения технических средств в ходе расследования уголовного дела. А отсутствие тактических и организационных рекомендаций использования видеозаписи или киносъемки в следственных действиях с участием несовершеннолетних порождают негативную практику отказа от их применения.

Полагаем, что следователь не должен избегать применения видеозаписи или киносъемки при производстве следственных действий с участием несовершеннолетних (допроса, очной ставки, опознания и проверки показаний на месте). При подготовке к следственному действию следователю надлежит разъяснить несовершеннолетнему и его законному представителю целесообразность применения технических средств, а также порядок видео- или киносъемки.

К первоначальным следственным действиям с участием несовершеннолетних могут быть отнесены получение образцов для сравнительного исследования, а также назначение и производство экспертизы. Названные следственные действия могут проводится как до, так и после возбуждения уголовного дела. Проблемы правоприменительного характера могут возникнуть на этапе доследственной проверки при отказе несовершеннолетнего или его законного представителя от участия в обозначенных действиях. Законодатель не обязывает лиц участвовать в доследственном производстве, не предусматривает ответственность за отказ от дачи объяснений, образцов для сравнительного исследования, прохождения экспертизы. Задача следователя состоит в том, чтобы убедить несовершеннолетних участников и их законных представителей действовать в соответствии с назначением уголовного судопроизводства. То есть своим поведением способствовать быстрому, качественному и объективному расследованию преступления. Если этого достигнуть не получается, то отказ от участия в следственных действиях должен быть зафиксирован документально и содержаться в материалах доследственной проверки.

Следует добавить, что в рамках доследственного производства для следователя не предусмотрена обязанность знакомить лиц, вовлеченных в сферу уголовно-процессуальных отношений на данном этапе (заявитель, лицо, в отношении которого проводится проверка) с постановлением о назначении экспертизы, как то предусмотрено для потерпевшего, подозреваемого, обвиняемого (ч. 1 ст. 198 УПК РФ). Полагаем, что несовершеннолетнего и его законного представителя надлежит знакомить с постановлением о назначении экспертизы (равно как и с постановлением о получении образцов для сравнительного исследования) исключительно в случаях, если несовершеннолетний является непосредственным участником

следственного действия. Закон не обязывает следователя знакомить субъектов доследственного производства с заключением экспертизы. Представляется, что данный пробел должен быть восполнен посредством законодательного закрепления обязанности следователя знакомить заявителя и лицо, в отношении которого проводится доследственная проверка, с заключением экспертизы в случаях, когда она назначается по их ходатайству, либо экспертное исследование проводилось в их отношении.

Уголовно-процессуальное законодательство в ст. 196 УПК РФ перечисляет случаи обязательного назначения экспертизы. В числе прочего в п. 5 указан возраст подозреваемого, обвиняемого, потерпевшего, когда это имеет значение для уголовного дела, а документы, подтверждающие его возраст, отсутствуют или вызывают сомнение. Возникает вопрос — можно ли назначить экспертизу по установлению возраста до возбуждения уголовного дела? Представляется, что ответ должен быть отрицательным. Это обусловливается несколькими моментами. Во-первых, в ст. 196 УПК перечислены субъекты уголовного судопроизводства, процессуальный статус которых определяется после возбуждения уголовного дела. Во-вторых, отдельные элементы предмета доказывания по делам о преступлениях несовершеннолетних, должны быть установлены вне зависимости будет ли привлечен несовершеннолетний к уголовной ответственности (например, влияние на несовершеннолетнего старших по возрасту лиц). В-третьих, недостижение возраста уголовной ответственности, влекущее прекращение уголовного дела (уголовного преследования) за отсутствием состава преступления не дает права на реабилитацию (ч. 4 ст. 133 УПК РФ). В-четвертых, экспертиза может установить, что несовершеннолетний хотя и достиг возраста, с которого наступает уголовная ответственность, но вследствие отставания в психическом развитии, не связанного с психическим расстройством, не мог в полной мере осознавать фактический характер и общественную опасность своих действий (бездействия) и руководить ими в момент совершения деяния. Следовательно, он может нуждаться в применении принудительных мер медицинского характера.

Таким образом, производство следственных и процессуальных действий с участием несовершеннолетних на первоначальном этапе расследования имеет свои особенности, учет которых является непременным условием для признания результатов данных действий имеющими доказательственное значение.

Список литературы

1. Асташкина Е.В. Процессуальные особенности допроса несовершеннолетних // Следственная деятельность: проблемы, их решение, перспективы развития: материалы III Всероссийской молодежной научно-практической конференции (Москва, 25 ноября 2019 года) / под общ. ред. А.М. Багмета. М.: Московская академия Следственного комитета Российской Федерации, 2020. 881 с.

2. Марковичева Е.В., Татьянина Л.Г. Проблемы участия педагога и психолога в уголовном процессе // Вестник Удмуртского университета. Серия «Экономика и право». 2017. № 2.

3. Семенцов В.А. Следственные действия в досудебном производстве (общие положения теории и практики): монография. Екатеринбург: Уральская государственная юридическая академия, 2006.

А.Г. Маркелов, *к.ю.н., доцент кафедры уголовно-правовых дисциплин*
Чувашского государственного университета им. И.Н. Ульянова, г. Чебоксары

КАЧЕСТВЕННОЕ УГОЛОВНОЕ СУДОПРОИЗВОДСТВО В ОСОБОМ (КОМПРОМИССНОМ) ПОРЯДКЕ ПРИНЯТИЯ СУДЕБНОГО РЕШЕНИЯ ПРИ СОГЛАСИИ ЛИЦА С ПРЕДЪЯВЛЕННЫМ ЕМУ ОБВИНЕНИЕМ

Какими свойствами должен обладать современный уголовно-процессуальный закон Российской Федерации (далее — УПК РФ) [1], чтобы его нормы реально оказывали положительное влияние на общественные отношения, закрепляли необходимые формы и гарантии, пресекали вредные последствия и в то же время обеспечивали прогрессивное развитие общества и государства? При этом чтобы действующий УПК РФ не нарушал неотъемлемые конституционные права и свободы граждан и соответствовал требованиям, а также идеям и принципам современного уголовного судопроизводства. Традиционно в данном контексте принято понимать качество современного уголовного судопроизводства.

Под качеством УПК РФ понимается совокупность существенных свойств, позволяющих определить способность и пригодность закона реально удовлетворять общественные потребности и частные интересы заинтересованных лиц в соответствии с назначением современного уголовного судопроизводства [2].

Очевидно, из этого определения мы не обнаружим конкретных свойств, предъявляемых к оценке качества современного УПК РФ. Если рассматривать качество уголовно-процессуального законодательства с точки зрения оформления и приемов юридической техники, то на первый взгляд УПК РФ, несомненно, должен обладать такими свойствами, как логичность, обоснованность, непротиворечивость и иные. В соответствии с этими критериями оценки качества, если не обращать внимания на отдельные фрагменты или нюансы, современный УПК РФ вполне законно соответствует предъявляемым требованиям.

Тем не менее, нам представляется, по большому счету ответ заложен не только в юридической технике составления УПК РФ, но и в идеологической направленности, смысле и характере современного уголовно-процессуального законодательства.

По нашему мнению, в идеологическом смысле оценка качества УПК РФ заключается в продуманности и надежности законодательных инициатив и предложений, проверенные и ободренные следственно-судебной практикой и научным сообществом [3]. Подобные мысли были изложены в работах А.Н. Конева, где автором утверждается, что именно через идеологические основы передается существо уголовного процесса и фундаментальная основа его нормативного выражения через уголовно-процессуальный закон РФ [4]. Подобная идеологическая направленность и смысловая форма законодателя, как мы полагаем, четко выражена в применении особого (компромиссного) порядка принятия судебного решения при согласии лица с предъявленным ему обвинением, предусмотренного главой 40 Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ).

В качестве качественного и эффективного исследовательского инструмента автор предлагает рассматривать особый порядок принятия судебного решения при согласии лица с предъявленным обвинением как действенную и специфическую технологию, позволяющая результативно реализовать назначение УПК РФ. На наш взгляд, в предложенный интерпретации заложена важная идеологическая, качественная и ценностная форма, которая выражается в следующем: «Техника всегда должна быть средством и никогда субъектом. И в современном уголовном судопроизводстве данный подход должен быть на первом месте. Более того, эта идея должна обрести статус идеологического принципа» [5].

Появление в УПК РФ главы 40 изначально прогнозировало оживленную дискуссию в научном мире и не могло не вызвать живого интереса со стороны правоприменителей. Многочисленные сторонники предложенной законодателем особой специфической технологии обосновывались позитивными мыслями и прагматическими идеями, которые в конечном

итоге приходили к утверждению о заключении государством сделки о признании вины с лицом, совершившим преступление. В частности, они констатировали факт упрощения и ускорения современного уголовного судопроизводства по отдельным категориям преступлений, а также экономии материальных и иных затрат, что в конечном итоге позволит разгрузить современную судебную систему от массы поступающих и не вызывающих сложности уголовных дел [6].

Противники введения данной технологии, наоборот, обосновывали и приводили аргументы о недопустимости применения по причине идеологического несоответствия назначения современного уголовного судопроизводства [7].

Несмотря на различные мнения и возражения, законодатель принял волевое решение и внес соответствующую качественную технологию в действующий УПК РФ и позволил применять по отдельным категориям уголовных дел, то есть в ограниченном виде. По результатам непосредственного правоприменения введенной законодателем особой технологии сложились две точки зрения: одни предлагают считать ее разновидностью упрощенного и ускоренного производства по уголовным делам (Б.Т. Безлепкин, К.А. Рыбалов и др.) [8]. Другие выступают за превращение его в российский аналог использования инструментов (технологий) компромисса, в том числе в форме заключения сделки о признании вины с лицом, совершившим преступление (А.В. Смирнов, К.Б. Калиновский и др.) [9].

Автор настоящей работы склоняется ко второй позиции. Для разъяснения сущности, ценности и качественного использования технологий компромисса, установленной главой 40 УПК РФ, приведем следующие аргументы.

Во-первых, данная компромиссная технология получила самое широкое распространение в правоприменительной и следственно-судебной практике. За прошедшие двенадцать лет (мы анализировали период 2007-2018 гг.) судами первой инстанции было рассмотрено 9 052 936 уголовных дел, из которых по 8 779 653 делам был вынесен приговор с осуждением 9 660 286 лиц, а 273 283 уголовных дела были прекращены по реабилитирующим и другим основаниям в отношении 3 037 800 лиц. При этом из общего числа рассмотренных судами по первой инстанции уголовных дел 73,7% (6 675 173 уголовных дела) были рассмотрены и разрешены в особом компромиссном порядке, установленном главой 40 УПК РФ, с учетом согласия обвиняемого (подсудимого) с предъявленным ему обвинением. Только за последние 8 лет (мы анализировали период 2011-2018 гг.) из рассмотренных судами первой инстанции 4 742 846 уголовных дел по 1 946 568 (41%) уголовное судопроизводство осуществлялось в соответствии с главой 40 УПК РФ и были осуждены 4 168 380 лиц, которые добровольно признали свою вину в совершении преступления[12].

При этом стоит отметить активность судов по применению данной компромиссной технологии в целях быстрого рассмотрения и разрешения отдельных категорий уголовных дел. Так, наибольшая активность судов по применению особой компромиссной технологии, предусмотренной главой 40 УПК РФ, пришлась на 2016-2019 гг.[13]

Притом сохраняется устойчивая тенденция ежегодного роста популярности данной процессуальной и качественной технологии в скорейшем разрешении уголовных дел и обеспечения назначения современного УПК РФ[14]. В нынешних условиях средняя нагрузка судьи по рассмотрению и разрешению уголовных дел составляет чуть более одного часа. В таких непростых условиях судья вынужден всячески приветствовать любую возможность сократить время по скорейшему рассмотрению и разрешению уголовных дел. Данная компромиссная технология существенно облегчает жизнь и непосредственно устраивает и других

[12] Выборочные сводные статистические сведения о работе судов общей юрисдикции и мировых судей в Российской Федерации по рассмотрению и разрешению уголовных дел по первой инстанции в период с 2007 по 2018 годы. URL: http://www.cdep.ru/index.php?id=79 (дата обращения: 08 ноября 2019).

[13] Там же.

[14] Данные, полученные при проведении экспресс-опроса судей судов Чувашской Республики и сотрудников СУ СК РФ по Чувашской Республики (ноябрь 2019 года).

заинтересованных участников процесса. В частности, для подозреваемого, обвиняемого или подсудимого сокращается время нахождения в следственном изоляторе и существенно снижается размер будущего наказания, участвующий в деле защитник законно получит свое вознаграждение, потерпевшему в полном объеме компенсируют вред от причиненного преступления, а органы расследования улучшат показатели своей профессиональной деятельности.

Таким образом, ценность и качество использования технологий компромисса при согласии обвиняемого с предъявленным ему обвинением заключается и позволяет констатировать, что больше половины всех уголовных дел в Российской Федерации рассматривается в особом (компромиссном) порядке, предусмотренном главой 40 УПК РФ.

Во-вторых, по нашему мнению, постановленный в порядке главы 40 УПК РФ обвинительный приговор есть не что иное, как судебное удостоверение достигнутого заинтересованными сторонами компромисса. Иными словами, заключается определенная сделка о признании вины и согласия с предъявленным обвинением, в котором лишь отражаются пределы ограниченного обжалования, установленные статьей 317 УПК РФ.

Таким образом, постановленный и провозглашенный в порядке статьи 316 УПК РФ обвинительный приговор и отсутствие оснований для его пересмотра свидетельствует о фактическом признании заинтересованными сторонами заключенной сделки и достигнутого компромисса. При этом выводы суда, отраженные в обвинительном приговоре, еще раз доказывают неопровержимую позицию и желание заинтересованных сторон заключить качественный компромисс и достичь непосредственного результата.

В-третьих, по мнению самих судей, рассматривающих уголовные дела в порядке главы 40 УПК РФ, данный порядок является компромиссной уголовно-процессуальной технологией в виде заключения сделки с правосудием между государством в лице правоохранительных органов и лицом, совершившим преступление. При этом судья является пассивной фигурой и какой-либо инициативы в части вынесения процессуальных решений согласно части 6 статьи 316 УПК РФ фактически не проявляет. Таким образом, суды инертны в этом вопросе и лишь удовлетворяются непосредственной ролью удостоверителя собранных по делу доказательств и формальной правомерностью представленной процедуры. В конечном итоге стороны заключают компромиссный договор о признании своей вины подсудимым и за судом остается лишь обязанность скорейшего вынесения обвинительного приговора[15].

В-четвертых, ценность и качество использования технологий компромисса при согласии лица с предъявленным обвинением в соответствии с главой 40 УПК РФ не противоречит современной идеологии уголовно-процессуального доказывания. Мы полагаем, что при применении технологий компромисса в процессе доказывания при согласии лица с предъявленным обвинением процессуальный акт признания обвиняемым (подсудимым) своей вины превращается автоматом в соответствующий договор (сделку) между заинтересованными сторонами. В данном случае указанный процессуальный акт о признании вины имеет не только доказательственное значение, но становится определенной парадигмой. То есть путем заключения компромисса между заинтересованными сторонами мы наглядно наблюдаем переход на новую договорную форму установления истины по уголовному делу. Юридическим значением признания вины обвиняемым будет отказ от уголовно-правового спора и согласие с предъявленным обвинением, в том числе согласие на вынесение в отношении него соответствующего процессуального решения. Если подсудимый признает себя виновным и соглашается с предъявленным обвинением, в том числе на рассмотрение в особом компромиссном порядке, то необходимость в доказывании всех обстоятельств отпадает. Весь собранный по уголовному делу доказательственный материал не подвергается системному анализу, а наоборот превращается в истинный и подлинный, не вызывающий никаких сомнений у заинтересованных сторон.

[15] Данные, полученные при проведении экспресс-опроса судей судов Чувашской Республики (ноябрь 2019 г.).

Итак, использование технологии компромисса позволяет установить истину по уголовному делу и определить необходимые обстоятельства, подлежащие доказыванию. Иными словами сделать качественными и доказанными факты и обстоятельства, которые позволяют разрешить уголовное дело по существу. Стоит отдельно акцентировать внимание на том, что действующий УПК РФ прямо не закрепляет обязанность устанавливать истину по уголовному делу. С учетом современной идеологии уголовного процесса нельзя уверенно сказать, что истина — цель доказывания, как это было ранее закреплено в прежнем УПК РСФСР [10]. Тем не менее при применении технологий компромисса в процессе доказывания необходимо тщательно исследовать отдельные существенные обстоятельства уголовного дела (событие, виновность и др.). Как мы уже отмечали, в любом случае истина по уголовному делу «автоматом» будет установлена.

Необходимо обратить внимание на то, что вопрос о цели доказывания в настоящее время также законодателем однозначно не прояснен. Мы считаем, что истина при применении технологий компромисса автоматом устанавливается по уголовному делу. В состязательном уголовном процессе приоритет имеет процессуальная форма, а не содержание, и поэтому при применении технологий компромисса нет необходимости дополнительно нацеливать участников процесса устанавливать истину по делу. Благодаря технологиям компромисса, истина будет качественно и объективно установлена и устроит каждого заинтересованного участника. Главная задача — обеспечить и соблюсти все права и свободы лиц, вовлеченных в сферу уголовного судопроизводства. В данном случае мы солидарны с Е.Б. Мизулиной, которая полагает, что «задачи уголовного судопроизводства — соблюдение прав и свобод граждан, вовлеченных в уголовный процесс, и если в ходе уголовного судопроизводства не будут нарушены права граждан, то его задачи выполнены» [11].

Иными словами, отсутствие спора между заинтересованными сторонами относительно отдельных обстоятельств уголовного дела порождает применение качественных технологий компромисса, а следовательно, процесс доказывания по уголовному делу становится эффективным и незатруднительным. В конечном итоге он сокращается или прекращается вообще. Стоит отметить, что согласие стороны защиты с предъявленным обвинением предполагает его качественную форму и, самое главное, доказанность всех обстоятельств уголовного дела и создает все необходимые предпосылки для применения технологий компромисса.

В-пятых, в пользу смелого применения технологий компромисса при согласии лица с предъявленным обвинением свидетельствует здравый смысл и жизненная опытность. В современных условиях борьбы с преступностью необходимы новые качественные и в то же время сокращенные и экономичные технологии реализации государством обвинительной власти, в том числе посредством компромиссных способов разрешения уголовных дел. Заключение подобных компромиссных сделок и разрешения уголовного дела по существу есть не что иное, как специфическая форма реализации государственной задачи по осуществлению качественного уголовного преследования. Считаем, что уголовная политика Российского государства должна и дальше двигаться в таком направлении и стать одним из важнейших современных инструментов борьбы с преступностью.

Таким образом, качественная компромиссная технология при согласии лица с предъявленным обвинением, установленная главой 40 УПК РФ, выражается во взаимных уступках заинтересованных сторон, где государственные органы и должностные лица правоохранительных и судебных органов полностью или частично отказываются от использования мер принуждения и наказания, а лицо, совершившее преступление, совершает посткриминальные общественно полезные действия, направленные на устранение последствий совершенного преступления и активно содействует уголовному правосудию.

Изложенные доводы позволяют с большой уверенностью констатировать качество и ценность использования современных технологий компромисса при особом порядке принятия судебного решения при согласии обвиняемого с предъявленным обвинением. В конечном итоге можно сделать категоричный вывод о высокой актуальности и значимости его для

уголовно-процессуальной теории и следственно-судебной практики. Качественное уголовное судопроизводство можно построить только благодаря множественности идей, подходов и уяснения истинного и смыслового предназначения современного уголовного процесса.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СЗ РФ от 24 декабря 2001 г. № 52 (часть I). Ст. 4921.
2. Свиридов М.К. О качестве уголовно-процессуального законодательства // Правовые проблемы укрепления Российской государственности: сборник статей / отв. ред. М.К. Свиридов, Ю.К. Якимович; под ред. О.И. Андреевой, И.В. Чадновой; Томский государственный университет. Томск, 2015. С. 3-7.
3. Маркелов А.Г. Компромисс в уголовном судопроизводстве России в свете реализации особого порядка судебного разбирательства по уголовным делам при согласии обвиняемого с предъявленным ему обвинением // Уголовно-правовая превенция в сфере оборота наркотических средств или психотропных веществ, алкогольной и спиртосодержащей продукции (региональный аспект): сборник материалов Всероссийской научно-практической конференции. Чебоксары, 2015. С. 505-509.
4. Конев А.Н. Идеологический подход к оценке качества уголовно-процессуального законодательства // Вестник Нижегородской академии МВД России. 2013. № 22. С. 157-158.
5. Поляков М.П., Смолин А.Ю. Технология уголовного процесса: «за» или «против» человека процессуального // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 189-192.
6. Лазарева В. Теория и практика судебной защиты в уголовном процессе. Самара, 2000. С. 184-202.
7. Петрухин И. Сделки о признании вины чужды российскому менталитету // Российская юстиция. М.: Юрид. лит., 2001. № 5. С. 35-37.
8. Безлепкин Б.Т. Настольная книга судьи по уголовному процессу. М.: Проспект, 2013. 400 с.
9. Смирнов А.В., Калиновский К.Б. Уголовный процесс: учебник / под общ. ред. А.В. Смирнова. 7-е изд., перераб. М.: Норма: ИНФРА-М, 2017. 784 с.
10. Уголовно-процессуальный кодекс РСФСР от 27 октября 1960 г. // Ведомости Верховного Совета РСФСР. 1960. № 40. Ст. 592.
11. Мизулина Е.Б. Совершенствование уголовно-процессуального законодательства. Проект УПК Российской Федерации // Информационный бюллетень Следственного комитета при МВД России. 2001. № 1. С. 146.

П.Г. Марфицин, *д.ю.н., профессор кафедры уголовного права и процесса ННГУ им. Н.И. Лобачевского, г. Н. Новгород*

УПК РФ ОБ ИНЫХ ПРОЦЕССУАЛЬНЫХ ДЕЙСТВИЯХ

Словосочетание «иные процессуальные действия» в тексте УПК РФ употребляется более тридцати раз. Однако не всегда его значения идентичны. Для иллюстрации приведем выдержки из двух статей. «… По результатам рассмотрения заявления председатель суда выносит мотивированное постановление, в котором может быть установлен срок проведения судебного заседания по делу и (или) могут быть приняты иные процессуальные действия для ускорения рассмотрения дела» (ч. 6 ст. 6.1 УПК РФ). «Собирание доказательств осуществляется в ходе уголовного судопроизводства дознавателем, следователем, прокурором и судом путем производства следственных и иных процессуальных действий, предусмотренных

настоящим Кодексом» (ч. 1 ст. 86 УПК РФ). Имеются и другие хитросплетения закона в обозначенной нами сфере, требующие особого внимания. Обозначим их.

Прежде всего, уточним, что же относится к процессуальным действиям. Дело в том, что единообразного подхода на этот счет не существует.

В пункте 32 ст. 5 УПК РФ указано, что процессуальное действие — это следственное, судебное или иное действие, предусмотренное настоящим Кодексом. Такой подход уже вызывает некоторое непонимание. Так, из указанной формулировки следует, что к процессуальным действиям отнесены: 1) следственные действия, 2) судебные действия, 3) другие действия, являющиеся процессуальными (т.е. предусмотренные УПК РФ и обладающие другими соответствующими признаками), которые не являются ни следственными, ни судебными. Это понимание возражений не вызывает. Однако законодатель нередко (например, в п. 40.1 ст. 5, ч. 1 ст. 86 УПК РФ) употребляет выражение «следственные и иные процессуальные действия». Куда в этом случае делись судебные действия? Они присоединились к категории «иные» (т.е. процессуальные, но не следственные) либо просто выпали из контекста? Данный вопрос остается без ответа (позже мы вернемся к нему).

Не ясно и не объяснено законодателем, какие именно действия (по классификации, содержащейся в п. 32 ст. 5 УПК РФ) относятся к числу иных.

В теории уголовного судопроизводства единства мнений здесь также не достигнуто. Так, Л.Г. Демурчев уверен, что иные процессуальные действия должны представлять собой предусмотренные уголовно-процессуальным законодательством действия следователя, дознавателя, руководителя следственного органа, начальника органа дознания, начальника подразделения дознания, органа дознания, прокурора и суда при участии иных участников процесса, а также иных лиц, направленные на собирание доказательств путем их представления, истребования, требования производства документальных проверок, ревизий и исследований [1].

Под процессуальными действиями (правда, с оговоркой, что не всеми, а лишь проводимыми в стадии возбуждения уголовного дела) Я.П. Ряполова предлагает понимать предусмотренные УПК РФ отдельные структурные элементы уголовно-процессуальной деятельности по приему, проверке сообщения о преступлении и установлению основания (либо его отсутствия) для него, а также по проверке законности и обоснованности производимых действий (бездействия) и принятых процессуальных решений. Таковые указанный автор предлагает классифицировать по целевому, волевому, системному основаниям; по субъектному составу; по степени регламентации в УПК РФ; по доказательственному значению; по ключевым направлениям уголовно-процессуальной деятельности (процессуальные действия организационно-обеспечительного характера, процессуальные действия по собиранию доказательств, процессуальные действия, связанные с осуществлением начального этапа задержания лица по подозрению в совершении преступления до возбуждения уголовного дела, контрольно-надзорные процессуальные действия) [2].

Указанные исследователи рассматривают категорию «иные процессуальные действия» в основном в контексте доказательственного права. Возможно, поэтому и авторы одного из комментариев к УПК РФ пишут, что под иными процессуальными действиями, направленными на собирание доказательств (в контексте ст. 86 УПК РФ), подразумеваются действия, вытекающие из властных полномочий участников, ведущих уголовный процесс. К таковым они отнесли официальные поручения и запросы, поручения, требования о производстве ревизий и документальных проверок и т.д. (оставив этот перечень открытым) [3]. Аналогичная позиция отстаивается рядом ученых, занимавшихся исследованием данных вопросов [4].

Но такой подход, по нашему мнению, является узким, односторонним. Положения п. 32 ст. 5 УПК РФ позволяют толковать словосочетание «иные процессуальные действия» гораздо шире. Например, вызов лица к следователю есть не что иное, как действие, выполняемое должностным лицом в рамках процедуры, регламентированной УПК РФ. Почему мы не можем именовать такое действие процессуальным? Применение меры пресечения (не путать с самой мерой пресечения) осуществляется посредством выполнения целого ряда процессуальных

действий (вынесение постановления, ознакомление с ним обвиняемого, разъяснение сути этой меры, последствий ее нарушения и пр., вручение копии постановления и т.д.). А еще есть процедура привлечения лица в качестве обвиняемого, ознакомление с материалами уголовного дела при окончании расследования и многое другой. Точка зрения о том, что такие действия являются процессуальными, в теории уголовного процесса обозначена. В соответствии с ней к «иным процессуальным действиям», в частности, относят обозначенное нами вышепредъявление обвинения, ознакомление участников уголовного процесса с материалами уголовного дела по окончании предварительного расследования, разъяснение судом прав участников судебного разбирательства и т.п. При этом отмечается, что исчерпывающего кодифицированного перечня «иных процессуальных действий» закон не содержит, а поэтому следует исходить из процессуального правила о дозволении только тех процессуальных действий, которые прямо предусмотрены законом [5].

В отличие от ранее рассмотренных такой подход основан, как нам представляется, на широком понимании термина «иные процессуальные действия».

Какой же из этих приемов использован законодателем в конкретном случае и как это определить? Попытаемся разобраться в этом вопросе.

Выше мы неоднократно обращались к содержанию ч. 1 ст. 86 УПК РФ. Конечно же, относительно этой нормы надо вести речь об узком понимании словосочетания «иные процессуальные действия» и согласиться с мнением о том, что к числу таковых не относятся судебные действия, но могут быть причислены: требования, поручения, запросы, осуществляемые органами расследования, принятие ими же от потерпевших, подозреваемых, обвиняемых, защитников предметов и документов, могущих стать доказательствами по делу, получение объяснений, производство ревизий и другие действия познавательного свойства, предназначенные для получения и удостоверения информации доказательственного характера.

Другое значение словосочетание «иные процессуальные действия» имеется в ч. 6 ст. 6.1 УПК РФ, где указано: «… По результатам рассмотрения заявления председатель суда выносит мотивированное постановление, в котором может быть установлен срок проведения судебного заседания по делу и (или) могут быть приняты иные процессуальные действия для ускорения рассмотрения дела».

Еще один вариант наблюдаем в п. 4 ч. 2 ст. 38 УПК РФ: «давать органу дознания … поручения о проведении оперативно-розыскных мероприятий, производстве отдельных следственных действий, об исполнении постановлений о задержании, приводе, об аресте, о производстве иных процессуальных действий, а также получать содействие при их осуществлении». Представляется, что здесь подразумевается несколько иной перечень действий, чем предполагается в ст. 86 УПК РФ.

Имеются и другие варианты.

Наконец, существуют законоустановления, в которых рассматриваемое словосочетание требует самого широкого (или почти такого) толкования словосочетания «иные процессуальные действия». Например, в п. 3 ч. 2 ст. 38 УПК РФ — определяющим одно из полномочий следователя; в п. 5 ч. 3 ст. 49 УПК РФ — указывающим на момент вступления защитника в производство по делу; в ч. 1 ст. 125 УПК РФ — устанавливающим предмет обжалования, и др.

Изложенное выше приводит к выводу о том, что рассмотренные формулировки позволяют правоприменителю понимать их суть в зависимости от контекста, в котором используется слово «иные». Другими словами, понимание и толкование закона отдано на усмотрение правоприменителя. Правильно ли это? Считаем, что однозначно и категорично на такой вопрос ответить нельзя.

Объективности ради обозначим, что имеются ситуации, где перечень иных процессуальных действий может быть определен достаточно четко. Например, в п. 8 ч. 4 ст. 223.2 УПК РФ имеется формулировка «… и иных процессуальных действий, предусмотренных частью второй статьи 29 настоящего Кодекса». К сожалению, такие случаи в законе единичны.

Таким образом, ситуация, связанная с разночтением словосочетания «иные процессуальные действия», многократно использованная в уголовно-процессуальном законодательстве, требующет своего разрешения.

Список литературы

1. Демурчев Л.Г. Собирание доказательств в ходе досудебного производства путем проведения процессуальных действий: дис. … канд. юрид. наук. Краснодар, 2012. С. 9.
2. Ряполова Я.П. Процессуальные действия, проводимые в стадии возбуждения уголовного дела: правовые, теоретические и организационные основы: дис. … канд. юрид. наук. Курск, 2012. С. 9.
3. Комментарий к Уголовно-процессуальному кодексу. М., 2014. Сер. 1. Профессиональные комментарии (7-е издание, переработанное и дополненное). С. 263.
4. Кузнецов А.Н. Следственные и иные процессуальные действия как способы собирания доказательств в уголовном процессе: дис. … канд. юрид. наук. Воронеж, 2005. С. 11.
5. Уголовный процесс. Проблемы теории и практики: учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / под ред. А.В. Ендольцевой, О.В. Химичевой. М., 2019. С. 163.
6. Курс уголовного процесса. URL: http:// librisum.com/ugpro/prockurs11.htm (дата обращения: 30.03.2019).

В.М. Мешков, *д.ю.н., профессор кафедры криминалистики Калининградского филиала Санкт-Петербургского университета МВД России, заслуженный юрист России, г. Калининград*

ПРОБЛЕМЫ ДОПУСТИМОСТИ ИСПОЛЬЗОВАНИЯ СВЕДЕНИЙ, ПОЛУЧЕННЫХ ОПЕРАТИВНО-РОЗЫСКНЫМ ПУТЕМ, В ДОКАЗЫВАНИИ ПО УГОЛОВНОМУ ДЕЛУ

Во всем цивилизованным мире общепризнанным является факт, что без использования результатов негласного расследования невозможно раскрыть и расследовать большинство совершаемых преступлений. Поэтому в законодательстве и в научной литературе вопросы получения и использования в доказывании оперативных и следственных материалов рассматриваются в едином ключе. По пути, опробованном в большинстве развитых стран, пошли и те страны, которые ранее входили в состав ССР.

Так, УПК Эстонской Республики 2003 г. содержит многие нормы, которые в Российской Федерации расцениваются как нормы законодательства об оперативно-розыскной деятельности. В частности, в разделе 8 «Собирание доказательств путем проведения оперативно-розыскных мероприятий» (ст. 110-122) определены условия «допустимости выполнения оперативно-розыскных действий при собирании доказательств» (ст. 110); зафиксировано, что «информация, полученная при проведении оперативно-розыскного действия, является доказательством, если при ее получении соблюдались требования законодательства» (ст. 111) и закреплены общие условия собирания доказательств путем проведения оперативно-розыскных мероприятий.

В Уголовно-процессуальном законе Латвии (УПЗ Латвии) оперативные мероприятия, к которым относятся, в частности, наблюдение и слежка за лицом, аудио- и видеоконтроль лица, специальный следственный эксперимент и пр., именуются специальными следственными действиями. Их результаты «используются в доказывании таким же образом, как результаты других следственных действий. А в ст. 230 УПЗ Латвии результаты специальных следственных действия прямо называются доказательствами.

В Уголовном процессуальном кодексе Украины (УПК Украины), действующем с 2012 г., предусмотрен институт негласных следственных действий, большинство которых помещено в главу 21 «Негласные следственные (розыскные) действия. В ст. 246 УПК Украины дано разъяснение о том, что негласные следственные (розыскные)действия — это разновидность следственных (розыскных) действий, которые наряду с уполномоченными оперативными подразделениями, имеет право проводить следователь [1].

В Российской Федерации фактически сохранились положения прежнего кодекса, где оперативно-розыскная деятельность (ОРД) и ее результаты никак не регламентируются. В нашей стране действует уникальное уголовно-процессуальное законодательство, которое практически никак не регламентирует порядок использования в материалах уголовного дела сведений, полученных негласным путем, которые в ст. 89 УПК РФ называются как «результаты оперативно-розыскной деятельности». Именно поэтому и в науке, и на практике постоянно возникают коллизии, причиной которых становится невозможность использования в доказывании оперативных материалов.

Более того, абсолютное большинство существующих российских учебников криминалистики зациклены на освещении только лишь легальной следственной деятельности, которая позволяет следователям лично получить примерно 15% новой информации по расследуемому делу, так как основная ее часть — около 85% — поступает следователю от сотрудников оперативных подразделений. Одним из немногих исключений в числе традиционных учебников криминалистики является учебник, вышедший в свет в Пятигорске в 2019 г., где наряду с традиционными разделами криминалистики излагаются и особенности использования оперативных сил и средств в доказывании по уголовному делу, и отдельный раздел об использовании в доказывании по уголовному делу сведений, полученных оперативно-розыскным путем [2].

На наш взгляд, особенно удручающе существующее положение с оперативно-розыскной информацией отражается на формировании личности юриста при обучении его в отечественном вузе. Даже на выпускном курсе слушатели с трудом понимают, что сведения, полученные оперативно-розыскным путем, не могут быть использованы в доказывании по уголовному делу непосредственно, в виде каких-либо актов, справок, меморандумов и пр. Даже отличники порой заявляют, что к материалам уголовного дела следует прикладывать подлинники сообщений конфидентов. Поэтому приходится практически на каждом занятии по методике расследования преступлений вновь и вновь возвращаться к этой теме и объяснять, что все материалы, поступившие к следователю из подразделений, уполномоченных производить оперативно-розыскную деятельность, следователь обязан лично перепроверить и лишь при получении подтверждений об их объективности и достоверности, может их использовать как источники доказательств.

Основная масса оперативно-розыскной информации содержит сведения, полученные оперативным работником либо самостоятельно (что распространено на этапе доследственной проверки), либо на основании исполнения отдельного поручения следователя, оформленная в полном соответствии с требованиями совместной Инструкции от 27 сентября 2013 г. [3]. Иные материалы, поступившие к следователю помимо установленного порядка, в том числе при отсутствии постановления о рассекречивании этих сведений, не могут быть допущены в качестве доказательств по делу.

Следователь обязан не только лично удостовериться в надлежащем оформлении порядка представления оперативных материалов, но и убедиться в законности их источника, в прозрачности процедуры хранения предметов, полученных оперативно-розыскным путем (например, наркотиков, полученных в ходе оперативно-розыскного мероприятия «проверочная закупка»). При возникновении подозрений относительно подлинности этих предметов следователь обязан выяснить, например, почему один оперативный сотрудник при передаче изъятого порошка у наркопродавца другому сотруднику не оформил факт передачи соответствующим образом. В случае невозможности устранения сомнений в подлинности этого порошка (который мог

быть подменен при хранении или транспортировке его судебному эксперту), он также не может быть использован в качестве источника доказательств по делу.

Критерии допустимости представляемых следователю источников доказательств во многом зависят от допустимости приемов и средств, с помощью которых они были обнаружены и изъяты. К основным критериям относят:

а) законность, т.е. проведение ОРМ, которые ограничивают конституционные права человека и гражданина, допускается на основании судебного решения и при наличии информации;

б) избирательность, т.е. направленность воздействия оперативных сил и средств только на определенных лиц (например, при получении судебного решения, связанного с тайной телефонных переговоров, в данном решении должен быть зафиксирован конкретный номер телефона, который подлежит прослушиванию);

в) нравственность, т.е. посредством проведения ОРМ не должна быть унижено достоинство личности, и не использованы низменные чувства лиц, вовлечённых в производство данного ОРМ.

В юридической литературе оперативно-розыскная информация постоянно находится в поле зрения специалистов, которые по не совсем понятной причине защищают в основном права подозреваемого и обвиняемого, в ущерб правам потерпевшего, в интересах которых в первую очередь осуществляется уголовное судопроизводство (ст. 6 УПК РФ). Образовавшийся в последнее время в процессуальной литературе крен на защиту прав обвиняемого превышает все разумные пределы. Любая ошибка или оплошность следователя в судебном процессе нередко представляется защитником как умышленное ущемление прав его подзащитного. Это неверно. В абсолютном большинстве случаев в правоохранительных органах работают фанаты своего дела, готовые устанавливать истину даже за вознаграждение, оставляющее их семью за чертой бедности. О существенных нарушениях законности с их стороны, как массовом явлении, говорить не приходится. Изобличая преступников, т.е. сознательно ущемляя их в правах, они восстанавливают справедливость по отношению к потерпевшим.

В настоящее время в доказывании по уголовному делу недопустимыми признаются следующие материалы:

1. Полученные в непредусмотренном законом процессуальном порядке и форме (например, явка с повинной — после повторного объяснения задержанного, который при первичном опросе категорически отрицал свою причастность к расследуемому событию).

2. Полученные в ходе незаконного проведения ОРМ (наиболее часто — в ходе прослушивания телефонных переговоров без решения суда). Вообще информация, связанная с ограничением конституционных прав граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также с проникновением в жилище против воли проживающих в нем лиц (кроме случаев, установленных Федеральным законом), полученная без разрешения суда, однозначно не может быть допущена к делу в качестве доказательств [4]. Поэтому как бы ни были интересны эти данные, использовать их в качестве доказательства закон запрещает.

Кроме того, оперативный работник на основании отдельного поручения следователя нередко привлекается к производству неотложных следственных действий, и в ряде случаев становится соучастником собирания недопустимых доказательств при следующих обстоятельствах:

1. При выполнении следственных действий при отсутствии в материалах уголовного дела отдельного поручения следователя.

2. При допросе лица в качестве подозреваемого, которому не были разъяснены или неполно разъяснены его права, например, не давать показания в отсутствии адвоката [5].

3. При допросе близких родственников подозреваемого (обвиняемого), которым не разъяснено их конституционное право отказаться от дачи показаний.

4. При несоблюдении порядка проведения следственного действия (допустим, производство обыска вместо осмотра места происшествия).

5. При отсутствии в протоколе допроса свидетеля или потерпевшего изобличающих задержанного сведений об источнике их осведомленности.

6. При проведении опознания до производства допроса опознающего лица.

7. В случае приобщения к делу материального объекта без указания на лицо, его представившего.

Оперативный работник обязан помнить, что при решении вопроса о допустимости материалов и объектов, полученных в ходе ОРД, следователь (судья) обязан проследить всю процедуру их движения (или их происхождения) с момента образования и обнаружения, вплоть до момента представления судье. Поэтому целесообразно рассматривать процедуру оформления сведений, полученных оперативно-розыскным путем, обращая внимание на следующие обстоятельства.

1. Как удостоверена подлинность вербальных сведений или факт изъятия объекта (имеется ли собственноручная запись объяснения очевидцем или его собственноручная подпись на объяснении; как упакована видео- аудиозапись, имеются ли на упаковке соответствующие надписи, подписи и печати, возможна ли фальсификация материалов и т.д.).

2. Как зафиксирован факт передачи полученных сведений или предметов следователю (имеется ли постановление о рассекречивании сведений, полученных оперативно-розыскным путем; обладает ли лицо, подписавшее данное постановление соответствующими полномочиями; имеется ли расписка следователя о получении всех объектов, перечисленных в приложении к данному постановлению; отражен ли в протоколе следственного осмотра материалов, полученных оперативно-розыскным путем, факт целостности упаковки и наличия удостоверяющих надписей).

При проведении занятий по методике расследования отдельных видов преступлений нашим курсантам и слушателям приходится неоднократно обращать внимание на эти, казалось бы, мелочи, в процедуре расследования преступлений. Но мы, преподаватели криминалистики, обязаны это делать, одновременно напоминая о своеобразии действующего УПК РФ. Как бы ни были успешны мероприятия, проведенные оперативными службами, результаты их деятельности не могут быть использованы в доказывании по уголовному делу, если обстоятельства их получения, хранения и оценки не соответствуют требованиям действующего закона. В отличие от российского закона, в котором в качестве доказательства в уголовном судопроизводстве не включены сведения, полученные оперативно-розыскным путем (смотри ст. 74 УПК РФ), Министерство юстиции США считает, что показания тайного агента вместе с результатами аудиовизуального наблюдения за подозреваемыми является столь мощным инструментом, что часто ему не остается никакой реальной защиты [6].

Однако мы обязаны действовать в полном соответствии с действующим законом. Как можно повысить достоверность сведений, полученных оперативно-розыскным путем?

Первое, на что следует обратить внимание — это использование *собственноручных записей лица, чья деятельность заинтересовала оперативного работника, т.е. следует рекомендовать собственноручное оформление своих показаний проверяемым лицом.* Почему это оправданно? В первую очередь потому, что нередко в судебном заседании эти лица отказываются от своих ранее данных сообщений, по-разному объясняя факт появления письменных документов. При этом наиболее часто используют следующие версии:

а) «я объяснение не давал вообще, моя подпись подделана»;

б) «я объяснение давал, но что написал оперуполномоченный, не знаю, я не глядя подписал протокол»;

в) «я давал объяснение, но сделал это из-за страха перед работником полиции».

Все эти и подобные им аргументы в ряде случаев успешно опровергаются в случае собственноручной записи опрашиваемым своих объяснений. При собственноручной записи своих показаний ни одна из перечисленных ситуаций просто бы не возникла. Почерк, отраженный

в протоколе объяснения, опровергал бы все домыслы. Существует, правда, вариант оглашения в суде версии о том, что текст был выполнен под угрозами расправы, но и эта версия достаточно легко опровергается с помощью заключения судебно-почерковедческой экспертизы (специалист имеет возможность не только идентифицировать автора и исполнителя текста, но и определить, в спокойном или в неспокойном состоянии был исполнен данный текст).

Второй путь повышения достоверности сведений, полученных оперативно-розыскным путем, — либо привлечение к ОРМ понятых, либо непрерывная фиксация всех действий, совершаемых при выполнении ОРМ, на видеокамеру. Оба способа создают дополнительные возможности для перепроверки действий оперативного сотрудника и проверяемого лица. Хотя в Федеральном законе РФ «Об ОРД» и УПК РФ не зафиксировано требование о присутствии понятых при проведении ОРМ, суды зачастую требуют от правоохранительных органов использовать их при удостоверении каких-либо действий или процедур. Понятые, участвовавшие в ОРМ, нередко допрашиваются в качестве свидетелей; видеозаписи просматриваются в суде, а стенограммы к ним внимательно изучаются.

Практика привлечения понятых в деятельности оперативных работников имеет давние традиции, что способствовало формированию «типичных ошибок» при их привлечении к проведению ОРМ. Одна из них — это привлечение для сотрудничества одних и тех же граждан, которых нередко именуют как «штатных понятых». Подобная практика в деятельности оперативных работников резко снижает качество и достоверность представляемых материалов следователю и в суд. Избавиться от этого недостатка оперативной деятельности просто. Достаточно в разумном пределе использовать одни и те же оперативные источники в проведении ОРМ.

Некоторые сложности имеет факт фиксации результатов ОРМ при помощи технических средств. Процедура фиксации должна быть непрерывной, а при необходимости ее приостановить оперативный сотрудник должен зафиксировать этот факт своим голосом, с указанием времени (с точностью до минуты), с объяснением причины приостановки фиксации ОРМ камерой. Любая неоговоренная пауза в видеофиксации — это повод для заявления защитником любого из участников уголовного процесса о фальсификации записи и всей процедуры ОРМ в целом.

Говоря о способе удостоверения подлинности вербальных сведений или изъятого объекта, необходимо обратить внимание на тот факт, что формальный подход к этому аспекту проблемы допустимости оперативных данных является одним из распространенных оснований непризнания данных сведений в качестве доказательств. Поэтому, например, в протоколе объяснения должен быть четко зафиксирован факт достоверности произведенной записи, с указанием, КАК был ознакомлен с текстом опрошенный (прочитан лично или зачитан вслух оперативным сотрудником).

Третий путь повышения достоверности сведений, полученных оперативным путем, в доказывании по уголовному делу — это использование только предусмотренных уголовно-процессуальным законодательством способов представления предметов на экспертное исследование. *Ненадлежащим образом* переданные источники доказательств (например, представление оружия или наркотиков в судебно-экспертную лабораторию оперативным работником лично, без упаковки), вообще не должны подвергаться экспертному исследованию, поскольку результаты исследования непременно будут исключены из совокупности доказательств по делу, как ненадлежаще оформленные и, возможно, подмененные кем-то из заинтересованных лиц.

Четвертый путь — повышение наглядности оперативных материалов. Не секрет, что большинство сотрудников не обладает читаемым почерком, а пишут как «курица лапой». Поэтому разобраться в написанном иногда практически невозможно. Поэтому оперативные сотрудники должны взять за правило оформлять материалы с использованием компьютера и принтера, и при возможности приобщать к этим материалам фототаблицы.

Пятый путь повышения достоверности состоит в максимальном приближении во времени фиксации признания проверяемого лица в причастности к расследуемому событию при помощи других действий. Например, посредством безотлагательного проведения иных ОРМ и следственных действий, включая допросы, обыски, проверки показаний и пр. Лишь совокупность протоколов ОРМ и следственных действий позволит реально повысить достоверность полученного признания.

Вероятно, существуют и иные пути повышения достоверности оперативных материалов, переданных следователю, но все они имеют временный характер. Кардинально этот процесс можно улучшить лишь после признания результатов ОРД в качестве доказательств по уголовному делу, как было сделано в ряде стран бывшего Советского Союза. Думается, что вскоре и наш законодатель согласится на внесение изменений в уголовно-процессуальное законодательство.

Список литературы

1. Уголовный процессуальный кодекс Украины. К.: Центр учебной литературы. 2012. С. 110.
2. Криминалистика: учебник для студентов высших учебных заведений / Н.Н. Лысов, В.М. Мешков, В.А. Фурсов, А.Г. Гантимуров, А.Ю. Кузнецов; под общ. ред. проф. Н.Н. Лысова. Пятигорск: РИА-КМВ, 2019. 284 с.
3. Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд утверждена совместным приказом МВД, МО, ФСБ ФСО, ФТС, СВР, ФСИН, ФСКН и СК РФ от 27 сентября 2013 г. // Российская газета. 13.12.2013. № 282.
4. Постановление Пленума Верховного Суда Российской Федерации № 8 от 31 октября 1995 г. // Бюллетень Верховного Суда РФ. 1996. № 1.
5. Постановление Пленума Верховного Суда Российской Федерации от 31 октября 1995 г.
6. Обзор для содействия следователю в его деятельности по проведению успешного расследования и судебного преследования общественного должностного лица, злоупотребившего общественным доверием / сост. Эндрю М. Палумбо, ст. агент ФБР. Нью-Йорк, 1996. С. 39.

О.С. Мигунов, *старший преподаватель кафедры криминалистики Барнаульского юридического института МВД России, г. Барнаул*

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ КРИМИНАЛИСТИЧЕСКИХ УЧЕТОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ПРИМЕНЕНИЕМ ОГНЕСТРЕЛЬНОГО ОРУЖИЯ ОГРАНИЧЕННОГО ПОРАЖЕНИЯ

В 1999 г. на территории Российской Федерации появился новый вид огнестрельного оружия, а именно огнестрельное оружие ограниченного поражения. Этому способствовала сертификация первого гражданского травматического оружия, пистолета ПБ-4 «ОСА» [1]. Его конструктивной особенностью являлось то, что ствол отсутствовал, а вместо него имелось четыре камеры для помещения патронов. В качестве снаряда в боеприпасах для вышеуказанного пистолета выступала резиновая пуля со стальным сердечником, а гильза имела особое устройство, при котором воспламенение порохового заряда происходило за счет электрического разряда. Кроме того, гильза выступала в качестве ствола для придания направления полета снаряда. До 2004 г. вышеуказанный пистолет был единственным отечественным представителем огнестрельного оружия ограниченного поражения на территории России. В указанном году

прошел сертификацию и был запущен в серийное производство пистолет ИЖ-79-9Т «Макарыч» [1]. В отличие от пистолета ПБ-4 «ОСА» в вышеуказанном пистолете в качестве боеприпасов использовались патроны центрального боя, где в качестве снаряда применялись резиновые шарики. Выстрел производился из стационарно закрепленного ствола.

Если рассматривать определение огнестрельного оружия ограниченного поражения, то в Российской Федерации оно официально было закреплено 28.12.2010 путем внесения изменений в Федеральный закон № 150-ФЗ «Об оружии» от 13.12.1996. В результате этого статья 1 была дополнена следующим абзацем: «Огнестрельное оружие ограниченного поражения — короткоствольное оружие и бесствольное оружие, предназначенные для механического поражения живой цели на расстоянии метаемым снаряжением патрона травматического действия, получающим направленное движение за счет энергии порохового или иного заряда, и не предназначенные для причинения смерти человеку» (ОООП) [2]. Однако в общепринятой разговорной речи оружие вышеуказанной категории продолжает называться «травматическим оружием».

Одной из основных характеристик огнестрельного оружия ограниченного поражения, в соответствии с приведенным выше определением, является то, что оно не предназначено для причинения смерти человека, а значит, является оружием самообороны. В соответствии с законодательством Российской Федерации практически любой человек, если он соответствует предъявляемым требованиям, пройдя достаточно несложную процедуру оформления разрешения, может получить разрешение на приобретение, а в последующем хранить и носить оружие вышеуказанной категории.

В настоящее время огнестрельное оружие ограниченного поражения пользуется достаточно большой популярностью, об этом свидетельствует количество разрешений, выдаваемых ежегодно. Так, в 2010 г. выдано 5 234 643 таких разрешений, а в 2015 г. — 4 443 277 [3].

Несмотря на то, что огнестрельное оружие ограниченного поражения разработано как оружие самообороны, то есть направленное на предотвращение правонарушений, оно нередко становится орудием преступления.

Одной из проблем, возникающих в ходе расследования уголовных дел, является идентификация орудия преступления, а именно идентификация огнестрельного оружия ограниченного поражения по следам его применения.

В случае применения нарезного огнестрельного оружия основным объектом, на котором имеются следы, способствующие его идентификации, является пуля. Внутренняя поверхность ствола оставляет свои следы на пуле, проходящей через него. Эти следы свойственны каждому оружию. Ствол огнестрельного оружия, в независимости от того, имеются ли в нем нарезы или нет, изготавливается из цельного куска стали путем его высверливания. Микроскопические следы сверления, оставленные на внутренней поверхности ствола, произвольно нерегулярны и сами по себе придают уникальность каждому стволу. Когда выпущенная пуля проходит через ствол, она входит в зацепление с нарезами. Затем эти нарезы направляют пулю через ствол, давая ей быстрое вращение, при этом оставляя на ней следы в виде трасс. Вышеуказанные следы индивидуальны для каждого ствола нарезного огнестрельного оружия.

Если рассматривать еще один объект, который может быть обнаружен на места преступления и содержать следы примененного оружия, то им является гильза. Следы на ней образуются в три этапа: при заряжании, при выстреле и при извлечении гильзы. В свою очередь, они бывают достаточно индивидуальны, что может способствовать идентификации оружия, из которого гильза выстрелена.

Идентифицирующие особенности следов на пулях и гильзах были реализованы в системе МВД путем создания пулегильзотеки. Принципом ее работы является формирование базы пуль и гильз со следами от нарезного огнестрельного оружия. В соответствии с законодательством РФ любое нарезное огнестрельное оружие подлежит обязательному отстрелу, для помещения отстрелянных пуль и гильз в пулегильзотеку. Кроме того, туда также помещаются пули и гильзы, изъятые с мест преступлений. При помещении в пулегильзотеку новых

объектов имеющиеся на них следы сопоставляются с уже существующими. Данное сопоставление в случае установления совпадений между следами способствует раскрытию совершенных преступлений.

Если рассматривать принцип работы механизмов огнестрельного оружия ограниченного поражения в результате выстрела, то он схож с принципом работы огнестрельного оружия. В соответствии с этим расположение следов на гильзах при выстреле из обоих видов оружия с соответствующими системами будет одинаковое.

Причины, по которым помещение гильз со следами применения огнестрельного оружия ограниченного поражения до настоящего времени не помещаются в пулегильзтеку, в литературных источниках не отражены.

Более подробно хотелось бы разобрать следы, образующиеся на пулях, применяемых в огнестрельном оружии ограниченного поражения, так как они отличаются от следов, образующихся на пулях используемых в нарезном огнестрельном оружии.

Пули к травматическому патрону, в отличие от пуль к нарезному огнестрельному оружию, изготавливаются из монолитного материала, имеющего свойства резины или полимерного материала, так называемый «пластизоль». Диаметр, форма, масса, цвет и плотность материала пуль бывает различной в зависимости от марки патрона [4].

Кроме того, стволы огнестрельного оружия ограниченного поражения, в отличие от нарезного огнестрельного оружия, нарезов не имеют, то есть их внутренняя форма гладкая цилиндрическая. При том, их конструкция выполнена таким образом, чтобы ограничить стрельбу боевыми патронами, а именно: сужением просвета канала ствола путем продольных вертикальных вдавлений его стенок вовнутрь, сужением просвета канала ствола у снарядного входа с образованием «окна» округлой, овальной или прямоугольной формы либо наличием вставок в виде продольных вертикальных штифтов в канале ствола [4].

Если бы можно было разрезать ствол вдоль, то тщательное исследование внутренней части выявило бы наличие тонких линий, или бороздок, многие из которых проходят по всей длине ствола. Эти бороздки впечатываются в металл как негативы мельчайших дефектов, они образуются мельчайшими стружками стали, прижатыми к внутренней поверхности ствола движущимся протяжным резцом. Случайное распределение и неровности этих отметин невозможно точно воспроизвести в любых двух стволах. Эти бороздки формируют индивидуальные характеристики ствола.

До недавнего времени считалось, что идентифицировать огнестрельное оружие ограниченного поражения по следам на выстрелянных пулях не представляется возможным. В связи с этим размещение контрольно-отстрелянных пуль в пулегильзотеку является нецелесообразным.

В настоящее время исследования проводимые экспертами в области баллистики стали давать положительные результаты. Так, к примеру, М.Ю. Ломакин проводил исследование следов образующихся на поверхности пуль, выстрелянных из огнестрельного оружия ограниченного поражения, а именно полос потертостей и находящиеся в них многочисленные зазубрины и задиры поверхностного слоя. В ходе проведенного исследования он пришел к выводу, что вероятность успешного проведения идентификации повышается с увеличением количества следов канала ствола, отобразившихся на пуле, что в совокупности приводит к возможности определения вида и модели травматического оружия, из которого был произведен выстрел [5].

Таким образом, из вышеизложенного следует, что в целях полного и всестороннего расследования уголовных дел, связанных с применением огнестрельного оружия ограниченного поражения, а также повышения раскрываемости преступлений вышеуказанной категории, необходимо на первоначальном этапе начать формирование в пулегильзтеке новой категории учета, связанной с гильзами, имеющими следы огнестрельного оружия ограниченного поражения. В последующем в случае разработки методики идентификации огнестрельного оружия ограниченного поражения по следам на пулях, так же помещать их пулегильзотеку.

Список литературы

1. Википедия «Травматическое оружие». URL: https://ru.m.wikipedia.org/wiki/ Травматическое_оружие.
2. Федеральный закон Российской Федерации от 13.12.1996 г. № 150-ФЗ «Об оружии».
3. Раскин А. Россияне все чаще пускают в ход оружие. URL: https://guns.allzip.org/topic/20/1908283.html (дата обращения: 20.06.20).
4. Ломакин М.Ю. Идентификационное исследование отображений свойств канала ствола травматического оружия на пулях // КНМУ. Вопросы морфологии и клиники. Алматы, 2012. Вып. 42.
5. Ломакин М.Ю. Выявление общих и частных признаков некоторых моделей травматического оружия по следам на пулях // Судебная экспертиза Белоруссии. 2019. № 1(8). С. 66-69.

Е.А. Мунгалов, *к.б.н., старший преподаватель кафедры криминалистики Барнаульского юридического института МВД России, г. Барнаул*

ОБ ОПЫТЕ ПРОВЕДЕНИЯ СРАВНИТЕЛЬНЫХ ИССЛЕДОВАНИЙ ЕДИНИЧНЫХ ВОЛОКОН И ПЕРЧАТОК, ИЗЪЯТЫХ С МЕСТА ПРОИСШЕСТВИЯ

При совершении различных преступных деяний преступники довольно часто пользуются перчатками, которые позволяют им не оставлять следы пальцев рук на месте происшествия. В силу своей доступности чаще всего применяются так называемые «строительные» трикотажные перчатки, которые легко можно приобрести в любом продовольственном магазине. Обычно они изготовлены из хлопковой или смесовой пряжи. На поверхность перчаток, как правило, наносится точечное покрытие из поливинилхлорида (ПВХ). Перчатки защищают поверхность рук от различных внешних механических воздействий, а точечное покрытие ПВХ обеспечивает хорошие сцепные свойства.

Если преступник использовал такие перчатки, то на месте происшествия могут быть обнаружены единичные волокна, отделившиеся от перчаток, которые необходимо изымать для дальнейшего сравнительного исследования. Единичные волокна могут быть обнаружены при помощи криминалистической лупы на осколках оконного стекла, на различных выступающих элементах (торчащие головки гвоздей, задиры деревянных поверхностей, необработанные металлические кромки) в местах проникновения, концы перерезанных проводов и т.д. Оптимальным способом изъятия является перенос обнаруженных волокон на липкий слой светлой (бесцветной) дактилоскопической пленки и последующее упаковывание. При проведении исследований волокна с липкого слоя дактилоскопической пленки достаточно легко отделяются и переносятся в микропрепараты.

Когда преступник (подозреваемый) задержан и в результате последующей выемки у него возможно будут изъяты перчатки — одна или несколько пар, то возможно проведение сравнительного исследования в рамках судебной экспертизы по исследованию волокон и волокнистых материалов (далее по тексту — экспертизы волокон). В этом случае при назначении экспертизы волокон с целью сравнения на исследование предоставляются единичные волокна, изъятые на месте происшествия, и изъятые перчатки. На разрешение эксперта ставятся следующие вопросы: «1. Пригодны ли волокна, изъятые на месте происшествия, для сравнительного исследования? 2. Если да, то имеют ли волокна, изъятые на месте происшествия, общую родовую (групповую) принадлежность с волокнами, входящими в состав перчаток, изъятых у… ?». Проведение данного вида исследования всегда подразумевает использование разрушающих методов. Поэтому в обязательном порядке в постановлении о назначении судебной

экспертизы должно иметься разрешение на уничтожение и полное или частичное видоизменение представленных на исследование объектов.

В ходе сравнительного исследования используются типовые экспертные методики исследования волокон и волокнистых материалов [1-4]. Первоначально эксперт исследует представленные на исследование единичные волокна, изъятые на месте происшествия, определяется их относимость к текстильным волокнам, так как нередки случаи предоставления на экспертизу волокон, которые по сути оказывались волосами животных или человека, пуха птиц, стеклянных волокон, пуха растений, фрагментов насекомых, паутиной. Далее определяется природа и цвет волокна, после чего на основании наличия или отсутствия достаточного и информативного комплекса признаков у исследованных единичных волокон делается вывод об их пригодности для сравнительного исследования.

После того как установлено, что единичные волокна, изъятые на месте происшествия, пригодны для сравнительного исследования, проводят само сравнительное исследование. Для этого изготавливаются средние пробы волокон, входящих в состав перчаток, изъятых у подозреваемого (обвиняемого) лица. Определяется природа и цвет волокон средних проб, которые впоследствии сопоставляются с аналогичными показателями единичных волокон, изъятых при осмотре места происшествия. При совпадении показателей делается предварительный вывод о схожести по природе и цвету волокон, изъятых на месте происшествия, и определенных волокон, входящих в состав перчаток. Затем раздельно исследуются структура (толщина, профиль поперечного сечения, наличие точечных включений), краситель (определяется технологический и химический класс красителя, хроматографическое исследование красителя) схожих волокон, то есть устанавливаются родовые и групповые признаки. При совпадении родовых (групповых) признаков делается вывод об общей родовой (групповой) принадлежности сравниваемых волокон и, наоборот, об ее отсутствии при несовпадении.

К сожалению, вывод об установлении общей родовой (групповой) принадлежности часто интерпретируется как прямое указание на то, что сравниваемые волокна с места происшествия произошли от конкретных перчаток, что, на наш взгляд, абсолютно не, допустимо. Единичные волокна не имеют индивидуализирующих признаков, позволяющих произвести идентификацию, то есть в прямом понимании осуществить отождествление объекта самому себе по оставленному следу в виде отделившихся единичных волокон. Важно отметить, что до сих пор отсутствует какая-либо научно обоснованная экспертная методика для решения данного вопроса. Не следует путать данную идентификацию с так называемой группификацией (установлением групповой «идентификации»).

Все вышесказанное подтверждается экспертной практикой при производстве экспертиз волокон с целью сравнения единичных волокон, обнаруженных на месте происшествия и перчаток, которые их возможно оставили. Мною, при производстве сравнительных экспертиз волокон, в ряде случаев было замечено несколько случаев установления общей родовой принадлежности единичных волокон, изъятых с места происшествия одновременно с волокнами нескольких пар перчаток. Именно тогда, я обратил внимание, что пряжа из которой изготовлены перчатки, а это была пряжа черного цвета, состоит из множества разновидностей волокон по структуре и цвету, количество которых колебалось в диапазоне 10-15 в образцах исследуемой пряжи.

Известно, что при производстве смесовой пряжи, из которой часто изготавливаются трикотажные перчатки, используются отходы текстильной промышленности, то есть волоконный состав данной пряжи непостоянен. Установление конкретного волокнистого состава такой смесовой пряжи представляет собой практически неразрешимую задачу. Напрашивается утверждение о том, что будет велика вероятность установления родовой принадлежности какого-либо волокна, входящего в состав такой смесовой пряжи, из которой изготовлена перчатка, и единичного волокна, изъятого на месте происшествия, которое могло отделиться как от конкретной перчатки, так и не иметь никакого отношения к ней.

Таким образом, полученный положительный результат об установлении общей родовой (групповой) принадлежности сравниваемых волокон позволяет предполагать, что волокна, обнаруженные на месте происшествия, могли быть оставлены сравниваемыми перчатками, а также и любым иным изделием, в состав которого входят аналогичные волокна.

Список литературы

1. Криминалистическое исследование волокнистых материалов и изделий из них. Вып. I / под ред. В.А. Пучкова, Л.Д. Беляевой. М., 1983.
2. Криминалистическое исследование волокнистых материалов и изделий из них. Вып. II. Исследование текстильных волокон / под ред. В.А. Пучкова. М., 1983.
3. Криминалистическое исследование волокнистых материалов и изделий из них. Вып. III. Исследование органических красителей окрашенных текстильных материалов / под ред. В.А. Пучкова. М., 1983.
4. Стецюк М.Н., Иванов Ю.Л. Диагностическое и сравнительное исследование волокон // Типовые экспертные методики исследования вещественных доказательств. Ч. II / под ред. А.Ю. Семенова. М.: ЭКЦ МВД России, 2012.

М.А. Сильнов, *доцент кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации, г. Москва*

К ВОПРОСУ О ЦЕЛИ УГОЛОВНО-ПРОЦЕССУАЛЬНОГО ДОКАЗЫВАНИЯ

Истине как цели доказывания в уголовно-процессуальной теории на протяжении десятилетий традиционно уделялось особое внимание. При этом при ее характеристике в научной литературе использовались такие высокие философские понятия, как «абсолютная», «относительная» истина [1, с. 221].

До принятия Уголовно-процессуального Ккодекса Российской Федерации в 2001 г. (далее — УПК РФ) в науке доминировала концепция материальной (объективной) истины, под которой понималось полное соответствие выводов следствия и суда объективным фактам действительности [2, с. 118].

Такая позиция основывалась на марксистско-ленинской теории отражения [3, с. 152] и подкреплялась отдельными положениями закона. Например, ст. 243 УПК РСФСР устанавливала обязанность председательствующего в судебном заседании принимать все предусмотренные законом меры к всестороннему, полному и объективному исследованию обстоятельств дела и установлению *истины*, устраняя из судебного разбирательства все, не имеющее отношения к делу, и обеспечивая воспитательное воздействие судебного процесса [4].

Как справедливо подчеркивала профессор Н.В. Радутная, именно с принципом «объективной истины» связывалась активная роль суда в доказывании, существование института направления дел на дополнительное расследование, возможность для суда вынести обвинительный приговор без учета мнения прокурора и др. [5, с. 3].

Судебная реформа, одной из важнейших задач которой стало укоренение принципа состязательности и равноправия сторон, потребовала фундаментального структурного пересмотра и изменения всего механизма правового регулирования уголовно-процессуальных правоотношений.

Для того чтобы принцип состязательности мог определять характер и содержание основных стадий уголовного судопроизводства, законодателю потребовалось отказаться от упоминания истины как цели доказывания и отдельных «традиционных» процессуальных институтов, в частности, направления судами дел для производства дополнительного расследования. В такой системе координат роль суда как независимого арбитра уже не предполагает

активного участия в собирании и проверке доказательств и предопределяет отказ от возложения на суд обязанности устанавливать истину по делу [6, с. 32].

Актуальные ныне дебаты о возможностях познания истины в уголовном процессе возникли не вчера. Они велись на всех ключевых точках новейшей истории.

Еще дореволюционные российские авторы И.В. Михайловский [7, с. 93], Н.Н. Розин [8, с. 303] считали, что состязательному процессу присуще стремление к истине юридической в силу его частно-исковой природы.

А вот в годы советской власти (особенно в период после октября 1917 до смерти И.В. Сталина в марте 1953 г.) в судебной деятельности проявились инквизиционные черты. Порой в такой высокой степени, что само упоминание о состязательном процессе могло повлечь отрицательные последствия для автора, поскольку состязательность считалась порождением «буржуазной» правовой системы [5, с. 3].

Во всей полноте проявились попытки воздействия исполнительной власти на судебную. В записке председателя Совнаркома РСФСР В.И. Ленина, датированной 1918 г., читаем: «Прошу поставить на порядок дня вопрос об исключении из партии тех ее членов, которые, будучи судьями по делу о взяточниках, ограничивались приговором на ½ года тюрьмы. Вместо расстрела взяточников выносить такие издевательски слабые и мягкие приговоры есть поступок позорный для коммуниста и революционера» [9, с. 282]. Исторический документ иллюстрирует попирание законности в угоду целесообразности.

Трудно не согласиться с А.С. Александровым и др. о том, что в советский период суд же и судебное разбирательство во многом были обрядовым, декоративным приложением к предварительному следствию. Навязываемая судьям, прокурорам, следователям, защитникам классовая (марксистская) идеология фактически полностью подчиняла себе правосознание, вытесняя иные нравственные императивы [10, с. 9].

В условиях состязательного правосудия подобные подходы немыслимы, ведь такой тип процесса намного гуманнее. Как в свое время точно отметил американский юрист Блэкстон Уильям, рассуждая о задачах правосудия, — «Лучше пусть десять виновных избежит наказания, чем пострадает один невиновный» [11, с. 314].

В современной теории доказывания актуальным считается вопрос о том, можно ли рассматривать истину как цель доказывания? Собственно он и вынесен в заголовок данной статьи. Действительно проблема существует. Ведь, с позиций законодателя, принцип презумпции невиновности и лежащие в его основе правила иммунитетов выглядят более приоритетными, чем установление истины «любыми средствами». Как справедливо отметила в свое время П.А. Лупинская, установленное в Конституции РФ и развитое в нормах УПК РФ правило о недопустимых доказательствах также служит гарантией прав обвиняемого [12, с. 5].

На первый взгляд кажется, что указанные гарантии могут стать препятствием на пути эффективного уголовного преследования, мешать рассмотрению дела в разумный срок.

При этом следует признать, что в условиях состязательности познавательный потенциал суда в известной степени ограничен, поскольку возможности суда в принятии решений напрямую связаны с волеизъявлением и процессуальной активностью сторон. При этом суд часто связан с определенными формальными правилами, процедурами и средствами доказывания: преюдициями, презумпциями, фикциями, формальными соглашениями, правилами об исключении доказательств и др.

Но указанные инструменты уголовно-процессуального доказывания лишь представляются несовершенными. Хотя в литературе можно встретить мысль о том, для состязательного процесса свойственна подмена фактов «лукавой игрой» презумпций. Альтернатива — истина или фикция — обычно решается в пользу последней [13, с. 63].

По нашему мнению, однако, давать оценку способам доказывания, применяемым в условиях состязательности, с позиций классической теории доказательств советского периода недопустимо в силу их принципиально разной природы.

Идеология состязательного процесса в ее исходной трактовке, опирающаяся на концепцию божественной справедливости, не укладывается исключительно в рамки диалектических закономерностей и предполагает возможность достижения в ходе поединка абсолютной истины, минуя познание объективной. Инквизиционный процесс, наоборот, технологичен и целиком основан на правилах формальной логики. Соответственно, идеология не может быть противопоставлена технологии в силу различной природы указанных категорий. Именно по этой причине недопустимо грубо сопоставлять элементы состязательного процесса с компонентами иного рода.

Нельзя также не учитывать, что состязательность благоприятствует достижению справедливого правосудия, поскольку, как известно, «истина рождается в споре». Следует, однако, отметить, что указанное суждение применимо к характеристике состязательного процесса лишь в той мере и в тех пределах, которые определяются границами соответствующих процедур и институтов. Судопроизводство в таком суде — это не спор ради спора, а метод разностороннего исследования обстоятельств дела. Истина, добытая вне судебного состязания и без обеспечения фактического равенства сторон, судом не признается.

Категория «истина», конечно, представляет собой определенную абстракцию, что, однако, не исключает описания отдельных ее свойств языком правовых норм.

Так, если в УПК РСФСР основаниями к отмене или изменению приговора при рассмотрении дела в кассационном порядке являлось несоответствие выводов суда, изложенных в приговоре, фактическим обстоятельствам дела (ст. 342, 344 УПК РСФСР) [4], то в УПК РФ применительно к основаниям отмены или изменения судебного решения в апелляционном порядке содержится немаловажное уточнение. Законодатель исходит из того, что основанием принятия соответствующего решения выступает несоответствие выводов суда только тем фактическим обстоятельствам уголовного дела, которые установлены судом нижестоящей инстанции. То есть он ограничивает круг доказательств, относимость, допустимость, достоверность и достаточность которых оценивается судом второй инстанции, лишь исследованными и положенными в основу акта суда первой инстанции. Такая правовая конструкция и позволяет говорить об известном сужении границ уголовно-процессуального познания и, в конечном счете, об установлении юридической, а не объективной истины. При этом юридическая истина, конечно же, является целью доказывания, но в известных пределах, определяемых результатам состязания сторон, предметом доказывания и его логическими границами.

Несмотря на солидный срок, прошедший с момента принятия УПК РФ, сопротивление узаконениям, продиктованным принципом состязательности, не ослабевает по сей день [10, с. 9-26]. Не смолкают призывы вернуть в уголовно-процессуальный закон упоминание об объективной истине как цели доказывания [14]. В 2014 г. в Государственную Думу РФ даже внесен соответствующий законопроект, предусматривающий закрепление объективной истины в числе основных понятий УПК РФ [15].

Тогда инициатива не прошла. Но попытки выстроить правовое регулирование в сфере уголовного судопроизводства по советскому образцу не прекращаются и по сей день.

Не стихают дебаты вокруг института возвращения судами дел для дополнительного расследования, т.е. процедуры, позволяющей многократно исправлять ошибки следствия в рамках новых сроков следствия и последующих судебных разбирательств [6, с. 30]. Не прекращаются попытки откатить законодательство к реалиям советского периода. Об остроте схваток свидетельствует хотя бы то, что то, что ни одна норма в УПК не подверглась таким масштабным и радикальным изменениям, как ст. 237 УПК РФ. Она, словно оборванный, израненный пулями и снарядами флаг судебной реформы, продолжает гордо реять над непокоренными продолжающими оборону бастионами.

Стремления идеологов и практиков антиреформы понятны. Ведь существовавшая когда-то практика доследования (ст. 258 УПК РСФСР) закрепляла серьезное преимущество стороны обвинения по отношению к стороне защиты, что весьма характерно для инквизиционного

процесса. Основы же состязательного правосудия несколько иные. Actum est, ilicet — дело закончено, можно расходиться — говорили римские юристы [16, с. 650].

Исходом состязательного поединка могут стать либо победа, либо проигрыш. Метафорически картинка похожа на поединок боксеров. Чистый спорт, в котором побеждает сильнейший. Но кто согласится играть в условиях, когда на место поверженного соперника, от проигравшей команды на ринг выходит свежий боец. Финал такой борьбы легко предсказуем [6, с. 30]. Тот же итог легко прогнозируем и по результатам процедуры доследования, когда сторона, фактически проигравшая процесс, получает неожиданные преимущества по отысканию и представлению в суд новых доказательств.

В основе упомянутых противоречий и дискуссий различные философские, социальные и правовые взгляды на природу правосудия. Не стоит забывать, что судебный процесс по сути представляет собой поединок, каковой по мысли русского историка В.О. Ключевского,– не что иное, как намек на вид суда Божия [17].

Однако вернемся к современным реалиям. К сожалению, последние годы состязательность утрачивала роль фундамента, основы системы принципов уголовного судопроизводства. Произошел отход от общепризнанного принципа запрета на поворот к худшему в судебных стадиях процесса. Под «советское доследование», путем внесения многих поправок и исправлений, по сути «переформатирован» институт возвращения дела прокурору (ст. 237 УПК РФ) [18].

А ведь если вспомнить, изначально эта процедура преследовала совсем другие цели. Она предназначалась для исправления огрехов обвинительного заключения и устранения других препятствий к рассмотрению дела технико-юридического свойства. Но никак не восполнение доказательственной базы, пробелов и ошибок следствия [19].

Сомнительно с точки зрения равноправия сторон дополнение ч. 2 ст. 75 УПК РФ п. 2.1 сужающим возможности адвоката по представлению доказательств, а именно ссылаться на предметы, документы или сведения, входящие в производство адвоката по делам его доверителей, полученные в ходе оперативно-розыскных мероприятий или следственных действий [20].

Не способствовала укреплению состязательных начал уголовного судопроизводства набиравшая силу последние годы тенденция к увеличению доли дел, рассматриваемых в особом порядке, по правилам гл. 40 УПК. Согласно обзору судебной статистики о деятельности федеральных судов общей юрисдикции и мировых судей в 2019 г., большинство уголовных дел (55%), как и прежде, рассматривается в особом порядке, который предполагает согласие обвиняемого с предъявленным обвинением [21].

Отметим, что означенная процедура имеет мало общего с североамериканским правовым институтом сделки с правосудием, необходимостью имплементации которого в российский процесс, в свое время обосновывалась его необходимость [22, с. 130-136].

Спор между сторонниками и противниками состязательных начал в уголовном судопроизводстве продолжается. Однако дело не только в разности теоретических воззрений. Как отмечалось, состязательный процесс исторически во многом продукт религиозного сознания [23, с. 148-164] и в своем первоначальном виде во многом был сродни церковному таинству. Было бы крайне наивно полагать, что идеи суда совести, покаяния, божественной справедливости могут быть восприняты сознанием правоприменителя после 74 лет советского строя, проповедовавшего оголтелый атеизм.

Уход от состязательной идеологии и упор на совершенствования законодательной техники связан во многом с этим. Следователям удобнее иметь дело с привычными категориями всесторонности, объективности и полноты, чем с маловнятными законностью, обоснованностью и мотивированностью принимаемых решений. Да и принятие решений на основе правосознания, на первый взгляд, более осязаемая основа, чем метафизическая категория совести.

Авторы инициатив, направленных на сворачивание состязательных начал уголовного судопроизводства стремятся к достижению кратковременных тактических преимуществ, направленных, прежде всего, на упрощение процедуры расследования и судебного разбирательства по советскому образцу. Их оружием в отстаивании своих взглядов служат исключительно правила формальной логики и сиюминутный интерес. Казалось бы: благие намерения. Но согласно известной истине, — такой путь представляет собой дорогу в ад [24, с. 217].

Количество поправок в УПК, продиктованных исключительно мотивами дальнейшего совершенствования механизма правового регулирования, превысило все разумные пределы. Всего за время действия кодекса — с 1 июля 2002 г. — было принято 265 федеральных закона. В других странах парламенты не спешат переписывать свои установления. Некоторым памятникам права не одна сотня лет [25].

Очевидно, что правовые обычаи, традиции, произрастающие в глубь веков, основанная на них незыблемость правовых устоев — важные факторы социальной стабильности.

И наоборот, достижение оперативных сиюминутных целей сулит проигрыш в долговременной стратегической перспективе. Уже понятно, что состязательный процесс декларативно навязать невозможно. Его становление осуществимо лишь в результате системной, целеустремленной деятельности, направленной на изменение, эволюцию общественного сознания. Тут важно приложение совместных усилий научного сообщества, законодателей, правоприменителей, представителей гражданского общества.

В указанной связи обнадеживает позиция Президента России В.В. Путина, который, выступая 16 февраля 2016 г. на съезде судей в Москве, поддержал развитие состязательных начал в уголовном судопроизводстве и предложил использовать суды присяжных на районных уровнях [26]. Как известно, идея воспринята законодателем и реализована. С 1 июня 2018 г. суды присяжных действуют на уровне районного звена судебной системы [27], что, конечно, свидетельствует о расширении состязательных основ деятельности по осуществлению правосудия.

11 апреля 2019 г. Пленум Верховного суда РФ одобрил для внесения в Госдуму проект поправок в Уголовно-процессуальный кодекс РФ, которым предлагается исключить рассмотрение судами в особом порядке, без проведения судебного следствия, уголовных дел по тяжким преступлениям. Ранее против чрезмерного использования особого порядка рассмотрения уголовных дел, как фактора ухудшающего качество предварительного расследования, высказалась Генеральная прокуратура России [28].

В статистике судебного департамента при Верховном суде за 2019 г. доля оправдательных приговоров в российских судах выросла — впервые с 2013 г. (на 8,3% до 2256). Это объясняется прежде всего увеличением количества судов присяжных в районных судах и числа рассмотренных ими дел [29].

Указанные позитивные изменения в законодательстве могут стать толчком к развороту уголовно-процессуальной реформы в направлении состязательного правосудия.

Затронутые вопросы (расширения категорий дел подсудных судам присяжных, упорядочения особого порядка), к вопросу о цели доказывания, только на первый взгляд имеют опосредованное отношение. Надо понимать, что они являются крупными штрихами к портрету всей системы уголовного судопроизводства, позволяют дать характеристику реформы уголовного судопроизводства на современном ее этапе, выявить закономерности и основные черты, среди которых вопрос о возможности познания истины несомненно играет, ключевое значение.

Список литературы

1. Уголовно-процессуальное право Российской Федерации: учебник / под ред. П.А. Лупинской. М., 2009. С. 221.

2. Теория доказательств в советском уголовном процессе. Изд. 2-е, испр. и доп. М., 1973. С. 118.

3. Ленинская теория отражения. Истина как гносеологическая категория: сборник научных трудов. Свердловск: Изд. УрГу, 1983. 152 с.

4. УПК РСФСР в ред. 27.08.1993.

5. Радутная Н.В. Особенности воплощения принципа состязательности и равноправия сторон в уголовно-процессуальном законодательстве Российской Федерации: учеб.-метод. пособие. М.: РПА МЮ РФ, 2003. С. 3.

6. Сильнов М.А. Категория истины в условиях состязательного правосудия // Вестник Академии Генеральной прокуратуры Российской Федерации. 2014. № 5. С. 32.

7. Михайловский И.В. Основные принципы организации уголовного суда. Томск, 1905. С. 93.

8. Розин Н.Н. Уголовное судопроизводство. СПб., 1914. С. 303.

9. Ленин В.И. Полное собрание сочинений (5-е изд). Том 36. Сборник публикаций, текстов выступлений и интервью, писем и телеграмм. Изд-е пятое. М.: Политиздат, 1969. С. 282.

10. Александров А.С., Лапатников М.В., Терехин В.В. Этапы «большого пути» русского уголовно-процессуального права от полусостязательности — к инквизиции // Актуальные проблемы взаимосвязи уголовного права и процесса: сборник материалов Всероссийской заочной научно-практической конференции с международным участием (Уфа, институт права БашГУ, 17-18 апреля 2014 г.). Уфа: БашГУ, 2014. С. 9.

11. Sir William Blackstone. ‘Commentaries on the Laws of England’ (1765) bk. 4, ch. 27. Source: Knowles, E. Oxford dictionary of quotations. Oxford: Oxford University Press. 2014. P. 314.

12. Лупинская П. Доказательства и доказывание в новом уголовном процессе // Российская юстиция. 2002. № 7. С. 5.

13. Смирнов А.В., Калиновский К.Б. Уголовный процесс: учеб. для вузов / под общ. ред. А.В. Смирнова. 4-е изд., перераб. и доп. М.: КНОРУС. С. 63.

14. Бастрыкин А. Суть суда // Рос. газ. 2012. 16 марта.

15. Проект федерального закона № 440058-6 «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации в связи с введением института установления объективной истины по уголовному делу» от 29.01.2014.

16. Крылатые латинские выражения / авт.-сост. Ю.С. Цыбульник; худож.-оформ. Б.Ф. Бублик, В.А. Мурлыкин. М.: АСТ; Харьков: Фолио, 2003. С. 650.

17. Ключевский В.О. Русская история: полный курс лекций в 3 кн. Кн. 1. М., 1995.

18. Часть 4 ст. 237 УПК РФ, препятствовавшая производству по делу возвращенному прокурору, каких-либо следственных или иных процессуальных действий, была исключена в 2008 г. См. Федеральный закон от 02.12.2008 № 226-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации».

19. Комментарий к Уголовно-процессуальному кодексу Российской Федерации / отв. ред. Д.Н. Козак, Е.Б. Мизулина. М.: Юристъ, 2002. 1039 с.

20. ФЗ № 73-ФЗ от 17.04.2017.

21. Право.ru: [сайт]. URL: https://pravo.ru/story/218428/ (дата обращения: 20.05.2020).

22. Кельбиев М.Р. Сравнительно-правовой анализ американской сделки о признании вины и особого порядка судебного разбирательства российского уголовного судопроизводства // Вестник РУДН. Серия Юридические науки. 2010. № 4. С. 130-136.

23. Ключевский В.О. Курс русской истории. Полное издание в одном томе. М.: АЛЬФА-КНИГА, 2019. 1197 с.

24. Кирсанова А. Толковый словарь крылатых слов и выражений. М.: Мартин, 2004. 448 с.

25. Хабеас корпус акт (Великобритания) 1679, Билль о правах (США) 1791, Кодекс Наполеона (Франция) 1804, Уголовное уложение Германии 1871 и др.

26. ТАСС — Информационное агентство: [сайт]. URL: https://tass.ru/politika/2671763 (дата обращения: 08.11.2018).

27. ФЗ от 23 июня 2016 г. № 190-ФЗ и ФЗ от 23 июня 2016 г. № 209-ФЗ.

28. Российская газета: [сайт]. URL: https://rg.ru/2019/04/11/vs-zapretit-rassmatrivat-dela-po-tiazhkim-prestupleniiam-v-osobom-poriadke.html (дата обращения: 20.05.2018).

29. Ведомости: [сайт]. URL: https://www.vedomosti.ru/opinion/articles/2020/05/14/830283-nadezhda-prisyazhnih (дата обращения: 20.05.2020).

Научное издание

ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: ТЕОРИЯ И ПРАКТИКА

Сборник статей XVIII Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае»

Выпуск XVI

Редактирование и подготовка оригинал-макета — *С.И. Тесленко*

Оформление обложки — Ю.В. Плетнёва

ЛР 020261 от 14.01.1997.
Подписано в печать 14.12.2020. Формат 60x84 / 16.
Бумага офсетная. Усл.-печ. л. 16,04
Тираж 200 экз. Заказ № 361

Издательство Алтайского государственного университета

Типография Алтайского государственного университета:
656049 Барнаул, ул. Димитрова, 66