# Проблемы борьбы с преступностью в условиях цифровизации: теория и практика

Сборник статей
XIX Международной
научно-практической
конференции

«Уголовно-процессуальные
и криминалистические
чтения на Алтае»,

*посвященной памяти
советского и российского
ученого-криминалиста
Вениамина Константиновича Гавло,
доктора юридических наук,
профессора,
заслуженного деятеля науки РФ,
заслуженного юриста РФ*

Выпуск XVII

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

# ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

*Сборник статей XIX Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае», посвященной памяти советского и российского ученого-криминалиста Вениамина Константиновича Гавло, доктора юридических наук, профессора, заслуженного деятеля науки РФ, заслуженного юриста РФ*

Выпуск XVII

Барнаул
Издательство
Алтайского государственного
университета
2021

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 :** сборник статей XIX Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае», посвященной памяти Вениамина Константиновича Гавло. — Вып. XVII / отв. ред. С.И. Давыдов, В.В. Поляков. — Барнаул : Изд-во Алт. ун-та, 2021. — 500 с.

ISBN 978-5-7904-2589-9.

В сборник включены статьи участников XIX Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае», посвященной памяти одного из крупнейших отечественных ученых-криминалистов — доктора юридических наук, профессора, заслуженного деятеля науки РФ, заслуженного юриста РФ, почетного профессора Алтайского государственного университета Вениамина Константиновича Гавло, которому в 2021 г. исполнилось бы 85 лет.

Сборник статей является тематическим, затрагивающим вопросы противодействия преступности в условиях цифровизации криминалистическими, уголовно-процессуальными, уголовно-правовыми и иными средствами и методами. Авторами публикаций являются ученые, преподаватели, сотрудники правоохранительных органов и аспиранты из более чем 20 регионов Российской Федерации, а также из других стран.

Предназначено для ученых, преподавателей, сотрудников правоохранительных органов, аспирантов и студентов.

УДК 343:004(08)
ББК 67.51с51я431

ISBN 978-5-7904-2589-9

© Оформление. Издательство Алтайского государственного университета, 2021
© Коллектив авторов, 2021

***Вениамин Константинович Гавло (1936-2016)***

*доктор юридических наук, профессор, заслуженный деятель науки РФ, заслуженный юрист РФ, заведующий кафедрой уголовного процесса и криминалистики Алтайского государственного университета с 1983 по 2016 год, инициатор проведения Уголовно-процессуальных и криминалистических чтений на Алтае и издания сборника материалов конференции*

## СОДЕРЖАНИЕ

### ПЛЕНАРНЫЕ ДОКЛАДЫ

***Александров А.С.***
ОТ ЦИФРОВИЗАЦИИ К СОСТЯЗАТЕЛЬНОСТИ ..... 12
***Гаврилов Б.Я.***
О ПРИМЕНЕНИИ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ..... 17
***Давыдов С.И., Шмидт А.А., Наливайко Е.О.***
ПРОБЛЕМЫ ПОНЯТИЯ И СОДЕРЖАНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ХАРАКТЕРИСТИКИ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА ..... 26
***Зуев С.В.***
ЦИФРОВИЗАЦИЯ КАК НЕИЗБЕЖНОСТЬ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ ..... 32
***Климович Л.П., Логинова Н.Г., Дмитриев Г.П.***
ЭЛЕКТРОННОЕ УГОЛОВНОЕ ДЕЛО В ОТЕЧЕСТВЕННОМ УГОЛОВНОМ ПРОЦЕССЕ: МИФ ИЛИ РЕАЛЬНОСТЬ? ..... 35
***Козлов В.Е.***
ОБ ОТДЕЛЬНЫХ АСПЕКТАХ МЕХАНИЗМА ОБРАЗОВАНИЯ СЛЕДОВ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ ..... 44
***Корж В.П.***
ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ В УСЛОВИЯХ РЫНОЧНЫХ ОСНОВ ХОЗЯЙСТВОВАНИЯ: КРИМИНАЛИСТИЧЕСКИЕ ПРИЗНАКИ, ПОНЯТИЕ, КЛАССИФИКАЦИЯ ..... 54
***Кучин О.С.***
ТАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ РАБОТЫ СЛЕДОВАТЕЛЯ С ЭЛЕКТРОННЫМИ ЦИФРОВЫМИ УСТРОЙСТВАМИ ..... 62
***Лебедев Н.Ю.***
ОБЯЗАТЕЛЬНОЕ УЧАСТИЕ СПЕЦИАЛИСТА ПРИ ИЗЪЯТИИ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ХОДЕ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ ..... 70

***Поляков В.В.***
ПОНЯТИЕ СРЕДСТВ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРЕСТУПЛЕНИЙ .....76
***Яковец Е.Н.***
«ГОСУДАРСТВЕННЫЙ» КИБЕРТЕРРОРИЗМ: ЧЕМ ОН ОТЛИЧАЕТСЯ ОТ КИБЕРТЕРРОРИЗМА КРИМИНАЛЬНОГО? .....87

**ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

***Александрова Е.Г.***
НАЗНАЧЕНИЕ СУДЕБНЫХ ЭКСПЕРТИЗ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ.....100
***Алексеева Т.А.***
ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРОИЗВОДСТВА КОММУНИКАТИВНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ С ПРИМЕНЕНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ.....106
***Ахмедшин Р.Л.***
МЕТОДИЧЕСКИЕ, ТАКТИКО-КРИМИНАЛИСТИЧЕСКИЕ И ПРОЦЕССУАЛЬНЫЕ ОСОБЕННОСТИ ПРОВЕДЕНИЯ СУДЕБНО-ПСИХОЛОГИЧЕСКОЙ ЭКСПЕРТИЗЫ В РЕЖИМЕ ДИСТАНТНОГО ВЗАИМОДЕЙСТВИЯ (ONLINE-РЕЖИМЕ).....109
***Букур А.И.***
НЕКОТОРЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО СОПРОВОЖДЕНИЯ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ТРАВМАТИЧЕСКОГО ОРУЖИЯ.....115
***Герасименко Н.И.***
СОДЕРЖАНИЕ РАБОЧЕГО ЭТАПА ОСМОТРА ИНФОРМАЦИОННОЙ СРЕДЫ В СЕТИ «ИНТЕРНЕТ».....122
***Горшкова В.С.***
К ВОПРОСУ О КЛАССИФИКАЦИИ СУДЕБНЫХ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ .....130

***Гришин А.В., Ломовская А.В.***
РОЛЬ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫЯВЛЕНИИ И РАСКРЫТИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ..... 135
***Давыдова О.С.***
ОБ ИСПОЛЬЗОВАНИИ ОПЕРАТИВНО-РОЗЫСКНЫМИ ПОДРАЗДЕЛЕНИЯМИ РЕЗУЛЬТАТОВ ЭКСПЕРТНО-ДИАГНОСТИЧЕСКИХ ИССЛЕДОВАНИЙ СВОЙСТВ ЛИЧНОСТИ НЕУСТАНОВЛЕННЫХ КИБЕРПРЕСТУПНИКОВ ПО ИХ ПИСЬМЕННЫМ РЕЧЕВЫМ СЛЕДАМ ..... 139
***Davydova V.O., Usvyat N.D., Yakusheva T.V.***
WOMEN AS A SUBJECT OF RAPE IN THE CONTEXT OF GLOBALIZATION ..... 145
***Денисенко Ю.В.***
О ПРАВОВОМ РЕГУЛИРОВАНИИ ПРОТИВОДЕЙСТВИЯ ПРОЯВЛЕНИЯМ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В СЕТИ «ИНТЕРНЕТ»: РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ ..... 149
***Долгушина П.Е., Караваева А.В.***
ОСОБЕННОСТИ И ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ LINUX ДИСТРИБУТИВА CAINE ДЛЯ ПРОВЕДЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ИССЛЕДОВАНИЙ И ЭКСПЕРТИЗ ..... 159
***Драпезо Р.Г.***
КРАТКИЙ ОБЗОР IT-ТЕХНОЛОГИЙ, ПРИМЕНЯЕМЫХ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ УБИЙСТВ, СОПРЯЖЕННЫХ С ОГНЕМ ..... 164
***Дубынин Е.А., Космодемьянская Е.Е.***
НЕКОТОРЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ИМУЩЕСТВЕННЫХ ПРЕСТУПЛЕНИЙ ..... 175
***Дудко Н.А., Прусс А.Р.***
ПРАКТИКА ПРИМЕНЕНИЯ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ ПРИ РАССМОТРЕНИИ СУДАМИ УГОЛОВНЫХ ДЕЛ ..... 183
***Ермаков М.Г.***
ИСПОЛЬЗОВАНИЕ ДАННЫХ ПСИХОЛОГИЧЕСКОГО ПРОФИЛЯ ПОДОЗРЕВАЕМОГО ПРИ ДОПРОСЕ ПО ГРАБЕЖАМ И РАЗБОЯМ ..... 194
***Заливохина О.С.***
О НЕКОТОРЫХ ВОПРОСАХ ПРОГНОЗИРОВАНИЯ ИНФОРМАТИЗАЦИИ СУДЕБНО-ЭКСПЕРТНОЙ ДЕЯТЕЛЬНОСТИ ..... 198

***Иванов В.Ю.***
О ВОЗМОЖНОСТИ ПРОИЗВОДСТВА ДОПРОСА СВИДЕТЕЛЯ ПОСРЕДСТВОМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ В УСЛОВИЯХ ПАНДЕМИИ КОРОНАВИРУСНОЙ ИНФЕКЦИИ .....205
***Казакова А.В.***
ВОПРОСЫ ПРИМЕНЕНИЯ СИСТЕМЫ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ ПРИ ПРОИЗВОДСТВЕ ДОПРОСА .....212
***Калашников В.С.***
ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ СЛЕДОВ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ.....220
***Калюжный А.Н.***
ОТДЕЛЬНЫЕ АСПЕКТЫ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ, НАПРАВЛЕННЫХ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ТЕХНИЧЕСКИМ КАНАЛАМ СВЯЗИ В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ СВОБОДЫ ЛИЧНОСТИ.....225
***Каменев А.С.***
СОБИРАНИЕ ДОКАЗАТЕЛЬСТВ В ЭЛЕКТРОННОМ ВИДЕ СТОРОНОЙ ЗАЩИТЫ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ .....234
***Караваева А.В., Федосеева В.С.***
МЕТОДЫ И СРЕДСТВА СУДЕБНЫХ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ИССЛЕДОВАНИЙ ПРЕДПОЛОЖИТЕЛЬНО ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....240
***Карепанов Н.В.***
НЕКОТОРЫЕ ОСОБЕННОСТИ ПОИСКА И ИССЛЕДОВАНИЯ СЛЕДОВ ПРЕСТУПЛЕНИЙ В КИБЕРПРОСТРАНСТВЕ .....249
***Кирюшина Л.Ю., Соколов А.С., Кирюшина И.В.***
ПСИХОЛОГИЧЕСКИЕ ПРЕДПОСЫЛКИ ВИКТИМНОГО ПОВЕДЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ ПОТЕРПЕВШИХ .....256
***Книс Д.А.***
О ЗНАЧЕНИИ ОПЕРАТИВНО-РОЗЫСКНЫХ ХАРАКТЕРИСТИК ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СРЕДЕ, В ДЕЯТЕЛЬНОСТИ ПО ИХ ПРЕДУПРЕЖДЕНИЮ И РАСКРЫТИЮ .....263

***Кокушев А.Б.***
ИДЕНТИФИКАЦИЯ СТРЕЛЯНЫХ ГИЛЬЗ ПРИ ПОМОЩИ АВТОМАТИЗИРОВАННОГО БАЛЛИСТИЧЕСКОГО ИНФОРМАЦИОННОГО КОМПЛЕКСА (АБИК) «EVOFINDER» (ПО МАТЕРИАЛАМ РЕСПУБЛИКИ КАЗАХСТАН) .....269
***Количенко А.А.***
ИСТОКИ НОВОЙ ТЕОРИИ ОЦЕНКИ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В РОССИЙСКОМ УГОЛОВНОМ ПРОЦЕССЕ .....277
***Кондратьев М.В.***
О НЕКОТОРЫХ ОСОБЕННОСТЯХ МЕХАНИЗМА НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ, СОВЕРШАЕМОГО БЕСКОНТАКТНЫМ СПОСОБОМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ.....281
***Корчагин А.А.***
ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ДРУГИХ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ В ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОМ ОБЕСПЕЧЕНИИ ПРЕДВАРИТЕЛЬНОГО И СУДЕБНОГО СЛЕДСТВИЯ ПО УГОЛОВНЫМ ДЕЛАМ ОБ УБИЙСТВАХ.....291
***Кудайбергенова Е.А.***
ПРИМЕНЕНИЕ ИНСТИТУТА ПРОЦЕССУАЛЬНОГО СОГЛАШЕНИЯ В ФОРМЕ СДЕЛКИ О ПРИЗНАНИИ ВИНЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ НА ПРИМЕРЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВА (ПО МАТЕРИАЛАМ РЕСПУБЛИКИ КАЗАХСТАН) .....308
***Кузнецов А.А., Макаров Р.А.***
ДОПРОС ПОТЕРПЕВШЕГО ПРИ РАССЛЕДОВАНИИ ХИЩЕНИЙ С БАНКОВСКИХ КАРТ, СОВЕРШЕННЫХ ДИСТАНЦИОННО С ИСПОЛЬЗОВАНИЕМ IP-ТЕЛЕФОНИИ (SIP-ТЕЛЕФОНИИ) .....313
***Кукарцев В.Н.***
ОРГАНИЗАЦИОННЫЕ ПРОБЛЕМЫ РАСКРЫТИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ.....323
***Кязимова Д.Р., Ключёва Д.Ю., Шавыркин Б.Б.***
ИСПОЛЬЗОВАНИЕ ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ.....327

***Левченко О.В.***
ПРОКУРОР В УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ ЦИФРОВОЙ ЭКОСРЕДЕ .....335
***Льянов М.М.***
ПОРЯДОК ИЗЪЯТИЯ ВИРТУАЛЬНЫХ СЛЕДОВ .....340
***Мазуров В.А., Стародубцева М.А.***
НЕКОТОРЫЕ ПРОБЛЕМНЫЕ АСПЕКТЫ СТЕПЕНИ ЗАЩИЩЕННОСТИ НАСЕЛЕНИЯ АЛТАЙСКОГО КРАЯ ОТ ТЕРРОРИСТИЧЕСКИХ АКТОВ И АКТОВ КИБЕРТЕРРОРИЗМА.....345
***Маркелов А.Г.***
ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СОВРЕМЕННОГО УГОЛОВНОГО ПРОЦЕССА: СОСТОЯНИЕ И ОТДЕЛЬНЫЕ ПЕРСПЕКТИВЫ РАЗВИТИЯ.....350
***Милич И.Д.***
ОБ ОДНОЙ ВОЗМОЖНОСТИ УЛУЧШЕНИЯ ОСУЩЕСТВЛЕНИЯ ПРАВА НА УСЛОВНО-ДОСРОЧНОЕ ОСВОБОЖДЕНИЕ.....358
***Мужчиль С.А., Чакилева О.А.***
УГОЛОВНЫЕ ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В ВОСТОЧНО-КАЗАХСТАНСКОЙ ОБЛАСТИ.....363
***Набиуллина В.Р.***
УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ ПУБЛИЧНОМУ РАСПРОСТРАНЕНИЮ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМОМУ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....367
***Пинчук А.П.***
ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ ОПЕРАТИВНО-РОЗЫСКНОГО ОБЕСПЕЧЕНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ.....373
***Попов В.А., Д.В. Бондарев***
ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В ДОКАЗЫВАНИИ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....381
***Порываева П.С., Прокофьева Е.В., Мерзликин Р.А.***
АНАЛИЗ МЕТОДОВ И СРЕДСТВ ВЫЯВЛЕНИЯ СЛЕДОВ ПАЛЬЦЕВ РУК НА РАЗЛИЧНЫХ ПОВЕРХНОСТЯХ ПРИ ОСМОТРЕ МЕСТА ПРОИСШЕСТВИЯ.....387

***Пуричи А.В., Якушева Т.В.***
ОСОБЕННОСТИ ВЛИЯНИЯ АМОРАЛЬНОГО И ПРОВОЦИРУЮЩЕГО ПОВЕДЕНИЯ НА НАЗНАЧЕНИЕ НАКАЗАНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ УГОЛОВНОГО СУДОПРОИЗВОДСТВА.....392
***Рыжков И.В.***
ТРАНСФОРМАЦИЯ ПОДХОДОВ К ОРГАНИЗАЦИИ И ВЕДЕНИЮ НАТУРНЫХ КОЛЛЕКЦИЙ В ОТЕЧЕСТВЕННЫХ ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКИХ ПОДРАЗДЕЛЕНИЯХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ.....401
***Самарин В.И.***
ИНСТИТУТ МЕЖДУНАРОДНОЙ ПРАВОВОЙ ПОМОЩИ ПО УГОЛОВНЫМ ДЕЛАМ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ .....408
***Сизова В.Н.***
СОВЕРШЕНСТВОВАНИЕ ПРАВОВЫХ МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ.....416
***Сильнов М.А.***
О КРИТЕРИЯХ ДОПУСТИМОСТИ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ .....423
***Соколов А.Б.***
СОБИРАНИЕ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, НАХОДЯЩЕЙСЯ НА ЦИФРОВЫХ НОСИТЕЛЯХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. I. ПРОБЛЕМЫ ЦЕЛЕПОЛАГАНИЯ .....429
***Соколов А.Б., Щербина Р.П.***
СОБИРАНИЕ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, НАХОДЯЩЕЙСЯ НА ЦИФРОВЫХ НОСИТЕЛЯХ. II. ОСМОТР, ОБЫСК, СУДЕБНО-КОМПЬЮТЕРНАЯ ЭКСПЕРТИЗА .....434
***Суханова Л.Г.***
ОСОБЕННОСТИ УЧАСТИЯ АДВОКАТА-ЗАЩИТНИКА ПРИ ДОПРОСЕ СВИДЕТЕЛЯ С ИСПОЛЬЗОВАНИЕМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ .....439
***Телевицкая Ю.А.***
ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИЗЪЯТИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ В УГОЛОВНОМ ПРОЦЕССЕ ГОСУДАРСТВ-УЧАСТНИКОВ СНГ .....449

***Теткин Д.В., Пудовкин А.А.***
ПРОБЛЕМНЫЕ АСПЕКТЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ СОВРЕМЕННОЙ ЦИФРОВИЗАЦИИ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ .....458
***Черкасов В.С.***
ЭТАПЫ РАЗВИТИЯ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ ОТНОШЕНИЙ ПОД ВОЗДЕЙСТВИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ .....465
***Шавыркин Б.Б.***
ТЕХНОЛОГИЯ 3D-ПЕЧАТИ В КОНТЕКСТЕ ПРОБЛЕМЫ КОНТРОЛЯ ЗА ОБОРОТОМ И ПРИМЕНЕНИЕМ 3D-ОРУЖИЯ .....470
***Шепель Н.В.***
ПРОБЛЕМЫ ПРАКТИКИ ПРИВЛЕЧЕНИЯ СОТРУДНИКОВ ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКИХ ПОДРАЗДЕЛЕНИЙ В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....476
***Шурухнов В.А.***
СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ....480
***Юань В.Л.***
АНАЛИЗ БИОГРАФИЧЕСКИХ СВЕДЕНИЙ ЛИЦ, СКЛОННЫХ К ГРУППОВОЙ МОРАЛИ, В РАМКАХ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ЗЛОУПОТРЕБЛЕНИЙ ДОЛЖНОСТНЫМИ ПОЛНОМОЧИЯМИ .....486
***Якушева Т.В., Темиржанова Л.А., Жадауова Ж.А.***
АКТУАЛЬНЫЕ ПРОБЛЕМЫ ВОЗМЕЩЕНИЯ УЩЕРБА И ОБЕСПЕЧЕНИЯ ПРАВ ГРАЖДАН В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ РЕСПУБЛИКИ КАЗАХСТАН В СВЕТЕ ПРЕДСТОЯЩЕГО СУДЕБНОГО РЕФОРМИРОВАНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ.....491

# ПЛЕНАРНЫЕ ДОКЛАДЫ

***А.С. Александров,*** *д.ю.н., профессор, профессор кафедры уголовного процесса Нижегородской академии МВД России, г. Нижний Новгород*

## ОТ ЦИФРОВИЗАЦИИ К СОСТЯЗАТЕЛЬНОСТИ

Тема цифровизации вполне овладела широкими массами научной юридической общественности. Не стали исключением и процессуалисты. Только ленивый из них не высказался о том, как цифровизация повлияла (или еще повлияет) на уголовное судопроизводство в целом, его отдельные процедуры. Это означает, что авторам, не способным к раскрытию специальных — технических вопросов и одновременно чурающихся банальностей, можно данную тему бросать. Теперь слово за криминалистом, специалистом-компьютерщиком, искушенным в закономерностях следообразования киберпреступлений, способным дать конкретное знание о закономерностях раскрытия и расследования преступлений по цифровым следам.

Будучи профаном в компьютерных технологиях, могу порассуждать только о том, каким должно быть уголовно-процессуальное право. Для меня как теоретика уголовного процесса осталось некоторое место для проявления оригинальности по означенной теме — на теоретико-методологическом уровне. Позволю себе поделиться с коллегами несколькими соображениями, которые, как мне известно, отличаются от их мнения. Суть наших разногласий проста: я и некоторые мои единомышленники [1, с. 199-207] считаем, что цифровая революция подготовила почву для перехода отечественного процесса от следственного (смешанного) типа к состязательному. Тогда как большинство коллег, будучи юрпозитивистами, остаются в следственной парадигме и рассуждают о новых явлениях по старым мыслительным схемам, созданным их старшими товарищами, в «доцифровую эпоху».

Отправным пунктом рассуждений будет констатация того, на мой взгляд, очевидного факта, что следственная форма доказывания исчерпала себя в условиях развития цифровых технологий, которая ведет к смене коммуникативной модели общества.

Современный уголовный процесс построен на власти следователя формировать доказательства — для суда и для всех остальных. Это авторитарная модель власти и знания. Обычный человек чужд ей. Цифровые технологии открывают совершенно новые возможности для *демонополизации* исполнительной (следственной) власти на установление истины, то есть *деэтатизации* уголовно-процессуального познания — это — с одной стороны, и гуманизации этого процесса — допущения к нему любого лица — с другой.

Суть следственной технологии доказывания состоит в письменной фиксации следователем обнаруженных им следов преступления в протоколах следственных действий. Приложение к протоколу в виде электронных носителей информации, создаваемых с помощью технических средств, подчас информативнее письменного протокола. Но формально юридическая сила протокола сильнее, ибо именно он называется источником доказательства, приложение производно от него и потому не всегда даже воспроизводится в суде. Важным достоинством следственного протокола является и то, что он облегчает работу судьи по ознакомлению с делом. И в судебном следствии зачастую имеет место то же самое: оглашаются одни протоколы. Прочитать протокол проще, чем воспроизводить, например, аудио- или видеозаписи, сделанные в ходе оперативно-разыскных мероприятий, следственных действий.

Для суда и сторон ознакомление с доказательствами через протокол проще, чем из первоисточника. Но в этом же и опасность попадания в информационную зависимость от следователя — прежде всего для судьи, ибо протокол есть интерпретация, пересказ следователем того, что он воспринял в ходе следственного действия. Отсюда известное в науке явление «следственного изоморфизма», когда все профессиональные участники процесса привычно презюмируют следственный стандарт процедурного знания как общий, универсаль-

ный. Забывая, что следователь — это не только субъект «объективного и всестороннего» расследования, но и представитель стороны обвинения в деле. Отсюда неизбежный, неискоренимый обвинительный уклон в его деятельности, а вместе с тем — и нашей системы уголовного правосудия.

На мой взгляд, в цифровой информационной революции есть перспектива как для демократизации, открытости общества и власти, так и угрозы тотализации власти и установления тотального контроля над человеком. Отсюда наш призыв — бороться за то, чтобы информационные технологии были использованы для развития свободы и безопасности, а не стали средством укрепления репрессивной власти и следственного механизма ее реализации в сфере противодействия преступности. Это глобальная политико-правовая проблема. В техническом же плане вполне очевидно то, что пора бросать следственную, письменную технологию фиксации и передачи информации и переходить к иной — судебной, состязательной модели доказывания истины. Это означает качественную перестройку работы всей системы правосудия, если в основу будет положена судебная модель формирования доказательств. Многие противники такой реформы указывают на данный момент. Это опасение снимается тем, что в других странах, например, США, такая система действует. При том условии, что более 90% уголовных дел слушаются в особом порядке ввиду согласия обвиняемого с обвинением, без представления и исследования доказательств. Так должно быть и у нас, но чтобы перейти на такую модель процессуального доказывания, необходимо изменить ряд принципиальных положений в доказательственном праве. Это и было сделано нами в нашем общеизвестном научном проекте [2].

Важнейшим средством юридикализации познания является устанавливаемый законом искусственный критерий отбора информации, а именно как допустимой, пригодной к установлению фактов. Можно сказать, что в стандарте допустимости сконцентрирована идеология данного типа процесса. Допустимым уголовно-процессуальным доказательством по нашему праву является доказательство, полученное и зафиксированное следователем по правилам УПК РФ. Надо пересмотреть следственный стандарт допустимости. Цифровая информация, представленная суду и сторонам в электронном виде на отдельном носителе

или через телекоммуникационные каналы связи любым лицом, может быть допущена при наличии возможности верификации ее аутентичности. Снятие следственного ограничителя, гуманизация доказывания, то есть допущение к получению доказательств и их источников любого субъекта, при одновременном привлечении обучаемых машин и автоматизированных систем — таковы основные направления изменения доказательственного права. Мы изложили их в «Доктринальной модели уголовно-процессуального доказательственного права РФ».

Впрочем, я вполне осознаю всю ограниченность нашего проекта: чтобы изменить парадигму знания, процессуально-правовую доктрину (доказывания), надо еще кое-что затронуть: то, что самое трудное. Это то, что лежит в основании правосознания, правовой культуры. Наша правовая культура сформировалась в условиях автократии, уголовно-процессуальное право, доказательственное право — все это порождения автократической власти и присущей ей публичной речи (модели коммуникации в общественной сфере). Отсюда и распространенные на уровне массовой психологии и в среде профессионалов стереотипы сознания, унаследованные из нашего коллективного опыта обществ, сформировавшихся в условиях авторитаризма. Так, известный украинский публицист, блогер, психиатр С. Глузман диагностировал, что в Украине и сегодня сильны прежние, советские правовые традиции. Так, при выведении обобщенных показателей солидарности граждан с уголовным законодательством в сравнении с процессуальным было выявлено, что показатели солидарности с уголовным правом во много раз выше. Превосходство уголовного права достигает десятикратного размера. Следовательно, массовое сознание в Украине расценивает репрессивную сторону права как более существенную, чем гарантийную. Законопослушные украинцы легче представляют себя потерпевшими, нежели обвиняемыми. Отсюда в ряде случаев возникает феномен процессуального нигилизма: недоверие к возможности обвиняемого получить реальное право на защиту, к недекларативности презумпции невиновности и т.п. [3.].

Уму россиянина привычно, что государство посредством права воздействует на общественные отношения, субъектом которых является человек. Человек является объектом и уголовно-правового воздействия государства. В этом корни

догмата о доминанте материального, уголовно-правового, а значит, и карательного момента в правовой системе противодействия преступности.

На мой взгляд, цифровая революция освобождает сознание от привычных представлений о государстве, праве, механизме правового регулирования. Нами был разработан и предложен альтернативный классическому концептуальный аппарат, позволяющий по-новому осмыслять правовую реальность и перестраивать «уголовно-процессуальный механизм» [4, с. 75-86]. Например, заменой классическому понятию государства выступает концепт «Государство-как-платформа», которое можно понимать как некое кибернетическое устройство, позволяющее представлять набор услуг (функций) населению и бизнесу в автоматизированном режиме. Его прообразом выступает современный портал государственных услуг (ЕПГУ), на котором будут размещены и услуги уголовно-процессуального назначения: обвинения, уголовного расследования, правосудия. Глобальная перемена в правосознании, связанная с представлением о сервисном государстве, состоит в деэтатизации правовой культуры, в освобождении от архетипа «государство-левиафан».

Понятие «право», как систему правовых норм, представленных в форме закона, мы предлагаем заменить на концепт «право-процесс», допускающее соучастие в производстве средства правового воздействия участников процесса: интерпретации смысла закона, аргументации, доказывания. Оно корреспондирует новому типу правового регулирования: «wiki-правовое регулирование», участники которого онлайн генерируют новые правила на базе законодательного акта, акцептируют их для разрешения конкретной правовой ситуации и включают их в общий корпус правовых предписаний, поддерживаемых технологией блокчейна. Каждый участник процесса может стать со-творцом «права» вместе с автором текста закона.

Отсюда уголовный процесс мы понимаем как цифровую экосреду, где участники процесса создают актуальное средство разрешения уголовного дела. Процесс — не просто форма правоприменения, но правотворчество. Уголовный процесс — не орудие борьбы государства с преступностью и место взаимодействия участников конфликта, поддерживаемое цифровыми технологиями,

по выработке оптимального правового средства разрешения конфликта. Поэтому не уголовное право, а состязательный уголовный процесс есть основа правовой организации противодействия преступности.

**Список литературы**

1. Александров А.С., Андреева О.И., Зайцев О.А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестник Томского гос. ун-та. 2019. № 448. С. 199-207.

2. Доктринальная модель уголовно-процессуального доказательственного права РФ и Комментарии к ней / А.С. Александров и др. М.: Юрлитинформ, 2015. 304 с.

3. Глузман С. О кроватях, девочках и правосудии. [Электронный ресурс]. URL: https://racurs.ua/b195-o-krovatyah-devochkah-i-pravosudii.html

4. Александров А.С., Александрова И.А., Власова С.В. Теоретическая концепция государственно-правовой организации противодействия преступности в 21 веке // Государство и право. 2019. № 9. С. 75-86.

***Б.Я. Гаврилов,*** *д.ю.н., профессор, профессор кафедры управления органами расследования преступлений Академии управления МВД России, г. Москва*

## О ПРИМЕНЕНИИ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Говоря о масштабах преступности с использованием информационно-телекоммуникационных технологий, следует указать на ее стремительный рост в последние годы. Наглядно это подтверждается статистическими данными ГИАЦ МВД России, согласно которым, в 2020 г. в России было зарегистрировано порядка 5,10 тыс. преступлений данного вида, что на 72% превышает уро-

вень 2019 г. (294,4 тыс. таких преступлений), а последний, в свою очередь, на 68,5% превышает аналогичный показатель 2018 г. Удельный вес деяний данной категории в общем массиве преступлений в 2020 г. составил 25,5% против 4,4% в 2017 г., или возрос более чем в 5 раз. Таких темпов прироста отдельных видов преступлений российская статистика не знала. Опасность данного вида преступлений состоит и в том, что в истекшем году 48,5% из них составили тяжкие и особо тяжкие преступления.

С учетом складывающейся криминологической обстановки, обусловленной в том числе цифровой трансформацией современной преступности [1, с. 204-212], особую актуальность приобретают вопросы преодоления противодействия расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Ведя речь о воздействии цифровых технологий на преступную деятельность, следует отметить еще и такой фактор, как ее поступательное развитие, ввиду появления новых способов совершения преступлений и интеграции, как отмечено, цифровых технологий в уже имеющиеся способы. Это обусловливает необходимость изучения не только этих способов методами как технических, так и юридических наук, но и развития подходов к изучению цифровых следов и производных от них электронных доказательств, без чего не может обходиться современный процесс расследования преступлений.

Рассматривая эти направления, следует обратиться к работе В.Б. Вехова и С.В. Зуева «Цифровая криминалистика» [2, с. 295-297], в которой указанные авторы разделяют преступления, связанные с использованием цифровых технологий, на два типа:

– посягающие на цифровую инфраструктуру, работоспособность информационных систем и банков данных и цифровую информацию. В этом случае цифровые технологии определяют общие или отдельные характеристики предмета преступного посягательства;

– при совершении которых цифровые технологии интегрированы в способ совершения преступления.

*К первой группе* В.Б. Вехов и С.В. Зуев относят преступления, связанные с использованием вредоносного программного обеспечения: вирусов, троянов, с помощью которых происходит заражение компьютерных устройств. Такие преступления в российском уголовном праве носят название преступлений в сфере компьютерной информации, и ответственность за них предусмотрена ст. 272-2741 УК РФ. Субъекты преступлений этого типа в большинстве случаев обладают специальными навыками в области программирования, сетевого администрирования, компьютерной безопасности и т.д.

Необходимо также учитывать, что преступления этой группы способны посягать не только на общественные отношения в сфере компьютерной информации и цифровых технологий, но и на конституционные права человека и гражданина, сферу экономики, здоровье населения и общественной нравственности. Преступления данного вида являются зачастую трансграничными, анонимными (по крайней мере, в начале расследования) и в своем большинстве латентными.

*Вторая группа* может включать в себя общеуголовные преступления, при совершении которых использование цифровых технологий является частью способа подготовки, совершения или сокрытия преступления. Примерами такого рода действий являются коммуникация преступников через мобильные приложения-мессенджеры, подмена номера sim-карты в целях совершения мошенничества, создание фишинговых сайтов для совершения мошенничества, легализация доходов, полученных преступных путем и т.д.

В этом случае необходимость анализа информации о соединениях между абонентами и/или абонентскими устройствами включается в план расследования, а изучение sms-сообщений и сообщений в мессенджерах и социальных сетях используется для подтверждения факта соучастия и выяснения ролей соучастников.

Особенностью преступлений обоих типов является то, что в процессе их совершения формируется система цифровых следов, которые, аналогично другим типам следовой информации, могут быть обнаружены, зафиксированы, исследованы и в конечном счете приобрести статус доказательств по уголовному

делу. Разумеется, каждый отдельный способ совершения преступлений, связанный с цифровыми технологиями, имеет самостоятельный механизм следообразования и, соответственно, различные типы объектов, подлежащих исследованию, а также способы сокрытия данных преступных действий, что обусловливает разнообразие как специальных технических средств, так и средств уголовно-процессуального доказывания.

Как отмечается в научной литературе, задача цифровых технологий, используемых в деятельности правоохранительных органов по раскрытию и расследованию преступлений, — адаптировать существующие базовые алгоритмы работы с информацией для решения задач криминалистической деятельности [3, с. 61].

Одним из ключевых классификационных оснований цифровых технологий в правоохранительной деятельности является их функциональное предназначение, то есть относимость к той или иной операции (действию). Ключевыми такими действиями являются обнаружение и фиксация доказательственной информации в цифровой форме как входе производства следственных действий, так и оперативно-розыскных[1] мероприятий и в ходе производства судебных экспертиз [4, с. 26-28; 5, с. 6-9; 6, с. 85-86].

Конкретные технические средства могут включать также и специализированные (например, специальные операционные системы, ориентированные на цифровые криминалистические исследования, стендовые компьютеры и т.д.).

Дальнейшее развитие цифровых технологий, как отмечается в научной литературе, требует унификации понятийного аппарата, процессуального закрепления использования информационных технологий в работе с доказательственной информацией при ее собирании и исследовании, совершенствования особенностей профессиональной подготовки субъектов применения научно-техни-

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

ческих средств и методов, использования в расследовании специальных познаний [7, с. 9-12] и т.д.

Рассмотрим более подробно информационные технологии в контексте следственных действий. С точки зрения следственной деятельности работа с цифровыми технологиями, как правило, оформляется протоколами следственного осмотра, получения информации о соединениях между абонентами и (или) абонентскими устройствами, контролем и записью переговоров.

Так, идентификационный модуль абонентов сотовой связи зачастую используется преступниками для обеспечения анонимности своей личности. Поэтому в пользовании у лиц, причастных к совершению преступления, нередко оказываются абонентские номера, оформленные на третьих лиц, либо в отношении которых оператор связи регистрационными сведениями не располагает. В целях противодействия использования таких «анонимных» абонентских номеров следственные органы в соответствии с действующим законодательством могут инициировать процедуру проверки регистрационных данных абонента оператором связи, запросить у него список абонентских номеров, с которыми связывалось интересующее лицо и тем самым установить круг его общения, состав преступной группы и иные обстоятельства.

Понимание специфики работы с носителями цифровой доказательственной информации облегчает производство таких следственных действий, как следственный осмотр, обыск, выемка. Даже при проведении проверки показаний на месте и следственного эксперимента возможно использование цифровых технологий, к примеру, для сравнения маршрута, демонстрируемого проверяемым лицом, с данными о его перемещении, полученными в ходе криминалистического исследования его смартфона. Проверка функциональности фишингового сайта в зависимости от конкретной задачи расследования может быть реализована в форме следственного осмотра, следственного эксперимента, либо производства судебной компьютерной технической экспертизы.

Приведенные примеры демонстрируют, что цифровые технологии могут использоваться следственными органами на разных уровнях: как средства об-

наружения и фиксации доказательственной информации, либо как источник проверяемых сведений.

Система мер, направленная на преодоление противодействия расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий, включает в себя правовые, организационные и криминалистические.

В число правовых мер входит, в первую очередь, комплекс положений действующего законодательства, направленных на деанонимизацию пользователей информационных ресурсов сети Интернет, а именно:

– ст. 10.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», возлагающая на интернет-провайдеров обязанности по идентификации пользователей и хранению на территории Российской Федерации передаваемого пользователями контента и фактов доступа к информационным ресурсам;

– ст. 44, 64 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», которой на оператора связи возложены аналогичные обязанности;

– Федеральным законом от 05.05.2014 № 110-ФЗ введены ограничения для анонимных платежей, совершаемых онлайн, и установлена процедура обязательной идентификации пользователей электронных средств платежа;

– Федеральный закон от 29.07.2017 № 241-ФЗ обязывает организатора обмена мгновенными сообщениями (мессенджеров) обеспечивать идентификацию своих клиентов;

– положение Банка России от 09.06.2012 № 382-П устанавливает перечень сведений, подлежащей фиксации оператором электронных платежных средств.

Во-вторых, к числу правовых средств преодоления расследования рассматриваемых преступлений входит комплекс норм, регламентирующих порядок формирования доказательств на электронных носителях информации, а именно:

– п. 5 ч. 2 ст. 82 УПК Российской Федерации (далее — УПК РФ), устанавливающий основания и порядок хранения электронных носителей информации — вещественных доказательств;

– ст. 164.1 УПК РФ, устанавливающая основания для изъятия электронных носителей информации, допускающая копирование информации и вводящая требование обязательного участия при этом специалиста;

– ч. 7 ст. 185, позволяющая производить осмотр и выемку электронных сообщений и др.

К организационным мерам преодоления противодействия расследованию рассматриваемых преступлений относятся:

– закрепление специализации следователей на расследовании преступлений в сфере информационных технологий, с учетом опыта и наличия специальных познаний в указанной области;

– заблаговременное обсуждение материалов доследственных проверок в аппаратах следственных органов МВД России по субъектам Российской Федерации, уделяя особое внимание их полноте и качеству, проведению необходимых исследований, результатам оперативно-розыскных мероприятий;

– использование территориальными органами внутренних дел систем электронного документооборота, а также заключение соглашений об информационном обмене с кредитно-финансовыми организациями, операторами платежных систем, операторами связи и интернет-провайдерами, что позволяет с минимальными временными затратами получать необходимые сведения об анкетных данных абонента по номерам телефона и СИМ-карты, о подключенных услугах и произведенных платежах, а также о движении денежных средств клиента кредитно-финансовой организации, включая данные об отправителе, получателе, сумме операции, дате и времени ее проведения, наименования сервиса, через который она была проведена, IP-адресе, с которого произведена транзакция, IMEI — номере абонентского устройства, при получении наличных через банкомат — его номер, место установки, видеозапись встроенной камеры наблюдения и другие сведения, имеющие значение для полного, всестороннего и объективного производства расследования в разумные сроки.

В числе криминалистических средств преодоления противодействия расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий, следует выделить, в первую очередь, обоснованные Г.З. Гаспаряном [8, с. 26-27] тактические приемы производства следственных действий, направленных на получение невербальной доказательственной информации, в частности:

– радиоподавление, направленное на недопущение приема/передачи информации, подачу команд с использованием беспроводных компьютерных сетей и сетей мобильной связи;

– преодоление аппаратно-программного шифрования данных, состоящее в использовании технико-криминалистических средств получения доступа к информации, находящейся на электронном носителе, защищенной алгоритмом шифрования;

– нелинейная локация, направленная на обнаружение и определение местонахождения устройств, содержащих электронные компоненты во включенном и в выключенном состоянии;

– криминалистический анализ данных, состоящий в систематизации содержащейся на электронном носителе информации, позволяющей выполнять поиск данных с заданными характеристиками;

– криминалистическое копирование данных, позволяющее создавать их дубликат, соответствующий оригиналу как по содержанию, так и по технологическим свойствам;

– формирование по особым алгоритмам контрольных сумм изымаемой в процессе следственного действия информации, обеспечивающее достоверность доказательств на основе сопоставления параметров изъятой и впоследствии исследуемой информации;

– изготовление «скриншотов» в процессе фиксации доказательственной информации, состоящее в копировании содержания экрана с использованием встроенной функции операционной системы;

– гибернация, состоящая в переводе изымаемого устройства в энергосберегающий режим, позволяющий сохранить содержание оперативной памяти.

Кроме того, повысить уровень информационно-аналитического обеспечения органов предварительного следствия в процессе расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, призвана повысить введенная в эксплуатацию в 2019 г. информационная система «Дистанционное мошенничество» [9], предназначенная для сбора, систематизации, обработки и анализа сведений, устанавливаемых в рамках расследования уголовных дел по преступлениям, совершенным дистанционным способом. Система аккумулирует данные об использованных при совершении преступления идентификационных данных средств связи, номерах банковских карт и банковских счетов, номерах документов, удостоверяющие личность, а также реквизитах организаций, упоминающихся в материалах дела.

В заключение следует отметить, что приведенный перечень не является исчерпывающим, постоянно расширяется и адаптируется к новым способам вызовам современной преступности.

## Список литературы


1. Гаврилин Ю.В. Тенденции цифровой трансформации преступности и факторы, ее обуславливающие // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сборник статей Международной научно-практической конференции / под общ. ред. И.Г. Чистобородова, А.Л. Ситковского, В.О. Лапина. 2020. С. 204-212.
2. Вехов Б.В., Зуев С.В. Цифровая криминалистика. М., 2021. С. 295-297.
3. Рудых А.А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. … канд. юрид. наук. Ростов н/Д, 2020. С. 61.
4. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. № 3. С. 26-28.
5. Вахмянина Н.Б., Иванов Э.А. Возможности использования программ-транскрайберов при производстве следственных действий // Российский следователь. 2019. № 2. С. 6-9.

6. Осипенко А.Л. Новое оперативно-розыскное мероприятие «Получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России. 2016. № 3. С. 85-86.

7. Гриб В.Г., Тюнис И.О. Криминалистика и цифровые технологии // Российский следователь. 2019. № 4. С. 9-12.

8. Гаспарян Г.З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: автореф. дис. … канд. юрид. наук. М., 2020. С. 26-27.

9. Приказ МВД России от 22.04.2020 «О вводе в эксплуатацию подсистемы «Дистанционное мошенничество» ПТК ИБД-Ф».

***С.И. Давыдов,*** *д.ю.н., заведующий кафедрой уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*

***А.А. Шмидт****, к.ю.н., начальник кафедры оперативно-разыскной деятельности органов внутренних дел Барнаульского юридического института МВД России, г. Барнаул*

***Е.О. Наливайко****, преподаватель кафедры оперативно-разыскной деятельности органов внутренних дел Дальневосточного юридического института МВД России, г. Хабаровск*

## ПРОБЛЕМЫ ПОНЯТИЯ И СОДЕРЖАНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ХАРАКТЕРИСТИКИ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА

Оперативно-розыскная характеристика (далее — ОРХ) преступлений как категория, используемая в теории оперативно-розыскной деятельности (далее — ОРД), с одной стороны, прочно вошла в понятийный аппарат оперативно-розыскной науки, а с другой — продолжает являться предметом дискуссий. Научные споры ведутся не только по вопросу ее структурных элементов и значения, но и по поводу того, нужна ли вообще ОРХ преступлений. К примеру,

С.И. Захарцев считает, что «разработка оперативно-розыскной характеристики преступлений научной значимости не имеет, <…> оперативно-розыскная характеристика практикой не востребована и ей не нужна. Необходимые для работы знания приобретались и приобретаются практиками в рамках других наук» [1, с. 159]. Мы же являемся сторонниками другой точки зрения относительно ОРХ преступной деятельности, которая поддерживается и развивается большинством ученых в области ОРД. В обобщенном виде ее сформулировал В.Д. Ларичев: «В теории оперативно-розыскной деятельности как отрасли научного знания, изучающей преступность и преступления, необходимо конструирование самостоятельной оперативно-розыскной характеристики преступлений, в содержание которой необходимо включать только такие сведения, использование которых способствует эффективному применению разведывательно-поисковых сил, средств и методов оперативных аппаратов органов внутренних дел в борьбе с преступностью» [2, с. 185].

Доказано теорией и практикой, что важнейшим условием разработки эффективных организационных мер, тактических приемов выявления и раскрытия преступлений является знание их ОРХ. Применительно к разработке методики раскрытия дистанционного мошенничества категория ОРХ приобретает особое значение, поскольку этот вид преступлений совершается с использованием информационно-телекоммуникационных сетей, для него являются специфическими способы совершения и механизмы следообразования. Специфику дистанционного мошенничества характеризует и нахождение преступников и потерпевших на удалении, как правило, в разных регионах, широкая распространенность этих преступлений. Указанные характеристики дистанционного мошенничества, безусловно, являются важным фактором, влияющим на организацию и тактику противодействия им оперативно-розыскными средствами и методами.

В теории ОРД институт ОРХ отдельных видов преступлений (групп преступлений) активно исследуется с конца 70-х гг. прошлого столетия. Именно в этот период появились первые публикации, содержащие попытки анализировать противоправные деяния с позиции теории ОРД. В конце XX столетия

И.А. Климов и Г.К. Синилов подвели некоторый итог, определив, что учение об ОРХ преступлений находится еще в стадии формирования [3, с. 34]. Несмотря на то, что вывод этот сделан более 20 лет назад, он актуален и для сегодняшнего времени, поскольку существуют разные подходы к определению понятия, сущности и содержания ОРХ преступлений.

В начальный период формирования теории ОРД проблему понятия ОРХ преступлений рассматривали в своих публикациях такие известные ученые, как А.И. Алексеев, В.М. Атмажитов, В.Г. Бобров, В.В. Гордиенко, Д.В. Гребельский, Ю.В. Дамов, В.Д, Ларичев, Б.П. Смагоринский, Л.Л. Тузов, В.Б. Утевский, Ю.М. Худяков, А.Ю. Шумилов и другие.

Свое развитие учение об ОРХ преступлений получает и в настоящее время, о чем свидетельствует целый ряд публикаций. Среди их авторов — Б.В. Борин [4], П.И. Иванов [5], В.Ф. Луговик [6], В.Н. Омелин [7], Д.Ю. Федорович [8], А.И. Хмыз [9] и др.

Нами также проанализирован ряд публикаций, посвященных специально ОРХ дистанционных мошенничеств (В.Г. Горбанев [10], В.Г. Любан, А.Ю. Молянов, Е.Н. Хазов [11], А.П. Подшивалов и А.С. Малахов [12] и др.).

При определении понятия и содержания ОРХ дистанционного мошенничества нам было весьма полезно обратиться к фундаментальным исследованиям проблемы криминалистической характеристики преступлений (Р.С. Белкин, А.В. Васильев, В.К. Гавло, В.Я. Колдин, Н.П. Яблоков и др.). Из числа последующих исследований выделим труды И.И. Рубцова [13], А.С. Князькова [14], А.А. Бессонова [15], определение криминалистической характеристики преступлений которого, с нашей точки зрения, важно учитывать при исследовании сущности и значения ОРХ преступлений. Он формулирует его таким образом: это информационная модель, «которая отражает криминалистическую сущность преступлений определенного вида (подвида, криминалистически схожих групп), заключающуюся в сведениях о его криминалистически значимых признаках и их закономерных связях между собой. Такая модель построена на основе анализа и изучения практики их расследования и судебного рассмотрения. Она имеет

значение для формирования частных методик расследования и решения задач деятельности по расследованию и предупреждению преступлений» [15, с. 11].

С учетом анализа научных источников приходим к выводу, что ОРХ дистанционного мошенничества целесообразно определить следующим образом: это совокупность наиболее характерной оперативно значимой взаимосвязанной информации о признаках их подготовки, совершения и сокрытия, имеющей значение для формирования частной методики раскрытия дистанционных мошенничеств и определяющей содержание практической деятельности оперативных подразделений по их раскрытию.

Представляется, что вопрос определения структурных элементов ОРХ дистанционного мошенничества следует решать исходя из следующих общих положений, сформулированных в разное время в оперативно-розыскной теории:

– в систему ОРХ должны входить обобщенные данные о наиболее типичных, устойчивых и повторяющихся оперативно-значимых признаках преступления;

– количество и содержание образующих ОРХ элементов не может быть универсальным и зависит от конкретного вида (группы) преступлений, поскольку одни элементы информативные в оперативно-розыскном отношении для одних групп преступлений, могут быть неинформативными или слабоинформативными для других групп; идею о главных и факультативных признаках ОРХ преступлений развивает, в частности, В.Ф. Луговик;

– для разработчиков частных оперативно-розыскных методик и практических сотрудников важны сведения о наличии корреляционных связей между элементами ОРХ, которые, как пишет А.А. Бессонов, применительно к криминалистической характеристике, могут быть двух видов: 1) корреляционные (однозначные), когда присутствие одного элемента позволяет совершенно определенно судить о существовании и другого, а изменение характеристики первого влечет изменение характеристики второго; 2) вероятностно-статистические, при которых установление одного элемента позволяет с большей или меньшей степенью вероятности предполагать наличие другого элемента [15, с. 12];

– при разработке ОРХ преступлений целесообразно использовать достижения других наук в области исследования преступности — уголовного права, криминологии, криминалистики, а также юридической психологии; при этом учитывать, что каждая наука, как пишет В.Ф. Луговик, изучает лишь те аспекты преступления, которые значимы для решения стоящих перед ней теоретических и практических задач [6, с. 14];

– ОРХ преступлений должна включать в себя такие данные, которые определяют содержание организации, тактики деятельности оперативных подразделений по выявлению, раскрытию преступлений оперативно-розыскными средствами и методами, преимущественно негласными.

Переходя к содержанию ОРХ дистанционного мошенничества, отметим, что нас интересуют те ее элементы, которые необходимы для достижения цели разработки эффективных мер по организации деятельности оперативных подразделений по выявлению и раскрытию указанных преступлений. Критериями отбора оперативно значимых элементов ОРХ дистанционного мошенничества являлись: их закономерная повторяемость (устойчивость), научная обоснованность, измеримость и формализуемость, предназначенность для организации деятельности оперативных подразделений по раскрытию указанных преступлений.

С учетом выделенных критериев элементы ОРХ дистанционного мошенничества и взаимосвязи между ними определялись нами в ходе исследования на основе анализа уголовных дел, дел оперативного учета, статистических данных. Наиболее значимыми ее структурными элементами, по нашему мнению, являются данные:

– о динамике, распространенности, результатах раскрываемости дистанционных мошенничеств;

– об обстановке совершения дистанционных мошенничеств;

– о способах подготовки, совершения и сокрытия дистанционного мошенничества (способы обмана потерпевших, приемы манипуляций их сознанием и поведением);

– об особенностях личности преступника;

– об информационно-коммуникационной среде, как сфере возникновения информации о совершении дистанционных мошенничеств;

– о механизме образования следов как источников информации о дистанционных мошенничествах;

– о видах электронных носителей информации об обстоятельствах дистанционных мошенничеств.

## Список литературы


1. Захарцев С.И., Игнащенков Ю.Ю., Сальников В.П. Оперативно-розыскная деятельность в XXI веке: монография. М.: Норма, 2015.
2. Ларичев В.Д. Содержание оперативно-розыскной характеристики преступлений в сфере экономики // Общество и право. 2013. № 2 (44).
3. Климов И.А., Синилов Г.К. Актуальные проблемы развития теории и совершенствования практики ОРД в условиях современного российского общества // Теоретические и практические проблемы оперативно-розыскной деятельности. Калининград: Калининградский юридический институт МВД России, 1999.
4. Борин Б.В. Понятие, определение и значение оперативно-розыскной характеристики преступлений экономической направленности // Пробелы в российском законодательстве. 2014. № 1. С. 202-205.
5. Иванов П.И. Об оперативно-розыскной характеристике легализации доходов, полученных преступных путем // Вестник Уральского юридического института МВД России. 2020. № 4. С. 130-136.
6. Луговик В.Ф. Проблемы формирования учения об оперативно-розыскной характеристике преступлений // Оперативник (сыщик). 2006. № 4 (9).
7. Омелин В.Н. Об оперативно-розыскной характеристике нецелевого расходования бюджетных средств // Закон и право. 2019. № 11. С. 153-155.
8. Федорович Д.Ю. Понятие и содержание оперативно-розыскной характеристики конвенциональных преступлений, посягающих на свободу личности // Научный портал МВД России. 2015. № 1. С. 52-56.

9. Хмыз А.И. О криминалистической и оперативно-розыскной характеристиках преступлений и их соотношении // Вестник Томского гос. университета. 2015. № 398. С. 163-166.

10. Горбанев В.М. Оперативно-розыскная характеристика мошенничеств, связанных с использованием средств сотовой связи // Общество и право. 2016. № 4 (58). С. 137-141.

11. Любан В.Г., Молянов А.Ю., Хазов Е.Н. Распространенные способы мошенничеств в сфере информационно-телекоммуникационных технологий // Вестник Московского университета МВД России. 2019. № 1. С. 190-194.

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. Рубцов И.И. Криминалистическая характеристика преступлений как элемент частных методик расследования: дисс. … канд. юрид наук. СПб., 2001.

14. Князьков А.С. Криминалистика: курс лекций / под ред. Н.Т. Ведерникова. Томск: ТМЛ-Пресс, 2008. С. 859-907.

15. Бессонов А.А. Частная теория криминалистической характеристики преступлений: автореф. дисс. … д-ра юрид. наук. М., 2017.

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

## ЦИФРОВИЗАЦИЯ КАК НЕИЗБЕЖНОСТЬ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Цифровизация — дань моде, или она действительно поможет решить накопившиеся проблемы в уголовном процессе? Этот вопрос пронизывает многие научные публикации последних лет, посвященных проблемам развития уголовного судопроизводства в эпоху технологических свершений.

Так, А.В. Победкин ставит под сомнение решенность безусловно важных вопросов и перечисляет их: права и свободы человека обеспечены на должном уровне, уголовный процесс справедлив и эффективен, обстоятельства по уголовным делам всегда устанавливаются быстро и правильно, потерпевший имеет доступ к правосудию в полном объеме, приговоры правосудны, правда и нравственность торжествуют в судах [2, с. 51]. К этому можно добавить также эффективность взаимодействия властных участников уголовного процесса, включая контроль и надзор; своевременное и полное информирование потерпевшего о движении уголовного дела; обеспечение участия всех заинтересованных лиц в рассмотрении дел в судах независимо от их места нахождения; процессуальная экономия и т.д. Нельзя не упомянуть и одну из задач уголовного процесса: борьба с преступностью, которая хоть и не находит прямого отражения в законе, но просматривается исходя из смысла некоторых его положений (ч. 1 ст. 6, ч. ст. 21 УПК).

Что может дать перевод уголовного судопроизводства на цифровую платформу? Какие проблемы он сможет закрыть? Попробуем определить это поэтапно.

**Признание электронных доказательств** на законодательном уровне позволит более точно конкретизировать требования к порядку их получения, хранения и использования в доказывании по уголовным делам, снизит эффект недоверия, позволит шире применять видеопротоколирование, видеопоказания, использовать электронную информацию в облачных пространствах, выйти на регулирование производства следственных действий трансграничного характера.

Расширение возможностей **применения цифровых технологий при обращении граждан** в правоохранительные органы, прокуратуру и в суд (с заявлениями о преступлениях, с жалобами и ходатайствами) сделает, учитывая индивидуальные особенности граждан, эту сферу более доступной, быстродействующей, когда реагирование на факт преступления не терпит отлагательств и требуется работа, что называется, «по горячим следам»; снизит укрывательства преступлений от регистрации; позволит гражданам, удаленным от места

расследования или рассмотрения дел в суде, реализовать свои права в уголовном судопроизводстве, пользуясь защитой государства.

Создание **единой автоматизированной системы** позволит предоставить всем участникам уголовно-процессуальных отношений дополнительные возможности в плане получения криминалистически значимой и правовой информации; выйти на качественно новый уровень взаимодействия; высокотехнологичный и доступный интерфейс создаст принципиально новые, удобные для работы электронные формы документов и, значит, потребуются иные правила их составления и учета.

Внедрение так называемого **Электронного уголовного дела** [3] создаст четко определенную сферу реализации уголовно-процессуальных отношений, соответствующей вызовам современной интернет-преступности; выведет доказывание в цифровой формат, что позволит использовать систему искусственного интеллекта; последнее окажет существенную помощь органам расследования и судам, освободив их от повседневной рутинной работы; контроль и надзор перейдет в доступный и повседневный цифровой контент, что приведет к снижению уровня нарушений законности.

В результате перехода на цифровой формат уголовного судопроизводства мы избавимся от бумажного документооборота [2]; ускорим обмен информацией, дадим возможность гражданам, не отвлекаясь от повседневных дел и забот, защищать свои права и законные интересы в судебном порядке (дистанционно); получим возможность осуществлять контроль над законностью вне зависимости от субъективных факторов проверяемых лиц, что позволит снизить коррупционные риски и повысить качество расследования и рассмотрения дел в суде.

Все это, безусловно, положительно скажется на состоянии борьбы с преступностью. Кроме того, цифровые технологии существенно изменят облик следственной структуры власти, что возможно приведет к повышению ее авторитета и профессионализма.

Цифровизация — не дань моде, а преддверие неизбежности преобразования всего общества и государства, а значит, и системы уголовного судопроизводства. Здесь нет смысла искать сторонников и противников реформ, вдохно-

вителей и авторов идей. Надо принять необходимость изменений как данность и попытаться взять с собой в будущий цифровой век все самое лучшее и ценное, что есть в теории и практике уголовного процесса.

**Список литературы**

1. Вилкова Т.Ю., Масленникова Л.Н. Законность и унификация в уголовном судопроизводстве: от бланков процессуальных документов — к электронному уголовному делу // Вестник Пермского университета. Юридические науки. 2019. № 46. С. 728-751.

2. Победкин А.В. Этико-аксиологические риски моды на цифровизацию для уголовного судопроизводства (об ошибочности технологичного подхода к уголовному процессу) // Вестник Московского университета МВД России. 2020. № 3. С. 50-55.

3. Познанский Ю.Н. Электронное уголовное дело в решении проблемы расследования уголовных дел в разумные сроки // Труды Академии управления МВД России. 2015. № 1 (33). С. 41-44.

***Л.П. Климович,*** *д.ю.н., к.э.н., профессор кафедры уголовного процесса и криминалистики Сибирского федерального университета, г. Красноярск*
***Н.Г. Логинова,*** *к.ю.н., доцент кафедры уголовного процесса и криминалистики Сибирского федерального университета, г. Красноярск*
***Г.П. Дмитриев,*** *секретарь судебного заседания Красноярского гарнизонного военного суда, г. Красноярск*

## ЭЛЕКТРОННОЕ УГОЛОВНОЕ ДЕЛО В ОТЕЧЕСТВЕННОМ УГОЛОВНОМ ПРОЦЕССЕ: МИФ ИЛИ РЕАЛЬНОСТЬ?

Цифровые технологии с каждым годом занимают все больше места в нашей повседневной жизни. 2020 год и вовсе столкнул нас с этим явлением «лицом к лицу». Практически каждому так или иначе пришлось осваивать для

коммуникации какие-то новые цифровые устройства или ресурсы в связи со сложившей в мире обстановкой, вызванной распространением новой коронавирусной инфекции (COVID-19). Естественно, происходящие процессы не могли не отразиться и на такой части сложной социальной системы, как уголовное судопроизводство.

При этом единства в вопросе внедрения в уголовное судопроизводство цифровых технологий в академической среде нет. Одни говорят о невозможности, другие ратуют за повсеместное внедрение. Между тем профессор Л.А. Воскобитова констатирует: «Цифровые технологии явочным порядком проникают в уголовное судопроизводство и постепенно получают законодательное оформление» [1, с. 93].

Действительно, под стать времени динамичный институт уголовного процесса также подвергается соответствующим нововведениям. К примеру, в распоряжении следователя сегодня имеется большое количество технических устройств и баз данных, значительно облегчающих решение профессиональных задач. Однако полагаем, что процесс цифровизации рассматриваемого института еще не достиг своего предела, поскольку до сих пор участники уголовного судопроизводства преимущественно работают с документами на бумажных носителях. Несмотря на наличие в УПК РФ норм, так или иначе относящихся к современным технологиям, отечественный законодатель не спешит с кардинальными изменениями как по части закрепления в ст. 5 основных понятий, так и по части применения цифровизации в основном виде деятельности — доказывании по уголовным делам и о возможности формировании доказательств посредством применения цифровых технологий, а также ведении уголовного делопроизводства в электронном виде.

Для того чтобы ответить на вопрос о том, насколько такая позиция правильна, мы решили исследовать проблемы, прежде всего, терминологического характера.

Обратимся к понятию цифровизации (цифрового развития) в отечественном законодательстве. Применительно к бизнес-процессам такое понятие пред-

ставлено в Приказе Минкомсвязи России № 428: это «процесс организации выполнения в цифровой среде функций и деятельности (бизнес-процессов), ранее выполнявшихся людьми и организациями без использования цифровых продуктов. Цифровизация предполагает внедрение в каждый отдельный аспект деятельности информационных технологий» [2]. Данное определение, в свою очередь, требует разъяснения таких понятий, как «цифровая среда», «цифровой продукт» и «информационные технологии».

Понятие «цифровой продукт» представлено в этом же документе — это «отдельная программа для ЭВМ (приложение) для выполнения некоего конечного процесса». Содержание термина «информационные технологии» дано в п. 2 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» — это «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» [3]. Понятие «цифровая среда» дает стандарт [4]: это «среда логических объектов, используемая для описания (моделирования) других сред (в частности, электронной и социальной) на основе математических законов». Содержание данного понятия в большей степени раскрывает техническую сторону организации самого процесса функционирования какой-либо среды.

Таким образом, используя вышеобозначенную универсальную терминологию, можно полагать, что цифровизация уголовного судопроизводства — это процесс организации функционирования уголовно-процессуальной деятельности с применением информационных технологий.

Поворотной точкой в развитии отечественного уголовного процесса в этом направлении, представляется, может стать внедрение в работу органов предварительного расследования так называемого электронного уголовного дела. Не претендуя на всестороннее исследование в рамках данной публикации этого вопроса, остановимся лишь на обосновании авторской позиции о возможности внедрения электронного формата ведения дела в отечественное уголовное судопроизводство. Такой опыт уже имеет место в системе законодательства зару-

бежных стран. Ряд авторов научных публикаций указывают, что электронное уголовное дело активно применяется в некоторых странах Европы, в Азербайджанской Республике. В Саудовской Аравии же внедрение указанной технологии и вовсе позволило оканчивать производство по некоторым уголовным делам в 2-суточный срок [5, 6].

В Казахстане деятельность по формированию электронного уголовного дела регулируется Инструкцией о ведении уголовного судопроизводства в электронном формате [7] (далее — Инструкция), где закреплено понятие «электронное уголовное дело» и требования, предъявляемые к такому формату судопроизводства, а также последовательность действий при ведении электронного уголовного дела. Пунктом 5 Инструкции при формировании электронного уголовного дела предусмотрено: заполнение учетных сведений и реквизитов электронных форм в едином реестре досудебных расследований; создание электронных документов на имеющихся шаблонах и PDF-документов в модуле е-УД; подписание электронных документов участниками уголовного процесса при помощи ЭЦП или планшета подписи; отправка SMS-оповещения для уведомления либо вызова участников уголовного процесса; электронное взаимодействие с судом в целях обеспечения процессов по рассмотрению уголовных дел и материалов в электронном формате; электронное взаимодействие с экспертами, специалистами для осуществления процедур назначения исследования и получения заключений в электронном формате либо перевода бумажных материалов в электронный формат в соответствии с Инструкцией; функционирование публичного сектора.

Разумеется, наличие регламентированного порядка и его нормативное закрепление в Инструкции само по себе не означает немедленное успешное внедрение и применение рассматриваемой технологии на практике, возникновение сложностей неизбежно на начальной стадии внедрения новых технологий. Вместе с тем, как отмечает Э.А. Алимова, несомненным преимуществом электронного формата судопроизводства в Республике Казахстан является упрощение

многих процедур, которое, в свою очередь, не должно восприниматься как ослабление процессуальных гарантий обеспечения прав и свобод граждан [8].

Учитывая опыт законодателя других государств, приведем некоторые достоинства и недостатки введения технологии «электронное уголовное дело» в отечественный уголовный процесс.

Первое, что обращает на себя внимание, это необходимость подготовки «качественно нового юриста», поскольку обращения с электронными ресурсами на уровне «обычного» пользователя будет недостаточно. Идею совершенствования цифровой образовательной подготовки будущих юристов развивают в своих публикациях Р.А. Абдусаламов, Л.В. Магдилова, Д.А. Рагимханова [9] и другие авторы [10]. Цифровизация ставит задачу подготовки качественно нового юриста, владеющего на достаточном уровне информационными технологиями. И если при получении основного образования по профилю подготовки «Юриспруденция» видится введение дисциплин, направленных на формирование компетенций в сфере цифровизации общего характера, то при назначении на должность необходимо в рамках дополнительного профессионального образования давать знания о специализированных информационных ресурсах, с помощью которых будет формироваться электронное уголовное дело. Только при таких обстоятельствах можно говорить о введении электронного уголовного дела.

Одним из условий формирования электронного уголовного дела, на наш взгляд, должно выступать и согласие таких участников, как потерпевший и обвиняемый (подозреваемый), поскольку уровень владения навыками обращения с информационными ресурсами может быть различным, а создание «виртуального» уголовного дела повлечет за собой, например, получение электронной цифровой подписи, непосредственное обращение к отдельным электронным документам.

Отмечая достоинства, следует указать, что внедрение рассматриваемой технологии позволит сократить материальные и временные затраты. Как уже было сказано, современному уголовному процессу не чуждо применение различного рода технических устройств, в том числе при подготовке процессуаль-

ных документов, из которых и формируется «бумажное» уголовное дело. Причем большая часть уголовного делопроизводства осуществляется с использованием тех технических средств, которые в первоначальном виде формируют электронный документ, который впоследствии переносится на бумажный носитель. Безусловно, часть протоколов следственных действий, (осмотр места происшествия, обыск, выемка и др.), проводимых «на месте», составляются рукописным способом, и отказаться от этого в ближайшее время вряд ли возможно.

Не нова для уголовного процесса проблема восстановления утраченных уголовных дел, порядок которого регламентирован ст. 158[1] УПК РФ. В этой связи перенос привычного «бумажного» уголовного дела в электронный формат, определенно снижает риск его утраты.

Электронное уголовное дело представляется удобным нововведением для ознакомления с материалами уголовного дела на завершающем этапе расследования. При выполнении требований ст. 215, 217 УПК РФ следователю нет необходимости находиться рядом с лицами, соответственно, это время может быть использовано на выполнение другой деятельности. Анализ же цифрового следа позволит точно зафиксировать время, затраченное на ознакомление; более того, может быть установлено, сколько времени было затрачено на изучение отдельного вида процессуального документа, соответственно, данная информация может быть использована в качестве фактических данных при принятии решения об ограничении во времени ознакомления.

Рассматриваемый вид уголовного делопроизводства, по мнению авторов, позволит снизить временные и материальные затраты, связанные со снятием копий с материалов уголовного дела при выделении в отдельное производство, при представлении в суд материалов для рассмотрения в порядке ст. 165 УПК РФ, для решения вопроса об избрании меры пресечения. В таких случаях органы предварительного расследования и суды смогут обмениваться необходимыми документами посредством специально разработанного программного обеспечения, что позволит сократить время, затрачиваемое на доставку документов почтовым отправлением.

Существует мнение, что внедрение технологии «электронное уголовное дело» в практическую деятельность субъектов уголовного процесса позволит добиться уменьшения волокиты. Так, Ю.Н. Познанский считает, что электронное уголовное дело является инструментом решения проблемы расследования уголовных дел в разумные сроки [11]. Действительно, электронное уголовное дело в перспективе упростит в какой-то степени производство по делу. Однако полагаем, что соответствующие временные затраты избежать в полной мере не удастся. К примеру, следователю помимо ведения уголовного дела в бумажном формате необходимо будет переводить письменные документы в электронный вид, что повлечет, без сомнения, лишние затраты по времени. Следователю нужно будет также освоить программное обеспечение. На его плечи ляжет обязанность объяснить участникам уголовного процесса, каким образом возможен доступ к материалам электронного уголовного дела. Таким образом, говорить о сокращении временных затрат в этой связи можно лишь в перспективе.

Нам видятся и определенные недостатки ведения уголовного дела в электронном формате. К примеру, непростой задачей, требующей первостепенного решения, является в таком случае обеспечение информационной безопасности, о чем также пишет в своей публикации С.В. Зуев [12]. Использование различных государственных электронных ресурсов всегда связано с достоверным установлением личности. Процесс идентификации, необходимый для доступа к материалам электронного уголовного дела, может оказаться сложным для человека, не обладающего специальными познаниями. Таким образом, доступ к уголовному делу будет значительно затруднен.

Кроме того, под угрозу подпадает сформулированный законодателем в ст. 161 УПК РФ принцип недопустимости разглашения данных предварительного расследования. Согласно ч. 2 указанной статьи, данные предварительного расследования могут быть преданы гласности лишь с разрешения следователя или дознавателя и только в том объеме, в каком ими будет признано это допустимым. Сложным в данной ситуации представляется контроль действий обвиняемого либо его защитника по неразглашению данных предварительного

расследования. Не представляется возможным установить, сколько конкретно лиц находится рядом с указанными участниками уголовного процесса, которые знакомятся с материалами уголовного дела «онлайн».

Интересным представляется также довод П.С. Пастухова: «Возможность иметь доступ к цифровой информации всегда будет вызывать сомнения в достоверности, и быть лишним поводом к ее дополнительной проверке. Несмотря на существующие различные методы защиты целостности цифровых данных, проблема связана с возможностью раскрытия персональных данных, кражи коммерческой, профессиональной, служебной и государственной тайны» [6]. Полагаем возможным согласиться с таким утверждением. Действительно, обеспечить сохранность данных уголовного дела, размещенного, к примеру, в облачном хранилище, дата-центре, — это непростая задача. Обеспечить полную сохранность таких данных достаточно сложно, что, скорее всего, вызовет некоторую озабоченность у стороны защиты.

Стоит отметить, что отказаться от ведения уголовного дела в традиционном формате на начальном этапе внедрения электронных технологий вряд ли возможно, поскольку производство по делу в таком случае напрямую зависит от наличия технической оснащенности каждого рабочего места следователя, необходимой для выполнения функций по ведению электронного дела, а также обеспечения бесперебойной работы систем электроснабжения и интернет-коммуникаций, позволяющих эффективно, реализовывать следователю процессуальные полномочия. Представляется, что электронное уголовное дело на этапе внедрения информационных технологий — это все же дополнение к его бумажному варианту.

Подведем итог. Учитывая изложенную выше аргументацию, полагаем, что отойти от формата ведения уголовного дела в его привычном «писаном» варианте на сегодняшний день представляется маловероятным. Технология «электронное уголовное дело» в современных условиях видится нам лишь дополнением к традиционному уголовному делу. Однако темпы внедрения цифровизации в различные сферы жизнедеятельности приводят к мысли том, что это вопрос ближайшего будущего. Законодателю при разработке правового регули-

рования ведения уголовного судопроизводства в цифровом формате следует помнить, что цифровое уголовное дело — это не панацея от всех бед, а лишь в некоторых случаях — удобная технология, отказываться от которой категорично, как и повсеместно внедрять, нужно с определенной долей осторожности.

## Список литературы


1. Воскобитова Л.А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex russica (Русский закон). 2019. № 5. С. 91-104.
2. Об утверждении Разъяснений (методических рекомендаций) по разработке региональных проектов в рамках федеральных проектов национальной программы «Цифровая экономика Российской Федерации»: приказ Минкомсвязи России от 01.08.2018 № 428.
3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ.
4. ГОСТ Р 52292-2004. Национальный стандарт Российской Федерации. Информационная технология. Электронный обмен информацией. Термины и определения.
5. Джафаров А.М. Цифровизация процесса отправления правосудия: достижения, перспективы, проблемы (на примере Азербайджанской Республики) // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 5 (72). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-protsessa-otpravleniya-pravosudiya-dostizheniya-perspektivy-problemy-na-primere-azerbaydzhanskoy-respubliki (дата обращения: 09.05.2021).
6. Пастухов П.С., Лосавио М. Использование информационных технологий для обеспечения безопасности личности, общества и государства // Вестник Пермского университета. Юридические науки. 2017. № 36. С. 231-236.
7. Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате: приказ Генерального прокурора Республики Казахстан от 03.01.2018 № 2. [Электронный ресурс]. URL: http://adilet.zan.kz/rus/docs/V1800017124 (дата обращения: 05.05.2021).

8. Алимова Э.А. Проблемы участия специалиста в современно уголовном процессе Республики Казахстан // Вестник криминалистики. 2019. № 1 (69). С. 59-66.

9. Абдусаламов Р.А., Магдилова Л.В., Рагимханова Д.А. Некоторые проблемы совершенствования юридического образования в условиях цифровизации // Юридический вестник Дагестанского гос. университета. 2019. № 3. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/ nekotorye-problemy-sovershenstvovaniya-yuridicheskogo-obrazovaniya-v-usloviyah-tsifrovizatsii (дата обращения: 25.05.2021).

10. Cybercrime in the Conditions of the Digital Economy and the New Tendencies in the Forensic Enquiry Development / L.P. Klimovich, V.V. Molokov // Вестник Национальной академии наук Республики Казахстан. 2019. № 5. С. 6-14.

11. Познанский Ю.Н. Электронное уголовное дело в решении проблемы расследования уголовных дел в разумные сроки // Труды Академии управления МВД России. 2015. № 1 (33). С. 41–44.

12. Зуев С.В. Электронное уголовное дело: за и против // Правопорядок: история, теория, практика. 2018. № 4 (19). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/elektronnoe-ugolovnoe-delo-za-i-protiv (дата обращения: 05.05.2021).

***В.Е. Козлов,*** *к.ю.н., доцент, доцент кафедры тактико-специальной подготовки Академии МВД Республики Беларусь, г. Минск*

## ОБ ОТДЕЛЬНЫХ АСПЕКТАХ МЕХАНИЗМА ОБРАЗОВАНИЯ СЛЕДОВ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Выделение преступлений, совершаемых с использованием средств компьютерной техники (СКТ), в отдельную группу предполагает активизацию научного поиска, направленного на исследование относительно новых в криминали-

стике и теории ОРД следов. Целостное представление о следовой картине, возникающей при подготовке, совершении, сокрытии так называемых «компьютерных преступлений», позволяет разрабатывать и внедрять новые научно-технические средства (НТС), либо осуществлять их заимствование из смежных областей деятельности, направленной на их предупреждение (например, деятельности по обеспечению компьютерной безопасности). Открываются также перспективы совершенствования основных положений тактики использования специальных знаний для обнаружения, фиксации, изъятия и исследования следов «компьютерных преступлений» при производстве следственных действий и проведении ОРМ.

Применительно к процессу совершенствования методики выявления и расследования обозначенной группы преступлений, компьютерную информацию (КИ) можно определить через две составляющих — фактические данные и пригодность для обработки СКТ. Следовательно, КИ может:

– служить орудием (элементом) подготовки, совершения и сокрытия преступления;

– сохранять следы преступления;

– быть объектом преступных действий;

– быть непосредственным или опосредованным результатом преступных действий.

Как отражение явлений реального мира, сущность КИ раскрывается действиями, в которых она участвует: передача, преобразование, хранение. На объектах, использующих СКТ, происходит ее непрерывный перенос в пространстве и времени от источника к приемнику, при этом возможно изменение ее материально-энергетической формы, но сохранение материальной сущности. Для КИ основополагающей категорией является «файл». Файлы являются хранителями КИ и для них характерны стандартные свойства: тип, локализация (местонахождение), объем, время создания (изменения), атрибуты. Приведенный набор свойств позволяет говорить о наличии необходимых с точки зрения

криминалистической идентификации свойств файлов, позволяющих идентифицировать КИ при соблюдении условий, установленных национальным уголовно-процессуальным законодательством, а материальность записи файла остается необходимым условием его существования. Материальный носитель является вторичным элементом относительно содержания информации, первичным — КИ и форма ее представления. Таковы обобщенные выводы исследователей криминалистического значения КИ [1, 2].

Зафиксированную на материальном носителе КИ невозможно непосредственно и однозначно воспринимать органами чувств человека и тем более ее идентифицировать без соответствующих НТС (аппаратно-программных средств), которые также включаются в процессы обработки и хранения КИ, порождая, а затем и оперируя следующими ее формами представления (рис.).

1. Отображаемая (КИ доступна для восприятия человеком непосредственно в виде символов, графики, звука).

2. Неотображаемая логическая (КИ представлена логическими структурами данных).

3. Неотображаемая физическая (КИ представлена физическими структурами — электромагнитным полем (ЭМП), а также проводниковыми, полупроводниковыми, магнитными, магнитооптическими и оптическими носителями).

Человек воздействует на КИ, которая находится в форме, доступной восприятию → КИ преобразуется в форму, доступную для обработки программными средствами СКТ → КИ преобразуется в электромагнитный сигнал, который может быть обработан аппаратными средствами СКТ.

Формы представления КИ

Таким, образом, сущность механизма следообразования при совершении «компьютерного преступления» состоит в том, что СКТ, как система устройств, реализующих логическое и одновременно физическое воздействие на КИ, является следообразующим объектом. Он взаимодействует с КИ, вызывая материальные последствия, возникшие в связи с подготовкой, совершением и сокрытием преступления, а именно — остаточные явления, представляющие собой материально фиксированные отображения на одном объекте внешнего строения (в данном случае — свойств КИ) другого объекта. Следовательно, КИ является следовоспринимающим объектом. Соответственно, следы «компьютерных преступлений» в общем случае являются КИ.

Является ли такое понимание механизма следообразования при совершении «компьютерного преступления» слишком широким? Ответ на этот вопрос будет зависеть от избранной прикладной области применения знаний об исследуемом механизме следообразования, иными словами, от цели деятельности ее субъекта. Мы полагаем, что применительно к исследованию следов «компьютерного преступления» в процессе его выявления, раскрытия и расследования оно достаточно. В случае иного подхода (например, в сторону усложнения — путем заимствования и механического переноса знаний иных, преимущественно технических наук в криминалистику) разработка и внедрение новых видов СКТ будет стимулировать проведение дальнейших исследований, все более удаляющихся от предмета криминалистики и теории ОРД.

Нелогичными выглядят также предпринимаемые отдельными исследователями попытки «размазывания» следовой картины, возникающей при использовании (видимо, для них самих) «новых» средств обработки КИ — терминалов сотовой подвижной электросвязи, смартфонов, «умных вещей» и т.д., поскольку каждое из них по существу также является СКТ. Полагаем, что дальнейшие подобные исследования должны заключаться не в объяснении механизма следообразования исходя из физических и логических принципов действия носителей КИ, а также архитектур различных СКТ, особенностей их операционных систем (ОС) и прикладного программного обеспечения (ПО), а в криминали-

стическом исследовании свойств (характеристик) следообразующего объекта — СКТ и их непосредственного влияния на искомый процесс, а именно следующих.

1. Аппаратных средств СКТ, прежде всего:

– микропроцессоров(ра), а также оперативной памяти, доступной для использования, хранимые промежуточные и окончательные результаты вычислений;

– системы запоминающих устройств, а также устройств ввода-вывода КИ;

– устройств, предназначенных для обеспечения работы в сетях (сетевых аксессуаров), а также дополнительных периферийных устройств.

2. Программных характеристик СКТ, а именно ОС и сервисного ПО, а также офисного и иного прикладного ПО, коммуникационного ПО.

3. Характеристик компьютерных сетей:

– степень географической распределенности и функциональное назначение, а также методы передачи данных;

– тип используемых СКТ, а также размещение КИ (централизованное, распределенное — облачное);

– непосредственных характеристик вычислительных сетей (топология; используемое ПО; физическая передающая среда; метод доступа; совокупность правил, регламентирующих формат и процедуры обмена КИ между узлами сети — протоколы).

4. Иных криминалистически значимых свойств: вероятность нарушения целостности, непрерывности, доступности и конфиденциальности КИ в случае форс-мажорных обстоятельств.

Анализ влияния каждого из указанных свойств (характеристик) СКТ на результат следообразования производится субъектами судебного исследования доказательств (лицо, осуществляющее дознание; следователь; прокурор; суд (судья)) при их собирании, исследовании, оценке и использовании. Такой путь представляется нам «эволюционным», предполагающий интеграцию знаний естественных наук в криминалистику.

Изложенное позволяет сделать принципиальные выводы. В процессе следообразования при совершении компьютерного преступления участвуют два взаимодействующих объекта СКТ в качестве следообразующего, КИ — следовоспринимающего. Сущность данного процесса заключается в опосредованном воздействии человека через СКТ на материальный объект — КИ. Подвергшись воздействию, КИ изменяет свои свойства, либо часть свойств, изменение которых являются **результатом процесса отражения.**

Пользователь СКТ, не обладающий специальными знаниями, осуществляя доступ к открытой КИ, размещенной на сайте в сети, например Интернет, может не знать географического расположения серверов, что создает иллюзию работы в некоем идеальном «киберпространстве». Однако расположение оборудования хостера, а следовательно, и принадлежащих ему серверов может выявить специалист. Впоследствии исследование следовой информации, расположенной на территории иного государства, возможно органами уголовного преследования этого же государства в рамках оказания правовой помощи по гражданским и уголовным делам. Именно таким естественным путем и идет практика раскрытия и расследования «компьютерных преступлений». Возможные предположения о «недоступности» национальным правоохранительным органам следов «компьютерных преступлений», вызванные тем, что таковые находятся «вне их поля зрения», сомнительны и больше напоминают повод для самоустранения от процесса расследования. Авторы подобных высказываний рассматривают процессы собирания следов «компьютерных преступлений» в отрыве от процесса доказывания по уголовным делам в целом. Нет оснований также ссылаться на то, что расположенные вне национальной юрисдикции следы «компьютерного преступления» могут быть значительно легче уничтожены, так как процесс сокрытия его следов определяется не их географической удаленностью или близостью, а прежде всего «криминальной квалификацией» субъекта противоправной деятельности и свойствами самих СКТ. Соответственно, необходимо рассматривать искомый процесс следообразования

не в некоем «кибернетическом пространстве», а в конкретных условиях обстановки совершения преступления, под воздействием на КИ посредством СКТ.

Кроме того, распространяя изложенный системно-логический подход на процесс собирания доказательств по делам о «компьютерных преступлениях», необходимо отметить следующие обстоятельства.

1. Компьютерные файлы, содержащие криминалистически значимую информацию, как правило, не являются электронными документами в информационно-правовом смысле — такое название им можно дать лишь с определенной долей условности.

2. Существует система признаков, позволяющих идентифицировать КИ в форме файла (файловой системы), которая образуется:

– свойствами (параметрами): признаками, атрибутами, содержанием и т.д. файла как предмета материального мира;

– условиями обстановки совершения «компьютерного преступления» — средой, в которой производились действия по его приготовлению, совершению и сокрытию, а также условиями обстановки, в которой осуществлялось обнаружение, изъятие и фиксация файлов при производстве следственного действия либо проведения ОРМ;

– отсутствие одного из названных элементов системы признаков не допускает криминалистической идентификации файла.

3. Собирание файлов-доказательств предполагает осуществление обнаружения, фиксации, изъятия и сохранения их копий, каждая из которых обеспечивает целостность КИ, полностью характеризует оригинал, и однозначно определяет его существование.

4. Для получения копий таких файлов используются отчуждаемые носители субъекта, осуществляющего деятельность по собиранию доказательств. При этом отчуждаемый носитель КИ никакого собственного доказательственного значения не имеет, а приобретает его в момент окончания записи копий файлов на него.

5. В процессе собирания доказательств по делам о «компьютерных преступлениях» определяющую роль играет законодательно закрепленная процедура действий с файлом как вещественным доказательством, придающая копии файла юридическую силу и позволяющая органу уголовного преследования одновременно с фиксацией и изъятием файла осуществлять фиксацию (документирование) элементов среды его существования в СКТ. Специальные требования к подобной процедуре должны устанавливаться национальным уголовно-процессуальным и оперативно-розыскным законодательствами

Изложенное дает основания сделать следующие общие выводы (отдельные положения которых частично реализованы в законодательствах Беларуси и России).

1. Для эффективного использования в качестве вещественных доказательств следов-предметов в виде регистрационных и иных файлов обязателен переход объектов информатизации на так называемые «защищенные средства вычислительной техники», так как преодоление средств защиты правонарушителем способствует следообразованию.

2. Необходимо активизировать процессы совершенствования национальных законодательств в области электросвязи и информатизации в части, касающейся обязанности провайдеров Интернет, а также операторов сотовой подвижной электросвязи, сохранять данные о пользователях и об оказанных им услугах, независимо от количества поставщиков информационных и телекоммуникационных услуг, вовлеченных в процессы хранения и передачи КИ. Такие данные должны потенциально обеспечивать идентификацию поставщиков услуг и маршруты передачи КИ. В рамках данного направления деятельности возможны разработка, внедрение и использование системы криминалистического учета и идентификации пользователей Интернет.

3. Сбор подобных данных правоохранительными органами должен осуществляться в режиме реального времени путем их документирования с использованием НТС самостоятельно, а также отдачей поручений поставщикам информационных услуг (провайдерам).

4. Реализация обозначенных положений может служить фундаментом совершенствования теории и практики осуществления оперативно-розыскной деятельности, в частности, основных положений ведения оперативного поиска и оперативной разработки, в особенности их оперативно-аналитической составляющей, основанной на перехвате и анализе КИ оперативными подразделениями правоохранительных органов.

5. Их практическая реализация требует совершенствования (реформирования) системы подготовки кадров, как для правоохранительных органов, так и подразделений, обеспечивающих компьютерную безопасность, способных глубоко теоретически осмысливать содержание современных меняющихся условий оперативной обстановки по линии противодействия преступлениям, совершаемым с использованием СКТ, и практически осуществлять противодействие преступлениям, совершаемым с использованием СКТ [3, 4].

Изложенная точка зрения в настоящее время активно дискутируются в научных кругах стран бывшего СССР и имеет как своих сторонников, так и противников.

## Список литературы

1. Козлов В.Е. Противодействие компьютерной преступности: проблемные вопросы и пути их разрешения: монография. Минск: Акад. МВД Респ. Беларусь, 2006. 256 с.

2. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. Волгоград: ВА МВД России, 2008. 404 с.

3. Козлов В.Е. Об учебной дисциплине «Облачные технологии в правоохранительной деятельности» // Вестник Академии МВД Респ. Беларусь. Научно-практический журнал № 2 (34). Минск: Акад. МВД, 2017. С. 202-206.

4. Козлов В.Е. Об отдельных аспектах криминалистического и оперативно-технического обеспечения противодействия преступлениям, совершаемым с использованием средств компьютерной техники // 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. Барнаул: Изд-во Алт. ун-та, 2020. С. 20-26.

***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*

## ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ В УСЛОВИЯХ РЫНОЧНЫХ ОСНОВ ХОЗЯЙСТВОВАНИЯ: КРИМИНАЛИСТИЧЕСКИЕ ПРИЗНАКИ, ПОНЯТИЕ, КЛАССИФИКАЦИЯ

Активное использование организаторами теневого и криминального бизнеса в сфере экономики современных достижений информационных технологий осложняет работу оперативных и следственных органов по выявлению признаков экономических преступлений, их расследованию. Анализ следственной и судебной практики позволяет сделать вывод о том, что в условиях рыночных отношений экономические преступления совершают организованные преступные группы с использованием современных электронных информационных систем, телекоммуникационных сетей и коррупционных связей с должностными лицами государственных органов власти и управления. Источником данных, содержащих криминалистическую значимую информацию о событии экономического преступления, служат следы материального и интеллектуального подлогов в документах, информационные следы на электронных носителях информации, контактные следы, микрообъекты. Организаторы крупного и среднего бизнеса посредством коррупции, политического лоббизма незаконно присвоили значительную часть государственной собственности на приоритетных направлениях экономики, проникли в политические, государственные институ-

ты, средства массовой информации и оказывают влияние на формирование законодательной, исполнительной и судебной власти. Организованная преступная деятельность поразила все базисные отрасли и сферы экономики Украины. Наиболее криминализированными оказались такие приоритетные сферы экономики, как финансовая, банковская, внешнеэкономическая, земельных правоотношений, приватизации государственной и коммунальной собственности, энергообеспечения, а также предприятия металлургической, нефтеперерабатывающей, химической промышленности, топливно-энергетического и агропромышленного комплекса, строительства. В этих условиях «развились новые отрасли и институты, во многом новой стала технология экономических взаимоотношений и документооборота, учета и регистрации финансово-экономической деятельности. Значительная часть признаков экономических преступлений изменилась» [2, с. 20].

В юридической литературе является дискуссионной проблема определения понятийного аппарата экономических преступлений. Так, П.С. Яни к преступлениям в сфере экономики относит все посягательства на собственность, налоговые, валютные, предпринимательские, таможенные преступления [3, с. 33]; тогда как Е.Л. Стрельцов экономические преступления определяет как предусмотренные уголовным законом деяния, направленные на нарушение отношений собственности (имущественные отношения) и существующего порядка осуществления хозяйственной деятельности [4, с. 113]. Несколько другая точка зрения у В.П. Верина, который к преступлениям в сфере экономики относит все преступления против собственности, в том числе и корыстно-насильственного характера, а также преступления в сфере экономической деятельности и преступления против интересов службы в коммерческих и иных организациях [5]. Данная точка зрения не бесспорна. На наш взгляд, экономические преступления в сфере отношений собственности отличаются от других корыстных имущественных (кража) и корыстно-насильственных преступлений (вымогательство, грабеж, разбой) спецификой формирования организованных групп на приоритетных направлениях экономики, обстановкой, использованием

при подготовке, совершении преступления, сокрытии следов преступной деятельности электронных информационных систем, телекоммуникационных сетей, коррупционных связей.

Для теории и практики расследования экономических преступлений, совершенных организованной группой, особую значимость приобретает выявление определенных изменений в реальной действительности, порожденных действиями субъектов организованной преступной деятельности, то есть признаков, свойственных технологии преступной деятельности. В этой связи криминалистическое исследование признаков экономических преступлений является актуальной проблемой для науки и практики криминалистики. Системный подход к исследованию преступлений экономической направленности позволяет определить их криминалистические признаки. Таковыми являются:

– *специальный субъект или субъектный состав* (ОПГ, преступная организация), который непосредственно связан с предметом преступного посягательства в сфере экономических отношений. Это должностные лица, коррумпированные чиновники, материально-ответственные лица, финансово-бухгалтерские работники, предприниматели легального, теневого производства, сферы услуг, работники предприятий, организаций и учреждений, которые относятся к приоритетным направлениям экономики;

– *специфические способы* формирования организованной группы в сфере экономики: формально-производственный, ситуативно-договорной, нелегитимно-производственный, функционально-договорной, ситуативно-волевой [5, с. 119-130];

– *специальный предмет преступного посягательства* — движимое имущество: деньги, ценные бумаги, валютные ценности; имущественные права и обязательства; недвижимое имущество — земельные и другие естественные угодья, любое имущество, размещенное на земле, связанное с ней (здания, сооружения и т.д.); другое имущество, предприятий, учреждений, организаций, отнесенных к приоритетным направлениям экономики. Таковыми являются: отрасли промышленности (машиностроения, металлургии, химическая и др.),

внешнеэкономическая деятельность, финансово-кредитная, бюджетная системы, аграрно-промышленная, топливно-энергетическая сферы, приватизации, строительства и транспортных перевозок.

Предметом преступного посягательства является:

– *криминально-коррупционная технология* экономического преступления — это совокупность действий, операций, приемов, коррупционных схем, методов использования легального и теневого бизнеса при выборе сферы и предмета преступного посягательства, способа преступления, который включает несколько способов самостоятельных составов преступлений; использование электронных информационных систем, телекоммуникационных сетей при подготовке и осуществлении преступных акций, сокрытии следов преступной деятельности; [5, с. 180-200];

– *коррупционные связи* с должностными лицами органов государственного управления, полиции, прокуратуры, таможни, службы безопасности, государственной фискальной службы, политическими деятелями, руководством «скамеечных», «заказных» (бизнесом) партий, обеспечивают членам ОПГ реализацию преступных планов на приоритетных направлениях экономики, путем предоставления таких коррупционных услуг, как *коррупционное содействие, коррупционное покровительство, коррупционный протекционизм, коррупционное вмешательство, коррупционное лоббирование, коррупционное противодействие* [5, с. 144-152];

– *негативные последствия преступного посягательства* для предприятий, учреждений, организаций, отнесенных к приоритетным направлениям экономики. Это реальные убытки, существенный вред и другие тяжкие последствия (доведение предприятия до банкротства и незаконная его приватизация).

Криминалистический анализ признаков указанных преступлений позволяет предложить новый подход к определению понятия *экономических преступлений*, совершаемых организованной группой в условиях рыночных отношений. Полагаем, что к *экономическим* следует относить *преступления, совершаемые организованной группой, против собственности, в сфере финансово-экономи-*

*ческой, хозяйственной, служебной деятельности на предприятиях, в учреждениях, организациях приоритетных направлений экономики в процессе производства, распределения, обмена, потребления материальных благ и услуг с использованием в криминально-коррупционных технологиях электронных информационных систем, телекоммуникационных сетей, коррупционных связей с коррумпированными должностными лицами государственных органов власти, управления, фискального, таможенного контроля.*

Криминалистические знания признаков экономических преступлений, совершаемых организованной группой, оказывают существенное влияние на формирование классификационных групп криминалистической классификации экономических преступлений, разработку методических рекомендаций по их расследованию. В юридической литературе изложены различные точки зрения на криминалистическую классификацию экономических преступлений, ее классификационные критерии. Одни исследователи проблемы экономических преступлений ограничивают рамками традиционных преступлений в сфере хозяйственной деятельности, другие — рассматривают криминалистическую классификацию корыстных преступлений в сфере экономики. Следует согласиться с Г.А. Матусовским, который рассматривал криминалистическую классификацию класса экономических преступлений и выделил такие классификационные группы: 1) преступления в сфере отношений собственности; 2) преступления в сфере исполнения бюджета; 3) преступления в сфере финансовых отношений; 4) преступления в сфере предпринимательских отношений; 5) преступления в сфере защиты от монополизма и недобросовестной конкуренции; 6) преступления в сфере обслуживания населения: выпуск или реализация недоброкачественной продукции; 7) преступления в сфере таможенного регулирования [6, с. 42-43].

Криминалистическая классификация преступлений в сфере экономической деятельности, совершаемых ОПГ, как и всякая классификация, предполагает дифференциацию деяний на большие или меньшие группы, исходя из уголовно-правовых и криминалистических критериев. Сочетание указанных критери-

ев криминалистической классификации преступлений в методике расследования вытекает из теоретических положений методики. Полагаем, что необходимо учитывать еще и криминологические факторы. Так, в Украине организаторы теневого бизнеса, лидеры организованной преступной деятельности в сфере экономики владеют огромным криминальным капиталом, многие — и депутатским мандатом, пролоббировали принятие законов о декриминализации 26 составов экономических преступлений в Уголовном кодексе Украины (в том числе контрабанды), взяточничества, фиктивного предпринимательства, об упразднении контрольно-ревизионной службы, надзорных функций прокурора, спецподразделений по борьбе с организованной преступностью, подразделений по борьбе с экономическими преступлениями и другие. Декриминализация экономических преступлений оказала существенное влияние на разработку криминалистической квалификации этих преступлений. Уголовно-правовая классификация преступлений — основополагающая в любой методике расследования. И как правильно отметил Р.С. Белкин, без уголовно-правовой классификации преступлений совокупность частных криминалистических методик утратила бы признаки системы, проследить связи между методиками оказалось бы невозможным из-за отсутствия основания их группировки, потребовалась бы разработка для каждой методики в отдельности того, что есть общего у их вида или рода, нарушилась бы логическая последовательность адаптации по принципу от общего к отдельному, а от отдельного к особенному [7, с. 197].

Вместе с тем уголовно-правовых критериев для методики расследования исследуемых преступлений явно недостаточно. Криминалистическая классификация преступлений должна базироваться на таких критериях, которыми достигалось бы эффективное применение средств, методов и приемов криминалистики при расследовании отдельных видов преступлений.

Системный анализ материалов оперативной, судебной, следственной, экспертной практики, результаты наших исследований позволили разработать криминалистическую классификацию экономических преступлений, совершаемых организованными группами, выделить в ней четыре классификационные

группы указанных преступлений. *Первая группа* — это преступления против собственности; *вторая* — преступления в сфере финансово-экономической деятельности; *третья группа* — преступления в сфере хозяйственной деятельности; *четвертая группа — преступления в сфере служебной деятельности, совершаемые коррумпированными должностными лицами государственных органов*. Указанные группы следует подразделить на подгруппы. В подгруппах мы выделяем виды экономических преступлений, совершаемых ОПГ. Резюмируя изложенное, полагаем, что криминалистическую классификацию экономических преступлений, совершаемых организованной группой, следует рассматривать как систему групп, подгрупп, видов отдельных экономических преступлений, совершаемых организованной группой, предусмотренных Уголовным кодексом.

К ***первой группе относятся экономические преступления против собственности, совершаемые организованной группой.*** В этой группе следует выделить такие виды *имущественных преступлений*: присвоение, растрата имущества или завладение им путем злоупотребления служебным положением, совершаемые организованной группой, экономическое мошенничество, совершаемое организованной группой; финансовое мошенничество, совершаемое организованной группой и др.

***Вторая группа охватывает экономические преступления в сфере финансово-экономической деятельности, совершаемые организованной группой***. Их можно подразделить на четыре подгруппы: *первая подгруппа* — это преступления в сфере внешнеэкономической деятельности, совершаемые организованной группой; *вторая подгруппа* — преступления в сфере функционирования и развития ценных бумаг, фондового рынка, совершаемые организованной группой*; третья подгруппа* — финансовые преступления, совершаемые организованной группой*; четвертая подгруппа* — преступления в бюджетной сфере, совершаемые организованной группой.

***Третья группа* — это *экономические* преступления в сфере хозяйственной деятельности*, совершаемые организованной группой.*** В ней следует вы-

делить три подгруппы: *первая подгруппа* — это преступления в сфере производства, совершаемые организованной группой*; вторая подгруппа* — преступления в сфере приватизации, совершаемые организованной группой; *третья подгруппа* — это преступления в сфере предпринимательских отношений, совершаемые организованной группой.

***Четвертая группа — это преступления в сфере служебной деятельности, совершаемые организованными группами коррумпированных* должностных *лиц***. В указанной группе можно выделить две подгруппы: *первая подгруппа* — преступления в сфере отношений собственности, совершаемые организованной группой коррумпированных должностных лиц; *вторая подгруппа* — преступления в сфере финансово-экономической деятельности, совершаемые организованной группой коррумпированных должностных лиц.

В основу классификации указанных преступлений были положены уголовно-правовые и криминалистические критерии. К последним относятся: организованная группа, криминально-коррупционная технология экономического преступления, предмет преступного посягательства; обстановка, сфера организованной преступной деятельности.

Новый подход к определению криминалистических признаков и понятия экономических преступлений, совершаемых организованной группой на приоритетных направлениях экономики в условиях рыночных основ хозяйствования, раскрытие их сущности имеет определенное научное и практическое значение. Актуальным для науки и практики криминалистики является разработка криминалистической классификации экономических преступлений, совершаемых организованной группой. Объединение указанных преступлений в отдельную систему (класс) и выделение классификационных групп, подгрупп позволит дифференцированно подходить к совершенствованию существующих и разработке новых групповых, подгрупповых, видовых методик расследования экономических преступлений, совершаемых организованной группой.

**Список литературы**

1. Александров И.В. К вопросу о проблемах расследования современных экономических преступлений // Эксперт-криминалист. 2013. № 3. С. 20.
2. Яни П.С. Экономические и служебные преступления. М.: ЗАО «Бизнес-школа «Интел-Синтез», 1997. 208 с.
3. Стрельцов Е.Л. Экономическая преступность в Украине: курс лекций. Одесса: АО БАХВА, 1997. 572 с.
4. Верин В.П. Преступления в сфере экономики: учебно-практическое пособие / науч. ред. Н.В. Радутная. 2-е изд., доп. М.: Дело, 2001. 200 с.
5. Корж В.П. Теоретические проблемы методики расследования преступлений в сфере экономической деятельности, совершаемых организованными преступными образованиями. Харьков: Изд-во Нац. ун-та внутр. дел, 2002. 412 с.
6. Матусовский Г.А. Экономические преступления. Криминалистический анализ. Харьков: Консум, 1999. 480 с.
7. Белкин Р.С. Курс советской криминалистики. М., 1979. Т. 3. 325 с.

***О.С. Кучин,*** *д.ю.н., доцент, академик РАЕ, Заслуженный деятель науки и техники РАЕ, Doctor of Science Honoris Causa, профессор кафедры судебных экспертиз и криминалистики Российского государственного университета правосудия, г. Москва*

## ТАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ РАБОТЫ СЛЕДОВАТЕЛЯ С ЭЛЕКТРОННЫМИ ЦИФРОВЫМИ УСТРОЙСТВАМИ

Современные цифровые технологии все больше и больше наполняют окружающий нас мир. Этот процесс цифровизации общественных отношений все только ускоряется и усовершенствуется. В обиходе любого человека уже сегодня присутствует большое число самых различных цифровых устройств,

каждое из которых имеет характеристики и свойства и значение которых оказывается не всегда известным и понятным для потребителя. Некоторые из ставших уже абсолютно привычными такие устройства, равно как и компьютерные программы, остаются для большинства потребителей некими «черными ящиками», устройство и принцип действия которых скрыто от обычного восприятия глазом человека.

Развитие электронных носителей информации коснулось многих сфер деятельности человека. В последние десятилетия электронные носители информации все больше и больше становятся объектами криминалистического исследования при расследовании уголовных дел по различным категориям преступлений.

Так, уже 2012 г. в УПК РФ ввели легальную дефиницию «электронный носитель информации». Таким образом, подобные устройства стали вещественными доказательствами по уголовным делам. Электронные носители информации стали важной деталью при расследовании уголовного дела, но только при соблюдении некоторых специальных условий. Например, цифровая информация, находящаяся в носителе, должна иметь прямое отношение к обстоятельствам расследуемого преступления. Кроме того, передачу цифровой информации должен осуществлять достоверный источник, который можно было бы проверить. Цифровая информация должна иметь особый вид и представлена следователю в виде видеозаписи, фотографии, скриншота, заключения эксперта и т.д. При изъятии электронного носителя цифровой информации нужно соблюдать установленные процессуальные правила и криминалистические рекомендации.

Криминалистическое исследование сферы цифровых отношений и технологий, а также дальнейшее применение его результатов при расследовании преступлений позволяет выделить три составляющих компонента в этих отношениях:

1. *Цифровое техническое устройство* (англ. digital device) — техническое устройство или приспособление (внешняя оболочка), в котором находится но-

ситель цифровой информации и, которое, предназначено для получения, обработки, сохранения и передачи этой информации в цифровом виде. Цифровая информация передается в виде сообщений от одного технического устройства к другому, посредством канала связи между ними. Источник посылает передаваемое сообщение, которое кодируется в передаваемый цифровой сигнал. Этот сигнал посылается по каналу связи. В результате в приемнике появляется принимаемый сигнал, который декодируется и становится принимаемым сообщением.

К таким техническим устройствам относятся компьютеры, ноутбуки, планшеты, смартфоны, айфоны, сотовые телефоны и т.п. устройства, которые могут передавать и принимать цифровую информацию. Многие из них в современном обществе называются гаджетами. Гаджет (англ. gadget — приспособление, устройство, безделушка) — это небольшое электронное цифровое устройство, предназначенное для облегчения и усовершенствования жизни человека. Одно из основных назначений цифрового технического устройства — это обработка и хранение информации.

С помощью цифрового технического устройства человек может видеть или слышать получаемую цифровую информацию.

2. *Электронный носитель цифровой информации* — к ним относят электронные накопители (материальный предмет, который непосредственно хранит информацию) для однократной или многократной записи информации (цифровым) электрическим способом.

К электронным носителям цифровой информации относят: оптические (CD-ROM, DVD-ROM, Blu-ray Disc); полупроводниковые (флеш-память, SSD-диски); магнитные (магнитные ленты, дискеты, жесткие диски). Электронные носители имеют значительные преимущества перед иными:

– по объему и размеру хранимой информации;

– по удельной стоимости хранения;

– по экономичности и оперативности предоставления актуальной информации;

– по возможности предоставления информации в виде, удобном потребителю и ее форматированию или сортировке.

3. *Цифровая информация* (лат. — informatio — разъяснение, изложение, осведомленность) — это информация, хранение, передача и обработка которой осуществляется с помощью информационно-коммуникационных технологий (ИКТ).

Цифровая информация может храниться не только в памяти компьютера, но и в иных различных устройствах. С их помощью можно переносить данные с одного устройства на другой. Поэтому все цифровые технологии основаны на методах кодирования и передачи информации. Цифровая информация в устройстве представляется с помощью нулей и единиц. Иными словами, цифровые технические устройства обычно работают в двоичной системе счисления, поскольку при этом устройства для их обработки получаются значительно более простыми. С помощью двух цифр 0 и 1 можно закодировать любое сообщение.

Человек не может видеть, что и как хранится в цифровом техническом устройстве или на электронном носителе цифровой информации, поскольку рабочий процесс полностью автоматизирован. Но, к сожалению, источники хранения электронной информации далеко не идеальны и выходят из строя. Поэтому обращаться с ними должен только специалист.

Так что же представляют собой современные носители информации с точки зрения их технической защищенности и надежности? Рассмотрим некоторые из таких устройств.

Практически в каждом компьютере или в похожем устройстве используется «винчестер» — жесткий диск, как основное хранилище файлов данных. Это высокотехнологичное устройство, которое выглядит, как небольшая металлическая коробочка, полностью герметичная, в которой находится магнитный диск толщиной несколько миллиметров. Обычно снизу или сверху на микронном расстоянии от диска плавает считывающая информацию электронная головка. Скорость вращения диска — порядка 10000 оборотов в минуту. Любая

микроскопическая пылинка, попавшая на поверхность магнитного диска, практически сразу вызовет выход из строя всего «винчестера». Это только одна из немногих объективных причин, которая может вызвать быстрый выход из строя этого цифрового носителя. На самом же деле любой сбой в работе жесткого диска может вызвать даже элементарный скачок напряжения.

Самым распространенным современным носителем цифровой информации, а даже точнее сказать, ее «накопителем» на данный момент является всем известная «флеш-карта», или «USB FlashDrive», которая состоит из электронных микросхем, способных удерживать заряды (электроны), в которых и содержится информация. Это самый удобный носитель, поскольку размеры его минимальны. Используется флеш-карта практически во всех современных устройствах, даже таких как телевизоры. Основной недостаток этого накопителя — в его непродолжительной жизни. Записать информацию на него можно примерно 10000 раз, потом это устройство обычно уже не работает или работает со сбоями.

Вместе с флеш-картами используются выносные носители, небольшие коробочки, которые подсоединятся к порту USB компьютера и имеют объем от 80 до 1000 гигабайт и даже выше. Если вскрыть это устройство, то мы увидим внутри обычный жесткий диск ноутбука, который через провод соединяется с нашим компьютером. По сути, это тот же жесткий диск, а поскольку размеры его миниатюрны, чтобы свободно помещаться в ноутбук, то и система более подвержена риску чем «винчестер» персонального компьютера.

В связи с тем, что криминалистическое исследование следователем (дознавателем) электронных носителей цифровой информации сопряжено со специальными знаниями и специальными навыками, законодателем Федеральным законом № 553-ФЗ от 27.12.2018 г. в действующий УПК РФ была введена ст. 164.1 «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий», а также были внесены изменения и дополнения в ст. 164 УПК РФ.

Во-первых, законодатель запретил необоснованное применение мер, которые могут привести к приостановлению законной деятельности юридических лиц или индивидуальных предпринимателей, в виде необоснованного изъятия электронных носителей информации, за исключением случаев, предусмотренных ч. 1 ст. 164.1 УПК РФ. К таким случаям относятся:

1. Когда следователем (дознавателем) вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации.

2. Когда изъятие электронных носителей информации производится на основании судебного решения.

3. Когда на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

Электронные носители информации могут изыматься при производстве следующих следственных действий: осмотра места происшествия, обыска, выемки. При этом действующий УПК РФ определил процессуальные особенности изъятия указанных носителей.

Так, согласно положениям ст. 164.1 УПК РФ, электронные носители информации изымаются в ходе производства следственных действий с участием специалиста.

Фактически эта уголовно-процессуальная норма запретила следователю (дознавателю) лично проводить изъятие в ходе следственных действий эти носители. И это, видимо, обоснованно. Следователь (дознаватель) априори не является специалистом в области IT-технологий, и их вмешательство в техническое состояние электронного носителя может просто уничтожить всю хранившуюся в нем информацию.

По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых

электронных носителей информации осуществляется копирование информации. Это также обоснованно, потому что владелец в ходе копирования может уничтожить данную информацию или изменить ее.

Копирование информации осуществляется на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации.

Снятие копий не осуществляется, когда на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе следственного действия делается запись.

Также следователь (дознаватель) в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации. 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 информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия.

Особенности восприятия следователем (дознавателем) цифровой информации, находящейся на электронном носителе, заключается в том, что он полу-

чает ее не напрямую, а только через заключение специалиста или судебного эксперта. То есть цифровая информация поступает в уголовное дело только в виде экспертного заключения, которое и имеет доказательственное значение.

Но почему-то все забывают о классической криминалистике, забывают о тех методах, которые должны использоваться в отношении электронных доказательств и их носителей. При изъятии электронной переписки основное внимание мы должны уделить не ее изъятию (изъять ее нам поможет специалист), а совсем иному.

Ведь в дальнейшем следователь (дознаватель) должен будет в ходе расследования уголовного дела совершить комплекс мероприятий по идентификации переписки, то есть определить, кто эту переписку осуществлял, привязать конкретную электронную переписку, конкретные электронные доказательства, конкретную компьютерную технику к конкретному человеку.

Для этого обязательно нужно предварительно снять с устройства все следы контакта с человеком (отпечатки пальцев, биологические следы, микроследы, которые он оставляет, с клавиатуры, мышки, коврика, со стола и т.п.).

Поэтому, по мнению автора, изъятие цифрового технического устройства, в котором находится носитель цифровой информации, должно осуществляться в ходе проведения отдельного следственного действия — осмотра места происшествия, обыска, выемки с элементами тактической операции, а также в ходе личного обыска.

Первое, что должен сделать следователь (дознаватель) при проведении указанных следственных действий, это подробно сфотографировать то место, где находится техническое устройство, составить подробный план помещения. Надо принять меры для обнаружения на поверхности и внутри технического устройства отпечатков папиллярных узоров пальцев рук, биологические следы ДНК. Это относится не только к компьютерам и ноутбукам, но и к «флэшкам», выносным дискам и т.д. Криминалистическому осмотру подлежит не только само устройство, но и его приложения: клавиатура, «мышка», коврик для «мышки», поверхность стола (подставки), электрические приборы и т.п. при-

ложения. Задача такого осмотра — «привязать» конкретное лицо к заинтересовавшему следствие техническому устройству, чтобы в дальнейшем следователь смог доказать, что именно это лицо им и пользовалось. При составлении протокола следственного действия следователь (дознаватель) должен подробно описать в нем всю обстановку, окружающую цифровое техническое устройство. Если в помещении находятся люди, то следует отметить их местонахождение, указать, какие еще технические устройства находятся в помещении и кто на них работает.

В ходе изъятия технические устройства должны быть подробно описаны в протоколе. Необходимо обращать внимание на фиксацию маркировочных надписей и иных номеров, которые помогут в дальнейшем индивидуализировать это устройство. Все изымаемые технические устройства надлежит упаковывать и опечатывать и в таком виде доставлять на экспертизу. Дальнейшую работу с ним обязаны проводить только судебные эксперты.

***Н.Ю. Лебедев,*** *д.ю.н., профессор кафедры уголовного процесса и криминалистики Новосибирского военного института имени генерала армии И.К. Яковлева войск национальной гвардии Российской Федерации, г. Новосибирск*

## ОБЯЗАТЕЛЬНОЕ УЧАСТИЕ СПЕЦИАЛИСТА ПРИ ИЗЪЯТИИ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ХОДЕ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Противодействие преступности является одной из основных социальных проблем любого государства. Незаконный оборот наркотиков и оружия, терроризм и экстремизм и многие другие преступления представляют серьезную угрозу для безопасного развития любого общества.

Однако современное расширение возможностей интернет-пространства, цифровизация всех видов деятельности, развитие IT-технологий, исследования по созданию искусственного интеллекта — все это позволило не только совершить конструктивно-технологический прорыв и улучшение всех социальных сфер жизни общества, но и создало благоприятные условия для возникновения и стремительного развития нового вида преступности, включающего в себя как преступления в сфере компьютерной информации, так и иные преступления, совершаемые с использованием компьютерной, телефонной или иной цифровой техники, а также в интернет-пространстве.

Например, современная оргтехника используется как орудие преступления, а специально создаваемые компьютерные программы позволяют в преступных целях преодолевать системы охраны и безопасности любых коммерческих организаций, а также государственных органов и учреждений.

Правоохранительной системе преступным сообществом «брошен» серьезный вызов, потребовавший не только срочного технического переоснащения силовых ведомств и подготовки соответствующих специалистов, но и серьезного реформирования всех отраслей российского права.

В Уголовный кодекс была внесена гл. 28 «Преступления в сфере компьютерной информации», в нормы Уголовно-процессуального кодекса внесены коррективы, касающиеся порядка правового регулирования изъятия электронной информации и электронных носителей, а ученые в области криминалистики осуществили разработку тактических приемов по производству следственных действий, связанных с осмотром и выемкой оргтехники, а также частных криминалистических и оперативно-розыскных методик по расследованию и раскрытию высокотехнологичных преступлений.

Существует достаточно много проблем, связанных с расследованием и раскрытием преступлений в сфере компьютерных технологий [1, с. 41-45; 2, с. 234-240], но в представленной статье нами будет затронут только один из проблемных аспектов, касающихся работы с электронными носителями.

В статье 164.1 УПК РФ законодатель постарался подробно описать правовые правила копирования информации с электронных носителей, а при необходимости и полного их изъятия. Конечно, данная норма сняла много вопросов, касающихся работы с электронными доказательствами, но при этом в ее содержании, как и практически в содержании любой нормы, содержится ряд дискуссионных аспектов, вызвавших определенное научное обсуждение в доктринальных публикациях как ученых в области уголовного процесса, так и криминалистики.

Мы хотели бы присоединиться к проблемной дискуссии, касающейся отсутствия нормативного правового закрепления понятия «электронный носитель информации», а также необходимости привлечения специалиста при ее изъятии.

До введения в 2018 г. в УПК РФ ст. 164.1, в ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ уже использовался термин «электронный носитель информации», однако в научной литературе при наименовании устройств, на которых содержится электронная информация, использовалось достаточно большое количество и других терминов, например, «электронное или цифровое устройство», «электронно-технические средства», «компьютерная или оргтехника», «накопители электронной информации» и многие другие.

Безусловно, принятие указанной статьи имело положительный эффект в части того, что законодатель еще раз подчеркнул необходимость использования единой для уголовного судопроизводства формулировки — «электронный носитель информации», в то же время он забыл о многообразии различных устройств, которые по своим техническим характеристикам имеют возможность выступить в качестве электронного носителя информации, что в свою очередь привело к отсутствию единой следственно-судебной практики, чаще всего связанной со спорами о правомерности изъятия электронных носителей информации при производстве следственных действий.

В настоящее время официальное понятие «электронного носителя информации» закреплено только в пп. 3.1.9 ГОСТа 2.051-2013, который определил, что это материальный носитель, используемый для записи, хранения и воспро-

изведения информации, обрабатываемой с помощью средств вычислительной техники.

На протяжении всего времени, с момента принятия ГОСТа, данное определение подвергалось критике со стороны ученых, и это вполне справедливо, так как в настоящее время цифровых устройств, которые могли бы подпадать под содержание данного определения, достаточно большое количество, а их использование практически во всех бытовых и промышленных приборах, а также оргтехнике, делает список подпадающих под термин «электронного носителя информации» практически бесконечным.

Представим только некоторые из электронных носителей информации:

– носители в форме диска — Компакт-диск (CD, CD-R), Цифровой многоцелевой диск (DVD), Цифровой Многослойный Диск (DMD), Флуоресцентный многоуровневый диск (FMD), Blu-ray Disc (BD), DVD высокой емкости (HD DVD), Многоцелевые многоуровневые диски высокой емкости (HDVMD), Голографический многоцелевой диск (HVD);

– носители в форме накопителя на жестких магнитных дисках (внутренние и внешние жесткие диски);

– носители, использующие технологию флеш-памяти — флеш-память, USB-флеш-накопитель, карта памяти.

В связи с этим многие ученые предприняли попытки предложить авторский вариант понятия «электронного носителя информации», например, Ю.В. Гаврилин, фактически взяв за основу определение, закрепленное в ГОСТе, добавил возможности выхода в Интернет, в итоге, по его мнению, это «устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах» [3, с. 48].

В.Н. Григорьев и О.А. Максимов, наоборот, пошли по пути упрощения, и, по их мнению, «электронный носитель информации» — это «предмет, содержащий значимую для уголовного дела информацию, созданную не в про-

цессе расследования (раскрытия) уголовного дела, восприятие которой невозможно без использования электронно-вычислительных средств» [4, с. 40].

В своем понятии А.А. Балашова, в отличие от предыдущего определения, заменила слово «содержащуюся» на «хранящуюся», а слово «восприятие» — на «использование», но в целом с точки зрения содержания его определение не претерпело кардинальных изменений: «Электронный носитель информации» — это «техническое средство, конструктивно предназначенное для хранения информации в электронно-цифровой форме, доступной для обработки с использованием средств вычислительной техники» [5, с. 40].

Как можем видеть, во всех представленных определениях упор делается на материальный носитель, который способен хранить электронную информацию и позволяет в последующем ее повторно использовать, при этом каким бы удачным по своему содержанию ни было предложено понятие «электронный носитель информации», оно не решает главный проблемный вопрос — в каком случае при производстве следственных действий, в ходе которых изымаются электронные носители информации, необходимо привлекать специалистов?

Если исходить из содержания понятия «электронный носитель информации», закрепленного в ГОСТе 2.051-2013, и буквального толкования статьи 164.1 УПК РФ, в ходе изъятия любого электронного носителя информации, будь то телефон, цифровой фотоаппарат, авторегистратор, умное устройство (часы) или другой электронный девайс, следователю необходимо привлекать к участию в производстве следственного действия специалиста, но есть ли необходимость усложнять процесс проведения следственного действия, если планируется простое изъятие и упаковка электронного носителя информации без его включения, просмотра или копирования имеющейся на нем электронной информации?

На наш взгляд, законодателю необходимо подойти к разрешению проблем, связанных с изъятием электронных носителей информации, несколько под иным углом, а именно сделать упор не только на то, какой электронный но-

ситель информации изымается, но и на то, какие манипуляции необходимо осуществить для его изъятия без потери информации.

Исходя из изложенного, в качестве рекомендаций можно было бы предложить скорректировать содержание ст. 164.1 УПК РФ на предмет обязательного привлечения специалиста при изъятии электронных носителей информации с учетом действий, которые следователь предполагает произвести непосредственно либо с электронным носителем, либо с электронной информацией, а именно электронные носители информации изымаются с участием специалиста:

– во-первых, если перед изъятием потребуется сохранение, просмотр или копирование электронной информации на электронном носителе информации;

– во-вторых, если перед изъятием потребуется сохранение, просмотр или копирование электронной информации с помощью электронного носителя информации на другом цифровом устройстве или в информационно-телекоммуникационной сети «Интернет»;

– в-третьих, если перед изъятием потребуется механическое вмешательство в корпус фиксации электронного носителя для его выемки.

Безусловно, данные предложения носят дискуссионный характер и требуют глубоко конструктивного обсуждения.

## Список литературы

1. Поляков В.В. Алгоритмизация разрешения криминалистических ситуаций при расследовании высокотехнологических преступлений // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика: сборник статей XVIII Международной научно-практической конференции / отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул, 2020. С. 41-45.

2. Давыдов С.И. Некоторые подходы к разработке частных оперативно-розыскных методик раскрытия преступлений в условиях цифровизации // Современные технологии и подходы в юридической науке и образовании: сборник

материалов Международного научно-практического форума. Калининград, 2021. С. 234-240.

3. Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4 (44). С. 48.

4. Григорьев В.Н., Максимов О.А. Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. 2019. № 2 (84). С. 40.

5. Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дисс. … канд. юрид. наук. М., 2020. С. 40.

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

## ПОНЯТИЕ СРЕДСТВ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРЕСТУПЛЕНИЙ

Научно-технический прогресс обозначил острую проблему использования его достижений в преступной деятельности. Это явление вначале привело к появлению преступлений в сфере компьютерной информации, а затем распространилось и на иные виды преступности и привело, например, к появлению бесконтактного сбыта наркотиков, кибертерроризма, мошенничества в сфере компьютерной информации и т.д. На сегодняшний день эта тенденция приобрела еще более социально опасную форму, а именно — форму высокотехнологичной преступности [1, 2]. С ней можно связать, в первую очередь, тенденцию к разработке новых или модификации в преступных целях существующих программных, аппаратных и программно-аппаратных средств, повышающих результативность преступной деятельности и одновременно резко снижающих раскрываемость таких преступлений. В связи с этим актуальной задачей современной криминалистики становится анализ применяемых преступниками но-

вых технологий, аппаратных и программных средств подготовки, совершения и сокрытия преступлений [3, с. 162]. Углубленное криминалистическое исследование типовых моделей средств высокотехнологичных преступлений позволяет сформировать знание о соответствующем элементе их криминалистической характеристики. Особую важность этому знанию придает то обстоятельство, что установление средств, с помощью которых совершаются преступления, входит в предмет доказывания (ст. 73 УПК РФ) и необходимо для успешного расследования.

В криминалистических исследованиях объектов, с помощью которых совершаются компьютерные преступления, обычно используются понятия «средство преступления» [4, 5 и др.] и «орудие преступления» [6]. Отметим, что эти понятия также широко применяются в уголовном праве, см., например [7, с. 9]. Некоторые исследователи эти понятия отождествляют, другие их отличают, но без должного указания на используемый критерий разграничения. На наш взгляд, теоретическая неопределенность в области определения таких базовых для криминалистики понятий, как «средство преступления» и «орудие преступления», является проблемой и требует разрешения. Особенно остро эта проблема стоит для новых видов преступлений, связанных с применением высоких информационных технологий. Для этого случая можно согласиться с мнением С.А. Ялышева, что проблемой «…при криминалистическом исследовании сложных высокотехнологичных компьютеризированных изделий является отсутствие сформированной, устоявшейся терминологии в области информационных (включая компьютерную) технологий» [8, с. 41].

Полагаем, что применительно к высокотехнологичным преступлениям определение понятия «средства преступлений» требует переосмысления. Это обусловлено, прежде всего, спецификой применяемых преступниками средств, которая заключается, по мнению В.А. Мещерякова, в использовании «специфического орудия преступления — средств программно-математического воздействия, объектов с уникальными свойствами» [9, с. 134]. Кроме того, указанная специфика связана с принципиальной ролью компьютерной информации,

на что справедливо обращал внимание В.Я. Колдин [10], а также с дистанционным характером преступных посягательств, в которых используются информационно-коммуникационные сети [11], то есть передача информации осуществляется с помощью процессов распространения электромагнитных колебаний.

Рассмотрим различные варианты употребления понятий «средство преступления» и «орудие преступления» в криминалистической и уголовно-правовой литературе.

По мнению А.С. Денисовой, орудия и средства являются самостоятельными категориями, которые отличаются друг от друга характером использования и возможностью контроля со стороны субъекта преступления. Так, орудия непосредственно воздействуют на предмет преступного посягательства и полностью находятся под контролем воли субъекта. Средства же используются с целью создания условий для совершения преступления и процесс их воздействия не поддается полному контролю субъекта [7, с. 9]. По вопросу об определении степени контроля преступника над средствами преступления в науке нет единого мнения и, на наш взгляд, разрешение этой задачи может представлять отдельную сложность, поэтому подход А.С. Денисовой представляет интерес, но требует дополнительной аргументации. В отношении компьютерной техники И.Г. Чекунов полагает, что «компьютер является либо орудием, либо предметом посягательств» [12, с. 39], то есть в определенных случаях относит компьютер к орудиям преступления. Аналогичной позиции придерживаются также и некоторые иные авторы, например, Д.В. Бочкин [13, с. 45]. Некоторые авторы полагают, что средство преступления является родовым понятием по отношению к орудию преступления, в частности, такой позиции придерживается А.М. Хлус [14, с. 26]. Другими словами, средства преступления должны рассматриваться по отношению к орудиям преступления как общее по отношению к частному.

Нам представляется, что последний подход наиболее соответствует позиции Законодателя. Так, в п. 8 ч. 1 ст. 73 УПК РФ «Обстоятельства, подлежащие доказыванию» содержится формулировка «... использовалось или предназнача-

лось для использования в качестве орудия, оборудования или иного средства совершения преступления ...», что подразумевает, на наш взгляд, понимание средств преступления как более широкого понятия по отношению к орудиям преступления, которые вместе с оборудованием и иными объектами входят в перечень средств. В силу этого мы будем придерживаться именно такого подхода. Таким образом, в общую категорию «средство преступлений» орудия преступления будем включать наряду с другими возможными видами средств. Кроме того, полагаем, что орудия преступления всегда являются материальными объектами (предметами), имеющими непосредственный характер воздействия при совершении преступлений. В силу этого компьютерную технику, на наш взгляд, не совсем корректно рассматривать в качестве орудия преступления, так как она оказывает воздействие на предмет преступления в большей степени не непосредственно, а опосредованно: во-первых, путем воздействия на компьютерную информацию (например, на программное обеспечение компьютерного устройства потерпевшего); во-вторых, посредством возможной дистанционной передачи этой информации через информационную сеть.

Основные составляющие понятия «средства преступления», раскрывающие его содержание, трактовались различными авторами весьма по-разному. Так, в уже упоминавшейся работе А.С. Денисовой средствами совершения преступлений назывались вещества, предметы и «виды энергии» [7, с. 9]. Весьма широко трактовали это понятие Я.В. Прудников, относивший к средствам «предметы объективной действительности, явления и процессы, которые лицо использует для совершения общественно опасного преступного деяния» [15, с. 191], и А.М. Хлус, считавший, что «под средством совершения преступлений следует понимать материальный объект, взаимосвязанный с иными элементами структуры преступления» [14, с. 31]. Ряд авторов трактует средства в еще более широком смысле, включая в их число не только одушевленные объекты (животных), но и человека [16, с. 261]. С.А. Яшков полагал, что к средствам совершения преступления нужно относить не только «орудия и приспособления», но и нематериальные объекты, а именно информацию

[17, с. 21]. Включение в перечень средств преступления информации, то есть нематериального объекта, представляется нам принципиально важным и справедливым развитием исследуемого понятия.

Опишем теперь свое видение тех групп объектов, которые характеризуют содержание исследуемой категории и формируют ее внутреннюю структуру, особо выделяя те из объектов, которые используются при высокотехнологичных преступлениях.

1. **Материальные объекты.** Эти объекты могут включать в себя две значительно отличающиеся друг от друга группы — предметы и материальные процессы различной природы.

1.1. *Предметы* — это аппаратные средства компьютерной техники, вещи, оружие, инструменты, вещества и т.д. Для высокотехнологичных преступлений интерес представляют в первую очередь различного вида технические устройства, которые обеспечивают решение широкого круга задач, возникающих при подготовке, совершении и сокрытии высокотехнологичных преступлениях. Так, к ним можно отнести, например, устройства, блокирующие сотовую связь на определенных волнах, радиоэлектронные устройства для контактных и бесконтактных подключений к каналам связи, устройства для идентификации пользователей и т.п.

Отдельно можно выделить одушевленные предметы, при этом важный вопрос о включении человека в эту группу представляется дискуссионным и заслуживающим отдельного изучения.

1.2. *Материальные процессы* — это, например, электромагнитное излучение (оптические волны, радиоволны), акустическое излучение (звуковые волны), радиационное излучение, химические реакции и т.п.

Такого рода процессы обычно не могут быть обнаружены органолептическими методами и об их наличии делается вывод или на основе диагностирования специальными средствами, или при обнаружении соответствующих следов их действия. Для высокотехнологичных преступлений в первую очередь значимы физические процессы распространения электрических колебаний по про-

водным и беспроводным каналам связи (процессы воздействия магнитного поля на материалы и специальные устройства (копирование, модификация, создание и удаление компьютерной информации). При этом беспроводная передача компьютерной информации осуществляется посредством электромагнитных волн, представляющих из себя распространяющиеся в пространстве колебания электромагнитного поля (являющегося, наряду с веществом, одной из двух форм существования материи).

2. **Информационные объекты.** По нашему мнению, эти объекты могут быть подразделены на две группы в зависимости от того, какая информация лежит в их основе — обычная или компьютерная.

2.1. *Обычная информация* — это информация, которая, в частности, может быть представлена документами, аудиозаписями, видеоизображениями и т.п. Часто источник такой информации бывает овеществленным, например, на бумажном носителе. Данная группа объектов может быть подразделена на вербальную (устную и письменную) и невербальную информацию. Отметим, что в случае высокотехнологичных преступлений обычная информация всегда используется в объединении с иными объектами, без которых самостоятельно не применяется. Например, методами социальной инженерии преступники получают данные о пароле (обычную информацию), но только в сочетании с компьютерными средствами ее использование позволяет получить доступ к компьютерной информации, которая является целью преступников.

2.2. *Компьютерная (электронная) информация* — это, согласно ст. 272 УК РФ, «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи», то есть «зафиксированные на материальном носителе сведения (сообщения, данные, команды), представленные в виде, пригодном для обработки с использованием компьютерных устройств» [18, с. 19]. Эта группа средств включает в себя все виды электронных документов, компьютерные программы (в том числе вредоносное программное обеспечение) и т.д.

3. **Комплексные объекты.** Это качественно новый вид объектов, возникающих при высокотехнологичном способе преступлений [19, 20] и характеризующийся следующими признаками: внутренним единством, взаимообусловленностью и устойчивостью сочетания отдельных объектов различной природы, именно, материальных и информационных объектов. Предложенная нами новая группа средств, которая названа комплексными объектами, содержит элементы как материальных, так информационных объектов, причем эти элементы находятся в неразделимом, взаимообусловленном и устойчивом сочетании. Полагаем, что комплексные объекты, удовлетворяющие указанным признакам, на сегодняшний день могут быть представлены двумя группами, именно, программно-аппаратными средствами и информационно-коммуникационными сетями.

3.1. *Программно-аппаратные средства* выступают комбинацией программных и аппаратных средств, работающих совместно и неразрывно для выполнения единой задачи. Такие средства часто включают в себя устройства сбора и обработки информации (например, электронная плата, электронный датчик) и специализированное программное обеспечение, разработанное для данного устройства, сохраняющее и обрабатывающее информацию, собранную аппаратной частью устройства, и управляющее его работой.

3.2. *Информационно-коммуникационные сети* включают в себя одновременно следующие связанные компоненты. Во-первых, материальные предметы, а именно аппаратные средства компьютерной техники, например, компьютеры граждан и организаций, серверы, коммутаторы, маршрутизаторы, устройства приема и передачи информации в каналах связи от источника к получателю (носители электрических, магнитных, оптических сигналов). Во-вторых, информационные объекты, например, файлы с компьютерной информацией, разнообразные компьютерные программы, обеспечивающие работу компьютерной техники (сетевые операционные системы, браузеры, сервисные программы, антивирусные программы и т.д.). В-третьих, материальные физические процессы, например, заключающиеся в передаче закодированных колебаний (например,

электрических или оптических) по проводным каналам передачи информации или в распространении радиоволн или инфракрасных волн (электромагнитных волн различной частоты) при беспроводной передаче информации. Принципиально важно, что все эти элементы представляют собой неразрывное единство, объединяемое понятием информационных сетей, отсутствие любого из них делает существование такой сети невозможным. Отметим, что, на наш взгляд, информационная сеть должна рассматриваться в качестве важнейшего и принципиального для высокотехнологичной преступности средства преступления.

4. **Комбинация объектов.** В преступной деятельности могут использоваться не только конкретные отдельные средства, входящие в приведенные три группы, но и различные сочетания (комбинации) объектов из всех этих групп.

Например, при хищении денежных средств из банкоматов могут одновременно использоваться специально созданные технические устройства для проникновения к механизмам банкоматов [21, с. 86] (материальные объекты), миниатюрные компьютеры (Raspberry Pi), оснащенные сетевым интерфейсом для передачи информации на сервер преступников по беспроводной информационной сети [22] (комплексные объекты), и использованная преступниками при неправомерном доступе конфиденциальная информация (информационные объекты).

Обобщая проведенное рассмотрение, дадим расширенную трактовку понятия «средства преступления», принимающую во внимание все вышеописанные группы объектов и учитывающую специфику высокотехнологичных преступлений. **Средства, используемые в высокотехнологичных преступлениях — это применяемые при их подготовке, совершении или сокрытии материальные объекты, включающие в себя предметы и материальные процессы; информационные объекты, включающие в себя обычную и компьютерную информацию; комплексные объекты, представленные неразделимыми, взаимообусловленными и устойчивыми комбинациями материальных и информационных объектов.** Такое определение не претендует на исчерпывающий перечень конкретных объектов, но обладает тем достоинством,

что допускает расширение и дополнение для любой из представленных групп средств преступления. Это обстоятельство представляется важным в связи с тем, что вследствие быстрого развития высоких технологий возникают благоприятные условия для появления у преступников новых средств, отсутствующих в настоящее время. Такие новые средства смогут легко вписаться в данное определение, не требуя изменения его содержания.

Полагаем, что проведенный анализ понятия «средства преступлений» важен для криминалистического исследования конкретных средств, используемых в случае высокотехнологичной преступности, и в практической деятельности по расследованию высокотехнологичных преступлений. Он может быть использован для последующей классификации этих средств на основе тех или иных критериев, а также для прогнозирования опасных тенденций в их развитии.

## Список литературы

1. Поляков В.В. Анализ обстоятельств, затрудняющих расследование и доказывание преступлений в сфере компьютерной информации // Уголовно-процессуальные и криминалистические чтения на Алтае: материалы Региональной науч.-практ. конф. / под ред. В.К. Гавло. Барнаул: Изд-во Алт. ун-та, 2006. Вып. 6. С. 111-117.

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. Гл. 2 параграф 2.2. Барнаул: Изд-во Алт. ун-та, 2019. С. 114-126.

3. Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2 (32). С. 162-166.

4. Вехов В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. 2015. № 2 (8). С. 43-46.

5. Бычков В.В. Информационно-телекоммуникационные сети как средство совершения преступлений экстремистской направленности // Вестник Академии Следственного комитета Российской Федерации. 2020. № 3 (25). С. 43-46.

6. Большаков Н.А., Гаврилин Ю.В. Арендованное компьютерное оборудование и программное обеспечение как орудия и средства совершения преступлений в сфере компьютерной информации // E-Scio. 2019. № 11 (38). С. 384-388.

7. Денисова А.С. Уголовно-правовое значение орудий и средств совершения преступления: автореф. дис. … канд. юрид. наук. М., 2005. 26 с.

8. Ялышев С.А., Семенов Н.В. Высокотехнологичные компьютерные изделия и некоторые проблемы их экспертного исследования // Эксперт-криминалист. 2008. № 2. С. 41-42.

9. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронежский государственный университет, 2001. 176 с.

10. Колдин В.Я. Электронная информация в праве // Вестник Московского университета. Серия 11. Право. 2016. № 2. С. 96-110.

11. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омская академия МВД России, 2009. 408 с.

12. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. № 2. С. 37-44.

13. Бочкин Д.В. Способы совершения компьютерных преступлений и использование информационных технологий как способ совершения преступления // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13). С. 40-46.

14. Хлус А.М. Средства совершения преступлений как элемент их криминалистической структуры // Российское право: образование, практика, наука. 2018. № 1 (103). С. 24-33.

15. Прудников Я.В. Поняття та види засобів вчинення злочину // Проблеми законності. 2018. № 142. С. 189-199.

16. Побережный Д.Б. О понятии средства совершения преступления // Известия Российского государственного педагогического университета им. А.И. Герцена. 2008. № 63-1. С. 260-263.

17. Яшков С.А. Информация как предмет преступления: автореф. дис. … канд. юрид. наук. Екатеринбург, 2005. 26 с.

18. Старичков М.В. Понятие «Компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. 2014. № 1 (68). С. 16-20.

19. Лапин С.А. Программное обеспечение как средство совершения компьютерных преступлений / С.А. Лапин, В.В. Поляков // Ползуновский альманах. - 2016. - №2. — С. 201-204.

20. Поляков В.В., Трушев В.А., Рева И.А., Поляков Вит.В., Малинин П.В. и др. Региональные особенности криминалистической характеристики преступлений в сфере компьютерной информации // Региональные аспекты технической и правовой защиты информации: монография. Барнаул: Изд-во Алт. ун-та, 2013. Гл. 1. С. 9-42.

21. Цимбал В.Н. Проблемы учета криминалистически значимой информации о способах хищений денежных средств из банкоматов // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2013. № 4 (34). С. 85-88.

22. Букова А.А., Бабешко В.Н. Хранение данных в облаке на Raspberry Pi // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020». Курск: Юго-Западный государственный университет; Московский политехнический университет, 2020. С. 34-36.

***Е.Н. Яковец,*** *д.ю.н., профессор, Заслуженный юрист РФ, ведущий научный сотрудник Центра исследования проблем российского права «Эквитас», г. Москва*

# «ГОСУДАРСТВЕННЫЙ» КИБЕРТЕРРОРИЗМ: ЧЕМ ОН ОТЛИЧАЕТСЯ ОТ КИБЕРТЕРРОРИЗМА КРИМИНАЛЬНОГО?

Информационные технологии и компьютерные сети все активнее используют транснациональные террористические и экстремистские организации с целью создания хаоса на мировой арене, что обусловило появление наиболее опасной разновидности компьютерной преступности — кибертерроризма. По имеющимся данным, такие террористические организации, как «Аль-Каида», «Братья-мусульмане», «Имарат Кавказ», «Исламское государство»[2] и др., активно используют возможности Интернета. В виртуальном пространстве ими осуществляются информационные кибератаки, пропаганда экстремистских идей, расовой, религиозной и других форм нетерпимости, а также вовлечение в свои ряды новых членов, осуществление незаконных финансовых операций и т.д.

В современной юридической науке однозначного определения данного понятия не имеется. Обобщение точек зрения различных специалистов приводит к выводу, что кибертерроризм — это комплекс преднамеренных преступных деяний в киберпространстве, создающих угрозу безопасности личности, общества и государства, связанных с насилием или угрозой насилия, применяемым негосударственными субъектами в отношении государств, международных организаций, хозяйствующих субъектов, объектов гражданской и военной инфраструктуры, политиков, других известных личностей, а также случайных лиц, — с целью оказания психологического воздействия на сознание людей в политических, социальных, религиозных или идеологических целях.

[2] Организации, запрещенные в России.

Потенциальная угроза кибератак со стороны международных террористов вырисовывается сегодня достаточно зримо. По данным экспертов, подобные нападения на государственные информационные системы, если они будут в широком аспекте реализованы на практике, могут иметь последствия, которые не менее опасны, чем традиционные террористические акты с использованием смертников, взрывчатки и т.п. Такие преступные деяния могут выводить из строя системы управления и функционирования АЭС и других важных объектов, нефте- и газопроводов, железных дорог, аэропортов, объектов водоснабжения и др. Поэтому кибертерроризм порой сравнивают по эффекту применения с воздействием ядерного, бактериологического и химического оружия. Не случайно поэтому, что в качестве приоритетных направлений научно-технических разработок в области борьбы с террористической угрозой *Концепция противодействия терроризму в Российской Федерации* [1] называет создание и внедрение эффективных средств систем связи, отвечающих требованиям защищенности от компьютерных атак (п. 37, пп. «в»).

С позиций уголовного законодательства кибертерроризм рассматривается мировым сообществом как особо тяжкое преступление против общественной безопасности и общественного порядка. В уголовно-правовой практике России деяния кибертеррористов в полной мере укладываются в рамки состава преступления, предусмотренного ст. 205 УК РФ (Террористический акт).

Кибертерроризм с момента своего зарождения стал стремительно обретать характер транснациональной, глобальной опасности. 23 ноября 2001 г. представители стран-членов Совета Европы, США, Канады, Японии и ЮАР подписали *Конвенцию о преступности в сфере компьютерной информации* [2] (Российская Федерация к данной Конвенции не присоединилась[3]), которая на сего-

[3] Нашей стране не удалось договориться о приемлемых для себя условиях трансграничного доступа к компьютерным системам. В марте 2008 г. по инициативе Президента РФ было признано утратившим силу ранее принятое распоряжение *«О подписании Конвенции о киберпреступности»* от 15 ноября 2005 г. № 557-рп, в соответствии с которым Россия оставляла за собой право определиться с участием в Конвенции при условии пересмотра положений п. «b» ст. 32, которого не последовало. Тем не менее большинство положений данной Конвенции являются ориентиром для российских государственных органов в ходе международного сотрудничества в данной области.

дняшний день является, пожалуй, единственным правовым инструментом, используемым международным сообществом для противодействия кибертерроризму.

Существенный интерес в рассматриваемой связи представляет Резолюция Генассамблеи ООН, принятая в 2019 г. по инициативе России. Этот документ призывает соблюдать принципы суверенного равенства и невмешательства во внутренние дела государств. Россия полагает, что Конвенция о преступности в сфере компьютерной информации, разработанная в конце 1990-х гг., не в состоянии регулировать многие современные отношения в данной сфере, а также противостоять кибертерроризму. Она допускает возможность нарушения принципов государственного суверенитета и невмешательства во внутренние дела других государств и по-прежнему создает угрозу легитимизации доступа специальных служб ограниченной группы стран к бесконтрольному сбору персональных данных пользователей со всего мира, а также сохраняет установленную рядом государств тенденцию консолидации их технических достижений в информационном пространстве и сохранения цифрового разрыва между развитыми и развивающимися странами [3, с. 74].

Обеспокоенность руководства России на этот счет вполне понятна, поскольку хакерские методы могут с успехом использоваться не только террористическими организациями и злоумышленниками-одиночками, но и представителями силовых структур развитых в кибернетическом отношении стран в ходе так называемых «гибридных войн» [4, с. 6].

За последние несколько лет было высказано немало опасений по поводу того, что террористы могут начать эффективные кибератаки против критической информационной инфраструктуры (КИИ) различных государств. Однако несмотря на то, что онлайн-пропаганда террористов выглядит весьма активной и они неплохо используют возможности шифрованных мессенджеров для коммуникаций, их хакеры пока еще крайне беспомощны в том, что касается использования продвинутого софта для осуществления разрушительных кибератак. Они не только не используют многофункциональные шпионские и боевые программы, но и продолжают закупать услуги хостинга, арендуют ботнеты

для DDoS атак и используют другой устаревший софт, характерный для подростков и одиночных преступников [5, с. 99].

На этом фоне методы ведения кибернетической войны, сходные до степени смешения с методами, практикуемыми кибертеррористами, активно заимствуются и используются силовыми ведомствами отдельных государств Запада. Причем, что характерно, подобные действия рассматриваются последними как оборонительные и их реализация предусматривается военными доктринами этих государств. Взять, к примеру, деятельность в этом направлении англоязычных стран. В 2011 г. Президент США еще только определял экстренные меры, необходимые для реализации стратегии кибербезопасности [6], а уже в наши дни — 30 октября 2020 г. — Центр передового опыта совместной киберзащиты НАТО (NATO Cooperative cyber defense centre of excellence, NATO CCDCOE) публикует отчет «Альянс «Пять глаз»[4] и наступательные возможности в киберпространстве: реализация «Инициативы киберсдерживания». В этом документе отмечается, что западные страны в отличие от «коварной» России выступают за признание и открытое обсуждение развития наступательных возможностей в киберпространстве, если они согласуются с действующими нормами международного права (а таких норм, по их мнению, в настоящее время для обоснования боевых действий в киберпространстве вполне достаточно). Поэтому применение кибероружия против своих противников западные государства считают само собой разумеющимся [7].

Из этих материалов также усматривается, что врагом номер один для них в этом плане является Россия, представляющая наибольшую угрозу национальной безопасности Америки и опережающая по степени опасности КНДР с его ядерным оружием и Исламское государство[5] с его джихадистами [8]. Основания и поводы для «наказания» нашей страны коллективным Западом изыскиваются уже давно, и проба сил в этом направлении произошла не вчера. Первым зафиксированным деянием подобного рода, предпринятым против нашей страны, считается взрыв сибирского газопровода «Уренгой — Сургут — Челя-

[4] В него входят Австралия, Великобритания, Новая Зеландия, Канада и США.
[5] Организация, запрещенная в России.

бинск» в 1982 г. Газопровод имел стратегическое значение для СССР, в связи с чем США были крайне заинтересованы в выведении его из строя. В начале 1980-х гг. президент Р. Рейган одобрил план диверсий против экономики Советского Союза. В этой связи советским специалистам под видом технической поддержки была передана компьютерная программа, содержавшая скрытые дефекты. Впоследствии она и спровоцировала взрыв газопровода [9].

Разведывательные органы США и их союзников ведут наблюдение за миллиардами людей по всему миру, в том числе с помощью различных электронных устройств, используемых в бытовых целях. Телевизоры, смартфоны и даже антивирусный софт — все это уязвимо для взлома ЦРУ и АНБ. Данные возможности включают записи звуков, изображений и приватных текстовых сообщений пользователей, даже если они прибегают в ходе общения к шифрующим приложениям. Все эти меры направлены на тотальный сбор информации, в том числе и с целью нанесения последующих ударов в виртуальном пространстве с помощью кибероружия, которые представляют собой, по сути, хакерские атаки на стратегические объекты вероятного противника. Вполне очевидно, что подобные деяния, совершаемые представителями спецслужб западных государств, выходят за рамки обычной общеуголовной практики и обретают черты *государственного кибертерроризма.*

Как справедливо отмечает в данной связи профессор О.В. Дамаскин, «кое-где информационный терроризм стал элементом государственной политики. В некоторых странах активно ведутся работы над компьютерными программами, являющимися информационным оружием. Причем объектами для такого оружия все чаще становятся отдельные личности, социальные группы, принимающие решения... Информационное воздействие на государство, общество, отдельно взятого человека, в конечном счете, оказывается более эффективным и экономичным, чем политическое, экономическое и даже силовое, военное» [10, с. 267].

В рамках тектонических сдвигов, происходящих на международной арене, страны Запада постоянно обвиняют в хакерских атаках на их информационные ресурсы Россию. Консультанты Белого дома даже включили нашу страну

в список «государств-хакеров». Можно назвать целый ряд громких киберпреступлений, в совершении которых за последние годы обвиняли российских хакеров [11, 12, 13]. Представители руководства нашей страны опровергают причастность России к этим акциям и заявляют, что не поддерживают киберпреступность. Пресс-секретарь президента Д.С. Песков неоднократно заявлял, что Москва предлагала Вашингтону сотрудничество в сфере обеспечения кибербезопасности, но ни разу не встретила понимания в этом вопросе.

В начале марта 2021 г. газета The New York Times со ссылкой на информированные источники объявила, что власти США в ближайшие три недели предпримут несколько кибератак против России в ответ на крупномасштабный взлом американских правительственных сетей, обнаруженный в конце 2020 г. [14]. Данное сообщение представляет особый интерес с позиций формулирования сущности и содержания государственного кибертерроризма. Попробуем определить его понятие, но не с помощью дефиниции, а путем перечисления его *основных признаков.*

Итак, хакерские атаки, как пишет газета, *будут скрытными и незаметными для остального мира, но «очевидными для российской разведки, вооруженных сил и Президента Владимира Путина».* Это означает следующее: в данном конкретном случае кибератаки носят демонстративный характер, поскольку они анонсированы через СМИ, однако подобные действия могут осуществляться и без предварительного предупреждения, то есть тайно.

Инициаторы их проведения рассчитывают оказать *политическое давление* на определенных лиц из числа руководства нашей страны. К числу таковых относятся руководители СВР и Минобороны России, а также лично Президент РФ В.В. Путин. В своем скандальном интервью от 17 марта 2021 г. телеканалу ABC News президент США Джо Байден продублировал эти угрозы, пообещав, что «Владимир Путин «заплатит» за вмешательство в американские президентские выборы», и допустив откровенно оскорбительные выпады в отношении нашего Президента. Хозяин Белого дома, однако, не пояснил, в чем именно будет заключаться обещанная им «расплата» [15].

Кибератаки, планируемые в отношении России, по словам газеты The New York Times, будут проводиться *в сочетании с дополнительными экономическими санкциями.* Одних лишь экономических мер Западу явно не хватает, поэтому чтобы более основательно наказать нашу страну, он предпринимает дополнительные шаги, в том числе реализуемые через киберпространство.

Причем вся эта возня происходит *на фоне концентрации натовских войск* вдоль западных российских границ, нагнетания напряженности в Донбассе, притязаний на северные акватории России в тающих льдах Арктики, наращивания противостояния в космосе и др. То есть киберудары сочетаются не только с экономическими, но и *военными мерами давления* на нашу страну, а также с активной *антироссийской пропагандой.*

Таковы основные признаки государственного кибертерроризма, угрозу воздействия которого испытывает на себе Россия.

Не следует полагать, что американцы в киберпространстве являются исключительно потерпевшей стороной. Под благообразной личиной «невинных овечек» они демонстрируют острые клыки, постоянно увеличивая число кибератак на КИИ России с территории Северной Америки и Европы, включая недружественные России страны ближнего зарубежья [16].

Таким образом, за последнее время наблюдается переход конкуренции в киберпространстве (как, впрочем, и в реальном мире) на качественно новый уровень: теперь это противоборство, *предполагающее нанесение противнику ощутимого ущерба.* Безусловно, данное обстоятельство повлечет за собой существенное повышение уровня международной конфронтации, которое приведет к стиранию грани между войной и миром. В подобной ситуации можно и не заметить, как «холодная» война перерастет в «горячую», тем более что в киберсфере на сегодняшний день не имеется никаких регуляторных договоренностей между странами, а в Военной доктрине РФ [17], как и у ее оппонентов, содержатся положения, гарантирующие нанесение ответных ударов по агрессорам.

Как известно, каждое государство вправе осуществлять разведывательную и контрразведывательную деятельность, и ничего необычного в этом нет. Подобные действия могут носить нелегальный характер либо осуществляться под

прикрытием определенных официальных структур. Представители противоборствующих разведывательных служб с целью сбора информации проникают на чужую территорию и в то же время защищают свои собственные информационные ресурсы от аналогичных действий противника. Так было, есть и будет. Это аксиома разведывательной и контрразведывательной деятельности. Помимо агентурной разведки в эпоху развития научных достижений широко практикуется и разведка техническая (ТР), которая классифицируется по видам, решаемым задачам и используемым в качестве источников информации физическим полям исследуемых объектов. К числу разновидностей ТР относится и *компьютерная разведка*. В XXI в. разведывательную информацию добывают в том числе и киберразведчики, «выуживающие» тайны из компьютеров потенциального противника. Для этого пересекать чужие границы им не требуются. В этой связи все те действия в киберпространстве, как реальные, так и мнимые, в которых огульно обвиняют Россию, целиком укладываются в концепцию современной *киберразведывательной деятельности.* Вполне закономерно, что заимствование определенных данных в ходе осуществления киберразведки может быть сопряжено с нанесением вероятному противнику некоторого материального ущерба, поскольку любая информация обладает соответствующей ценностью или потребительской стоимостью, и в отдельных случаях ее можно рассматривать как *товар*. Однако нанесение в мирное время в ответ на похищение информации кибер ударов по своим оппонентам, предполагающих причинение крупного материального ущерба, возможную гибель людей и дестабилизацию жизни населения целых стран, — это уже явный «перебор». Ни с правовой, ни с моральной точек зрения оправдать такие действия невозможно. С нормативных позиций их следует квалифицировать как *существенное превышение пределов необходимой обороны.* Инициаторов и исполнителей подобных акций, осуществляемых на государственном уровне, следует приравнивать к международным кибертеррористам и судить уголовным порядком.

Ситуация в этом вопросе осложняется еще и тем, что достоверно установить субъектов разведывательной деятельности в киберпространстве чрезвычайно сложно, если вообще возможно, а вся политика «коллективного Запада»

в отношении России традиционно строится на принципе, выражающимся англоязычным словосочетанием highly likely, которое можно перевести на русский язык как «с высокой степенью вероятности» или просто — «весьма вероятно».

Кстати, практически одновременно с анонсированным кибернаступлением на Россию в Америке проявился и «китайский след». Агентство Bloomberg опять же highly likely сообщило, что мартовский взлом почтовых серверов Microsoft, который затронул около 60 тыс. организаций по всему миру и превратил его в глобальный кризис кибербезопасности, осуществлён китайскими хакерами.

Без сомнения, американские чиновники задумались над тем, стоит ли им предпринимать ответные меры против Китая. Ведь США могут оказаться в таком положении, при котором им придется вступить в потенциально опасный конфликт с двумя своими крупнейшими противниками, обладающими ядерным оружием. К тому же Китай — важнейший торговый партнер западных стран, и лишиться китайского рынка американцы не торопятся. За последние годы китайцы значительно преуспели в развитии IT-технологий и в ближайшее время намерены полностью избавиться от иностранной зависимости в данной области [18]. Так что обострять конфронтацию с Китаем в киберпространстве американцы явно не желают, переключая весь свой негативный запал на Россию.

В рассматриваемом контексте следует обозначить ряд важнейших проблем в данной области, связанных с обеспечением безопасности отечественной виртуальной среды. Практически все важнейшие хозяйствующие субъекты в России, не говоря уже о рядовых пользователях компьютерной техники, работают на иностранном программном обеспечении и оборудовании. На закупку всего этого «добра» за последние десятилетия истрачены сотни миллиардов долларов. В результате вероятный противник с помощью всевозможных «спящих» вредоносных программ и созданных в этом оборудовании преднамеренных уязвимостей получает возможность контролировать нас изнутри и при случае делать с нами все что угодно [19, с. 1, 8, 9]. Поэтому весьма серьезную проблему в рассматриваемом плане представляет отсутствие на сегодняшний день *отече-*

*ственных* предприятий, которые на *отечественной* элементной базе выпускали бы *отечественные* процессоры, контроллеры и прочие компоненты [20, с. 8-9]. По словам известного IT-эксперта, одного из разработчиков отечественной операционной системы А. Смирнова, если мы хотим избавиться от технологической зависимости в рассматриваемой сфере, необходимы значительные вложения для того, чтобы создать *новую отрасль промышленности, целую новую индустрию* [21].

В связи с этим одним из главных направлений усиления безопасности компьютерных сетей является активное импортозамещение. Специалисты заговорили об этом уже давно [22, 23, 24]. Однако как отмечают многие специалисты, для защиты российской КИИ значительно дешевле и эффективнее обеспечить широкое применение технологий, разработанных, испытанных и внедренных еще в конце 1990-х — начале нулевых годов в Санкт-Петербургском государственном научном центре РФ «Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики». Они связаны с созданием защитных программ-невидимок, реализованных в микропроцессорах (так называемый «компьютерный стелс»). Данные технологии могут и должны быть положены в основу российской глубокоэшелонированной системы защиты, включая частные приложения, операционные системы, облачные структуры и телекоммуникационные каналы связи [19, с. 1, 8, 9].

В условиях обострения межгосударственных отношений, разрушения системы однополярного мира, возвращения на мировую арену России и появления новой сверхдержавы — Китая, киберорружие становится действенным инструментом глобального противостояния. От того, кто быстрее сможет освоить передовые цифровые технологии, создать мощную систему защиты от государственного кибертерроризма, зависит не только национальная безопасность той или иной страны, но и в целом мировой порядок.

Кроме того, само по себе применение киберорружия в силу колоссального разрушительного потенциала последнего необходимо поставить под междуна-

родный контроль и приравнять его к использованию иных видов оружия массового поражения.

## Список литературы


1. Концепция противодействия терроризму в Российской Федерации, утвержденная Президентом РФ 5 октября 2009 г. // Российская газета. 2009. 20 октября.
2. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). [Электронный ресурс]. URL: https://base.garant.ru/4089723/ (дата обращения: 22.03.2021).
3. Доклад Генерального секретаря ООН по Резолюции Генеральной Ассамблеи ООН от 30 июля 2019 г. № 73/187 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». [Электронный ресурс]. URL: https://www.unodc.org/ (дата обращения: 11.03.2021).
4. Третья мировая на пороге. Какая она?: интервью генерал-полковника, специалиста в области геополитики, конфликтологии, международных отношений и военной истории, президента Академии геополитических проблем Л.Г. Ивашова главному редактору газеты «Аргументов недели» А. Угланову // Аргументы недели. 2021. № 5 (749). 10-16 февраля. С. 6.
5. Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Мировой опыт. М.: Международные отношения, 2020. 288 с.
6. Cybersecurity 3 апреля 2011 // Официальный сайт Президента США. [Электронный ресурс]. URL: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity (дата обращения: 15.03.2021).
7. Федотов А. Альянс «Пять глаз» и наступательные возможности в киберпространстве — отчет НАТО // d-russia. ru. 2020. 11.11. [Электронный ресурс]. URL: https://d-russia.ru/aljans-pjat-glaz-i-nastupatelnye-vozmozhnosti-v-kiberprostranstve-otchjot-nato.html (дата обращения: 09.03.2021).
8. Кто главный враг Запада: Россия или терроризм? // ОБЗОР.PRESS. Переводы иностранной прессы. 2016. 23 марта. [Электронный ресурс]. URL:

https://obzor.press/press/18386-kto-glavnyij-vrag-zapada-rossiya-ili-terrorizm (дата обращения: 17.03.2021).

9. Черных Е. Рейган — отец первой кибервойны. Против СССР // Комсомольская правда. 2014. 20 марта. [Электронный ресурс]. URL: https://www.kp.ru/daily/26209.3/3093616/ (дата обращения: 17.03.2021).

10. Дамаскин О.В. Россия в современном мире: проблемы национальной безопасности: монография. М.: Флинта; Наука, 2007. 429 с.

11. Саенко Л. Русских хакеров обвинили по полной программе. Власти США насчитали ущерб от их действий на $10 млрд // Коммерсантъ. 2020. 19 октября. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4539225 (дата обращения: 14.03.2021).

12. Вахрушева Я. Российских хакеров снова обвинили в атаках — на этот раз на вакцину от COVID-19 // 5 канал. 2020. 16 июля. [Электронный ресурс]. URL: https://www.5-tv.ru/news/304167/rossijskih-hakerov-snova-obvinili-vatakah-naetot-raz-navakcinu-otcovid19/ (дата обращения: 14.03.2021).

13. Назарова А. «Российских хакеров» бездоказательно обвинили во взломе системы минфина США // Взгляд. Деловая газета. 2020. 14 декабря. [Электронный ресурс]. URL: https://vz-ru.turbopages.org/vz.ru/s/news/2020/12/14/1075576.html (дата обращения: 14.03.2021).

14. Котляр М. NYT сообщила о готовящейся в США серии кибератак на Россию // РБК. 2021. 8 марта. [Электронный ресурс]. URL: https://www.rbc.ru/politics/08/03/2021/6045814a9a7947d87795a619 (дата обращения: 09.03.2021).

15. Наумов А. «Он заплатит». Джо Байден ответил утвердительно на вопрос, считает ли он Владимира Путина убийцей // Коммерсант. 2021. 17 марта. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4731349?utm_source=yxnews&utm_medium=desktop (дата обращения: 17.03.2021).

16. Большая игра. Выпуск от 11 марта 2021 г. [Электронный ресурс]. URL: https://www.1tv.ru/shows/big-game/vypuski/bolshaya-igra-vypusk-ot-11-03-2021 (дата обращения: 12.03.2021).

17. Военная доктрина Российской Федерации (утв. Президентом РФ 25 декабря 2014 г. № Пр-2976). П. 21, пп. «у» // Российская газета. 2014. 30 декабря.

18. Сангер Д., Барнс Дж., Перлрот Н. The New York Times (США): готовясь выступить с ответными мерами против России, США столкнулись с очередной хакерской атакой китайцев // Иносми. Ру. [Электронный ресурс]. URL: https://inosmi.ru/politic/20210308/249284861.html (дата обращения: 12.03.2021).

19. Угланов А. Кто парализовал Москву 10 марта? // Аргументы недели. 2021. № 10. С. 1, 8, 9.

20. Чуйков А. Россия: отстать навсегда? // Аргументы недели. № 27 (671). 2019. 17 июля. С. 8-9.

21. Васильченко С. Россия проигрывает Третью мировую войну: технологическое отставание стало критическим. Почему страна стала аутсайдером в IT-конкуренции // MKRU. 2019. 19 августа. [Электронный ресурс]. URL: https://www.mk.ru/politics/2019/08/19/rossiya-proigryvaet-tretyu-mirovuyu-voynu-tekhnologicheskoe-otstavanie-stalo-kriticheskim.html (дата обращения: 23.02.2021).

22. В российской армии официально созданы кибервойска // Вести.RU. [Электронный ресурс]. URL: http://www.vesti.ru/doc.html?id=2858596 (дата обращения: 24.02.2021).

23. Критическую информационную инфраструктуру защитят отечественным ПО // Концорциум Кодекс. 2019. 4 июля. [Электронный ресурс]. URL: https://kodeks.ru/news/read/kriticheskuu-informacionnuu-infrastrukturu-zaschityat-otechestvennym-po (дата обращения: 18.03.2021).

24. Объекты критической информинфраструктуры переведут на российское оборудование к 2025 году // ТАСС. 2020. 29 октября. [Электронный ресурс]. URL: https://tass.ru/ekonomika/9851951 (дата обращения: 18.03.2021).

# ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

***Е.Г. Александрова,*** *аспирант кафедры судебных экспертиз и криминалистики Российского государственного университета правосудия, г. Москва*

## НАЗНАЧЕНИЕ СУДЕБНЫХ ЭКСПЕРТИЗ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

В России гражданские беспилотные летательные аппараты активно приобретаются как коммерческими организациями, так и гражданским населением. Аналитик кластера космических технологий и телекоммуникаций инновационного центра «Сколково» Валерий Комиссаров утверждает, что «исторические темпы роста продаж дронов (88,2%) превосходят исторические темпы роста продаж смартфонов» [1]. Помимо того, прогнозируется рост рынка к 2020 г. до 9,5 млрд долларов [2, с. 43]. Однако наряду с ростом продаж гражданских беспилотных летательных устройств увеличивается и количество преступлений, совершаемых с их использованием.

В нашей стране наиболее часто совершаются правонарушения и преступления на территориях органов уголовно-исполнительной системы: осуществляется доставка запрещенных предметов осужденным с использованием беспилотных летательных устройств. Как правило, на территории тюрем доставляются наркотические средства, алкогольная продукция, телефоны, зарядные устройства и сим-карты. По данным Федеральной службы исполнения наказаний России, 6 марта 2017 г. в городе Казани была предпринята попытка перевозки на территорию исполнительной колонии № 2 пластиковой бутылки со спиртосодержащей жидкостью и свертком с порошкообразным веществом

белого цвета. Посредством производства экспертизы было установлено, что порошкообразное вещество являлось синтетическим наркотическим веществом [3]. В 2017-2018 гг. была предотвращена доставка 262 телефонов в места лишения свободы. В 2018 г. пресекли 27 попыток перевозки, было перехвачено 130 средств мобильной связи, в 2017 г. — 38 попыток и 132 мобильных телефона [4].

В связи с учащением случаев неправомерного использования беспилотников в России разрабатывают и внедряют различные способы предупреждения и пресечения противоправного их использования. Одним из способов является законодательное регулирование. С июля 2017 г. беспилотные летательные устройства с максимальной взлетной массой от 0,25 до 30 килограммов подлежат обязательному учету в соответствии с Федеральным законом № 291-ФЗ [5]. В конце сентября 2019 года вступило в силу Постановление Правительства № 658, обязывающее владельцев беспилотных летательных аппаратов ставить их на учет [6]. Порядок постановки беспилотного судна на учет содержится на официальном интернет-ресурсе Федерального агентства воздушного транспорта [7]. В июле 2019 г. были внесены изменения в Кодекс об административных нарушениях: введены штрафы за игнорирование требований по постановке беспилотника на учет, что приравнено к нарушениям правил использования воздушного пространства [8].

Другим важным способом противодействия общественно опасной эксплуатации беспилотных устройств является использование систем мониторинга, обнаружения и уничтожения посторонних беспилотных летательных аппаратов. Примером таких систем являются комплексы обнаружения и защиты «Стриж», установленные в территориальных органах уголовно-исполнительной системы городов Казани и Курске. Данная система имеет радиус действия один километр и обладает такими функциями, как обнаружение и нейтрализация беспилотных летательных устройств.

Однако ни законодательное регулирование, ни использование систем обнаружения и защиты от беспилотников не могут полностью предотвратить их

противоправное использование. В связи с этим правоохранительные органы должны быть подготовлены к расследованию преступлений, совершаемых с использованием беспилотных летательных устройств. В качестве примера расследуемого преступления, совершаемого с использованием беспилотного летательного аппарата, взята незаконная перевозка наркотического средства на территорию тюрьмы — ст. 228 Уголовного кодекса Российской Федерации.

При подготовке к совершению указанного преступления злоумышленник придерживается следующей тактики. Для начала он согласовывает с заключенным вид груза, дату, время и место сброса. Для этого, как правило, используются средства мобильной связи. Для места сброса выбирается территория с наличием сыпучего грунта: песка, древесных опилок и т.д. Для определения места взлета беспилотника преступником учитываются технические возможности беспилотного летательного аппарата, а также наличие скрытого пути отхода за счет особенностей рельефа местности и наличия дорожной сети. Необходимо отметить, что преступники упаковывают груз в противоударную упаковку, например, в поролон, и снаружи ей придают липкую основу, например, упаковка оборачивается лентой двойного скотча. При падении такой упаковки с наркотическим средством происходит налипание на него сыпучего грунта, за счет чего предмет сброса маскируется.

При совершении данного вида преступления, как правило, складывается следующая типичная следственная ситуация. Злоумышленник неизвестен, он пытается скрыться с места запуска дрона. Беспилотное летательное судно, скорее всего, сбито системами обнаружения и уничтожения дронов либо сотрудниками Федеральной службы исполнения наказаний. Наркотическое средство либо прикреплено к беспилотному устройству, либо было сброшено и лежит на территории тюрьмы.

При расследовании указанного преступления в первую очередь следственной оперативной группе необходимо обнаружить, зафиксировать и изъять следы преступления, а также начать производство розыскных мероприятий. По модели беспилотного летательного судна можно установить дальность его

полета, данная информация позволяет определить максимальные границы его запуска. С учетом полученных сведений осматривается территория вокруг тюрьмы с целью поиска следов преступника, устанавливается наличие камер видеонаблюдения, изымаются видеозаписи, опрашиваются возможные свидетели. На месте совершения преступления беспилотное летательное судно следует упаковывать таким образом, чтобы не были уничтожены следы пальцев рук, которые могут находиться на корпусе. Для этого беспилотник можно обернуть простыней. Упаковку наркотического средства необходимо проверить на наличие отпечатков пальцев рук, само средство необходимо взвесить и направить на судебно-химическую экспертизу для установления того, чем является данное вещество.

После осмотра места происшествия и протоколирования следователь назначает судебные экспертизы в зависимости от того, какие объекты были ранее обнаружены, зафиксированы и изъяты. Необходимо обратить внимание на то, какие следы могут быть обнаружены на беспилотном летательном аппарате. Помимо традиционных следов, таких как отпечатки пальцев рук и засохший след крови, на беспилотнике могут сохраниться запаховые следы человека. С высокой вероятностью пахучие вещества имеются на литий-ионном аккумуляторе и флеш-носителе беспилотного летательного аппарата. Указанные части беспилотника являются пригодными для данного исследования по причине того, что их часто достают из дрона и вставляют обратно (частый физический контакт), а также они находятся в корпусе беспилотного устройства (отсутствие разрушающего воздействия окружающей среды). При производстве экспертизы запаховых следов извлекается запаховый след с носителя, устанавливается его пригодность к идентификации (определяется наличие или отсутствие в нем запахового следа человека). Далее при обнаружении запахового следа человека он хранится при определенных условиях для последующего проведения идентификационного исследования.

После назначения экспертизы запаховых следов следует назначить дактилоскопическую экспертизу. Исследуется корпус беспилотного летательного ап-

парата, его внутренние части. После устанавливается пригодность следов пальцев рук к идентификации. Далее они также сохраняются до того момента, когда будет назначено идентификационное исследование.

При наличии на изъятых предметах следов крови назначается судебно-биологическая экспертиза: устанавливается группа крови, резус-фактор, а также при необходимости и ДНК. Следует отметить, что след высохшей крови — крайне удачный объект для экспертизы запаховых следов, так как он сохраняет запаховый след человека не менее чем на 17 лет.

Далее отметим необходимость назначения исследования беспилотного летательного аппарата, с моей точки зрения, в рамках компьютерно-технической экспертизы. Задачами данного исследования будут являться установление точек взлета и посадки беспилотника, а также определение координат полета. Указанная информация хранится на флеш-носителе в виде лог-файлов, которые в последующем расшифровываются специализированными программами. Одной из наиболее распространенных платформ для чтения логов является Mission planner.

Таким образом, при расследовании преступлений, совершаемых с использованием беспилотных летательных устройств, в зависимости имеющихся объектов необходимо назначить следующие виды экспертиз в определенном порядке:

- экспертиза запаховых следов, объектами которой будут являться литий-ионный аккумулятор, флеш-носитель беспилотника;
- компьютерно-техническая экспертиза беспилотного летательного аппарата, объектом которой будет являться флеш-носитель беспилотника;
- экспертиза следов пальцев рук (дактилоскопическая экспертиза), объектами которой будут являться внешняя и внутренняя поверхности беспилотного летательного устройства и упаковка наркотического вещества;
- судебно-химическая экспертиза, объектом которой будет являться наркотическое средство;

- судебно-биологическая (генетическая) экспертиза, объектами которой будут являться следы крови на беспилотном летательном судне.

## Список литературы


1. Байбеков Ш. Регулирование рынка беспилотников пока вне поля зрения органов власти. [Электронный ресурс]. URL: https://www.eg-online.ru/article/318959/ (дата обращения: 20.04.2021).
2. Тихонов А.И., Краев В.М. Инвестиционный потенциал рынка беспилотных летательных аппаратов // Современный ученый. 2017. Т. 1. № 1. С. 42-45.
3. Федеральная служба исполнения наказаний. [Электронный ресурс]. URL: http://фсин.рф/news/index.php?ELEMENT_ID=305886&sphrase_id=997585 (дата обращения 21.04.2021).
4. Куликов В. ФСИН научилась блокировать дроны преступников. [Электронный ресурс]. URL: https://rg.ru/2019/01/31/reg-cfo/fsin-nauchilas-blokirovat-drony-prestupnikov.html (дата обращения: 21.04.2021).
5. О внесении изменений в Воздушный кодекс Российской Федерации: Федеральный закон от 03.07.2016 № 291-ФЗ // Офиц. текст: по состоянию на 24.04.2021 // КонсультантПлюс.
6. Об утверждении Правил учета беспилотных гражданских воздушных судов с максимальной взлетной массой от 0,25 килограмма до 30 килограммов, ввезенных в Российскую Федерацию или произведенных в Российской Федерации: Постановление Правительства РФ от 25.05.2019 № 658 // Офиц. текст: по состоянию на 24.04.2021 // КонсультантПлюс.
7. Официальный Интернет-ресурс Федерального агентства воздушного транспорта. [Электронный ресурс]. URL: https://favt.ru/dejatelnost-ucet-bespilotnyh-grajdanskih-vozdyshnih-sudov/ (дата обращения: 21.04.2021).
8. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 26.07.2019 № 217-ФЗ // Офиц. текст: по состоянию на 24.04.2021 // КонсультантПлюс.

***Т.А. Алексеева,*** *ст. преподаватель кафедры геоинформатики и кадастра Томского государственного архитектурно-строительного университета, г. Томск*

# ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРОИЗВОДСТВА КОММУНИКАТИВНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ С ПРИМЕНЕНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Цифровые технологии все больше расширяют сферу влияния, регулируют различные стороны жизни общества. Криминалистика как прикладная наука всегда использовала передовые технологии для целей расследования преступлений, находя им и практическое применение, и теоретическое обоснование. В процессе производства коммуникативных следственных действий, в частности, допроса, перед следователем стоит одновременно несколько задач: 1) установление психологического контакта с допрашиваемым; 2) фиксация в протоколе его показаний; 3) определение признаков недостоверности его слов. Указанная многозадачность порождает и проблемы, когда возможность сосредоточиться на чем-то одном идет за счет уменьшения внимания к другому аспекту. Цифровые технологии в этом смысле призваны не только облегчить работу следователя, но и могут являться источником получения новой информации о личности допрашиваемого.

Рассмотрим несколько вариантов применения цифровых технологий при производстве коммуникативных следственных действий.

1. Видеозапись. Одной из наиболее доступных и распространенных цифровых технологий остается видеозапись. Использование видеозаписи во время производства коммуникативных следственных действий дает возможность следователю, не отвлекаясь на фиксацию показаний в протоколе, уделять внимание анализу вербального и невербального поведения допрашиваемого с целью определения его эмоционального состояния и возможных признаков недостоверности показаний. Кроме того, наличие видеозаписи предполагает наличие

еще одного доказательства по расследуемому делу, на основе которого в случае необходимости возможно провести экспертное исследование. Видеозапись позволяет вернуться к интересующим или спорным моментам в показаниях допрашиваемого, а также исключает возможность отказаться от сказанных слов или обвинить допрашивающего в осуществлении давления.

2. Программы распознавания речи. Средства распознавания речи можно разделить на две группы: первая группа — автономное программное обеспечение для персонального компьютера и мобильных устройств (Braina Voco Professional, Real Speaker, Amazon Transcribe), вторая группа — интернет-сервисы (Speechlogger и Speechpad от компании Goodle, Go Transcribe). Это классические инструменты, которые ориентированы в первую очередь на диктовку, то есть большинство из таких программ предназначены для того, чтобы преобразовывать голос одного конкретного человека в текст [1]. Проблемой использования программ распознавания речи является то, что не все они рассчитаны на русский язык, а если программа все-таки работает с русским языком, то качество полученного распознанного текста далеко от идеального. Тем не менее сфера машинного перевода является динамично развивающейся, и нельзя исключать возможности использовать указанные технологии в интересах следствия. Так, распознавание речи допрашиваемого и преобразование ее в текст значительно упростили бы работу следователя по составлению протокола, позволив сосредоточиться на личности допрашиваемого. Кроме того, программы распознавания речи, при условии получения качественных расшифровок голоса, позволят следователю проводить допрос за пределами кабинета следственного органа, в месте, которое будет удобным для допрашиваемого в случае тактической целесообразности.

3. Программы распознавания эмоций (EmoDetect [2], FaceReader, the FacE Analysis System [3]). Выражение лица человека служит источником информации о его эмоциональном состоянии, отношении к собеседнику и готовности идти на контакт. Как правило, программы распознавания эмоций позволяют определить шесть базовых эмоций: радость, удивление, грусть, злость, страх,

отвращение. Рассогласованность испытываемых эмоций с содержанием показаний может свидетельствовать о неискренности допрашиваемого, о наличии тревожащего его фактора, об отношении к допрашивающему лицу. Перспективы использования подобных программ представляют ценность не только для следователя, но и для эксперта при назначении различного рода криминалистических экспертиз.

4. Программы распознавания лжи (Ex-Sense-PRO-R [4], приложение Verity [5]). Выявление ложных показаний, пресечение лжи являются одними из приоритетных задач во время производства коммуникативных следственных действий. До сих пор существуют споры о том, возможно ли достоверно установить ложь и какие методики использовать для достижения указанной цели. Цифровые технологии в вопросе распознавания лжи также не стоят на месте, предлагая как отдельные программы, так и приложения на мобильные устройства. В их основе лежит анализ голоса, считывание пульса, анализ жестов, мимика и движения зрачков.

Подводя итог вышесказанному, важно отметить, что стремительное развитие цифровых технологий и внедрение их в следственную практику неизбежно, поэтому важно извлекать из этого плюсы, совершенствуя процесс расследования преступлений. Однако остается ряд проблем, таких как процессуальное оформление применения различных компьютерных программ, этичность использования технологий, разработка достоверных методик, позволяющих использовать рассмотренные технологии как в следственной, так и в экспертной практике, которые предстоит решить в ближайшем будущем.

## Список литературы

1. Программы распознавания речи. Что понимает искусственный интеллект? [Электронный ресурс]. URL: https://www.primavista.ru/blog/2017/08/03/programmyi-raspoznavaniya-rechi (дата обращения: 20.05.2021).

2. Программа распознавания эмоций по лицу. [Электронный ресурс]. URL: https://emodetect.ru/ (дата обращения: 20.05.2021).

3. Исследование рынка систем распознавания эмоций. [Электронный ресурс]. URL: https://habr.com/ru/post/133686/ (дата обращения: 20.05.2021).

4. Голосовой детектор лжи «Ex-Sense-PRO-R». [Электронный ресурс]. URL: https://ntcarc.com/services/golosovye-analizatory/26/ (дата обращения: 20.05.2021).

5. Разработка первого в мире мобильного детектора лжи. [Электронный ресурс]. URL: https://ruward.ru/cases/843/ (дата обращения: 20.05.2021).

***Р.Л. Ахмедшин,*** *д.ю.н., профессор кафедры криминалистики Томского государственного университета, г. Томск*

## МЕТОДИЧЕСКИЕ, ТАКТИКО-КРИМИНАЛИСТИЧЕСКИЕ И ПРОЦЕССУАЛЬНЫЕ ОСОБЕННОСТИ ПРОВЕДЕНИЯ СУДЕБНО-ПСИХОЛОГИЧЕСКОЙ ЭКСПЕРТИЗЫ В РЕЖИМЕ ДИСТАНТНОГО ВЗАИМОДЕЙСТВИЯ (ONLINE-РЕЖИМЕ)

Активная, пусть порой и бездумная практика дистантного (online) взаимодействия, наблюдаемая в наше время в современном российском обществе, актуализирует необходимость дистант-алгоритмов во всех сферах жизнедеятельности общества. Не является исключением из сказанного и область судебно-психологической экспертизы. Без сомнения, при возможности выбора режим непосредственного взаимодействия эксперта и исследуемого в рамках судебной экспертизы предпочтителен, однако иметь разработанный алгоритм подобного взаимодействия в дистантной форме сегодня необходимо.

Как и любая новация, online следственное действие (в том числе и психологическая экспертиза) обладает рядом преимуществ, к которым относятся:

1) снижение судебных расходов государством;

2) снижение судебных расходов сторонами в процессе (указанное обстоятельство может способствовать формированию пока отсутствующей у граждан

установки на повышенную целесообразность обращения в суд. Недоверие государству предопределяет недоверие суду, и чем меньше дискомфорта принесет гражданам судебная процедура, тем более активно, вероятно, они будут отстаивать свои права);

3) существенное сокращение времени рассмотрения уголовного и гражданского дела;

4) некоторый психологический комфорт для участников взаимодействия, проистекающий из освобождения от временных затрат;

5) некоторый психологический комфорт для участников взаимодействия, проистекающий из меньшего дискомфорта ввиду нахождения на «собственной» территории;

6) невысокий риск подлога процессуального документа.

Несмотря на положительные моменты проведения судебно-психологической экспертизы в режиме online, исследователям только еще предстоит решить комплекс проблем, к которым мы относим:

1) программную адаптацию психодиагностических методик, включающую не только «цифровизацию» этих методик, но также и создание баз данных, которые, с одной стороны, имеют достаточную доступность и удобство интерфейса, с другой — закрытость от взлома;

2) разработку приемов установления и поддержания психологического контакта в ситуациях дистантного взаимодействия в процессе судебно-психологической экспертизы;

3) разработку приемов определения истинности сообщаемой исследуемым информации в условиях ограниченного восприятия объекта наблюдения;

4) разработку приемов, способствующих повышению уровня надежности доказательства с позиций уголовно-процессуальной техники.

Система видеоконференц-связи раньше применялась судами только для обеспечения участия осужденных в рассмотрении их кассационных и надзорных жалоб. Насколько обоснованно введение в судебную практику этой новой формы взаимодействия (видеоконференции) в контексте эффективного получе-

ния доказательств, должны показать последующие исследования. Следует отметить, что наблюдаемая реализация положений, внесенных в ст. 278.1 УПК РФ «Особенности допроса свидетеля путем использования систем видеоконференц-связи» Федеральным законом от 20.03.2011 № 39-ФЗ ввиду достаточной эффективности вполне может быть распространена и на практику расследования преступлений.

Основной проблемой для исследователей на настоящий момент становиться решение вопроса о возможности внедрения online следственных действий в практику предварительного расследования. С одной стороны, признанное в суде, оно не может быть лицемерно не распространенно на предварительное расследование. С другой стороны, наивно оспаривать объективность комплекса возникающих проблем, начиная от недостаточности технических знаний у эксперта, не имеющего такой сервисной технической поддержки как в системе судов, и заканчивая проблемой фиксации показаний. Надеемся, что решением проблемы фиксации результатов online следственных действий не будет задействование института, позорящего российский уголовный процесс и de-facto постулирующего презумпцию вины следователя — института понятых.

Использование в следственной практике online следственных действий без сомнения целесообразно, но, конечно, требует осторожного научного осмысления. Однако предыдущее утверждение в наименьшей степени относится к практике проведения судебно-психологической экспертизы.

Вероятно, целесообразно разработать хотя бы на уровне «черновом» тактико-криминалистическое обеспечение проведения судебно-психологической экспертизы, гипотетически оптимизирующее процесс проведения этого следственного действия в режиме дистантного взаимодействия (online-режиме). По нашему мнению, криминалистической ценностью будут обладать следующие тактико-криминалистические рекомендации:

1. На начальном этапе внедрения такой новации, как online-экспертиза, целесообразно выбирать место ее проведения в ближайшем государственном учреждении судебной системы, однако со временем оно может переместиться

в место жительства или работы исследуемого, или как компромиссный вариант — в офис его адвоката, хотя, конечно, присутствие последнего, как показывает практика, в том числе и из собственного опыта, вызывает для эксперта целый комплекс проблем, особенно если профессиональный уровень адвоката невелик, либо стиль его взаимодействия с участниками процесса выраженно агрессивен.

2. Находясь в привычной ситуации, недобросовестный исследуемый более уверен в себе, не склонен к излишней нервозности. Неудивительно, что удаление от стрессообразующего фактора с высокой степенью вероятности предопределит отстаивание лживой позиции. У исследуемого формируется установка, что расстояние между экспертом и ним — это фактор, его защищающий. Серия шуток на тему «как будто удаленности участников» приведет к неосознаваемому понижению уверенности исследуемого в психологической безопасности.

3. Эксперту необходимо помнить, что в случае взаимодействия в режиме дистантного взаимодействия (online-режиме) ситуационная тревожность исследуемого тем меньше, чем привычнее обстановка для него. Сказанное не касается ряда случаев, в которых в помещении помимо исследуемого могут оказаться заинтересованные в исходе дела лица. Например, родители исследуемого ребенка при проведении судебно-психологической экспертизы, направленной на установление места жительства ребенка с конкретным родителем.

4. Не прекращает быть актуальным крайне низкий уровень развития навыков использования программного обеспечения особенно среди лиц старшего возраста. Стандартизированный под интерфейс программ Microsoft office и наиболее распространенных мессенджеров типа WhatsApp позволит оперативно адаптироваться к новым условиям взаимодействия эксперта и исследуемого. Естественно, разработка подобных интерфейсов — это современный вызов профессионализму работников Министерства юстиции, но, надеемся, их квалификации будет достаточно для решения столь сложной задачи. Как временную меру можно практиковать предварительную встречу психолога и ис-

пытуемого в режиме обучения программному сопровождению предстоящего экспертного исследования. Естественно, протоколирование данной встречи также должно быть обязательным.

5. Так же как и в процессе online-допроса, находясь вне привычного сценария распределения ролей, некоего доминирующего начала, эксперт чувствует себя менее уверенно. Можно предположить, что в силу этой неуверенности он, проецируя психическое напряжение, неосознанно воспринимает исследуемого как фигуру, личностно окрашенную негативно в большей степени, чем это произошло бы в процессе непосредственного взаимодействия [1, с. 8].

6. Помимо вышесказанного можно упомянуть еще одно обстоятельство, которое приводит к повышению неосознанной критичности у эксперта в адрес исследуемого. Речь идет о том, что при ограниченной возможности восприятия, исследуемого в полный рост, эксперт несколько ограничен в наблюдении за частью реакций исследуемого, лежащих за пределами обзора камеры, что обусловливает неосознанно повышенную критичность анализа воспринятого.

7. Оптимально такое расположение допрашиваемого, чтобы в кадр входило не только его лицо и фигура, но и прилегающее пространство. В идеале справа-сзади от допрашиваемого оптимально расположить повернутое под 45 градусов к плоскости объектива зеркало.

8. При реализации приемов определения лжи в речи исследуемого необходимо принимать во внимание искажение голоса, возникающие в силу качества используемой аппаратуры. Искажения будут всегда, необходимо на уровне методических рекомендаций указать допустимую степень их отклонения, определяя диапазон допустимых характеристик устройств online-связи. Последнее — еще один вызов сотрудникам Министерства юстиции от научного прогресса.

9. Освещение допрашиваемого должно быть сверху-спереди, как наиболее четко передающее мимику. Эксперту необходимо помнить, что наихудшее расположение — съемка под источником освещения. В рассматриваемом случае мы имеем дело с так называемым «жестким» светом, направленным вниз,

из-за которого у объекта проявятся синяки под носом и надбровными дугами, что формирует несколько «злодейский» вид. Если вы не специалист-светотехник, то лучше использовать рассеянный и мягкий свет, который подойдет к любой внешности и даст стабильно позитивный результат. Необходимо помнить, что по умолчанию осветительные приборы дают жесткий свет, поэтому они используются с насадками, предназначенными для рассеивания света.

10. Криминалистам уже сегодня необходимо обратить внимание на новые формы извещения лица о вызове на online следственные действия. Логичным было бы использование таких элементов, как электронная почта в качестве доставки и электронная подпись в качестве свидетельства ознакомления с повесткой.

11. При фиксации хода экспертного исследования необходимо указывать технические параметры интернет-соединения и аппаратуры, которая была использована.

12. Подлежат фиксации факты прерывания связи, длительность прерывания связи и указание на лицо, у которого связь прервалась, так как, возможно, это сделано испытуемым для получения консультаций.

13. Совершенно новая проблема, ранее не свойственная для сферы криминалистического обеспечения расследования, — информационная безопасность. Сохранение тайны следствия и тайны психологического исследования немыслимы без создания собственного российского программного обеспечения и собственных российских online-сервисов и облачных хранилищ. К сожалению, на данный момент у правоохранительной системы отсутствует программный инструментарий, с высокой степенью вероятности гарантирующий, что к данным online не получит доступа посторонний.

Все вышеназванные проблемы вполне преодолимы в рамках развития нового вектора криминалистической тактики в части приемов взаимодействия участников расследования в режиме дистантного взаимодействия (online-режиме).

**Список литературы**

1. Ахмедшин Р.Л. Тактические особенности допроса в online-режиме // Сборник материалов криминалистических чтений. 2015. № 11. С. 7-9.

***А.И. Букур**, к.ю.н., преподаватель кафедры технико-криминалистического обеспечения экспертных исследований Московского университета МВД России имени В.Я. Кикотя, г. Москва*

## НЕКОТОРЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО СОПРОВОЖДЕНИЯ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ТРАВМАТИЧЕСКОГО ОРУЖИЯ

Борьба с преступлениями всегда была и остается одной из прерогативных задач государства. Из всего объема совершаемых преступлений особое внимание заслуживают вооруженные, так как посягают на самое дорогое — жизнь и здоровье. Указанные деяния характеризуются особой дерзостью, поскольку совершаются с применением оружия различных моделей, видов и целевого назначения. На каждый подобный преступный вызов обществу государство обязано отвечать применением адекватных мер противодействия, использованием современных методов расследования, не уступающих преступности. Однако как показывает практика, сегодня правоохранительные органы играют роль догоняющего, не успевая адекватно реагировать на каждый факт вооруженного преступления [2, с. 119].

Указанная ситуация складывается не только потому, что преступность использует инновационные средства, но и потому, что имеющийся у органов расследования «инструментарий» используется не в полном объеме. Речь идет об информационном сопровождении раскрытия и расследования преступлений, совершаемых с применением оружия самообороны.

Сегодня порядка 6 млн жителей нашего государства на законных основаниях владеют и используют одно или несколько видов оружия различных моделей и целевого применения. Каждый год в органы государственного контроля и лицензионно-разрешительной системы Росгвардии России обращаются свыше полумиллиона человек за правом приобретения оружия самообороны.

Оружие самообороны составляет группу гражданского оружия, в которую входит: огнестрельное гладкоствольное длинноствольное оружие, огнестрельное оружие ограниченного поражения (далее — травматическое оружие), газовое оружие, а также электрошоковые устройства и искровые разрядники [1]. Из данного списка интерес представляют травматическое оружие и газовое оружие, поскольку внешне они схожи с известными образцами боевого огнестрельного оружия, имеют возможность поразить цель на расстоянии, могут быть портативными или пригодными для скрытого ношения, а также применяются для последующей переделки с целью стрельбы металлическим снарядом. По указанным причинам преступники используют их для совершения преступлений чаще всего.

Анализ статистических данных Главного информационно-аналитического центра МВД России (далее — ГИАЦ МВД) показал, что число вооруженных преступлений, совершаемых ежегодно, в целом не уменьшается. Это несмотря на то, что приискать для совершения преступления боевое огнестрельное оружие, которое можно носить скрытно, например, пистолет, весьма не просто. По экспертным оценкам более половины вооруженных преступлений сегодня совершаются именно с использованием оружия самообороны, которое используется как в промышленном, так и в переделанном виде.

Говоря об информационном сопровождении раскрытия и расследования преступлений, в первую очередь подразумевается обмен данными, содержащими важные сведения о преступлении. Правоохранительные органы государства зачастую применяют различные информационные системы для обмена информацией, составляющей сведения для служебного пользования. Сегодня достижения научно-технического прогресса в сфере обмена информацией внедряют-

ся в целый спектр различных услуг государственных органов. Надо признать, что в целом внедрение различных информационных систем стало особенностью современного общества.

Главное отличие современных информационно-поисковых систем от их предшественников — каталогизированных учетов, ведущихся в форме журналов и картотек, заключается в реальной возможности оперативного сопровождения раскрытия и расследования преступлений. Используя автоматизированные средства, почти вся криминалистически значимая информация находится в состоянии максимальной готовности, автоматически сравниваясь с новыми объектами, поступающими в систему.

Сегодня толкование криминалистической регистрации устарело. Данная отрасль криминалистики уже не представляется как совокупность отдельных видов и групп учетов, ограниченных по функциональным возможностям, действующим в режиме «запрос — ответ» [7, с. 64]. В настоящий момент криминалистическая регистрация — это автоматизированная информационно-поисковая система (АИПС). Потенциал данной системы относительно велик, но в практике раскрытия и расследования преступлений, совершаемых с применением оружия самообороны, не используется в полном объеме. АИПС — есть еще одна форма работы hi-tech-технологий, которая сегодня противоречит современному состоянию ее методического и организационного обеспечения, так как она практически не применяется в раскрытии и расследовании указанных видов преступлений. Фактически отсутствует связь со следами применения оружия самообороны, обнаруживаемыми в ходе ОМП и иных следственных действий, с информационными банками данных, ведущимися на федеральном, региональном и местном уровнях.

Раскрытие и расследование преступлений, совершаемых с применением оружия самообороны, в некоторой мере зависит от уровня информационного сопровождения, что подразумевает использование специальной электронно-вычислительной техники, баз данных и т.д. Лица, расследующие преступления исследуемой категории, все чаще обращаются к учетам, ведущимся в органах

внутренних дел, для получения данных криминалистического и оперативно-розыскного значения. Речь идет об учетах (дактилоскопических, трасологических и иных), не связанных со следами выстрела из газового и травматического оружия, которые, по нашему мнению, очень важны для расследования уголовного дела по указанным преступлениям.

Сегодня нормативно-правовая база, регламентирующая деятельность органов внутренних дел, обязывает их вести криминалистические, оперативно-справочные и розыскные учеты. Указанные учеты содержат данные об объектах, являющихся частью события преступления или имеющих с ним связь. Они имеют большое значение в раскрытии и расследовании преступлений, представляя собой ведущую роль информационного сопровождения. Вместе с этим они не содержат всей информации об обороте оружия самообороны, патронов к нему и следах их применения. Для того чтобы разобраться со сведениями, содержащимися в указанных учетах относительного травматического оружия, рассмотрим весь путь с момента покупки его лицом для собственных нужд.

Согласно действующему законодательству, приобретение оружия и патронов на территории Российской Федерации подлежит лицензированию [1]. Таким правом наделены граждане Российской Федерации, достигшие возраста 18 лет [1].

Лицензия на приобретение травматического оружия и патронов к нему выдается подразделениями Росгвардии России. Срок рассмотрения ведомством заявления на право приобретения составляет до одного месяца. Затем с момента получения лицензии и в течение последующих шести месяцев лицо может купить в специализированном магазине оружие самообороны и патроны к нему на законных основаниях. Приобретенное оружие необходимо зарегистрировать в соответствующих ведомствах с включением в электронную базу данных сведений о собственнике и оружии: марка и модель, серийный номер и калибр, ФИО владельца, адрес регистрации и фактического пребывания и т.д. Указанные сведения помещаются в информационную базу данных (ИБД). В случаях, когда собственник оружия самообороны меняет место проживания или совер-

шает действия по отчуждению оружия (дарение, продажа), новая информация помещается в ИБД.

Информация о собственнике оружия самообороны, содержащаяся базе, при обнаружении последнего на месте происшествия может быть получена лицом, расследующим преступление, и применена для оперативного установления лиц, причастных к совершению преступления, о чем свидетельствуют многочисленные примеры.

По экспертным оценкам количество осмотров мест происшествий с изъятием оружия исследуемого вида не более 10-12% от общего числа осмотров по преступлениям, совершаемым с его применением. Надо полагать, что в ходе ОМП по данным преступлениям чаще изымаются основные следы выстрела (стреляные гильзы, выстрелянные пули и пр.), однако определить конкретную модель оружия самообороны и, соответственно, его владельца, в настоящий момент не представляется возможным. Указанная ситуация складывается потому, что информация об оружии самообороны содержится в базе не в полном объеме. Например, при регистрации данного оружия не производится его контрольный отстрел, как при регистрации огнестрельного нарезного оружия. В связи с этим сегодня перед практикой раскрытия и расследования преступлений, совершаемых с применением оружия самообороны, стоит весьма непростая проблема.

В настоящее время в правоохранительных органах нашей страны отсутствует нормативно-правовое регулирование контрольного отстрела травматического оружия при его регистрации и постановке на учет. Согласно авторской позиции, указанное положение является упущением со стороны правоохранительных структур, потому как большинство моделей травматического оружия, так же, как и образцы огнестрельного нарезного оружия, при стрельбе оставляют на гильзах следы, пригодные для идентификации. Исключение составляют образцы травматического оружия, где воспламенение заряда осуществляется за счет тока (например, бесствольный травматический пистолет «Оса»), однако надо понимать, что такие образцы редко используются при совершении пре-

ступлений, поскольку преступники отдают предпочтение образцам, внешне схожим с боевыми аналогами оружия, выбрасывающими при стрельбе гильзу со следами оружия.

Необходимость ведения учета гильз, стреляных в травматическом оружии, в первую очередь, вытекает из потребностей практики. Как показал опрос практических работников следствия и дознания ОВД, 91% из них ответили, что считают необходимым ведение централизованного учета гильз, стреляных в травматическом оружии. В данном случае речь идет именно о стреляных гильзах, поскольку на выстрелянных пулях ввиду пластичности материала, из которого они изготавливаются, следов от канала ствола травматического оружия не остается.

Необходимо отметить, что в некоторых субъектах нашей страны данный учет ведется на добровольных началах. Так, к концу 2015 г. в региональной пулегильзотеке ЭКЦ ГУ МВД России по Алтайскому краю насчитывалось чуть более 1,5 тыс. гильз со следами, полученными в ходе контрольного отстрела травматического оружия. Данное количество сформировано благодаря владельцам травматического оружия, согласившимся добровольно предоставить по три патрона травматического действия для контрольного отстрела. Однако указанное не является нормой, в связи с чем большинство моделей приобретаемого травматического оружия не отстреливается и стреляные в них гильзы на учет не ставятся.

Согласно положениям приказа МВД России № 70 от 10.02.2006 «Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации» (п. 6), на каждый объект со следами заводится информационная карта с описанием основных свойств объекта и криминалистически значимых признаков (следов). Затем информационная карта помещается в электронную базу данных (картотека), а объект — в натурную коллекцию, откуда он может быть изъят при наличии соответствующих оснований.

Если рассматривать возможность ведения учета травматического оружия по аналогии с учетом нарезного огнестрельного оружия, а также стреляных

гильз и выстрелянных из него пуль, то можно выделить следующие виды: *учет самодельного и переделанного травматического оружия, учет экспериментальных гильз выявленного травматического оружия, учет контрольных гильз регистрируемого травматического оружия, а также учет гильз и патронов со следами травматического оружия, изъятых с мест происшествий*.

Для более детального анализа рассмотрим каждый из возможных учетов на примере информационных карт с описанием основных свойств и признаков травматического оружия и стреляных гильз.

Учет самодельного и переделанного травматического оружия необходимо вести из-за следов, остающихся на оружии в результате внесения в его конструкцию изменений. Давно известно, что указанные изменения в определенной мере характеризуют лицо, их осуществляющего, помимо этого переделка оружия носит индивидуальный характер. Если следы самодельного изготовления и переделки травматического оружия регистрировать, то при поступлении нового объекта можно будет получать информацию о ранее поступавших объектах с аналогичными следами.

## Список литературы

1. Федеральный закон Российской Федерации от 13.12.1996 г. № 150-ФЗ «Об оружии». [Электронный ресурс.] URL: http://www.consultant.ru/ document/cons_doc_LAW_12679/

2. Волынский А.Ф. Криминалистическое обеспечение раскрытия и расследования преступлений: учебное пособие для слушателей магистратуры и адъюнктов по кафедре криминалистики. М., 2016.

3. Технико-криминалистическое сопровождение расследования преступлений: учебное пособие / под ред. А.М. Багмета. М.: Юрлитинформ, 2016.

4. Исаева Л. Обыск: роль специалиста // Законность. 2001. № 6.

5. Шмонин А.В. Обыск и выемка в кредитной организации: проблемы и пути их решения // Банковское право. 2005. № 5.

6. Чулахов В.Н. Криминалистичекое значение и особенности исследования навыков изготовителя самодельного огнестрельного оружия // Вестник криминалистики. Вып. 1. М.: Спарк, 2000. С. 68-71.

7. Ялышев С.А. Криминалистическая регистрация: проблемы, тенденции, перспективы. М.: Академия управления МВД России, 1998.

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

## СОДЕРЖАНИЕ РАБОЧЕГО ЭТАПА ОСМОТРА ИНФОРМАЦИОННОЙ СРЕДЫ В СЕТИ «ИНТЕРНЕТ»

Центральное место во всем следственном действии занимает рабочий этап, поскольку именно в этот период производится непосредственное исследование информации, позволяющей установить обстоятельства, имеющие значение для уголовного дела.

Отмечая непосредственную актуальность данного этапа, следует сказать, что именно правильность действий с точки зрения криминалистической тактики, соответствие их процессуальному законодательству, сложившиеся требования практической деятельности, а также выработанные научным миром рекомендации позволяют признать рассматриваемый вид доказательства допустимым, следствием чего является его использование судом в рассмотрении дела по существу.

В юридической литературе приводится классификация относительно способов осуществления данного следственного действия:

1. Деревенский вариант, в котором следователь или оперуполномоченный совместно со специалистом (из числа сотрудников, обслуживающих осматриваемый сервер) проводит осмотр содержимого сервера, используя штатные программные и аппаратные средства. В протоколе осмотра при подобном

осмотре отражаются: характеристики сервера (версия операционной системы), рабочее состояние генерирующей и обрабатывающие логи программы, файлы с логами (их временные метки), права доступа к лог-файлам, учетные записи (аккаунты) пользователей, имеющих права на запись в лог файлы.

2. Провинциальный вариант. Для участия в следственном действии приглашается независимый специалист, при этом представитель владельца сервера (желательно из числа технических сотрудников) также участвует в осмотре. В протоколе отражаются сведения о защищенности системы, ее проверке на наличие вредоносных программ, сведения об установленных обновлениях (патчах); подробные данные о генерирующей логи программе, всех ее настройках и окружении (чтобы можно было узнать о выявленных ошибках и оценить вероятность невыявленных); подробные данные о логирующей программе, в том числе настройки, касательно размещения, срока хранения и ротации логов; сведения, помогающие интерпретировать логи, например, описания используемых программ. При этом полные логи, задействованные программы и их настройки копируются на компакт-диск типа CDR или DVDR (однократная запись), который опечатывается и в случае необходимости отправляется на экспертизу.

3. Столичный вариант, в котором нужный сервер отключается, опечатывается должным образом и отправляется на экспертизу. Перед экспертом ставятся вопросы касательно содержания логов, их интерпретации, а также вопросы об известных ошибках, приводящих к некорректности логов, о защищенности системы, о следах возможной фальсификации или несанкционированного удаления логов [5, с. 65].

Следует отметить, что рассмотренная классификация отражает общие варианты производства осмотра компьютерной техники и является ориентирующей для последующего раскрытия преступления.

Рабочий этап осмотра информационной среды в сети «Интернет» начинается со сбора участвующих лиц в заранее отведенном месте. Исходя из общего правила, следователь объявляет о начале производства следственного действия,

его характере, целях и содержании. Факультативным на данной стадии является объявление судебного решения лицу, чьи права будут ограничены в ходе производства осмотра путем исследования информации, правообладателем которой он является. По окончании ознакомления лица с указанным судебным решением последний ставит на нем отметку об ознакомлении с указанием времени. Далее разъясняются права и обязанности участвующим лицам. Особую роль стоит отвести специалисту, чью цель участия необходимо довести до остальных участников. Указанное связано с высокой степенью участия специалиста и его значением для правильности и полноты производства осмотра.

Обязательным, по нашему мнению, является объявление о применении технических средств и программного обеспечения. К числу технических средств следует отнести: персональный компьютер или ноутбук, модем, роутер или иное устройство, посредством которого осуществляется доступ к информационно-коммуникационной сети «Интернет». В протоколе необходимо отразить модель ноутбука или персонального компьютера, модема (роутера), его Мас-адрес, а также организацию интернет-провайдера и абонентский номер (при наличии).

Среди программного обеспечения следователю необходимо отразить вид браузера, который будет использоваться для осуществления доступа к тому или иному информационному ресурсу, а также иные программы, используемые в ходе выполнения следственного осмотра.

После выполнения указанных действий настает стадия фактического выполнения осмотра. Следователь объявляет о том, к какому информационному ресурсу будет осуществляться доступ, после чего предоставляет возможность выполнения доступа к нему специалисту. При этом положение участвующих лиц должно быть таким, чтобы имелась возможность полного визуального контакта с монитором персонального компьютера для осуществления наблюдения за выполняемыми действиями. Для выполнения указанных целей не лишним будет использовать дополнительный монитор, дублирующий изображение с основного. Соблюдение такой рекомендации позволит исключить все сомне-

ния по поводу допустимости данного доказательства в части заявлений о том, что понятые или иные участники следственного действия не в полной мере могли наблюдать за выполняемыми действиями.

Непосредственное исследование информации в сети «Интернет» должно происходить по заранее выстроенной следователем схеме. Очевидным является, что веб-ресурсы могут иметь различную структуру. Потребность в осмотре того или иного сайта возникает у следователя в зависимости от категории уголовного дела. Так, по делам о преступлениях в сфере незаконного оборота наркотических средств и психотропных веществ актуальным может являться осмотр сайта в виде «интернет-магазина». В свою очередь такой тип сайтов имеет определенную структуру, некоторое количество разделов по категориям, на которые может осуществляться как последовательный, так и случайный переход.

По делам о компьютерных преступлениях или преступлениях в сфере мошеннических действий может возникнуть потребность в производстве осмотра сайта, имеющего линейную структуру. Такая структура подразумевает под собой последовательный переход со страницы на страницу в пределах одного веб-ресурса. На рабочем этапе такого осмотра фиксируется текущее состояние компьютерной информации, делается вывод о произошедшем событии и его последствиях: уничтожение, блокирование, модификация, копирование информации, нарушение работы ЭВМ, их системы или сети; устанавливается способ совершения преступления. Особое внимание уделяется содержимому файлов регистрации, в которых может содержаться информация о паролях пользователях, их именах, идентификационных номерах.

По делам, например, экстремисткой направленности, чаще всего возникает потребность в осмотре интернет-страниц в социальных сетях, поскольку указанные ресурсы позволяют привлечь достаточно большую аудитории и позволяют любому пользователю осуществлять демонстрацию запрещенных в России материалов. Согласно определению, предложенному учеными, социальная сеть — это веб-сайт, онлайн-платформа, предназначенные для построения, ор-

ганизации и отражения общественно-социальных взаимоотношений в сети «Интернет» [2, с. 201].

Вышеуказанное подтверждает необходимость наличия у следователя предварительного плана в части последовательности действий при производстве осмотра интернет-ресурса.

В научной литературе отмечается, что в целях получения допустимых доказательств необходимо соблюсти не только требования, прямо предъявляемые законом, но и удостовериться, что: 1) устройство, при помощи которого производится осмотр, на протяжении всего следственного действия имеет связь с сетью «Интернет», а передаваемая и получаемая информация не искажается или подменяется кем-либо; 2) информация получается непосредственно из сети «Интернет», а не из временного буферного хранилища; 3) пользователям, которые обращаются к осматриваемому веб-сайту с разных адресов, передается одинаковая информация; 4) осматриваемая веб-страница одинаково отображается в различных браузерах [3, с. 189].

По нашему мнению, указанные требования являются необходимыми для соблюдения положений, поскольку прямо влияют на достоверность отраженных в ходе следственного действия данных.

При непосредственном исследовании информации, выражающемся в визуальном осмотре, следователю необходимо акцентировать внимание участников на имеющие значение для уголовного дела обстоятельства, содержащиеся на интернет-ресурсе. При осуществлении перехода с одного раздела (вкладки) на другой следователю также необходимо акцентировать внимание участвующих лиц на это.

В некоторых следственных ситуациях также может возникнуть потребность в выяснении вопроса о правах на домен, на котором размещена исследуемая страница. Имя или фирменное наименование администратора домена и некоторые другие его данные можно получить в официальной базе данных доменных имен регистратора российской доменной зоны «RU» Российского научно-исследовательского института развития общественных сетей (РосНИ-

ИРОС) с помощью сервиса «WhoIs». Для того чтобы это выполнить, в поисковом окне браузера указываем наименование сервиса, то есть «WhoIs», в появившемся диалоговом окне указываем имя сайта, получаем информацию. Информация РосНИИРОС достоверна.

Также следователь должен указывать и URL-адрес. При необходимости узнать конкретную информацию на странице следователю нужно описывать все фрагменты, относящиеся к делу, и приводить их описание. При этом хочется акцентировать внимание, что процессуальная фиксация тех или иных данных осуществляется самостоятельно по собственному усмотрению.

Для оценки последующей допустимости такого доказательства важной является такая характеристика, как достоверность содержащейся в протоколе информации. Поскольку каждый интернет-ресурс имеет свой определенный адрес, который имеет как численное выражение, так и буквенное, выступающее определенной альтернативой, важным является установления соответствия между указанными формами выражения адреса. В связи с изложенным не лишним будет привести позицию А.В. Бегичева относительно нотариальной практики по обеспечению доказательственной базы. Как указывает автор, к задачам нотариуса в ходе процедуры обеспечения доказательств в обязательном порядке относятся следующие положения:

1) установление администратора домена (владельца сайта), т.е. информацию о принадлежности доменного имени информационного ресурса;

2) проверка соответствия символьного адреса сайта его настоящему IP-адресу (трассировка), чтобы убедиться в том, что браузер отображает страницы подлинного сайта;

3) фиксация содержания конкретного интернет-сайта.

Изложенное обязывает нас особенно акцентировать внимание на процедуру трассировки. Как отмечает А.В. Бегичев, «трассировка, прежде всего, производится с целью исполнения мер защиты от возможных фальсификаций. Технически она позволяет осуществить следующее: установить IP-адрес, на котором размещен сайт; проверить принадлежность этого IP-адреса; провести трассировку от компьютера нотариуса до сервера, содержащего сайт; собрать ин-

формацию о DNS-записях домена интернет-сайта; установить принадлежность домена на момент осмотра и др.» [1, с. 208].

С целью всестороннего изучения всех обстоятельств уголовного дела, а также получения как ориентирующей, так и доказательственной информации, возникает необходимость установления IP-адреса, а в последующем и сведений о нем и использования в деятельности по расследованию преступлений [4, с. 88].

Важно понимать, что конечная цель рабочего этапа и в целом следственного осмотра информации в сети «Интернет» определяется категорией самого уголовного дела и предметов обстоятельств, подлежащих доказыванию по нему. По нашему мнению, в ходе исследования информации могут решать следующие специальные задачи:

1. Процессуальная фиксация наличия (отсутствия) материалов определенного содержания. Доказывание настоящего факта может иметь место по делам об экстремизме или нарушению авторских прав.

2. Определение работоспособности интернет-ресурса, возможности или необходимости совершения определенных действий, в том числе скачивания в память устройства, через которое осуществляется доступ к сайту, определенных данных. При этом частной задачей является определение следующего: является ли скачивание информации добровольным, то есть посредством действий посетителя интернет-ресурса, или принудительным, то есть скрытно от пользователя. Фиксация указанного факта может быть важным обстоятельством по уголовным делам в сфере распространения вредоносного программного обеспечения или же интернет-мошенничества, направленного на хищение персональных данных, данных банковских карт или иной информации, позволяющей в дальнейшем совершить конкретное хищение.

3. Поиск и фиксации IP-адресов, через которые осуществляется управление сайтом, персональных данных и иной информации, позволяющей установить владельца сайта и иных лиц, причастных к совершению преступлений указанных категорий.

Важно также обозначить, что хотя указанное следственное действие и предполагает определенное исследование информации, но все же осмотр

предполагает работу по правилу «Что вижу — то пишу». В связи с чем спорным является вопрос о фиксации в рамках такого осмотра выводов, сделанных как специалистом, так и следователем при участии последнего. Фиксация таких выводов допустима, например, в ходе последующего допроса лица, привлекаемого в качестве специалиста по обстоятельствам производства следственного действия при его участии. Именно в ходе такого допроса допускается фиксация следователем каких-либо выводов вероятностного характера, что недопустимо в ходе следственного осмотра.

Подводя итог, следует отметить, что качественное выполнение рабочего этапа определяет полноту всего следственного действия, его значимости непосредственно для доказывания преступного события и виновности лиц. Соблюдение тактических и процессуальных рекомендаций, объемов информационного исследования и правильности последующего отражения определяет последующую допустимость такого доказательства при решении вопроса о привлечении к уголовной ответственности конкретных лиц и рассмотрении уголовного дела по существу.

## Список литературы

1. Бегичев А.В. Использование протоколов осмотров Интернет-сайтов в судебной практике // Вестник Московского университета МВД России. 2014. № 11. С. 208-212.

2. Верченов Л.Н., Ефременко Д.В., Тищенко В.И. Социальные сети и виртуальные сетевые сообщества. М., 2013. 360 с.

3. Санчат Ч.А. К вопросу о допустимости в качестве доказательств компьютерной информации, размещенной в сети интернет // Новая наука: от идеи к результату. 2017. № 3. С. 187-189.

4. Сидорова К.С. Способы установления IP-адреса и сведений о нем при расследовании уголовных дел // Вестник Сибирского института бизнеса и информационных технологий. 2018. № 2. С. 88-92.

5. Федотов Н.В. Форензика — компьютерная криминалистика. М., 2007. 432 с.

***В.С. Горшкова,*** *адъюнкт Барнаульского юридического института МВД России, г. Барнаул*

# К ВОПРОСУ О КЛАССИФИКАЦИИ СУДЕБНЫХ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ

Бурное развитие техники (в том числе робототехники) и информационных технологий привело к формированию «цифрового общества», в котором новые технические устройства, приборы, оборудование, средства связи активно внедряются в каждодневную жизнь граждан, деятельность государственных и негосударственных органов, различных структур. В некоторых случаях они становятся предметом либо средством совершения преступлений («киберпреступления», «преступления в сфере информационно-телекоммуникационных технологий», «компьютерные преступления»). Важное значение при выявлении, предупреждении, раскрытии и расследовании указанных противоправных посягательств правоохранительными органами имеет производство судебных компьютерно-технических экспертиз (далее — СКТЭ). СКТЭ представляет собой проводимое в установленном нормативными правовыми актами порядке процессуальное действие, осуществляемое экспертом, обладающим соответствующими специальными познаниями в области техники и иных смежных областях (электроники, информационных систем и процессов, связи и т.п.), в целях установления закономерностей образования, обработки (сбор, запись, ввод, вывод, обмен, преобразование, модификация, блокирование, хранение, копирование, уничтожение) и сокрытия цифровых следов совершения противоправных посягательств с использованием компьютерных средств и устройств. Как самостоятельное направление проведения экспертных исследований в Российской Федерации окончательно сформировалась в 2000-х гг., и большинством представителей научного сообщества относится к классу инженерно-технических экспертиз. Разработка научного и методического обеспечения производства СКТЭ в указанный период проходили, главным образом, на страницах научных трудов Е.Р. Россинской, А.И. Усова. Большой вклад в развитие представлений

об объекте, предмете, методе, методике указанного направления экспертных исследований, закономерностей формирования следовой картины «компьютерных» преступлений также внесли ученые: В.Б. Вехов (электронная криминалистика), Е.И. Галяшина (судебная экспертология), А.И. Семикаленова (цифровые следы, СКТЭ), Н.Н. Федотов (компьютерная криминалистика), Р.Р. Хаснутдинов (роль СКТЭ в раскрытии преступлений) и другие. Одними из первых Е.Р. Россинская и А.И. Усов классифицировали СКТЭ на основе компонентов компьютерного средства на следующие виды: аппаратно-компьютерная, программно-компьютерная, информационно-компьютерная, компьютерно-сетевая [1].

В связи разнообразием «цифровых» объектов А.И. Семикаленова подчеркивает, что помимо указанных Е.Р. Россинской и А.И. Усовым видов СКТЭ дополнительно возможно выделить следующие самостоятельные направления экспертных исследований [2, с. 257-260]:

1) экспертиза нетипичных компьютерных средств, объектами которой выступают модели бытовой техники с функциональными возможностями компьютера (телевизоры, фоторамки и т.д.). В ходе производства экспертных исследований определяются работоспособность, информационное содержание, возможности микропроцессорного устройства;

2) экспертиза средств сотовой связи, объектами которой являются мобильные телефоны, планшеты, смартфоны, коммуникаторы, айфоны (сим-карты, чипы, микросхемы, USB-накопители, флэш-карты, карты памяти и т.п.). В ходе производства экспертных исследований устанавливаются факты и обстоятельства, возникшие в ходе изготовления, эксплуатации, ремонта средств сотовой связи, дополнительных носителей данных.

Кроме того, в рамках существующих видов СКТЭ начинают формироваться новые подвиды, которые приобретают актуальность и, представляется, в ближайшее время могут стать автономными — например, экспертиза подлинности электронно-цифровой подписи и электронных документов [3, с. 19].

Стоит согласиться с мнением А.Р. Смолиной о том, что объекты СКТЭ достаточно разнообразны (компьютерные устройства, средства сотовой связи, компьютерные программы и т.д.), поэтому она производится «путем комплекс-

ного исследования компьютерных средств: технической (аппаратной) части компьютерных средств; программного обеспечения; объектов сетевых информационных технологий; информации, содержащейся в компьютерной системе» [4, с. 19]. На наш взгляд, в постановлении о назначении судебной экспертизы целесообразно указывать род и конкретный вид — например, «комплексная (программно-компьютерная, информационно-компьютерная) СКТЭ». Кроме того, В.В. Поляков и А.В. Шебалин справедливо указывают на то, что «при составлении постановления о назначении компьютерно-технической экспертизы следователи в названии этого документа обычно не указывают вид назначаемой компьютерно-технической экспертизы, ограничиваясь родовым названием, о виде экспертизы можно получить представление из анализа вопросов, ставящихся перед экспертом и предоставляемых в распоряжение эксперта материалов» [5, с. 83]. В данном случае должностное лицо органов предварительного расследования не в полной мере использует возможности института судебной экспертизы, не ставит перед экспертом вопросы, ответы на которые позволят сформировать доказательственную базу противоправного посягательства, выявить и устранить способствующие совершению преступления причины и условия.

Производство СКТЭ осуществляют государственные (ЭКЦ МВД РФ, Минюст РФ, ФСБ РФ) и негосударственные экспертные учреждения (например, некоммерческое партнерство «Палата судебных экспертов Сибири», ООО «Независимая экспертная лаборатория»). Стоит отметить, что экспертно-криминалистические подразделения полиции в соответствии с требованиями ведомственного нормативно-правового акта осуществляют «Компьютерную экспертизу (исследование компьютерной информации)» [6]. В свою очередь, В.И. Шаров утверждает, что СКТЭ не относится к классу инженерно-технических экспертиз, а формирует самостоятельный класс экспертиз, где базовыми являются знания из области информатики [7, с. 168]. По мнению ученого, формулировка «Компьютерная экспертиза» должна справедливо применяться к СКТЭ. На наш взгляд, такой вариант обозначения класса судебных экспертиз

возможен, но при этом в обязательном порядке необходимо выделять ее отдельные виды и указывать данную информацию в постановлении о назначении судебной экспертизы. Производство традиционных (аппаратно-компьютерная, программно-компьютерная, информационно-компьютерная, компьютерно-сетевая) и нетрадиционных (экспертиза нетипичных компьютерных средств, средств сотовой связи и иных объектов, которые только начинают практически использоваться) видов СКТЭ должно осуществляться в рамках узкой специализацией не только в ряде государственных, негосударственных и иных экспертных учреждениях (например, в экспертных подразделениях Следственного комитета РФ проводят компьютерно-техническую экспертизу цифровой информации и компьютерных средств, а также информационно-аналитическую экспертизу цифровых массивов данных), но, прежде всего, в экспертно-криминалистических подразделениях полиции, которые непосредственно участвуют в борьбе с преступностью. Заключение эксперта и заключение специалиста по результатам производства СКТЭ является одним из доказательств по уголовному делу, что подтверждает необходимость решения указанных проблем.

Таким образом, в рамках разрешения сложившейся ситуации необходимо четко разграничить СКТЭ на виды — традиционные (аппаратно-компьютерная, программно-компьютерная, информационно-компьютерная, компьютерно-сетевая) и нетрадиционные (экспертиза нетипичных компьютерных средств, средств сотовой связи, экспертиза электронных документов и т.д.); разработать общую для всех экспертных подразделений методику производства СКТЭ; сформировать единообразную методическую базу подготовки и повышения квалификации экспертов по вышеуказанным направлениям в специализированных учебных заведениях системы МВД России, а также иных образовательных организациях. Важно отметить, что в постановлении о назначении судебной экспертизы необходимо указывать род и вид проводимого экспертного исследования, а в некоторых случаях обозначать комплексный характер применения специальных познаний экспертом — «комплексная (программно-компьютерная, информационно-компьютерная) СКТЭ».

## Список литературы

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

2. Судебная экспертология: история и современность (научная школа, экспертная практика, компетентностный подход) / под ред. Е.Р. Россинской, Е.И. Галяшиной. М.: Проспект, 2020. 272 с.

3. Фанина М.Н., Хаснутдинов Р.Р. Компьютерно-техническая экспертиза при электронном заключении сделок // International Journal of Humanities and Natural Sciences. 2020. Vol. 12-2 (51). С. 100-102.

4. Смолина А.Р. Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы: дисс. ... канд. техн. наук: 05.13.19. Томск, 2017. 132 с.

5. Поляков В.В., Шебалин А.В. К вопросу о назначении компьютерно-технической экспертизы, объектом которой является смартфон, по преступлениям в сфере компьютерной информации // Сборник материалов криминалистических чтений. 2013. № 9. С. 83-86.

6. Приказ МВД России от 29.06.2005 № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации». [Электронный ресурс.] URL: http://www.consultant.ru/document/cons_doc_LAW_55315/.

7. Шаров В.И. Об основаниях классификации судебных экспертиз // Вестник Нижегородского университета им. Н.И. Лобачевского. 2018. № 4. С. 166-170.

***А.В. Гришин,*** *к.ю.н., начальник кафедры уголовного процесса Орловского юридического института МВД России имени В.В. Лукьянова, г. Орел*
***А.В. Ломовская,*** *курсант факультета подготовки следователей Орловского юридического института МВД России имени В.В. Лукьянова, г. Орел*

# РОЛЬ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫЯВЛЕНИИ И РАСКРЫТИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В настоящее время развитие общественных отношений связано с экономической сферой, которая базируется на информационных ресурсах. Нельзя не упомянуть о том, что вообще все виды деятельности в мировом обществе базируются именно на компьютерных технологиях. Это связано с тем, что сейчас прослеживается период цифровизации общества. Так, в соответствии с приведенной Международным союзом электросвязи статистикой, Всемирной сетью Интернет пользуется более 4,5 млрд человек. Несмотря на то, что процесс цифровизации с каждым годом прогрессирует, нельзя не отметить тот факт, что появляются преступления в сфере компьютерной информации.

В связи с развитием информационных и компьютерных технологий стало проще совершать различного рода преступления. Именно поэтому в Уголовном кодексе Российской Федерации была закреплена глава, посвященная преступлениям в сфере компьютерной информации. Стоит отметить, что в законодательстве, регулирующем рассматриваемые общественные отношения, имеются определенные пробелы. Так, в гл. 28 УК РФ отсутствует ответственность за преступления, совершаемые в сфере телекоммуникаций, а также на законодательном уровне не находят свое отражение понятия преступлений, совершаемых использованием высоких технологий.

Обращаясь к статистическим данным Генеральной прокуратуры, необходимо сказать о том, что статистика преступлений демонстрирует печальную динамику, а именно за прошедший 2019 г. число преступлений в сфере IT выросло почти на 50% по сравнению с предыдущим. Так, за первое полугодие

2019-го из 1 млн преступлений 117 640 совершили с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что составило в процентном соотношении 46,8% от общего количества зарегистрированных преступлений.

Согласно статистическим сведениям ФКУ «ГИАЦ МВД России» в 2020 г. на территории Российской Федерации зарегистрирован 62 871 факт мошенничества, совершенного с использованием средств мобильной связи (прирост преступлений по сравнению с аналогичными показателями прошлого года составил 47,2%), с использованием сети Интернет — 73 692 (30,8%).

Такая тенденция свидетельствует о необходимости оперативного и комплексного использования всех имеющихся информационных и технических ресурсов органов внутренних дел Российской Федерации для предупреждения, пресечения и раскрытия преступлений в данной сфере, совершенствование методов их документирования, а также процесса доказывания по уголовным делам.

Для наибольшей наглядности при проведении исследования по данному вопросу будет актуальным также обращение к статистическим показателям Судебного департамента при Верховном Суде РФ, которые отражают реализацию применения уголовной ответственности за совершение преступных деяний в сфере информационных технологий. На первое полугодие 2020 г. за данные преступления был осужден 61 человек, приговоры в отношении которых вступили в силу. Тем не менее данные цифры отразили лишь преступления, предусмотренные ст. 272-274.1 УК, не затронув увеличивающееся число мошеннических действий в сфере компьютерной информации (ст. 159.6 УК) или с использованием электронных средств платежа (ст. 159.3 УК).

Стоит отметить тот факт, что случаи выявления лиц, совершивших преступления, предусмотренные гл. 28 УК РФ, уменьшаются, что свидетельствует о сложностях в раскрытии и расследовании данных преступлений [1, с. 241]. Наиболее наглядно указанный факт представлен в статистике преступлений, предусмотренных ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» (число выявленных лиц снизилось с 3973 до 290 человек).

Согласно результатам проведенного исследования ВНИИ МВД России за текущий год, к сожалению, прогнозируется дальнейший рост киберпреступлений [2, с. 49]. Это обусловлено тем, что действующее уголовное законодательство содержит несовершенную нормативно-правовую базу для охраны общественных отношений, складывающихся в сфере компьютерных технологий. Стоит указать на отсутствие разъяснений Верховным судом РФ вопросов оценки преступлений, предусмотренных гл. 28 УК РФ, что свидетельствует о сохранении условий для дальнейшей криминализации виртуального пространства. Таким образом, указанные данные позволяют говорить о высокой степени латентности, а также о низкой раскрываемости. В связи с этим злоумышленники пользуются данной проблемой, что открывает перед ними широкое поле деятельности с целью получения прибыли с минимальной возможностью быть задержанными.

Стоить отметить, что без тактических приемов оперативно-розыскной деятельности, а также проведения оперативно-розыскных мероприятий невозможно представить выявление и раскрытие преступлений в рассматриваемой сфере [3].

По нашему мнению, на латентность преступлений в сфере компьютерной информации влияет отсутствие материальных следов, как на этапе подготовки к совершению преступления, так и во время его совершения. Также на латентность может влиять и то, что не всегда представляется возможным определить точное время и место совершения преступления, так как, например, вредоносное программное обеспечение может быть создано в одном месте, а реализовано в другом.

Стоит отметить, что при выявлении, раскрытии и расследовании преступлений правоохранительные органы сталкиваются с проблемой, связанной с несовершенствами законодательной базы в рассматриваемой области, а также с латентностью данного вида преступлений.

Основываясь на результатах оперативно-розыскной и следственной деятельности, можно сделать вывод о том, что при раскрытии и расследовании преступлений в сфере компьютерной информации важно уделять внимание не только техническим средствам, с помощью которых совершалось преступ-

ление, но и непосредственно на канал связи. Канал связи включает в себя информацию, касающуюся отправленных сообщений, протоколов соединений, а также любые другие сведения, находящиеся в LOG-файлах. При получении той или иной информации, в первую очередь, необходимо обращать внимание на имя отправителя, его дату рождения, номер телефона, адрес проживания, электронном почты, IP-адрес и др. Указанные сведения возможно получить в рамках проведения оперативно-розыскных мероприятий, санкционируемых решением суда. Особое внимание хотелось бы уделить Cookie-файлам.

Множество интернет-сайтов хранят информацию своих пользователях, сбор и анализ которых происходит посредством Cookie-файлов.

Cookie-файл — это фрагмент данных, который интернет-сайт передает в интернет-браузер своего нового пользователя, чтобы идентифицировать его. При следующих посещениях данного сайта информация о подключившемся пользователе будет увеличиваться:

– сайт запоминает логин и пароли пользователя — именно благодаря Cookie-файлам не нужно каждый раз заново вводить пароли в социальных сетях и других сайтах;

– сайт запоминает предпочитаемый язык;

– сайт запоминает последние просматриваемые пользователем страницы;

– сайт запоминает историю посещений пользователя (данная функция Cookie имеет для органов предварительного следствия и органов дознания ключевое значение).

Важной особенностью Cookie-файлов является их неизменность — мошенник сколько угодно раз может менять свой IP-адрес через VPN, проходить регистрацию с разных абонентских номеров, но сайт все равно поймет, что все это время к нему подключается один и тот же пользователь, то есть используются браузер одного и того же персонального компьютера.

Стоит отметить, что в ФЗ «Об оперативно-розыскной деятельности», а именно в ст. 6 были внесены изменения — добавлен новый вид оперативно-розыскных мероприятий «Получение компьютерной информации». На сегодняшний день на законодательном уровне нет четкого определения, как именно

необходимо проводить данный вид оперативно-розыскных мероприятий, в связи с этим необходимо в кратчайшие сроки установить и закрепить порядок его проведения. Стоит указать на то, что от правильного и своевременного использования возможностей, имеющихся у правоохранительных органов, при предупреждении преступлений в сфере компьютерной информации зависит благосостояние нашей страны в финансовой и экономической сфере.

Таким образом, своевременная разработка мер, направленная на предупреждение преступлений в сфере компьютерной информации и высоких технологий, позволит повысить уровень, как информационной безопасности страны, так и противодействия данным видам преступлений.

**Список литературы**

1. Доровских Л.А. Преступления в сфере высоких технологий // Киберпреступность. 2016. № 4 (28). С. 240-243.

2. Антонян Ю.М., Бражников Д.А. Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития: аналитический обзор. М.: ФГКУ «ВНИИ МВД России», 2018. 86 с.

3. Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 30.12.2020) «Об оперативно-розыскной деятельности» // СЗ РФ. 1995. № 33. Ст. 3349.

***О.С. Давыдова,*** *Главное управление МВД России по Алтайскому краю, г. Барнаул*

## ОБ ИСПОЛЬЗОВАНИИ ОПЕРАТИВНО-РОЗЫСКНЫМИ ПОДРАЗДЕЛЕНИЯМИ РЕЗУЛЬТАТОВ ЭКСПЕРТНО-ДИАГНОСТИЧЕСКИХ ИССЛЕДОВАНИЙ СВОЙСТВ ЛИЧНОСТИ НЕУСТАНОВЛЕННЫХ КИБЕРПРЕСТУПНИКОВ ПО ИХ ПИСЬМЕННЫМ РЕЧЕВЫМ СЛЕДАМ

Как свидетельствуют статистические данные, в январе-июне 2021 г. зарегистрировано 271,1 тыс. киберпреступлений (преступлений, совершенных с ис-

пользованием информационно-телекоммуникационных технологий или в сфере компьютерной информации), что на 20,3% больше, чем за аналогичный период прошлого года. Отмечается тенденция увеличения их удельного веса в общем числе зарегистрированных преступлений — с 22,3% в первом полугодии 2020 г. до 26,5% в 2021 г. Практически все киберпреступления (98,2%) выявляются органами внутренних дел. Больше половины таких преступлений (57,1%) относится к категориям тяжких и особо тяжких. Важно отметить, что две трети киберпреступлений (67,4%) совершается с использованием сети «Интернет» (182,7 тыс.), отмечается их рост на 42,1%. Более трети таких преступлений (40,2%) совершены с использованием средств мобильной связи (108,9 тыс., рост на 14,2%). Почти три четверти киберпреступлений (74,7%) — это кражи или мошенничества, каждое девятое преступление (11,1%) связано с незаконным производством, сбытом или пересылкой наркотических средств. Раскрываемость преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, составила по итогам первого полугодия 2021 года 27,9%[6]. Для характеристики современной преступности отметим также, что информационно-телекоммуникационное пространство является основным средством коммуникации для экстремистских и террористических организаций.

К числу проблемных вопросов противодействия киберпреступлениям относится сохраняющаяся возможность у лиц, занимающихся преступной деятельностью, избегать идентификации путем использования различных программных технологий. Как пишет Р.А. Усманов, условия компьютерно-опосредованной коммуникации позволяют преступникам сохранять анонимность в виртуальном пространстве, что порождает сложности при получении исходной поисково-познавательной информации, необходимой для их розыска и последующего отождествления. Исследователями отмечается, что правонарушители, которые выступают в роли поставщиков и потребителей незаконных услуг, все чаще используют различные сервисы, программы (анонимайзеры),

[6] Состояние преступности в России за январь-июнь 2021 года. [Электронный ресурс.] URL: https://мвд.рф/reports/item/25094008/. (дата обращения: 01.08.2021).

позволяющие сохранить в тайне сведения, которые способствовали бы их идентификации [1, с. 134].

В таких условиях приобретает особую актуальность поиск новых и совершенствование имеющихся способов поиска, обнаружения, получения информации о неустановленных лицах, использующих компьютерные сети для совершения преступлений.

Как известно, для установления лиц, совершающих преступления, наиболее эффективным является инструментарий оперативно-розыскной деятельности (далее — ОРД). Федеральный закон «Об оперативно-розыскной деятельности» (далее — Закон об ОРД) предоставляет оперативным подразделениям ряда правоохранительных органов полномочия по проведению оперативно-розыскных мероприятий (далее — ОРМ), в том числе негласно. К таковым ОРМ относятся, к примеру, наведение справок, сбор образцов для сравнительного исследования, исследование предметов и документов, отождествление личности, оперативное внедрение, прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации и другие. ОРМ могут проводиться только при наличии оснований и условий, предусмотренных соответственно ст. 7 и 8 Закона об ОРД. Посредством проведения ОРМ обеспечивается достаточно эффективное решение задач раскрытия преступлений и установления лиц, их совершивших. Тем не менее половина преступлений остается нераскрытой, а по киберпреступлениям — почти три четвертых.

Можно выделить комплекс причин низкой раскрываемости преступлений организационного, тактического, правового характера. Мы же остановимся на одном из перспективных, с нашей точки зрения, направлений совершенствования деятельности, связанной с установлением лиц, совершивших киберпреступления. Полагаем, что при решении этой задачи оперативно-розыскные органы недостаточно используют потенциал экспертно-диагностических исследований. В частности, возможность получение данных о демографических характеристиках личности киберпреступников посредством экспертно-диагностических исследований его письменных речевых следов.

При формировании частных оперативно-розыскных методик раскрытия преступлений, как правило, вне поля зрения разработчиков остаются вопросы использования специальных знаний для получения информации о свойствах личности и признаках внешности предполагаемого преступника. Между тем при организации и проведении ОРМ, как отмечено в ст. 6 Закона об ОРД, оперативные сотрудники могут использовать помощь должностных лиц и специалистов, обладающих научными, техническими и иными специальными знаниями.

Обращаясь к проблеме диагностирования свойств личности неустановленного преступника, надо отметить, что в этой области проведен ряд исследований, которые имеют не только теоретическое, но и практическое значение, в том числе для оперативно-розыскных подразделений. Так, в 2005 г. С.В. Дубровиным была защищена докторская диссертация «Основы теории криминалистической диагностики» [2]. К фундаментальным работам, безусловно, относится и докторская диссертация О.А. Соколовой «Криминалистическая диагностика человека по его следам и отображениям», где имеющиеся знания систематизированы и представлены в виде самостоятельной частной теории — криминалистической диагностики человека по его следам и отображениям. В диссертации сформулировано авторское понятие «свойств» человека, подлежащих диагностированию, под которым автор понимает «объективные, внутренние качественные и количественные отличительные особенности человека, выражающие такие его стороны, которые обусловливают их различие или общность с аналогичными свойствами других людей и обнаруживаются в его отношении к ним независимо от сознания, и проявляющиеся в признаках [3, с. 52].

Как правило, в литературе выделяются три группы свойств человека, которые имеют значение в деятельности по установлению лица, совершившего преступление, составлению его комплексного портрета. К таковым относят, во-первых, биологические свойства личности: анатомические особенности (рост, телосложение, черты лица и т.д.), функциональные особенности (походка, осанка, мимика, жестикуляция и т.п.), генетические особенности (состав крови, слюны, пота, спермы, тканей тела, потожировые вещества, образующие запах). Во-вторых, психолого-психиатрические свойства личности: темперамент, ха-

рактер, одаренности и способности, направленность (интересы и склонности), психические аномалии и др. В-третьих, социально-демографические характеристики личности: пол, возраст, семейное положение, образование, профессиональная принадлежность, род занятий; социальное, материальное положение; наличие судимости и др. [4, с. 12-13].

Если же говорить о возможностях судебной автороведческой экспертизы по установлению оперативно значимых демографических характеристик киберпреступника по его письменным речевым следам, то здесь необходимо обратиться к исследованию Т.А. Саакова [5, с. 16]. По его мнению, в группу демографических характеристик автора речевого продукта входят: пол; возрастная группа; этническая принадлежность; территориальная принадлежность; уровень образования и речевой культуры; род занятий (хобби); профессиональная принадлежность; социальный статус. Автор приходит к выводу, что результаты экспертно-диагностического исследования позволяют на основе выявленных речемыслительных навыков индивида, отображенных в письменном речевом следе, сконструировать речевой портрет, в котором отражаются демографические характеристики автора (пол, возраст, этническая, территориальная, профессиональная принадлежность и др.). Интересны данные, приведенные автором диссертации, — около 82% правоприменителей недостаточно осведомлены о потенциальных возможностях автороведческой экспертизы по установлению демографических характеристик автора по признакам письменной речи.

Оперативным сотрудникам важно знать, что в процессе экспертно-диагностического исследования возможно получение ориентирующей информации об указанных характеристиках. Такая информация будет иметь значение для выдвижения версий о неустановленном киберпреступнике для его розыска. Вот некоторые составы преступлений, по которым может возникнуть потребность в экспертно-диагностическом исследовании свойств личности киберпреступника по его речевым следам — преступления террористического характера или экстремистской направленности, предусмотренные ст. 205.2 УК РФ, ст. 280 УК РФ, ст. 280.1 УК РФ, ст. 282 УК РФ (как правило, лица используют вымышленное имя пользователя в социальных сетях); ст. 110.2 УК РФ (организация дея-

тельности, направленной на побуждение к совершению самоубийства), если такая деятельность осуществлялась при помощи использования сети «Интернет»; преступления, связанные с незаконным оборотом наркотических средств, совершаемые с использованием сети «Интернет».

О необходимости развития рассматриваемого направления деятельности оперативно-розыскных подразделений по поиску, получению информации о лицах, совершающих киберпреступления, свидетельствует и внимание к этим проблемам со стороны МВД РФ. Так, решением коллегии МВД РФ от 1 ноября 2019 г. было предложено реализовать комплекс мер по разработке методического и аппаратно-технического инструментария экспертного исследования письменных, голосовых сообщений, статических и динамических изображений, передаваемых и синтезируемых с применением технологий искусственного интеллекта [6].

**Список литературы**

1. Усманов Р.А. Характеристика преступной деятельности, осуществляемой в сети Интернет посредством сервисов-анонимайзеров // Юридическая наука и правоохранительная практика. 2018. № 4 (46). С. 134-141.

2. Дубровин С.В. Основы теории криминалистической диагностики: автореф. дисс. … д-ра юрид. наук. М., 2005. 51 с.

3. Соколова О.А. Криминалистическая диагностика человека по его следам и отображениям: дисс. … д-ра юрид. наук. М., 2018. 650 с.

4. Милюков С.В. Современные возможности использования свойств человека при установлении личности в раскрытии и расследовании преступлений: автореф. дисс. … канд. юрид. наук. М., 2011. 23 с.

5. Сааков Т.А. Судебно-диагностическое исследование демографических характеристик автора по признакам письменной речи: дисс. … канд. юрид. наук. М., 2020. 277 с.

6. Решение коллегии МВД России от 1 ноября 2019 года « О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-

телекоммуникационных технологий. Объявлено приказом МВД России от 25 ноября 2019 г. № 878 // Справочная правовая система «Консультант-Плюс». [Электронный ресурс]. URL: http: www. consultant.ru.

***Davydova V.O.,*** *student of the Law Institute of Altai State University, Barnaul*
***Usvyat N.D.,*** *Ph.D, Associate Professor of the Department of Foreign Languages of Economic and Legal Profiles, Altai State University, Barnaul*
***Yakusheva T.V.,*** *PhD, Associate Professor of the Department of Criminal Procedure and Criminalistics, Altai State University, Barnaul*

## WOMEN AS A SUBJECT OF RAPE IN THE CONTEXT OF GLOBALIZATION

Currently, the inevitability of the digital transformation of law enforcement practice has emerged in connection with the outbreak of the COVID-19 pandemic. As well as for most states, the issue of online justice and the definition of the framework for its use have become urgent for Russia. According to L.V. Golovko, digitalization in the criminal process is only a local and rather routine optimization of some procedural forms and institutions, which does not carry any risks for traditional criminal justice [8, p. 19].

In the context of the digitalization of justice, the problem of defining a unified approach to recognizing a woman as an accomplice of such a crime as rape remains. Men commit crimes more often than women. At different times, the proportion of women who committed serious crimes did not exceed 20%.

In 2003, the percentage was 11.8%, in 2004 – 13.4%. In 2005-2006, the number of recorded crimes rise sharply, their percentage is 13.9% and 15.3%, respectively. The highest percentage of female crime was in 2007 – 16%. In the next six years, the percentage of female crime decreased in 2008 to 15.5%, in 2009 – 15.4%, in 2010 – 15.3%, in 2011 – 15.4%, in 2012 – 15.4%, in 2013 – 15.7% [4].

This can be explained by differences in the conditions of moral formation of men and women, in their position at home and at work, in the nature of their needs and interests, orientations and attitudes, in the motivation of their behavior and so on. From 2017 to 2021, however, there was a trend of growth in female crime – up to 3% annually, and the number of women who committed serious crimes also increased more than 4 times [7]. When we qualify crimes, a review of the characteristics of a special subject is necessary, as well as a review of the characteristics of the general subject of the crime, because they are the basis of criminal responsibility on an equal with others.

The special subject of the crime expresses the features of specific types of crimes, the degree of their public danger. Only special subjects can cause harm provided for by law, for example, the subject of high treason can not be a foreigner, and the subject of rape can not be a woman, although with rape, everything is not so clear.

According to Article 131 "Rape" of the Criminal Code of the Russian Federation, we will not see the designation of the gender of the subject and referring, for example, to the comment, it will become clear – the subject of criminal assault as an implementer can only be a sane male person, 14 years old.

This interpretation is given due to the fact that rape is understood as sexual intercourse between a man and a woman, in a natural form, against the will of the victim with the use of violence, threats of its use, or with the use of her defenseless state. Woman can also act as an organizer, instigator, accomplice, and implementer of rape [5].

Co-accomplice is interpreted in the Resolution of the Plenum of the Supreme Court of the Russian Federation of December 4, 2014 N 16 "On judicial practice in cases of crimes against sexual inviolability and sexual freedom of the individual", Item 10. The actions of persons who have not personally committed violent sexual intercourse or violent sexual acts, but who have assisted others in committing a crime through the use of violence or threats, should be qualified as co-accomplices in the commission of rape or violent sexual acts [2]. So, if a woman participates in overcoming the resistance of the victim (through the use of physical or mental violence), she should be recognized as a co-accomplice of rape.

This is also confirmed by judicial practice, in particular, by the verdict of the Nizhny Novgorod Regional Court of June 09, 2007. F. was found guilty of committing rape as an accomplice in relation to S. The court concluded that the violent sexual act with the victim was committed by X., and F. actively assisted him by using violence to the victim: she took off S's clothes, then held her, covering her mouth. Therefore, the court correctly qualified her actions as an accomplice in the rape of the victim [3].

There is no doubt about the rules for qualifying the actions of women who are organizers, instigators or accomplices of rape. But in our opinion, there is a need to consider the specifics of bringing a female person to criminal responsibility as an implementer of rape.

Let us look at part 2 of Article 33 "Types of partners of a crime" of the Criminal Code of the Russian Federation. The implementer is a person who has directly committed a crime or who directly participated in its commission together with other persons, as well as a person who has committed a crime through the use of other persons who are not subject to criminal responsibility due to age, insanity or other circumstances provided for by this Code [1]. This raises an interesting question – does the criminal law exclude the possibility of recognizing a woman as the only implementer of rape in a situation where she commits a crime by using a person who has not reached the age of criminal responsibility, or a mentally ill man who is not legally considered the subject of the crime? This topic is still controversial – for example, from the interpretation of Part 2 of Article 33 of the Criminal Code of the Russian Federation, we can conclude that in fact the law allows responsibility for the rape of a woman not only as a co-accomplice, but also as an implementer, therefore, the act provided for in Article 131 of the Criminal Code of the Russian Federation is incorrectly considered as a crime with a special subject.

But the legal meaning of the special subject establishes limits on the circle of persons who can commit a specific crime. Ragulina A.V. noted: "A special subject is a person who, in addition to the three necessary signs (an individual, sanity and age), also has additional characteristics that are the main ones for a particular crime." [6, p. 85].

In our opinion, here we must proceed from a direct interpretation of the criminal law, which allows for the recognition of a woman as the only implementer of rape in the case of its commission by persons given in part 2 of Article 33 of the Criminal Code of the Russian Federation.

Based on the literal interpretation of Part 4 of Article 34 of the Criminal Code, the actions of a woman as a co-accomplice should be qualified as the actions of an organizer, instigator or accomplice. But neither the role actually performed by a woman, nor the judicial interpretation given by the Supreme Court, completely blend into the provision given in Part 4 of Article 34 of the Criminal Code, and her actions do not fall under the legislative description of either the organizer, instigator, or accomplice.

That is why, when qualifying such actions, it is impossible to refer to any of the three parts (3-5) of Article 33 of the Criminal Code. Thus, there is a barrier to the qualification of the actions of persons who do not have the attribute of a special subject, but who took a direct part in its commission.

It is possible to offer the following way out of this situation:

- addition of the fourth part of Article 34 of the Criminal Code with the following sentence:

"A person who does not have the attribute of a special subject, but who directly participated in the commission of a crime with a special subject, may be criminally responsible as a co-accomplice."

## References

1. "The Criminal Code of the Russian Federation" dated 13.06.1996 N 63-FZ (as amended on 24.02.2021): website. URL http://www.consultant.ru/document/cons_doc_LAW_10699/ (date of access: 03/26/2021). Text: electronic.

2. Resolution of the Plenum of the Supreme Court of the Russian Federation of December 4, 2014 N 16 "On judicial practice in cases of crimes against sexual inviolability and sexual freedom of the individual": website. URL http://www.consultant.ru/document/cons_doc_LAW_171782/ (date of access: 03/26/2021). Text: electronic.

3. Supreme Court of the Russian Federation Judicial College on Criminal Cases Definition of September 4, 2007 N 9-O07-61 The convict was reasonably recognized as a co-perpetrator in the commission of rape by a group of persons (Extract): website. - URL http://sudrf.kodeks.ru/rospravo/document/902101819 (date of access: 03/26/2021). Text: electronic.

4. The state of crime in Russia in January - December 2003-2016. M.: Main information and analytical center of the Ministry of Internal Affairs of Russia, 2004-2017. S. 31, 34.

5. Commentary on Article 131 of the Criminal Code of the Russian Federation: website. URL http://ukodeksrf.ru/ch-2/rzd-7/gl-18/st-131-uk-rf (date of access: 03/26/2021). Text: electronic.

6. Criminal law. General part: Textbook. Revised and enlarged edition / Ed. Doctor of Law, Professor L.V. Inogamova-Khegai, Doctor of Law, Professor A.I. Rarog, Doctor of Law, Professor A.I. Chuchaev. M.: Legal firm "Contract": INFRA-M, 2005. P. 221.

7. Selezneva, I. G. Gender analysis of crime (regional aspect): monograph / I.G. Selezneva, A. S. Sukhova; VolgSTU. Volgograd, 2019. 68 p.

8. Golovko L.V. Digitalization in Criminal Procedure: Local Optimization or Global Revolution? // Bulletin of economic security. 2019. No. 1. S. 15-25.

***Ю.В. Денисенко,*** *начальник отдела ГУПЭ МВД России, г. Москва*

## О ПРАВОВОМ РЕГУЛИРОВАНИИ ПРОТИВОДЕЙСТВИЯ ПРОЯВЛЕНИЯМ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В СЕТИ «ИНТЕРНЕТ»: РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ

Анализ проблематики противодействия преступлениям экстремистской направленности, совершаемых с использованием информационно-телеком-

муникационных технологий[7] показал, что текущее состояние криминогенной ситуации в данной области характеризуется сформировавшейся устойчивой тенденцией роста рассматриваемых противоправных деяний. Согласно статистическим данным, в 2020 г. более половины (56,8%) преступлений экстремистской направленности совершено с использованием сети «Интернет» — 473 (+52,6%).

Современные технологии привели к активному использованию в противоправных целях международными террористическими организациями и членами бандформирований на территории Российской Федерации иностранных интернет-сервисов, предназначенных для обмена текстовыми, голосовыми и иными сообщениями. Стратегия противодействия экстремизму в Российской Федерации до 2025 г. [9] определяет информационно-телекоммуникационные сети, включая сеть «Интернет», как основное средство связи для экстремистских организаций, которое используется ими для привлечения в свои ряды новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии.

Указанные обстоятельства автоматически относят проявления экстремизма[8] в сети «Интернет» к числу основных источников угроз современной России [9]. В связи с этим за последние годы существенным дополнениям и изменениям подверглись нормы Федерального закона «Об информации, информационных технологиях и о защите информации» [1], в котором определены правовое положение организатора распространения информации в сети «Интернет» (далее — ОРИ), а также полномочия Роскомнадзора.

---

[7] В основном эти деяния представлены размещением в соцсетях и мессенджерах информационных материалов и комментариев, содержащих призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ), совершению преступлений, предусмотренных ст. 282, 282,1, 282,2 УК РФ, по мотивам расовой, национальной или религиозной ненависти или вражды, а также по мотивам политической ненависти или вражды в отношении социальной группы, выделенной по принадлежности к органам государственной власти.

[8] Проявления экстремизма (экстремистские проявления) — общественно опасные противоправные действия, совершаемые по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, способствующие возникновению или обострению межнациональных (межэтнических), межконфессиональных и региональных конфликтов, а также угрожающие конституционному строю Российской Федерации, нарушению единства и территориальной целостности Российской Федерации.

Во-первых, расширен перечень информации, распространение которой влечет ограничение к ней доступа в информационно-телекоммуникационных сетях, в том числе в сети «Интернет» [2] (информационные материалы иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации [3], сведения, позволяющие получить доступ к указанным информации и материалам (далее — распространяемая с нарушением закона информация).

Во-вторых, введен запрет для владельцев информационно-телекоммуникационных сетей, информационных ресурсов (сайт в сети «Интернет» и (или) страница сайта в сети «Интернет», информационная система, программа для электронных вычислительных машин), посредством которых обеспечивается доступ к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации, на предоставление возможности использования таких анонимайзеров для получения доступа к информационным ресурсам, доступ к которым ограничен в соответствии с федеральным законодательством [4].

В-третьих, возложены [5] дополнительные обязанности на ОРИ[9]:

– осуществлять идентификацию пользователей сервиса обмена мгновенными сообщениями по абонентскому номеру оператора подвижной радиотелефонной связи;

– в течение суток с момента получения требования уполномоченного федерального органа исполнительной власти (Роскомнадзор, ФСБ России или МВД России) ограничить возможность передачи электронных сообщений, содержащих информацию, распространение которой в Российской Федерации запрещено, а также информацию, распространяемую с нарушением закона;

[9] В случае осуществления деятельности по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены для обмена электронными сообщениями исключительно между пользователями этих информационных систем и (или) программ для электронных вычислительных машин, при котором отправитель электронного сообщения определяет получателя или получателей электронного сообщения, не предусматриваются размещение пользователями сети «Интернет» и передача электронных сообщений неопределенному кругу лиц (далее — организатор сервиса обмена мгновенными сообщениями).

– обеспечивать техническую возможность отказа пользователей сервиса обмена мгновенными сообщениями от получения электронных сообщений от других пользователей;

– не допускать передачу электронных сообщений пользователям сервиса обмена мгновенными сообщениями в случаях и в порядке, которые определены Правительством Российской Федерации.

При этом организатор сервиса обмена мгновенными сообщениями, являющийся российским юридическим лицом или гражданином Российской Федерации, вправе осуществлять идентификацию пользователей сервиса обмена мгновенными сообщениями самостоятельно путем определения его абонентского номера подвижной радиотелефонной связи, а также обязан хранить такие идентификационные сведения об абонентском номере только на территории Российской Федерации.

В-четвертых, в целях пресечения распространения идентификационных модулей (SIM-карт) без заключения договоров, а также оказания услуг связи анонимным абонентам (пользователям), вступили в силу нормы [6], которые позволяют приостанавливать оказание услуг связи в случае не подтверждения достоверности сведений об абоненте, сведений о пользователях услугами связи абонента-юридического лица либо индивидуального предпринимателя, представленных лицом, действующим от имени оператора связи.

В связи с возникающими в правоприменительной практике вопросами Пленум Верховного Суда Российской Федерации постановлением от 20 сентября 2018 г. № 32 [8], внес изменения в свое постановление от 28 июня 2011 г. № 11 [7], в котором разъяснил, в частности, что размещение лицом в сети «Интернет» на своей странице или на страницах других пользователей материала (например, видео, аудио, графического или текстового), созданного им самим или другим лицом, включая информацию, ранее признанную судом экстремистским материалом, может быть квалифицированно по ст. 282 УК РФ только в случаях, когда установлено, что лицо, разместившее такой материал, осознавало направленность деяния на нарушение основ конституционного строя,

а также имело цель возбудить ненависть или вражду либо унизить достоинство человека или группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии либо принадлежности к какой-либо социальной группе. При решении вопроса о наличии или отсутствии у лица прямого умысла и цели возбуждения ненависти либо вражды, а равно унижения человеческого достоинства при размещении материалов в сети «Интернет» суду следует исходить из совокупности всех обстоятельств содеянного и учитывать, в частности, форму и содержание размещенной информации, ее контекст, наличие и содержание комментариев данного лица или иного выражения отношения к ней, факт личного создания либо заимствования лицом соответствующих аудио-, видеофайлов, текста или изображения, содержание всей страницы данного лица, сведения о деятельности такого лица до и после размещения информации, в том числе о совершении действий, направленных на увеличение количества просмотров и пользовательской аудитории, данные о его личности (в частности, приверженность радикальной идеологии, участие в экстремистских объединениях, привлечение ранее лица к административной и (или) уголовной ответственности за правонарушения и преступления экстремистской направленности), объем подобной информации, частоту и продолжительность ее размещения, интенсивность обновлений.

Эти и другие принимаемые на законодательном уровне меры позволили правоохранительным органам организовать более эффективную работу по предупреждению экстремистской деятельности, в том числе по выявлению и последующему устранению причин и условий, способствующих размещению экстремистских материалов, на электронных площадках крупнейших российских платформ медиаконтентов. На контроль поставлено более 2 тыс. интернет-ресурсов, в том числе групп в социальных сетях. В 2020 г. по материалам подразделений по противодействию экстремизму МВД России ограничен доступ к более чем 103 тыс. материалам и интернет-ресурсам, удалено более 7600 материалов, признанных судами экстремистскими и запрещенных к распространению на территории Российской Федерации [1, ст. 15.1, 15.3].

Вместе с тем несмотря на имеющиеся положительные результаты оперативно-служебной деятельности, возникает ряд проблемных вопросов выявления и правильной квалификации содеянного, эффективного раскрытия и расследования совершенных деяний:

1. Длительность предоставления ответов на запросы от администраций социальных сетей, вследствие чего срок получения информации составляет порядка 4-6 и более месяцев, в результате чего теряется актуальность и оперативность получаемых данных.

2. Отсутствие действенного механизма блокировки противоправного интернет-контента в связи с его размещением на иностранных площадках и возможностью просмотра с использованием «VPN» и «PROXY» серверов.

3. Отсутствие взаимодействия с зарубежными интернет-компаниями по вопросам противодействия экстремистской и террористической деятельности ввиду отсутствия на международном уровне единых правовых подходов по получению сведений о сетевой активности и пользователях многих иностранных приложений для коммуникации в сети «Интернет».

Таким образом, тенденция увеличения числа зарегистрированных экстремистских проявлений в сети «Интернет» и определенные трудности, с которыми сталкиваются сотрудники органов внутренних дел в процессе их выявления и документирования, обусловили необходимость обращения к зарубежному опыту законодательного регулирования в области противодействия распространению противоправной информации в сети Интернет для выработки соответствующих предложений по дальнейшему совершенствованию деятельности в рассматриваемой области, основываясь на исследованных практиках.

Проведенный анализ зарубежной нормативно-правовой базы свидетельствует с одной стороны, что зарубежная практика достаточно разнообразна в плане подходов к борьбе с противоправным контентом. С другой стороны, механизмы ее реализации универсальны для большинства стран — блокировки, механизмы изъятия контента по требованиям уполномоченных органов,

штрафные санкции и т.д. и в большинстве случаев они уже внедрены или внедряются в Российской Федерации.

В большинстве развитых стран внедрены формализованные механизмы взаимодействия с изготовителями/владельцами или распространителями контента и информационных ресурсов. При этом существует практика учета интересов правоохранительных органов, например, в ФРГ социальные сети должны не только оценивать и принимать решения об ограничении предположительно незаконного контента нескольких типов, но и сообщать о нем в Управление Федеральной уголовной полиции, а также раскрывать персональные данные пользователя, который разместил соответствующий контент. Кроме того, компания-оператор социальной сети не имеет права сообщать пользователю в течение минимум 14 дней о том, что уведомление о размещении им противозаконного контента было направлено в полицию. Наряду с этим существует прозрачная система обжалования решений о признании контента противоправным. Целесообразно следующим шагом провести аудит российских процедур и алгоритмов уведомления и взаимодействия с игроками рынка и по его результатам подготовить предложения по их модернизации при необходимости, в том числе специальных инструментов публичного уведомления — формализовать алгоритмы уведомления изготовителей/владельцев контента и информационных ресурсов, на которых этот контент размещается, о признании контента противоправным, о блокировках и удалении контента и обжаловании решений о признании контента противоправным.

Одновременно предлагается проработать возможные пути взаимодействия с зарубежными государствами в деле противодействия размещению противоправного контента, принимая во внимание глобальный характер его размещения в сети «Интернет» и необходимость координации усилий разных стран на уровне профильных ведомств, курирующих информационно-коммуникационную технологическую отрасль.

Борьба с преступлениями в сети «Интернет», в том числе с противоправной информацией, является прерогативой правоохранительных органов, а международное взаимодействие должно осуществляться по линии Интерпола. При

этом существует ряд направлений, по которым международная работа может вестись другими профильными ведомствами на двусторонней/региональной основе или в рамках международных площадок, таких как ООН (МСЭ, WIPO, КНТР и др.), G20, БРИКС/CyberBRICS, РСС и т.д. Крайне маловероятно подписание глобальных обязывающих правовых документов по данному вопросу в ближайшем будущем, однако это не отменяет практические двухсторонние/региональные инициативы, в числе который можно назвать:

– разработка и принятие единых подходов по категоризации противоправного контента с другими странами,

– обмен опытом и лучшими практиками по борьбе с противоправным контентом;

– разработки механизмов по оперативному обмену информацией об источниках противоправного контента (учитывая трансграничный характер угроз);

– внедрение региональных или взаимоувязка национальных инициатив по борьбе с противоправным контентом;

– взаимодействие с глобальными провайдерами услуг по вопросам реализации в их продуктах/сервисах средств, механизмов предотвращения и борьбы с противоправным контентом, процедур взаимодействия с национальными ведомствами.

Признание информационной продукции противоправной, как уполномоченными ведомствами, так и самими субъектами, вовлеченными в размещение и распространение контента (социальными сетями, платформами хостинга, платформами обмена сообщениями и т.д.), представляет один из самых больших вызовов в интернет-индустрии. Для этих целей создаются экспертные советы, предпринимаются попытки выработки формальных критериев и рекомендаций/требований к операторам связи и провайдерам услуг, разрабатываются алгоритмы действий с указанием последовательности действий и сроков принятие тех или иных мер и т.д. Доступная информация не позволяет однозначно оценить эффективность мер, принятых в той или иной стране, но активная работа по данному направлению ведется в большинстве стран. Целесообразно

следующим шагом в рамках общего тренда на совершенствование системы борьбы с противоправной информацией формализовать порядок действий по признанию информационной продукции противоправной для разных категорий «противоправного контента» и его опасности для общественных интересов.

Также предлагается по аналогии с практикой по взаимодействию с заинтересованными сторонами интернет-рынка в зарубежных странах, создать профильную экспертную площадку интернет-сообщества по противодействию размещению противоправного контента, которая бы объединила регулятора, представителей государственных заинтересованных ведомств, представителей отрасли и представителей гражданского общества.

В Российской Федерации создана развитая система некоммерческих организаций в сфере развития, операционной деятельности и регулирования сети «Интернет»: РОЦИТ, РАЭК, МКС, Лига безопасного Интерната, Общественная палата Российской Федерации, многочисленные совещательные и координационные органы при органах государственной власти. Однако большая их часть не является носителями технической, организационной/операционной и бизнес экспертизы, практические же мероприятия по борьбе с противоправной информацией включают в себя, в том числе, разработку регуляторных норм, реализация которых затрагивает инфраструктуру сети, аспекты безопасности, требует глубокого понимания архитектуры сети, протоколов и современных технологий, а также особенностей их практической реализации на оборудовании российских операторов. Минцифры России применяет механизмы предварительного проактивного обсуждения регуляторных инициатив с игроками рынка. Создание же профильной экспертной площадки (рабочей группы) с вовлечением заинтересованных сторон для рассмотрения практических инициатив будет способствовать систематизации, преемственности и непрерывности работы по подготовке мер по борьбе с противоправной информацией. Включение туда представителей гражданского общества целесообразно с точки зрения многовекторности и придания ей большей легитимности, но ядром такой группы должны являться эксперты отрасли.

Сформулированные предложения по совершенствованию российской нормативно правовой базы могут быть гораздо шире и в чем-то опережать зарубежный опыт. В частности, например, в ходе анализа не было найдено правовых норм, регулирующих прямое противодействие противоправному контенту с использованием технологии deepfake, так как эта технология достаточно нова. В силу этого предложенные рекомендации имеют ряд ограничений.

## Список литературы


1. Федеральный закон от 25 ноября 2017 года № 327-ФЗ «О внесении изменений в статьи 104 и 153 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 6 Закона Российской Федерации «О средствах массовой информации».
2. Федеральный закон от 28 декабря 2012 года № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации».
3. Федеральный закон от 29 июля 2017 года № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 29 июля 2017 года № 241-ФЗ «О внесении изменений в статьи 101 и 154 Федерального закона «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 29 июля 2017 года № 245-ФЗ «О внесении изменений в Федеральный закон «О связи».
6. Федеральный конституционный закон от 5 февраля 2014 года № 3-ФКЗ «О Верховном Суде Российской Федерации».
7. Постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 года № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (в редакции постановления Пленума от 3 ноября 2016 года № 41).
8. Постановление Пленума Верховного Суда Российской Федерации от 20 сентября 2018 года № 32 «О внесении изменений в постановление Пленума

Верховного Суда Российской Федерации от 28 июня 2011 года № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности».

9. Стратегия противодействия экстремизму в Российской Федерации до 2025 года, утверждена Указом Президента Российской Федерации от 29 мая 2020 года № 344.

***П.Е. Долгушина,*** *студентка кафедры «Цифровая криминалистика» Московского государственного технического университета имени Н.Э. Баумана (МГТУ им. Н. Э. Баумана), г. Москва*

***А.В. Караваева,*** *преподаватель кафедры «Цифровая криминалистика» Московского государственного технического университета имени Н.Э. Баумана (МГТУ им. Н. Э. Баумана), г. Москва*

## ОСОБЕННОСТИ И ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ LINUX ДИСТРИБУТИВА CAINE ДЛЯ ПРОВЕДЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ИССЛЕДОВАНИЙ И ЭКСПЕРТИЗ

В связи активно осуществляющимся в настоящее время переходом федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения, а именно с переходом на операционную систему (далее — ОС), основанную на базе ядра Linux, возникает необходимость в изучении, модификации и дальнейшем усовершенствовании методов работы с данной ОС. Рассматриваемая ОС устроена совершенно иным образом в отличие от ОС Windows, что напрямую влияет на возможности эксперта при производстве экспертизы и применение методик судебных компьютерно-технических экспертиз (далее — СКТЭ) с использованием средств ОС на базе ядра Linux. Большинство существующих на сегодняшний день методик СКТЭ организовано под ОС Windows, следовательно, смена ОС

приведет к потребности модернизации старых и создания новых методик. В связи с этим возникает необходимость совершенствования всех имеющихся методик исследования под новое программное обеспечение (далее — ПО), либо усовершенствование уже существующих методик — добавлением экспертного инструментария ОС на базе ядра Linux.

На современном этапе переход на отечественное ПО достаточно активно обсуждается в научной литературе, уровень актуальности данной задачи достигает своего максимума, поскольку ее решение затрагивает различные аспекты внутренней и внешней безопасности Российской Федерации, базирующейся, как и в других современных странах, на информационных технологиях. И хотя крупные иностранные разработчики, такие как Microsoft, предоставляют российским государственным ведомствам доступ к исходным кодам своих программ, сохраняется риск наличия в их скомпилированных версиях недокументированных «закладок». Такие «закладки» являются скрытыми от пользователя и предоставляют злоумышленнику несанкционированный доступ к компьютеру, на котором данная программа используется, и, соответственно, к хранящейся на нем информации [3].

Помимо использовавшегося практически с момента возникновения в нашей стране направления СКТЭ, программного обеспечения иностранных производителей, рядом российских компаний разработаны и постепенно внедряются в экспертную деятельность программные продукты, обладающие аналогичными или даже более широкими возможностями. Однако и те, и другие, как правило, отличаются высокой стоимостью, что нередко заставляет экспертов обращаться к бесплатным аналогам, сочетающим в себе функциональность и доступность, при этом избегая трудностей с лицензионным использованием ПО. Такими продуктами, наряду с некриминалистическими программами, предназначенными для обычных пользователей, были и остаются специализированные Linux-дистрибутивы. Причина их редкого использования и даже упоминания в экспертном сообществе заключается в определенном «барьере», ко-

гда сомнения в возможности освоения незнакомого перевешивают желание достичь положительных результатов.

Это обусловливает необходимость качественного теоретического и практического изучения функционирования Linux-дистрибутивов, предназначенных для использования в целях СКТЭ, которое должно осуществляться с учетом достижений развития информационных технологий, процессуального права, а также регулярного анализа действующего российского законодательства на предмет его соответствия современным реалиям в части использования различного программного обеспечения.

Прежде всего, затронем понятие дистрибутива. Дистрибутив (от англ. distribute — распространять) — форма распространения программного обеспечения [2]. В рассматриваемом случае — это форма распространения операционной системы Linux. Дистрибутив Linux состоит из ядра операционной системы и набора конкретно-определенных программ, настроенных специальным образом под ту или иную профессиональную деятельность. Для удобства речи операционную систему Linux, установленную на компьютере, тоже называют дистрибутивом, чтобы было понятно какая именно разновидность Linux используется.

Таким образом, Linux — ядро ОС, а дистрибутив Linux — установочный пакет какой-либо из разновидностей этой операционной системы в совокупности с дополнительными компонентами [1]. Такие разновидности называют операционными системами на базе Linux.

В отношении дистрибутива CAINE (Computer Aided Investigate Environment) (далее — Caine Linux) можно сказать следующее — дистрибутив Caine является установочным пакетом для развёртывания открытой и свободной операционной системы, состоящей из ядра Linux, утилит GNU, дополнительного специализированного экспертного программного обеспечения и диспетчера пакетов. Дистрибутив также осуществляет установку необходимых обновлений в процессе установки, а развернутая на базе определенного дистрибутива ОС — в дальнейшем.

Предполагаемое использование пакетов-инструментов с открытым исходным кодом может положительно отразиться на процессе СКТЭ, так как наборы инструментов для решения огромного спектра задач предоставляются бесплатно как часть специализированных Linux-дистрибутивов. К сожалению, на данный момент для подобных дистрибутивов не существует универсальной документации, подробно описывающей специализированные встроенные инструменты и задачи, ими решаемые. Поэтому возможности подобного программного обеспечения необходимо раскрывать методом проб и ошибок [5].

Caine Linux включает в себя программные средства, поддерживающие изучение баз данных, памяти, сетевого анализа, а также иные криминалистические инструменты. Дистрибутив содержит множество программных приложений и библиотек, которые можно использовать в графической среде или в среде командной строки для выполнения криминалистических задач. Также существует возможность выполнения анализа объектов данных, созданных в Microsoft Windows, Linux и некоторых других системах UNIX.

Caine Linux предоставляет перечень инструментов, необходимый для выполнения задач СКТЭ. Он укомплектован определёнными блоками экспертного специализированного программного обеспечения, многие из которых будут рассмотрены ниже.

Основными целями создания данного дистрибутива были:

– обеспечение рабочей среды всеми криминалистическими инструментами, необходимыми для осуществления процессов криминалистического расследования, таких как сохранение информации, сбор и анализ данных, экспертиза и др.;

– обеспечение удобным графическим интерфейсом пользователя с полезным для использования судебным экспертом инструментарием;

– возможность загрузки со съемных носителей, например с флеш-накопителя или оптического магнитного диска;

– возможность установки на физическую или виртуальную систему;

– работа с объектами хранения данных в режиме реального времени без обязательной загрузки операционной системы.

Дистрибутив Caine Linux является свободным программным обеспечением с открытым исходным кодом. Поэтому для исследования его возможностей необходимо скачать образ с официального сайта разработчика [4]. Исследование дистрибутива может основано на использовании любого программного средства для виртуализации.

Таким образом, практическая значимость исследования специализированных экспертных дистрибутивов заключается в выявлении и анализе особенностей работы с данным конкретным дистрибутивом. Разработчикам Caine Linux удалось собрать в одном пакете большое количество экспертных инструментов (в том числе и собственной разработки), необходимых при проведении компьютерно-технических исследований и экспертиз, а также напрямую или косвенно позволяющих осуществлять те или иные виды компьютерно-технического анализа. Кроме того, операционная система Caine может быть использована в качестве исследовательского инструмента и теми, кто хочет только начать знакомство с данным направлением более подробно. Следовательно, опираясь на вышесказанное, можно прийти к выводу о том, что для решения основных задач, которые ставятся перед экспертом, нет необходимости самостоятельного поиска, установки и использования дорогостоящего программного обеспечения, а также специализированных программных средств, так как наиболее востребованные инструменты для осуществления деятельности эксперта уже включены в состав Caine. Также необходимо отметить то, что в случае развития данного направления, подобные экспертные программные комплексы, безусловно, смогут стать преимущественно используемой базой для проведения экспертных исследований.

## Список литературы

1. Уорд Б. Внутреннее устройство Linux. СПб.: Питер, 2016. 384 с.

2. Баррет Д. Дж. Linux: основные команды. Карманный справочник / пер. с англ. М.: КУДИЦ-ОБРАЗ, 2007. 288 с.

3. Калюжный К.А. Состояние и перспективы импортозамещения в российской ИТ-отрасли // Управление наукой и наукометрия. 2016. Т. 11, № 2. С. 85-103.

4. CAINE Computer Forensic Linux Live Distro. [Электронный ресурс.] URL: https://www.caine-live.net/. Дата доступа: 01.04.2021.

5. Carranza Aparicio, Ngaide Alassane, Zafar Sunda, Nestor Landaez. Methodology for an Open Digital Forensics Model Based on CAINE // IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing. 2015. 935-940 с.

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

## КРАТКИЙ ОБЗОР IT-ТЕХНОЛОГИЙ, ПРИМЕНЯЕМЫХ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ УБИЙСТВ, СОПРЯЖЕННЫХ С ОГНЕМ

Известный знаток пожарного дела на Руси Бернардацци утверждал, что самым тяжким народным бедствием является пожар [1]. Сегодня, как и в недалеком прошлом, пожарное бедствие становится общенациональной проблемой. Огонь часто используется для совершения и сокрытия других преступлений, в том числе убийств. Начиная с 2009 г. в Российской Федерации только официально зарегистрировано более тридцати случаев массовой гибели в пожарах среди социально незащищенных слоев населения (пенсионеры, дети, граждане, имеющие психические расстройства и т.п.). Не случайно американский крими-

налист Пауль Кирк [2] писал: «Огонь такое же оружие как нож, топор, ружье. Он может быть направлен прямо на людей. Огонь — самое устрашающее оружие».

По словам современного американского специалиста в пожарном деле Дж. Де-Хаана [2], расследование пожаров — настолько трудная задача, что подавляет инициативу следователя при выполнении своих профессиональных обязанностей. Также на современном этапе поджоги, убийства посредством огня стали доступны для широкого круга лиц, которые могут осуществить заказ подобных преступлений через темный сектор сети Интернет (Darknet) [3, с. 82]. Все это делает актуальным дальнейшее развитие и внедрение информационных технологий (IT-технологии) в деятельность по раскрытию и расследованию криминальных пожаров и убийств посредством огня.

Целью исследования стал обзор наиболее подходящих и отвечающих современным требованиям IT-технологий, направленных на сопровождение раскрытия и расследования убийств, сопряженных с огнем. На разрешение были поставлены следующие задачи: 1) изучить современный отечественный и зарубежный опыт; 2) выбрать комплекс IT-технологий, оптимально подходящий для целей раскрытия и расследования убийств, сопряженных с огнем; 3) предложить вектор дальнейшего развития информационно-технического оснащения экспертно-криминалистических подразделений.

Следует отметить, что расследование по «горячим следам» Б.В. Мегорский [4] и другие основоположники методологии исследования пожаров рассматривают как расследование на месте пожара, а Пауль Кирк и Ганс Кестле [5] особое внимание при этом уделяют взаимодействию с пожарными подразделениями как при тушении пожара, так и при выявлении его причины. Понятно, что для решения вопросов оптимального взаимодействия потребуются методы экспресс-анализа и мобильные технические комплексы.

Эмпирическая база исследования[10] показала, что подобные информационно-технические и программные комплексы применительно к раскрытию

[10] 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; около

и расследованию убийств с использованием огня должны отвечать следующим требованиям:

1. Так как изучаемая категория преступлений характеризуется многоэпизодностью, многообразием типов горючих веществ и материалов, неочевидностью, когда непонятно, какое событие имело место быть (убийство, самоубийство, несчастный случай или его инсценировка [6, с. 674]), желательно сочетание экономичности с экспрессностью, применяемые методы и комплексы должны быть технически простыми в воспроизведении.

2. Содержать по возможности максимум идентифицирующих признаков, не только способствующих установлению очага возгорания, механизма горения, причин возгорания и других особенностей пожара, но и решению идентификационных или диагностических задач установления личности обгоревшего трупа и лиц, вероятно совершивших преступление.

3. Методы и комплексы должны быть портативными, мобильными и пригодными для полевых условий.

4. Должны быть пригодны не только для раскрытия и расследования криминальных пожаров, но и убийств, сопряженных с огнем.

5. Комплексы должны обеспечивать создание единой сетевой (посредством технологий сети Интернет) базы данных обгоревших костей и костных останков с возможностью их дальнейшего 3-мерного моделирования.

В таблице приведено сравнение современных работ на предмет пригодных характеристик информационно-технических комплексов применительно к раскрытию и расследованию убийств с использованием огня.

---

80 актов судебно-медицинского исследования обгоревших трупов БСМЭ города Кемерово за период с 2005 по 2018 года; 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 соответствующих onion-ресурсов сети darknet (например, «Medusa»), где можно оставить заказ «наемному факелу».

Значение оперативной информации полученной в ходе информационно-технического сопровождения раскрытия и расследования убийств с использованием огня

| Объект исследования | Информационно-техническое оснащение | Авторы методов и подходов | Значение оперативной информации |
|---|---|---|---|
| Неопознанный труп | - автоматизированные рабочие места (АРМ) для следователей и оперативников;<br>- АИПС («Опознание», «Портрет-Поиск») | Ю.П. Дубягин [8], М.Н. Шухнин [9], Г.С. Воропаев [10], В.А. Афицинский [11], А.Т. Аманов [12] и др. | - установление личности трупа;<br>- половозрастная идентификация обгоревших останков;<br>- отработка версий по данным исследований специалиста |
| Следы биологического происхождения (следы рук, ног, кровь, слюна, моча, кал, пот и т.п.), запаховые следы | - использование ДНК-учетов;<br>- биоскопические комплексы для полевых условий;<br>- модель фактической информации;<br>- техника сбора запахов | В.А. Мамурков [13], Т.А. Ткачук [14], Ю.Г. Торбин [15], Л.О. Барсегянц [16], Е.В. Левченко [17], Л.Р. Садыков [18] и др. | - идентификация личности (по ДНК);<br>- генетическое установление целого по его частям;<br>- установление связи в системе «личность — предметы — действие» |
| Следы от огня | - технические наборы «Пожар»;<br>- газоанализатор «Колион»;<br>- технические комплексы «Сириус», «Орион»;<br>- передвижные лаборатории | А.Н. Евтушенко [19], А.И. Колмаков, С.О. Шульгин [20], Ф.Г. Аминев [21] и др. | - установление паров инициаторов горения (средств поджога);<br>- идентификация очага возгорания;<br>- фиксация специфических признаков на месте пожара;<br>- изъятие иных следов |
| Отождествляемая личность (лицо оперативной заинтересованности) | - биометрические технологии;<br>- интегрированные базы данных биометрических параметров человека;<br>- мобильные комплексы / лаборатории | Ю.П. Дубягин [22], А.Г. Гульянц [23], Е.Г. Барковская [24] и др. | - дистанционная идентификация неустановленных лиц;<br>- идентификация лица в системе криминалистической регистрации и т.п. |

Видно, что субъект раскрытия и расследования преступления, осматривая место происшествия, в первую очередь должен установить личность неопознанного трупа (в том случае, когда труп не был опознан родственниками, знакомыми). Далее осмотр может проходить параллельно по сбору и фиксации иных следов, исходя из исследованных нами уголовных дел — это разнообразные следы биологического происхождения, и сбору и фиксации следов, остающихся от воздействия огня. Понятно, что для осуществления поиска, сбора и фиксации указанных в таблице следов требуется адекватное техническое и программно-компьютерное оснащение. Например, в случае неопознанного трупа следователь, оперативный работник при обязательном участии врача судмедэксперта в целях идентификации личности могут воспользоваться автоматизированными компьютерными системами, указанными в таблице. Особо подчеркнем, что в свое время С.А. Ялышев [24] предложил автоматизировать деятельность по криминалистической регистрации, создав единую систему информационного криминалистического обеспечения правоохранительных органов.

Как только будет собрана достаточная предварительная база, указывающая на лицо оперативной заинтересованности, оперативные сотрудники разрабатывают тактические приемы проведения необходимых оперативно-розыскных мероприятий (опрос, наведение справок, наблюдение, отождествление личности, оперативный эксперимент и т.п.). Последние могут быть направлены на дистанционную идентификацию лиц, причастных к преступлению, на составление запроса в систему оперативного и криминалистического учета, на публикацию в СМИ фоторобота лиц, подозреваемых в совершении преступлений. Это не только не противоречит ведомственному Приказу МВД России [25], но и соответствует мало реализуемым на практике межведомственным приказам по Кемеровской области [26]. Особую актуальность это приобретает для таких тяжких преступлений, как убийства, сопряженные с огнем, где, судя по нашим исследованиям[11], в среднем 7-8% обгоревших трупов остаются неопознанными.

[11] Согласно изученному архиву актов Бюро судебно-медицинской экспертизы г. Кемерово по делам об убийствах, сопряженных с огнем, за период с 2005 по апрель 2020 года.

А.Г. Гульянц [22, с. 153] предлагает ввести в следственную, а мы по аналогии предлагаем внедрить и в оперативную практику (оперативных подразделений, которые, с наших авторских позиций, должны специализироваться на выявлении, предупреждении и раскрытии убийств, сопряженных с огнем), мобильные программно-технические комплексы для осмотра места происшествия, интегрированные с ноутбуком, что удобно в полевых условиях. Непосредственно для раскрытия убийства с использованием огня такой комплекс способствовал бы установлению связей между обнаруженными следами на месте происшествия и следами, отражающими гипотетически существующий объект, «заданным» следователем.

Внедрение информационно-технических комплексов в оперативную работу неизбежно потребует проведения не только необходимого набора оперативно-розыскных мероприятий (то есть их техническое сопровождение), но и внесение соответствующих корректировок в тактические комбинации и приемы. Это утверждает нас в нашей правоте о том, что одной из научных предпосылок оперативно-розыскного обеспечения раскрытия и расследования убийств с использованием огня служит современное информационно-техническое оснащение оперативно-розыскной деятельности уполномоченных органов.

Изучение зарубежных источников показало, что исследование убийств, сопряженных с огнем, идет по пути проведения серий экспериментов in vivo [27-30]. Общая суть проводимых зарубежными учеными экспериментов сводится к сжиганию невостребованных человеческих трупов в аэробной или анаэробной среде в контролируемых либо неконтролируемых температурных условиях (от 100 до 1100° С). Далее к обгоревшим костям и костным останкам применяются методы оптической и нейтронной колебательной спектроскопии (инфракрасное, комбинационное и неупругое рассеяние нейтронов). По получаемым в результате спектрограммам, именуемым биомаркерами нахождения обгоревшего тела в огне, зарубежные авторы способны идентифицировать температуру горения, время горения, искусственно создаваемые преступником усло-

вия горения, горючие материалы, если они были использованы в целях сокрытия следов преступления и т.п.

Мы предлагаем расширить эксперимент, взяв за основу как опыт зарубежных авторов, так и те исследования отечественной судебной медицины [31, с. 348], которые проводились еще в начале 2000-х гг. Если в эксперименте дополнительно учесть влияние различных видов горючих веществ на химический состав обгоревших костных останков, то появятся диагностические методики, позволяющие установить вид применяемого топлива, регион проживания, половозрастные особенности лица, чьи останки были обнаружены. Важность такого эксперимента состоит еще и в том, что у экспертов появится возможность разграничивать криминальную активность «случайных» преступников от профессиональных действий «наемных факелов» [3, с. 82].

Также можно предложить создавать мобильные устройства, которые в экспресс-режиме ориентировочно будут оценивать по обнаруженным на месте происшествия обгоревшим костным останкам температуру, время горения, тип горючего вещества и т.п.

Другим нашим авторским предложением может стать создание на территории Российской Федерации единой (единого интернет-пространства, которая объединяла бы БСМЭ всех субъектов РФ) базы данных (БД) костей и костных останков человека. В настоящее время ведутся переговоры с ГБУЗ КО ОТ КОКБСМЭ по г. Кемерово создать подобную БД в виде пилотного проекта. В конечном итоге проект должен иметь федеральное значение. Действующий в настоящее время Приказ МВД России от 10.02.2006 № 70 (ред. от 28.12.2016) «Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации» в отношении п.п. 100-106, а именно, создание и ведение краниологических учетов, выполняется не в полной мере и не во всех субъектах РФ. Кроме того, данный Приказ не предполагает ведение иных, кроме учетов черепов неопознанных трупов.

Однако как показывает судебно-медицинская практика по Кемеровской области и других субъектов Сибирского Федерального округа, учет иных кроме

черепа костей и костных останков человека имеет высокую востребованность в правоохранительной сфере.

Данная новизна предполагает решение ряда актуальных задач:

а) мониторинг методов сканирования 3-мерных объектов с выбором наиболее пригодного для обгоревших костей и костных останков;

б) выработка единых количественных показателей для БД;

в) подбор унифицированных в судебно-медицинской практике математических расчетных методов идентификации человека.

Таким образом, можем сделать несколько выводов: 1) тот информационно-технический комплекс, который представлен в таблице, наиболее оптимален для целей раскрытия и расследования убийств, сопряженных с огнем; 2) предлагаем создать мобильные устройства, способные в «полевых условиях» по обгоревшим костным останкам идентифицировать температуру, время, иные условия горения, тип горючего вещества и т.п.; 3) создать на базе ГБУЗ КО ОТ КОКБСМЭ по г. Кемерово пилотный проект единой автоматизированной базы данных обгоревших костей и костных останков в 3D-проекции в целях идентификации человека.

## Список литературы

1. История отечественного государства и права. Часть 1: учебник / под ред. О.И. Чистякова. М.: Юристъ, 2004. 544 с.

2. Дехаан Джон. Расследование пожаров Кирком. США, 1997. 496 с.

3. Драпезо Р.Г. Оперативно-разыскная характеристика «наемного факела» в сети Интернет с некоторыми элементами тактики // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика: сборник статей XVIII Международной научно-практической конференции / отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул, 2020. С. 82-88.

4. Мегорский Б.В. Методика установления причин пожаров (общие положения методики и основы пожарно-технической экспертизы). М.: Стройиздат, 1966. 347 с.

5. Кестле Г. Поджоги: выявление, исследование, предупреждение. На немецком языке. Рихард Боорберг. Штуттгарт; Мюнхен; Ганновер; Берлин; Веймар, 1992.

6. Драпезо Р.Г. Возможные ситуации инсценировки некриминального пожара (в целях сокрытия следов преступления с помощью поджога) // Тенденции развития юридической науки на современном этапе: материалы IV Всероссийской научной конференции с международным участием (18 октября 2019 г.) / отв. ред. Е.С. Трезубов. М.: Проспект, 2020. С. 674.

7. Дубягин Ю.П. Руководство по розыску и расследованию неочевидных убийств. М., 1997. 470 с.

8. Шухнин М.Н. Применение технико-криминалистических и судебно-экспертных методов установления личности по неопознанному трупу при расследовании преступлений: дис. …канд. юр. наук. Саратов, 2000. 246 с.

9. Воропаев Г.С. Проблемы идентификации трупов в криминалистике: дисс. … канд. юр. наук. Владивосток, 2001. 196 с.

10. Афицинский В.А. Криминалистическое обеспечение деятельности по установлению личности неопознанного трупа: автореф. дисс. … канд. юр. наук. Тюмень, 2009. 23 с.

11. Аманов А.Т. Теория и практика установления личности по неопознанным трупам при расследовании убийств: автореф. дисс. … канд. юр. наук. М., 2009. 23 с.

12. Мамурков В.А. Основы криминалистического учения о биологических объектах: дисс. … докт. юр. наук. М., 2002. 326 с.

13. Ткачук Т.А. Использование результатов исследований и экспертиз в поиске преступника: дисс. ... канд. юрид. наук. М., 2001. 166 с.

14. Торбин Ю.Г. Теоретические и прикладные проблемы обнаружения и использования в уголовном судопроизводстве следов и особых примет на живых лицах: дисс. … докт. юр. наук. М., 2003. 506 с.

15. Барсегянц Л.О. Судебно-медицинское исследование вещественных доказательств (кровь, выделения, волосы): учебное пособие для слушателей системы последипломного образования. М.: Медицина, 2005. 448 с.

16. Левченко Е.В. Новые возможности идентификации личности при исследовании вещественных доказательств биологического происхождения // Российский следователь. 2006. № 8.

17. Садыков Л.Р. Тактические особенности работы с запаховыми следами человека // Вестник криминалистики. 2010. № 1 (33). С. 59-65.

18. Евтушенко А.Н. Осмотр места происшествия и его значение для производства судебной пожарно-технической экспертизы: дисс. ... канд. юрид. наук. М., 1998. 232 с.

19. Колмаков А.И., Шульгин С.О. О внедрении в практическую деятельность результатов научно-исследовательских работ, проводимых Экспертно-криминалистическим центром МВД России в области пожарно-технических экспертиз и исследований // Эксперт-криминалист. 2007., № 4.

20. Аминев Ф.Г. Об использовании криминалистических технологий при осмотре места происшествия // Российский следователь. 2009. № 20.

21. Дубягин Ю.П. Криминалистическое отождествление человека в обычных условиях расследования и чрезвычайных ситуациях: дисс. … канд. юрид. наук. Мд, 2002. 255 с.

22. Гульянц А.Г. Основные направления повышения эффективности осмотра места происшествия: дисс. … канд. юрид. наук. М., 2005. 210 с.

23. Барковская Е.Г. Основы использования биометрических параметров человека при раскрытии и расследовании преступлений: автореф. дис. … канд. юрид. наук. Краснодар, 2009. 27 с.

24. Ялышев С.А. Криминалистическая регистрация: проблемы, тенденции, перспективы: автореф. дисс. … докт. юрид. наук. СПб., 1999. 41 с.

25. Приказ МВД России от 21 июля 1993 г. № 349 «Об организации медико-криминалистического обеспечения установления личности неопознанных трупов».

26. Приказ СУ СК по Кемеровской области от 12.09.2011 № 69 «Об организации расследования тяжких и особо тяжких преступлений, совершенных в условиях неочевидности»; Приказ Прокуратуры Кемеровской области, ГУ МВД России по Кемеровской области, СУ СК Российской Федерации по Кемеровской области от 11.06.2013 № 32/359/23 «О совершенствовании деятельности при регистрации и рассмотрении сообщений о смерти и об обнаружении трупов»; Приказ СУ СК Российской Федерации по Кемеровской области, ГУ МВД России по Кемеровской области, Департамент охраны здоровья населения Кемеровской области от 27.04.2020 № 85/383/496 «Об организации взаимодействия работников следственного управления Следственного комитета Российской Федерации по Кемеровской области, сотрудников органов внутренних дел и судебно-медицинских экспертов по сообщениям об обнаружении трупов при отсутствии данных, указывающих на признаки преступления, и проведению проверок по этим сообщениям».

27. Efford M. The Implications of Thermogenic Modification for Anthropological Recovery of Burned Bone. The Arbutus Review. 2016. Vol. 7, № 1. Pp. 20-37. http://dx.doi.org/10.18357/tar71201616054.

28. Marques M., Gonçalves D., Mamede A., Coutinho T., Cunha E., Kockelmann W., Parker S., Carvalho L. Profiling of human burned bones: oxidising versus reducing conditions. Scientific Reports. 2021. 11. 10.1038/s41598-020-80462-3.

29. Rubio L. & Diaz-Vico R. & Smith-Fernandez I. & Smith-Fernandez A. & Suárez J. & Martín de las Heras, Stella & Santos I. Spectrophotometric Color Measurement to Assess Temperature of Exposure in Cortical and Medullar Heated Human Bones: A Preliminary Study. Diagnostics. 2020. 10. 979. 10.3390/diagnostics10110979.

30. Медико-криминалистическая идентификация. Настольная книга судебно-медицинского эксперта / под общ. ред. доктора медицинских наук, профессора В.В. Томилина. М.: НОРМА-ИНФРА, 2000. 472 с.

***Е.А. Дубынин,*** *к.ю.н., доцент, доцент кафедры уголовного процесса и криминалистики Юридического института Сибирского федерального университета, г. Красноярск*
***Е.Е. Космодемьянская,*** *к.ю.н., доцент, доцент кафедры криминалистики Сибирского юридического института МВД России; доцент кафедры уголовного процесса и криминалистики Юридического института Сибирского федерального университета, г. Красноярск*

# НЕКОТОРЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ИМУЩЕСТВЕННЫХ ПРЕСТУПЛЕНИЙ

Очевидным является тот факт, что внедрение цифровых технологий в настоящее время прослеживается во всех сферах общества. Этот процесс является глобальным и необратимым. Цифровизация не обошла стороной и органы предварительного расследования, призванные раскрывать и расследовать преступления.

Нельзя сказать, что данный процесс является новым, поскольку авторы с ним столкнулись порядка 30 лет назад. В частности, в Свердловском РОВД г. Красноярска в 1992 г. в связи с появлением персональных компьютеров была внедрена автономная автоматизированная база данных начального уровня, которая наполнялась сведениями о похищенном автотранспорте и о лицах, представляющих оперативный интерес, с их фотографиями и кратким описанием общих и частных признаков. По мере наполнения данная база стала давать результаты. По введенным данным программа выдавала фотографии лиц, подходящих под описание, что позволяло проводить оперативное опознание преступников потерпевшими.

В настоящее время внедрение цифровых технологий ведется по двум направлениям: 1) справочно-информационное обеспечение расследования и 2) решение логико-поисковых задач на первоначальном этапе расследования,

связанных с построением версий и определением целей и задач расследования, а соответственно, и планированием по конкретному уголовному делу.

За прошедшее время для повышения эффективности производства расследования были разработаны и внедрены в практическую деятельность правоохранительных органов соответствующие АРМы (автоматизированные рабочие места) следователя, дознавателя, руководителя целью которых было упростить процессуальное делопроизводство по уголовному делу. В данном случае речь идет об информационно-аналитическом обслуживании. В данном направлении в настоящее время широко используются автоматизированные информационно-поисковые системы (АИПС) — АИПС «Сейф», АИПС «Картотека», АИПС «Розыск номерных вещей», АИПС «Розыск оружия», АИПС «Досье», АИПС «Гастролеры» и др.; автоматизированные дактилоскопические идентификационные системы (АДИС), в частности «Папилон» (Papillon Systems)[12]; автоматизированные базы данных (АБД) — например АБД «Регион» и др.

Вместе с тем практика показывает, что АРМ(ы) используются не во всех органах предварительно расследования, и связано это с технической стороной вопроса.

Как уже отмечалось выше, цифровизация затрагивает все стороны деятельности общества, поэтому в деятельности по раскрытию и расследованию преступлений необходимо опираться не только на системы, предназначенные для правоохранительных органов, но и использовать комплексы, разрабатываемые для отдельных нужд в гражданских сферах жизнедеятельности. В частности, интересующая следствие информация может содержаться в автоматизированных базах данных различных организаций, предприятий, учреждений, например, таких как гостиницы, транспортные узлы (вокзалы, порты и т.д.), таможенные пункты, пункты пограничного контроля и пр. С их помощью можно

[12] Модульная масштабируемая система для автоматизации процессов регистрации, обработки, сравнения и отождествления дактилоскопической информации и создания дактилоскопических/ мультибиометрических банков данных любого объема и различной целевой направленности.

обнаружить определенных лиц, зафиксировать их действия, пути и способы их перемещения и перемещения похищенного имущества.

Так, еще в 2003 г. авторами публикации была разработана программа демонстрации системы исходных ситуаций, тактических задач и средств их решения при расследовании краж чужого имущества и в ее рамках — программа изучения очагов преступлений и их связи с местом жительства преступника как одного из средств установления последнего [3].

В настоящее время при раскрытии преступлений наиболее востребованными являются результаты использования средств видеофиксации, установленных в организациях, на предприятиях торговли, в общественных местах и на территории частных владений. Однако полученной таким образом информации не всегда бывает достаточно для идентификации личности преступника и его розыска, а также розыска похищенного имущества и ценностей.

Мы полагаем, что перспективным направлением в раскрытии преступлений является использование биометрической информации. Например, технологии распознавания лиц для различных целей, в том числе и для общественной безопасности, успешно применяются в Китае. Так, «китайская полиция опознала в 60-тысячной толпе мужчину, подозреваемого в совершении преступления. Сделать это позволила внедряемая в Китае система компьютерного распознавания лиц. Мужчина был опознан камерой при входе на концерт. Его задержали вскоре после того, как он сел на свое место в зале. Полиция заявила, что Ао разыскивался по подозрению в совершении экономических преступлений. Он был потрясен при задержании, сообщили полицейские» [7].

Еще одним примером современных зарубежных разработок средств идентификации личности по биометрическим данным, особенно ставшим актуальными в период пандемии, может быть следующий: «Когда весь мир начинает носить маски из-за коронавируса, технологии распознавания лиц могут оказаться менее эффективными. Но компания из Китая сумела довести точность распознавания даже открытого наполовину лица до 95% или даже выше. Алгоритм работает так: камера делает фото человека и преобразует его в вектор чи-

сел, который описывает расположение черт лица. Когда человек надевает маску, у программы остается гораздо меньше черт, на основе которых можно провести распознавание. Кроме того, может быть несколько людей с похожими чертами. Когда вектор рассчитан, программа сравнивает его с набором чисел в базе данных и ищет совпадение с определенной долей точности.

Компания и до коронавируса и масок сталкивалась с проблемой частично закрытых лиц: например, в случае с бородатыми мужчинами в Турции и Пакистане, а также с клиентами с севера Китая, которые зимой носят одежду, закрывающую уши и лицо.

В случае с масками программе приходится предполагать, какие черты лица могут быть скрыты и как человек выглядел бы без маски. Компания «Ханьвань» установила больше 2 млн камер для распознавания лиц по всему миру, а теперь научила их определять даже тех людей, которые носят медицинские маски. Точность распознавания полностью открытых лиц компания довела до 99,5%. В случае с масками в лаборатории она добилась результата в 95%. При этом в реальности результат может быть еще выше, потому что технология в случае провальной попытки будет делать еще снимки человека и пытаться установить его личность» [2].

В России во исполнение «Стратегии национальной безопасности Российской Федерации до 2020 года» [5] была подготовлена и утверждена Концепция построения и развития аппаратно-программного комплекса «Безопасный город» (далее — АПК «Безопасный город»).

АПК «Безопасный город» включает в себя комплексы средств автоматизации в области общественной безопасности, правопорядка и безопасности среды обитания на уровнях от федерального до муниципального, а также на конкретных отдельных объектах. Одним из ключевых элементов данного АПК является система видеонаблюдения.

Несмотря на имеющуюся критику отдельных правозащитников, АПК «Безопасный город» внедряется и используется в ряде субъектов Российской Федерации в режиме постоянной либо опытной эксплуатации.

Так, согласно сведениям, размещенным на официальном сайте администрации Санкт-Петербурга, в городе «системой видеонаблюдения охвачены все 18 районов города. В 2020 году количество источников видеоизображения в рамках сервисной модели увеличилось до 39 609 камер. Количество терминалов экстренной связи «Гражданин-Полиция» на ноябрь 2020 года составляет 119 терминалов. В городскую систему видеонаблюдения также интегрированы камеры сторонних систем видеонаблюдения различных социально важных объектов. Сейчас количество источников видеоизображения сторонних систем, интегрированных с городской системой видеонаблюдения, возросло до 6 368 (аэропорт «Пулково» — 38, СПб ГКУ «МФЦ» — 228, ОАО «Пассажирский порт Санкт-Петербурга «Морской фасад» — 11, ГУП «Петербургский метрополитен» — 3 983, КВЦ «Экспофорум» — 30, стадион «Санкт-Петербург» — 435 и др.). Одним из самых масштабных комплексных инфраструктурных проектов является «Умный двор». Главная его задача — сделать дворы и парадные максимально безопасными для жителей. Проект предусматривает создание единой комплексной системы мониторинга, обеспечивающей безопасность и контроль ситуации на дворовых территориях. В рамках проекта предусмотрена комплексная модернизация домофонной инфраструктуры парадных многоквартирных домов и размещение на входах в парадные современных устройств мониторинга.

Мобильное приложение «Безопасный Санкт-Петербург» предоставляет всем пользователям доступ к городской системе видеонаблюдения. В приложении пользователь может найти ближайшую видеокамеру к месту события и увидеть ее обзор, направить заявку на сохранение видеоархива, передать видео с места происшествия в городскую систему видеонаблюдения и многое другое» [6].

Другим примером может быть следующий: «…в Сахалинской области в АПК «Безопасный город» внедрена биометрическая система распознавания лиц «Визирь», которая используется в России для охраны общественного порядка в местах массового скопления людей. Распознавание строится на нейросетевом алгоритме, который анализирует доступную часть лица, а не

сопоставляет расположение ключевых точек. Свою эффективность она продемонстрировала по выявлению нарушителей карантина в условиях пандемии COVID-19» [1].

Интересен пример использования цифровых технологий зарубежными странами в борьбе с мошенничеством как одним из видов имущественных преступлений. Так, «власти Китая с этого месяца обязали всех пользователей мобильной связи проходить процедуру распознавания лиц при покупке SIM-карты. В опубликованном заявлении Министерства промышленности и информатизации КНР значится, что новые меры направлены на борьбу с телефонным и интернет-мошенничеством и призваны обеспечить защиту личной информации граждан. Подобные "умные" технологии постепенно становятся неотъемлемой частью жизни простых граждан Китая. Путешествующие поездом могут забыть о бумажных и даже электронных билетах: достаточно подойти к специальному считывающему устройству при проходе на станцию, после чего система идентифицирует гражданина, откроется турникет, и пассажир пройдет на посадку в вагон. Для того чтобы это произошло, нужно заранее пройти регистрацию в специальном приложении мессенджера WeChat, к которому привязана банковская карта. После успешного сканирования лица пассажира средства автоматически спишутся со счета владельца карты. Такие устройства появляются не только на железнодорожных вокзалах, но и на станциях метро. Удобный и быстрый способ оплаты распространен не только "под землей", но и в городских автобусах и такси…

Современные технологии используются не только для упрощения жизни китайских граждан, но и для обеспечения общественного порядка. Например, в январе этого года шанхайская полиция начала устанавливать на перекрестках камеры, фиксирующие перемещения велосипедистов и скутеров: устройства следят, чтобы участники дорожного движения не пересекали стоп-линию и не выезжали на красный сигнал светофора. Установить личность нарушителя помогают встроенные в камеры технологии распознавания лиц. Ловят нарушителей не только на дорогах, но и в образовательных учреждениях, местах обще-

ственного питания и др. Камеры способны автоматически отправить соответствующие фото контролирующим ведомствам. Подобное оборудование устанавливается в общественных местах, гостиницах, и т.д. Список сфер жизни китайского общества, куда все сильнее проникают новые технологии, постоянно увеличивается. Здесь и мобильные приложения, и онлайн-игры, которые с помощью распознавания лиц отслеживают, сколько времени юные пользователи проводят перед экранами мобильных телефонов, и многие другие» [4].

В России при раскрытии преступлений, предусмотренных п. «г» ч. 3 ст. 158 УК РФ кража, т.е., тайное хищение чужого имущества с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ), возможно использование ресурсов созданной экосистемы (SberX) Сбербанка, и, в частности, указанной биометрической системы, которая осуществляет ведение структурированной картотеки фотоизображений и сопутствующей информации, и ведет поиск в картотеке по фотоизображению и сопутствующей информации. Объем картотеки фотоизображений лиц с произвольной сопроводительной информацией позволяет вводить до нескольких миллионов карточек, при этом ввод данных в картотеку может быть осуществлён из любых источников (фотоизображения, видеофайлы, фотокамеры, сканеры, веб-камеры).

Использование этой биометрической системы станет возможным в случае ее повсеместного внедрения. На текущий момент она используется на 7 объектах транспорта, 16 спортивных сооружениях и в 6 АПК «Безопасный город» [8].

Таким образом, как следует из проведенного анализа возможностей и реальностей использования цифровых технологий в раскрытии и расследовании имущественных преступлений, не всегда имеющиеся в потенциале разработки и программные средства оказываются доступными для практиков в силу различного рода факторов, как то: материальное обеспечение подразделения, технические возможности, навыки использования таких технологий самим субъектом раскрытия и расследования преступлений. Тем не менее знание возможного потенциала в практике противодействия преступности в условиях цифрови-

зации позволяет наметить пути совершенствования свой деятельности в данном направлении субъектом расследования (например, посредством проведения специализированных курсов повышения квалификации), для повышения эффективности деятельности по раскрытию и расследованию преступлений, в целом, и преступлений имущественного характера, в частности.

## Список литературы


1. Биометрическая система распознавания лиц от группы ЦРТ работает в составе АПК «Безопасный город» на Сахалине. [Электронный ресурс]. URL: https://www.speechpro.ru/media/news/07-04-2020 (дата обращения: 13.04.2021).
2. В Китае научились распознавать 95% лиц в масках. [Электронный ресурс]. URL: https://www.forbes.ru/newsroom/biznes/395425-v-kitae-nauchilis-raspoznavat-95-lic-v- maskah (дата обращения: 24.04.2021).
3. Космодемьянская Е.Е. Возможности использования инновационных технологий в процессе преподавания курса «Криминалистика» // Вестник Сибирского юридического института МВД России. 2010. № 1 (5). С. 48-52.
4. Не спрятаться, не скрыться: система распознавания лиц в Китае стала нормой жизни. Новости от 24 декабря 2019 г. [Электронный ресурс]. URL: https://tass.ru/mezhdunarodnaya-panorama/7407689 (дата обращения: 24.04.2021).
5. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 31 декабря 2015 года № 683 // СПС КонсультантПлюс.
6. Официальный сайт Администрации Санкт-Петербурга. [Электронный ресурс]. URL: https://www.gov.spb.ru/gov/otrasl/c_information/napravlenie-deyatelnosti-komiteta/bezopasnyj-gorod/ (дата обращения: 13.04.2021).
7. Распознавание лиц: почему в Китае не скрыться даже в 60-тысячной толпе. [Электронный ресурс]. URL: https://www.bbc.com/russian/news-43751391 (дата обращения: 24.04.2021).

8. Финансовые организации. Готовые решения. [Электронный ресурс]. URL: https://www.speechpro.ru/solution/finansovye-organizacii (дата обращения: 13.04.2021).

***Н.А. Дудко,*** *к.ю.н, доцент, доцент кафедры уголовного процесса и криминалистики юридического института Алтайского государственного университета, г. Барнаул*
***А.Р. Прусс,*** *помощник судьи Алтайского краевого суда, советник юстиции второго класса, г. Барнаул*

## ПРАКТИКА ПРИМЕНЕНИЯ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ ПРИ РАССМОТРЕНИИ СУДАМИ УГОЛОВНЫХ ДЕЛ

Активное развитие информационных технологий последовательно охватывает все сферы общественной жизни. Следствием является масштабная цифровизация даже тех областей деятельности, которые еще в недалеком прошлом не ассоциировались с повсеместным применением информационных технологий. «Информационное пространство является новой реальностью, пронизывающей практически все области жизни человека, общества и государства… Внедрение информационно-цифровых технологий повлияло и на развитие действующего российского уголовно-процессуального законодательства» [1, с. 190].

Одно из направлений применения цифровых технологий в уголовном судопроизводстве — использование систем видеоконференц-связи при рассмотрении судами уголовных дел. Технология видеоконференц-связи впервые в России была применена 18 ноября 1999 г. в Челябинском областном суде при рассмотрении уголовного дела для связи с Челябинским следственным изолятором № 74/1, где находился в то время осужденный [2, с.50].

Использование систем видеоконференц-связи в судебном производстве соответствует Федеральной целевой программе «Развитие судебной системы Рос-

сии на 2013-2024 годы» [3]. Программа имеет целью техническое обеспечение прав граждан на участие в судебных заседаниях, повышение уровня доступности правосудия и содержит перечень мероприятий по развитию использования в судах системы видеоконференц-связи. По итогам реализации Программы предусмотрено оснащение 95 процентов федеральных судов общей юрисдикции комплектами видеоконференц-связи.

За время действия с 2002 г. УПК РФ [4] законодатель использует «фрагментарный» подход к цифровизации уголовного судопроизводства, при котором цифровые технологии применяются к отдельным относительно самостоятельным этапам уголовно-процессуальной деятельности [5, с. 37].

Так, были внесены положения о видеоконференц-связи в следующие статьи УПК РФ: 2001 г. — ст. 376 ч. 3 (№ 174-ФЗ от 18.12.2001); 2009 г. — ст. 407 ч. 2 (№ 37-ФЗ от 14.03.2009); 2009 г. — ст. 35 ч. 6 (№ 346-ФЗ от 27.12.2009); 2010 г. — ст. 376 ч. 3, ст. 407 ч. 2 (№ 323-ФЗ от 29.11.2010); 2010 г. — ст. 389.12 ч. 2, 401.13 ч. 2 (№ 433-ФЗ от 29.12.2010); 2011 г. — ст. 240 ч. 4, ст. 278.1 (№ 39-ФЗ от 20.03.2011); 2011 г. — ст. 399 ч. 2 (№ 40-ФЗ от 20.03.2011); 2014 г. — ст. 241 ч. 6.1, ст. 293 ч. 1 (№ 251-ФЗ от 21.07.2014).

В результате участвовать в судебном производстве путем использования систем видеоконференц-связи вправе свидетели и потерпевшие (ст. 240 ч. 4, ст. 278.1 УПК РФ), обвиняемые (ст. 35 ч. 6 УПК РФ), подсудимые (ст. 241 ч. 6.1, ст. 293 ч. 1 УПК РФ), осужденные (ст. 389.12 ч. 2, ст. 401.13 ч. 2, ст. 399 ч. 2 УПК РФ).

Дополнительно к изменениям в УПК РФ был принят «Регламент организации применения видеоконференц-связи при подготовке и проведении судебных заседаний» [6].

Статистика рассмотрения судами уголовных дел позволяет сделать вывод об эффективности и расширении применения систем видеоконференц-связи. Например, статистические данные использования видеоконференц-связи в судебных заседаниях при рассмотрении Алтайским краевым судом уголовных дел и материалов по первой инстанции: 2013 г. — 8 дел (9 судебных заседаний),

2014 г. — 11 дел (19 судебных заседаний), 2015 г. — 9 дел (24 судебных заседания), 2016 г. — 11 дел (40 судебных заседаний), 2017 г. — 5 дел (19 судебных заседаний), 2018 г. — 7 дел (10 судебных заседаний), 2019 г. — 10 дел (20 судебных заседаний), 2020 г. — 14 дел (24 судебных заседания) [7].

Вместе с тем по сравнению с процессуальным законодательством иных отраслей права (АПК РФ, ГПК РФ, КАС РФ) механизмы, позволяющие использовать ресурсы электронного правосудия, в уголовно-процессуальном законе развиты в меньшей степени. Успешный опыт применения видеоконференц-связи в гражданско-правовых видах судопроизводства способствовал внесению в Государственную Думу РФ законопроекта, предусматривающего возможность удаленного участия сторон в судебных заседаниях [8]. Законопроект 02.06.2021 принят в первом чтении.

Природа уголовного процесса, которому свойственна возможность ограничения прав и законных интересов граждан и юридических лиц, традиционно характеризуется деятельностью, осуществляемой людьми, а не технологиями. Непосредственное исследование судом с участием сторон всех обстоятельств дела является проявлением межотраслевых принципов непосредственности и устности судебного разбирательства, состязательности процесса и равенства сторон перед законом и судом. Право обвиняемого (подсудимого) на личное участие в судебном заседании также является формой реализации его права на защиту от предъявленного обвинения. В настоящее время обеспечение реализации указанного права на стадии судебного разбирательства в судах первой и вышестоящих инстанций осуществляется в том числе посредством цифровой технологии видеоконференц-связи.

Для правоприменителя ситуация осложняется тем, что, в отличие от производства в суде второй инстанции, ч. 1 ст. 247 УПК РФ устанавливает требование об обязательном участии подсудимого в судебном разбирательстве суда первой инстанции при рассмотрении уголовного дела по существу. При этом форма такого участия — непосредственно путем личного присутствия или посредством видеоконференц-связи в законе не указана.

Указание о непосредственной форме участия подсудимого в судебном заседании содержится в ч. 6.1 ст. 241 УПК РФ в качестве одного из проявлений гласности судебного разбирательства, а также в п. 4 разъяснений Пленума Верховного Суда РФ в Постановлении от 30 июня 2015 года № 29 «О практике применения судами законодательства, обеспечивающего право на защиту в уголовном судопроизводстве» [9]. Согласно правовой позиции высшей судебной инстанции, право обвиняемого лично осуществлять свою защиту реализуется посредством его участия в судебном разбирательстве и обеспечивается судом. Участие подсудимого в судебном разбирательстве суда первой инстанции путем видеоконференц-связи допускается законодателем лишь в качестве исключений: только в целях обеспечения безопасности участников уголовного судопроизводства и в случае предъявления обвинения по перечисленным в законе составам преступлений (ч.6.1 ст. 241 УПК РФ), а также для осужденных в целях их участия в судебном заседании суда первой инстанции на стадии исполнения приговора (ч. 2 ст. 399 УПК РФ). Также уголовно-процессуальным законом не предусмотрена смешанная форма участия подсудимого в судебных заседаниях, когда в части из них он участвует непосредственно, а в других — с использованием видеоконференц-связи [10].

Расширение использования современных систем передачи информации предоставило возможность преодолеть принимаемые государством ограничительные меры по противодействию распространению новой коронавирусной инфекции (COVID-19). В сложившихся условиях цифровизация не могла не затронуть и отправление правосудия по уголовным делам.

В 2020 г. постановлениями Президиума Верховного Суда Российской Федерации и Совета судей Российской Федерации от 18 марта 2020 года № 808 и от 8 апреля 2020 г. № 821 в целях противодействия распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) всем судам было рекомендовано при наличии технической возможности инициировать рассмотрение дел и материалов безотлагательного характера (об избрании, продлении, изменении или отмене меры пресечения) путем использо-

вания систем видеоконференц-связи [11, 12]. С учетом обстоятельств дела, мнений участников судопроизводства и условий режима повышенной готовности, введенного в соответствующем субъекте Российской Федерации, суды были наделены правом самостоятельно принимать решение о рассмотрении в такой форме участия сторон и иных категорий дел.

Эти рекомендации были приняты в сложившихся экстраординарных условиях, в связи с чем у судов общей юрисдикции возникли вопросы о порядке отправления правосудия по уголовным делам и осуществлении судебного контроля по поступающим материалам. Для ходатайств об избрании, продлении, изменении или отмене мер пресечения, отнесенных в указанных рекомендациях к категории материалов безотлагательного характера, которые рассматриваются только с участием обвиняемого (подсудимого), законом установлены сокращенные процессуальные сроки разрешения, что связано с их спецификой. В то же время уголовные дела, поступающие для рассмотрения по существу, материалы в порядке исполнения приговора также связаны с применением мер пресечения, ограничением прав иных лиц, поэтому требовали своевременного рассмотрения и принятия по ним процессуальных решений. Поэтому от судов требовались не только оперативные меры для своевременного рассмотрения уголовных дел и материалов с учетом принципов гласности, разумности сроков судопроизводства, но и обеспечение права обвиняемых (подсудимых) на участие в судебных заседаниях в условиях объективной ограниченности технических ресурсов.

Очевидно, что в условиях сложной эпидемиологической ситуации и введенными ограничительными мерами, в том числе в учреждениях уголовно-исполнительной системы, приостановивших вывоз обвиняемых (подсудимых) на судебно-следственные действия, реализация права указанных категорий лиц на непосредственное участие в судебных заседаниях суда первой инстанции при рассмотрении уголовных дел по существу и материалов представлялась затруднительной. В таких условиях единственным способом реализации данного права стало повсеместное использование судами видеоконференц-связи.

Из изученной нами судебной практики следует, что до 2020 г. приведенные выше нормы закона правоприменителем толковались единообразно как обязывающие суд обеспечить непосредственное участие обвиняемого (подсудимого) в судебном заседании. Рассмотрение дела судом первой инстанции без непосредственного участия подсудимого признавалось вышестоящими инстанциями существенным нарушением уголовно-процессуального закона, связанным с ограничением права на защиту [13, с. 109] и допущенным несоблюдением принципа непосредственности судебного разбирательства. Такие судебные решения безусловно отменялись с направлением уголовного дела на новое судебное рассмотрение [14, 15].

Обеспечение участия обвиняемых (подсудимых) в судебных заседаниях судов первой инстанции посредством видеоконференц-связи предсказуемо привело к соответствующим доводам в апелляционных жалобах на итоговые и промежуточные судебные решения. В качестве основания для отмены судебных решений авторы жалоб называли нарушение права на защиту, которое выразилось в их участии в судебных заседаниях суда первой инстанции посредством видеоконференц-связи [16].

В отсутствие законодательных изменений уголовно-процессуального закона ответ на вопрос о возможности рассмотрения судами уголовных дел и материалов с использованием видеоконференц-связи в суде первой инстанции в период действия ограничительных мер был дан Верховным Судом РФ в Обзоре по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2, утвержденном Президиумом Верховного Суда РФ 30 апреля 2020 г. Допуская возможность использования технических систем, со ссылкой на правовые позиции Европейского Суда по правам человека, высшая судебная инстанция указала, что «использование в ходе судебного разбирательства системы видеоконференц-связи не противоречит понятию справедливого и публичного слушания», «позволит обеспечить личное участие и соблюдение процессуальных прав подозреваемого, обвиняемого, подсудимого и других лиц в судебном заседании» [17].

Спустя год повсеместного действия ограничительных мер Верховный Суд РФ также разъяснил, что наличие возражений сторон, в частности, подсудимого (обвиняемого) против участия посредством видеоконференц-связи в суде первой инстанции правового значения для суда не имеет, так как определение порядка проведения судебного разбирательства относится к исключительной компетенции суда [18].

Приведенные нами ответы Верховного Суда РФ на вопросы, поступившие от судов общей юрисдикции, обобщенные в виде обзоров, являются примерами судебного нормотворчества, острая необходимость которого возникла в условиях, когда законотворчество оказалось неспособным быстро и эффективно преодолеть возникший в сложившихся условиях пробел в праве.

Таким образом, в условиях отсутствия законодательного регулирования, применение систем видеоконференц-связи при рассмотрении уголовного дела или материала судом первой инстанции в условиях действия ограничительных мер признается законным, а доводы жалоб об обратном судами вышестоящих инстанций отклоняются как необоснованные [19, 20, 21].

Форсированное расширение использования систем видеоконференц-связи судами, которое ранее осуществлялось поэтапно и только в связи с реализацией федеральных целевых программ, актуализировало вопрос о возможности обеспечения участия подсудимых в рассмотрении уголовных дел и материалов в судебных заседаниях судов первой инстанции в указанной форме и после полного снятия ограничительных мер.

Следует признать, что в условиях действия ограничительных мер применение видеоконференц-связи позволило судам первой инстанции не только отправлять правосудие с соблюдением разумных сроков, но и обеспечило значительную экономию ресурсов, в том числе связанных с конвоированием в суд подсудимых (обвиняемых), находящихся под стражей.

Однако несмотря на положительные результаты применения видеоконференц-связи при рассмотрении уголовных дел по существу в период ограничительных мер, полагаем, что необходимость изменения уголовно-процессуального закона в части установления данной формы участия подсудимого (обвиня-

емого) в судебных заседаниях суда первой инстанции в качестве альтернативы непосредственному участию, при определении формы такого участия исключительно судом, не является бесспорной.

По мнению Л.А. Воскобитовой, человеческой коммуникации свойственна эмоциональная составляющая, которая безусловно является компонентом и уголовно-процессуальной деятельности [22, с. 97]. В случае применения при коммуникации технических средств эта составляющая утрачивается [23, с. 32]. Считаем, что именно этим обусловлено желание подсудимых (обвиняемых) участвовать в рассмотрении уголовных дел по существу и материалов лично в форме непосредственного присутствия в зале судебного заседания. В такой форме участия они имеют не только формальную возможность донести свою позицию до суда и участников процесса, но и придать ей эмоциональную составляющую, наблюдать ответную реакцию. Указанное имеет особое значение при рассмотрении дела судом с участием присяжных заседателей, на чувства и эмоции которых пытаются воздействовать как сторона защиты, так и сторона обвинения, используя при этом не только процессуальные средства.

Не следует исключать объективное значение эмоций и самих судей при осуществлении ими процессуальных полномочий. Как отмечается в научных исследованиях, эмоциональная компетентность позволяет выявлять и различать при разрешении дела подлинные и мнимые интересы участников процесса, принимать во внимание не только формальные предписания права, но и искать баланс между интересами правосудия и конкретного человека, учитывать моральную значимость последствий судебного решения [24, с. 135]. Рационально-эмоциональное восприятие наряду с мыслительно-аналитической деятельностью судьи происходит на всех стадиях процесса [25, с. 250].

По нашему мнению, использование цифровых технологий не станет препятствием для достижения назначения уголовного судопроизводства, позволит экономить человеческие ресурсы и ускорить отдельные процедуры. В то же время развитие цифровых технологий не должно приводить к снижению гарантий прав и свобод участников уголовного судопроизводства.

Полагаем, что после снятия ограничительных мер участие подсудимого (обвиняемого) посредством видеоконференц-связи может быть установлено законодателем в качестве формы участия в судебном заседании суда первой инстанции, применяемой по ходатайству самого подсудимого (обвиняемого) и при условии обеспечения возможности следить за ходом судебного процесса, видеть и слышать участников процесса, а также беспрепятственно быть заслушанным сторонами и судом.

## Список литературы


1. Андреева О.И., Зайцев О.А. Правовое регулирование уголовно-процессуальных отношений в цифровую эпоху // Вестник Томского государственного университета. 2020. № 455. С. 190-198.
2. Правосудие в современном мире: монография / под ред. В.М. Лебедева, Т.Я. Хабриевой. М.: Норма, Инфра-М, 2012. 565 с.
3. Постановление Правительства РФ от 27.12.2012 № 1406 (ред. от 29.12.2020) «О федеральной целевой программе «Развитие судебной системы России на 2013-(2020) 2024 годы». [Электронный ресурс]. URL: http://pravo.gov.ru.
4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.05.2002; ред. от 30.04.2021 с изм. от 13.05.2021) // Собрание законодательства РФ. 2001. № 52 (ч. I). Ст. 4921.
5. Воскобитова Л.А. Использование функционального подхода для цифровизации уголовного судопроизводства // Вестник Университета имени О.Е. Кутафина. 2020. № 10 (74). С. 34-51.
6. Приказ Судебного департамента при Верховном Суде РФ от 28.12.2015 № 401 (ред. от 30.12.2020) «Об утверждении Регламента организации применения видеоконференц-связи при подготовке и проведении судебных заседаний» // Бюллетень актов по судебной системе. 2016. № 3.
7. Статистическая форма № 1 «Отчет о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции»: краевой суд, 2013-

2020 гг. [Электронный ресурс]. URL: http://kraevoy.alt.sudrf.ru/ modules.php?name=docum_sud&rid=35.

8. О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования дистанционного участия в судебном процессе: Законопроект № 1144921-7. Система обеспечения законодательной деятельности. [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/1144921-7.

9. О практике применения судами законодательства, обеспечивающего право на защиту в уголовном судопроизводстве: пост. Пленума Верховного Суда РФ от 30 июня 2015 № 29: по состоянию на 20 мая 2021 г. // Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

10. Апелляционное определение судебной коллегии по уголовным делам Свердловского областного суда от 20 июля 2017 года по делу № 22-5193/2017 // Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

11. О приостановлении личного приема граждан в судах: пост. Президиума Верховного Суда Российской Федерации и Совета судей Российской Федерации от 18 марта 2020 г. №808: по состоянию на 20 мая 2021 г. // Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

12. О приостановлении личного приема граждан в судах: пост. Президиума Верховного Суда Российской Федерации и Совета судей Российской Федерации от 8 апреля 2020 года № 821: по состоянию на 20 мая 2021 г. // Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

13. Курченко В.Н. Толкование принципа непосредственности судебного разбирательства в уголовном судопроизводстве // Уголовное право. 2019. № 6. С. 104-110.

14. Апелляционное определение судебной коллегии по уголовным делам Свердловского областного суда от 20 июля 2017 года по делу № 22-5193/2017 //

Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

15. Обзор судебной практики Владимирского областного суда № 1 за 2016 год // Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

16. Определение Шестого кассационного суда общей юрисдикции от 26 января 2021 года №77-205/2021 // Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

17. Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2 (утв. Президиумом Верховного Суда РФ 30 апреля 2020 года) // [Электронный ресурс]. URL: https://www.consultant.ru/online/.

18. Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 3 (утв. Президиумом Верховного Суда РФ 17 февраля 2021 года) // Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

19. Определение Восьмого кассационного уда общей юрисдикции от 7 апреля 2021 года №77-1197/2021 // Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

20. Определение Шестого кассационного суда общей юрисдикции от 28 октября 2020 года №77-2725/2020 // Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

21. Определение Шестого кассационного суда общей юрисдикции от 20 октября 2020 года № 77-2650/2020 // Справочно-правовая система Консультант Плюс. [Электронный ресурс]. URL: https://www.consultant.ru/online/.

22. Воскобитова Л.А. Уголовное судопроизводство и цифровые технологии: проблемы современной совместимости // LexRussica. 2019. № 5. С. 91-104.

23. Скабелина Л.А. Влияние цифровизации на профессиональную коммуникацию адвоката // Адвокатская практика. 2020. № 4. С. 30-33.

24. Морхат П.М. Правосубъектность искусственного интеллекта в сфере интеллектуальной собственности: гражданско-правовые проблемы: дисс. … д-ра юрид. наук: 12.00.03. М., 2018. 420 с.

25. Фиошин А.В. О судейской дискреции при рассмотрении дел, связанных с оценочными понятиями наследственного и семейного права // Вестник гражданского процесса. 2019. № 4. С. 250-264.

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

## ИСПОЛЬЗОВАНИЕ ДАННЫХ ПСИХОЛОГИЧЕСКОГО ПРОФИЛЯ ПОДОЗРЕВАЕМОГО ПРИ ДОПРОСЕ ПО ГРАБЕЖАМ И РАЗБОЯМ

Одним из важнейших следственных действий при расследовании уголовных дел по фактам грабежей и разбоев является допрос подозреваемого. При подготовке и проведении допроса следователь должен заранее учитывать особенности психологического типа преступника, чтобы умело применять соответствующие тактические приемы. Чтобы допрос подозреваемого привел к желаемому положительному результату, следователь должен проводить его как можно более эффективно. В результате в ходе допроса должна быть получена достоверная и полная информация о совершенном преступлении. Для установления психологического контакта с подозреваемым важно знать психологические особенности личности преступника и мотивационную направленность его поведения.

Психологический контакт во время допроса обеспечивается за счет правильно подобранной тактики, основанной на изучении индивидуальных особенностей допрашиваемого, материалов уголовного дела, а также коммуника-

тивных навыков следователя с целью пробуждения у допрашиваемого интереса к общению. При этом необходимо исключить конфликты и напряженность, чтобы создать благоприятную атмосферу для проведения допроса. Психологический контакт невозможен без умения дознавателя расположить к себе допрашиваемого, внушить ему доверие и подготовить к спокойному, целенаправленному допросу. Каждый этап общения характеризуется особыми методами установления и поддержания психологического контакта. Для вводной части допроса — беседа с целью получения и уточнения демографических данных, при необходимости — информации о жизненном пути и интересах допрашиваемого. При этом следует обращать внимание на обстоятельства, которые его положительно характеризуют. Следователь на этом этапе определяет линию своего поведения, уточняет тему и задает общие вопросы. Тогда психологический контакт укрепляется и поддерживается. Это достигается не только путем постановки вопросов, представления доказательств, сравнения их с уже имеющейся информацией по делу, но также путем привлечения внимания допрашиваемого и подчеркивания необходимости разобраться в реальных обстоятельствах совершения преступления. Выбор метода установления психологического контакта следователем во многом зависит от того, к какому типу преступника относится допрашиваемый.

В юридической литературе на основе изучения протоколов допросов подозреваемых по грабежам и разбоям выделяют наиболее типичные группы преступников, которые по критериям мотивации делятся на следующие типы [1, 2].

1. «Ситуационный» тип. Люди этого типа совершают преступления под воздействием неблагоприятной внешней среды, то есть действуют не по заранее сформировавшемуся умыслу, а в силу сложившейся ситуации, часто в состоянии опьянения. В литературе приводятся следующие данные: «Анализ грабежей и разбоев, совершенных на открытой местности, показал, что в 23,9% случаев преступники были в состоянии легкого либо среднего алкогольного опьянения, в 2,1% случаев — в состоянии токсического или наркотического опьянения. При этом преступление ими было совершено впервые» [3, с. 11].

«Ситуацией» для совершения грабежа или разбоя может послужить конфликт (например, «пьяная» драка, в результате которой «победитель» собрал «трофеи» и т.п.). В большинстве случаев подозреваемые данного типа не создают конфликта в ходе допроса. Они часто дают полные признательные показания, раскаиваются в содеянном, нередко стремятся сами помочь следователю установить все обстоятельства преступления. Поэтому для следователя наиболее целесообразно допросить «ситуационного» преступника, используя тактические приемы, которые способствуют лучшему психологическому расположению допрашиваемого. Одним из таких приемов является обращение к положительным качествам допрашиваемого. Например, следователь подчеркивает положительные стороны биографии подозреваемого — общественную деятельность, образцовую службу в армии, занятия спортом, хорошее поведение в школе, институте, успехи на работе и т.д., акцентирует внимание на положительных качествах характера — честности, принципиальности и т.д. Следователь должен быть тактичен в разговоре с людьми из этой категории, избегать возникновения конфликтных ситуаций, давать отпор допрашиваемым. В некоторых случаях для установления психологического контакта желательно обеспечить допрашиваемым комфортные условия (например, в жаркую погоду предложить стакан холодной воды, курильщику — сигарету и т.д.). Отмечается, что «полезным при допросе «ситуационного» грабителя использовать общие интересы. При определенных условиях следователь может подчеркнуть то, что он обучался в одной школе (институте) с допрашиваемым, занимается однородным или таким же видом спорта, имеет схожие увлечения (например, интересуется одной литературой, музыкой, компьютерными играми и т.д.). В свою очередь, не следует при этом поощрять чрезмерную свободу поведения, граничащую с развязностью» [2, с. 43].

2. «Антисоциальный» тип. Во время допроса они выбирают конфликтную форму общения — грубят, угрожают следователю, ведут себя высокомерно, в некоторых случаях отказываются давать показания, ссылаясь на ст. 51 Конституции РФ. Как показывает практика, в большинстве случаев допрашива-

емый, избравший такое поведение, как правило, является причастным к совершению преступления — либо сам совершил грабеж или разбой, либо выступал соучастником преступления. Кроме того, такие люди склонны нападать на следователя или причинять себе телесные повреждения во время допроса. Чтобы избежать подобных ситуаций, следователь должен предусмотреть возможные варианты поведения подозреваемого, а также убрать с рабочего стола любые острые предметы, которыми может воспользоваться допрашиваемый. Если подозреваемый ранее привлекался к уголовной ответственности, его поведение, жаргон, наличие татуировок могут дать следователю определенную информацию о статусе допрашиваемого в криминальной среде, что позволит спрогнозировать его поведение и установить психологический контакт. Одним из тактических приемов подавления поведенческих конфликтов может быть процессуальное право следователя продемонстрировать вещественные доказательства, документы, протоколы других следственных действий (включая протоколы допросов), а также воспроизвести аудио- и/или видеоматериалы. Тактически оправдано представление доказательств в порядке возрастания убедительности и доказательной ценности.

Данная типология условна, поскольку поведение некоторых преступников нельзя отнести ни к одной из перечисленных групп или, наоборот, они образует смешанный тип. Для успешного допроса следователь должен четко понимать, какую информацию и какими методами он намеревается получить. В то же время знание наиболее типичных психологических характеристик тех или иных преступников и причин совершения преступлений имеет большое значение для выбора наиболее эффективной тактики их допроса. Таким образом, при подготовке к допросу следователь должен изучить личностные особенности опрашиваемого.

## Список литературы

1. Антонян Ю.М., Голубев В.П., Кудряков Ю.Н. Личность корыстного преступника. Томск, 1989. 160 с.

2. Антонян Ю.М., Еникеев М.И., Эминов В.Е. Психология преступника и расследования преступлений. М., 1996. 336 с.

3. Долинин В.Н., Рачева Н.В. Особенности расследования грабежей и разбойных нападений, совершаемых на открытой местности: учеб.-метод. пособие. Екатеринбург: Изд-во Уральского юридического института МВД России, 2002. 82 с.

***О.С. Заливохина**, аспирант Российского государственного университета правосудия, г. Москва*

## О НЕКОТОРЫХ ВОПРОСАХ ПРОГНОЗИРОВАНИЯ ИНФОРМАТИЗАЦИИ СУДЕБНО-ЭКСПЕРТНОЙ ДЕЯТЕЛЬНОСТИ

Одной из ключевых функций общей теории судебной экспертизы является прогностическая функция, служащая методологической и операционной основой частной теории экспертного прогнозирования. Однако следует отметить, что на сегодняшний день теория экспертного прогнозирования находится в зачаточном состоянии. Это объясняется отсутствием актуальных научно-исследовательских работ в данной области. Очевидно, что описание и моделирование процесса прогнозирования является сложной задачей, поскольку прогноз, хотя и опирается на исходные данные о прошлом и настоящем объекта, всегда ориентирован на будущее. Реализация или же нереализация прогноза зависит не только от качества исходных данных об объекте, знаний закономерностей развития объекта, качества операций по прогнозированию и оценки прогноза, но и от множества случайных факторов.

В настоящее время особую актуальность в научных исследованиях приобретают такие общенаучные подходы, как информационный, кибернетический, синергетический и др. Например, раскрытие и расследование преступлений в криминалистике рассматриваются как кибернетические (управляемые) про-

цессы [1, с. 231]. Данный аспект заслуживает внимания, поскольку прогнозирование является одной из задач подсистемы наблюдения в кибернетической системе. Наблюдение (контроль) представляет собой базовую функцию системы управления и включает в себя сглаживание — ретроспективную оценку объекта, фильтрацию — оценку объекта на данный момент времени и, наконец, прогнозирование — оценку на будущее. Причем прогнозирование является наиболее сложной задачей, осуществить которую представляется возможным только при соблюдении принципов рационального управления. В частности, необходимо обеспечить наличие обратной связи от объекта управления, по которому должна передаваться осведомляющая информация об управляемом объекте к управляющему. Кроме того, важно достичь независимости подсистемы наблюдения, решающей задачу прогнозирования, от внешних указаний и целей (политических, экономических и т.п.).

Однако даже при выполнении всех базовых требований для обеспечения рационального управления и использовании уже разработанной в кибернетике абстрактной концептуальной модели кибернетической системы, еще нельзя говорить о познании сущности процесса экспертного прогнозирования и завершенности модели. Это объясняется сложностью данного процесса, поскольку согласно теореме К. Гёделя о неполноте сложный динамический объект (процесс) невозможно описать в рамках одной модели, требуется множество взаимосвязанных частных моделей, упорядоченных по уровням иерархии. Например, если говорить о судебно-экспертной деятельности, которая также является сложным объектом, то теория судебной экспертизы дает целостное представление о ней, разрабатывая целый ряд учений и моделей, которые интегрируются в единую теорию. Тем не менее любая модель реального сложного объекта в той или иной степени субъективна, поскольку зависит от целей, которые преследует субъект ее разрабатывающий, а также от его компетентности. Так, можно утверждать, что сама общая теория судебной экспертизы находится в процессе развития, поскольку в настоящее время существует несколько научных школ, представляющих разные взгляды на ее структуру и содержание.

Несмотря на это, нельзя отрицать, что одной из функций теории является прогнозирование. В целом прогностическая функция общей теории судебной экспертизы проявляется в следующих направлениях: прогнозирование расширения и пополнения круга объектов экспертизы; прогнозирование расширения арсенала частнонаучных и специальных методов экспертного исследования; прогнозирование интеграционных процессов в области указанных методов; прогнозирование путей развития технического арсенала экспертов; прогнозирование развития и совершенствования организационных и методических основ и форм комплексирования методов экспертного исследования [2, с. 61].

Соответственно, в круг задач частной теории экспертного прогнозирования входит прогнозирование: путей развития собственно теории судебной экспертизы и входящих в ее содержание частных теорий; путей развития объекта теории — практической экспертной деятельности и методов этой деятельности; организационных и методических основ этой деятельности [2, с. 102].

Говоря о прогнозировании развития информационного обеспечения судебно-экспертной деятельности, следует исходить из общей направленности процессов информатизации. Очевидно, что по мере совершенствования компьютерной техники данные процессы будут ярче проявляться в судебно-экспертной деятельности.

Так, руководствуюсь современным состоянием и тенденциями информатизации, уже сейчас можно формировать прогнозы относительно развития информационной системы технического обеспечения судебно-экспертной деятельности по следующим направлениям.

Первое направление — это расширение арсенала компьютерной техники и программного обеспечения, используемого экспертами. Данное направление включает в себя, во-первых, внедрение в экспертную практику компьютеров и компьютеризированных приборов нового поколения; во-вторых, создание специализированного программного обеспечения для экспертов, ориентированного на решение задач конкретного вида экспертизы; в-третьих, адаптацию уже разработанных и применяемых в иных областях новых технологий для нужд судебной экспертизы. Говоря о третьем аспекте, можно упомянуть о тех-

нологии 3D-моделирования, которая относительно недавно проникла в экспертную практику, но была успешно адаптирована для целей судебно-медицинской, баллистической, трасологической и других экспертиз. Также представляется перспективным использование в экспертной практике 3D-печати для создания материальных (физических) моделей, в том числе биологического происхождения, и технологии виртуальной реальности, прежде всего, для решения реконструкционных задач.

Второе направление заключается в создании новых и совершенствование уже разработанных АРМ экспертов с учетом их специализации. АРМ должны быть просты в использовании, эргономичны, функциональны и, кроме того, доступны.

Также представляется возможным строить прогнозы относительно развития информационной системы научно-методического обеспечения судебно-экспертной деятельности. Основными тенденциями в данной области является расширение спектра специальных знаний эксперта, обусловленное объективной необходимостью работы с новыми технологиями, а также появлением новых объектов экспертизы, и разработка новых методов экспертного исследования. Одной из проблем, актуальных для любого вида экспертизы, является объективизация ее результатов. Решение данной проблемы достигается путем внедрения в экспертную практику методов математического моделирования. В настоящее время получила развитие математическая модель искусственной нейронной сети, которая в будущем может быть адаптирована и для целей судебной экспертизы.

Важным аспектом является и тенденция перехода системы научно-методического обеспечения судебно-экспертной деятельности в электронный формат. Ярким примером может выступать оцифровка библиотечного фонда, возможность получения архивных справок в электронном виде и т.д. Таким образом, в ближайшем будущем эксперт может получить возможность знакомиться со всей интересующей его литературой и иной информацией с персонального компьютера, подключенного к сети Интернет.

Очевидно также, что в дальнейшем роль сети Интернет как источника информации и средства коммуникации в экспертной практике будет возрастать. Развитию Интернета уделено особое внимание в Стратегии развития информационного общества в Российской Федерации на 2017-2030 гг., утв. Указом Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» (далее — Стратегия развития информационного общества). Данный документ не только предусматривает формирование единого развитого информационного пространства, но и предписывает принять меры для обеспечения безопасности и конфиденциальности пользователей. Последнее особенно важно в контексте информационного обеспечения судебно-экспертной деятельности. Кроме того, реализация Стратегии развития информационного общества предполагает развитие российских компьютерных технологий, что также отразится и на информационной системе технического обеспечения судебной экспертизы.

Что касается прогнозирования информационного обеспечения судебно-экспертной деятельности в части исходной информации, предоставляемой эксперту, то по мере совершенствования компьютерной техники следует ожидать расширение перечня объектов экспертизы, появления новых, нетрадиционных вопросов, требующих разрешения экспертом. Материалы дела, предоставляемые эксперту, также должны претерпеть качественные изменения. Помимо традиционных постановлений, определений о назначении экспертизы, протоколов осмотра и т.п., эксперту могут предоставляться, например, 3D-модели места происшествия, что уже используется за рубежом. В целом необходимо отметить, что процессы информатизации протекают в криминалистике даже более активно, нежели в судебно-экспертной деятельности. Поэтому развитие рассматриваемой информационной системы исходной экспертной информации во многом зависит от развития криминалистических средств обнаружения, фиксации и изъятия следов.

Представляется, что составляющие информационное обеспечение судебно-экспертной деятельности подсистемы организационно-правового регулирова-

ния и информации, полученной в ходе и по результатам исследования, являются наиболее латентными для целей экспертного прогнозирования.

Так, подсистема организационно-правового обеспечения наиболее подвержена влиянию внешних, не связанных непосредственно с экспертной деятельностью, управляющих воздействий. Стратегия развития информационного общества предусматривает совершенствование нормативно-правового регулирования не только в области информационно-телекоммуникационных технологий, но и в иных направлениях. Поскольку, как отмечалось ранее, нельзя отрицать влияние информатизации на судебно-экспертную деятельность, логично сделать вывод о необходимости реформирования законодательства в данной сфере.

Однако прогнозирование изменений нормативно-правового регулирования судебно-экспертной деятельности в настоящее время видится затруднительным. Это объясняется тем, что объективные предпосылки к реформированию законодательства в области судебной экспертизы появились уже достаточно давно, однако не нашли соответствующего отклика у законодателя [3, с. 186-187]. В связи с этим следует заключить, что зависимость процесса развития законодательства от политической воли фактически исключает возможность объективного прогнозирования. Кроме того, прогнозирование изменений нормативно-правового регулирования судебно-экспертной деятельности можно отнести к задачам теории судебной экспертизы лишь с определенной долей условности. Очевидно, что для формулирования такого прогноза необходимо привлекать экспертов, обладающих большим опытом и способных дать оценку пробелов и коллизий законодательства, негативно влияющих на их практику, однако в конечном счете правовые нормы являются предметом изучения юриспруденции.

С другой стороны, нельзя не отметить, что в последние годы повысилась доступность правовой информации: о деятельности государственный органов, о принятых нормативных правовых актах, рассматриваемых законопроектах. Например, эффективно функционирует и продолжает развиваться ГАС «Правосудие» и другие системы. Кроме того, завершается процесс подключения всех судов Российской Федерации к единой информационной сети, оснащение их системой видеоконференц-связи в целях обеспечения эффективного взаимодей-

ствия. Исходя из этого, представляется возможным строить прогнозы о создании единого информационного пространства взаимодействия судов, органов расследования и экспертных учреждений с использованием новых компьютерных технологий. Это позволит частично решить практические проблемы, возникающие при необходимости оперативного взаимодействия эксперта с лицом, назначившим экспертизу. Например, если требуется заявить ходатайство о предоставлении в распоряжение эксперта дополнительных материалов, без которых проведение исследования невозможно или нецелесообразно. Такие ходатайства нередко теряются, долго рассматриваются, что влечет к увеличению срока производства экспертизы. Помимо этого, создание единого информационного пространства позволит повысить эффективность взаимодействия экспертов и экспертных учреждений между собой, что особенно актуально при производстве комплексных и комиссионных экспертиз.

Говоря непосредственно об организации труда экспертов, следует отметить перспективность внедрения в экспертные учреждения новых организационных технологий, представляющих собой совокупность эффективных методов (программ, процедур) реализации управляющих решений и поддержания информационных связей, контроля и подготовки персонала, планирования и отчетности [4, с. 89-90].

Таким образом, можно заключить, что в настоящее время теория экспертного прогнозирования находится на первоначальном этапе своего развития. Тем не менее использование общенаучных подходов и методов, анализ современного состояния и устойчивых тенденций информатизации в целом и судебно-экспертной деятельности в частности позволяет формировать прогнозы относительно состояния информационного обеспечения указанной деятельности.

Так, на данном этапе представляется возможным прогнозировать следующее: расширение арсенала компьютерной техники и программного обеспечения, используемого экспертами; создание новых и совершенствование уже разработанных АРМ экспертов с учетом их специализации; расширение спектра специальных знаний эксперта, обусловленное объективной необходимостью работы с новыми технологиями; появление новых объектов и методов (особен-

но модельных) экспертного исследования; переход системы научно-методического обеспечения судебно-экспертной деятельности в электронный формат и повышение роли сети Интернет; создание единого информационного пространства взаимодействия судов, органов расследования и экспертных учреждений с использованием новых компьютерных технологий; внедрение в практику экспертных учреждений новых организационных технологий.

**Список литературы**

1. Ефремов Д.А. Философские и кибернетические основы функционирования информации в деятельности по расследованию преступлений // Вестник СГЮА. 2014. № 2 (97).

2. Аверьянова Т.В. Судебная экспертиза. Курс общей теории: монография. М.: Норма: ИНФРА-М, 2015.

3. Волынский А.Ф. Реформа судебно-экспертной и технико-криминалистической деятельности как необходимость // Вестник Московского университета МВД России. 2018. № 3. С. 186-187.

4. Ловцов Д.А. Информационная теория эргасистем: Тезаурус. М.: Наука, 2005. С. 89-90.

***В.Ю. Иванов,*** *преподаватель кафедры криминалистики Уральского юридического института МВД России, г. Екатеринбург*

## О ВОЗМОЖНОСТИ ПРОИЗВОДСТВА ДОПРОСА СВИДЕТЕЛЯ ПОСРЕДСТВОМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ В УСЛОВИЯХ ПАНДЕМИИ КОРОНАВИРУСНОЙ ИНФЕКЦИИ

Информационно-телекоммуникационные технологии все больше проникают в жизнь современного человека. Деятельность по расследованию уголовных дел также видоизменяется, совершенствуются способы раскрытия и расследования преступлений, модифицируются способы производства следствен-

ных действий. Так, еще в 2011 г. были внесены изменения в ст. 240 Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ), а также была введена ст. 278.1 УПК РФ [1]. Данные нормы позволили суду производить допрос свидетелей и потерпевших посредством использования системы видеоконференц-связи.

Судебная практика свидетельствует, что данная норма активно применяется в практической деятельности и способствует реализации таких процессуальных принципов, как рассмотрение дела в разумный срок, полное и всестороннее исследование всех обстоятельств уголовного дела и минимизирует время следователя (дознавателя).

Анализ становления правовых основ использования видеоконференц-связи в сфере уголовного судопроизводства показывает, что эта современная и эффективная технология в Российской Федерации применяется повсеместно, и ее преимущества зримо отражаются в статистических показателях о деятельности судов общей юрисдикции. По официальным данным, в судах общей юрисдикции ежегодно проводится более 800 сеансов связи более чем в 160 000 судебных процессах в год. В течение 13 лет произведено более 650 000 видеоконференций [2, с. 160].

Современное общество в XXI в. во всем мире столкнулось со значительной проблемой, поработившей практически весь мир. Пандемия COVID-19 вызванная коронавирусом SARS-CoV-2 во многом дала сбой в привычном образе жизни граждан практически всех стран, затронув все сферы жизнедеятельности. Безусловно, данная проблема затронула и органы государственной власти. Правоохранительным органам стало сложнее и опаснее работать в новых реалиях, так как данная инфекция нового типа смогла подтолкнуть криминальный мир к увеличению преступности в информационно-телекоммуникационной сфере. В настоящее время преступления в сфере IT-технологий стали привычным явлением, поскольку определенная часть людей перешла на удаленную работу и свою профессиональную деятельность осуществляют дистанционно.

Некоторая часть людей находится на самоизоляции в связи с подтвержденным диагнозом коронавирусной инфекции, а также пребывают по месту жительства по случаю контактирования с такими людьми. Данные лица могут находиться в каком-либо процессуальном статусе при осуществлении расследования по уголовному делу, что, соответственно, затрудняет производство следственных действий с их участием.

В настоящее время уголовно-процессуальное законодательство нуждается в изменениях по предоставлению возможности следователю (дознавателю) производить следственные действия в режиме видеоконференц-связи.

Действительно, данный положительный опыт использования видеоконференц-связи в суде целесообразно перенять и на досудебную стадию уголовного судопроизводства.

Разработка данной нормы в законодательных органах ведется относительно давно, но в настоящее время поправки не вступили в силу. Предложенные изменения значительно облегчат работу следователям, будут способствовать более качественному и эффективному расследованию преступлений и сократят срок производства по уголовному делу.

Нельзя не согласиться с мнением председателя Комитета Совета Федерации по экономической политике А.В. Кутеповым, который подготовил данный проект поправок в УПК РФ, по его мнению, «такой шаг избавит правоохранительную систему от лишних материальных и временных затрат, так как неявка свидетелей или потерпевших, проживающих в другом городе или регионе, становится весомым основанием для бесконечных продлений сроков следствия» [3].

Положительно поправки отметил и статс-секретарь Федеральной палаты адвокатов К.Э. Добрынин, пояснив, что «введение дистанционной формы допроса также позволит обезопасить свидетелей в том числе от внепроцессуального давления» [4].

Предполагается, что изменения в уголовно-процессуальном законе коснутся ст. 5 УПК РФ, которая дополнится п. 8.1 следующего содержания: «Допрос посредством видеоконференц-связи — это допрос, который проводится с ис-

пользованием технических средств и программного обеспечения для персонального компьютера, мобильных устройств и браузера, обеспечивающих передачу звука и изображения в реальном времени» [5].

По нашему мнению, данные поправки являются как никогда актуальными в период пандемии COVID-19. В рассматриваемом случае дополнения нового положения в УПК РФ значительно помогло бы в работе следователю (дознавателю). Производство следственного действия как допрос с человеком, находящемся на самоизоляции, было бы крайне сложным без видеоконференц-связи. Также допрос лица дистанционным образом посредством современных технологий имеет существенные плюсы и преимущества. Использование систем видеоконференц-связи не только в суде, но и на стадии предварительного расследования:

- будет способствовать осуществлению уголовного судопроизводства в разумный срок;
- производство допроса при помощи систем видеоконференц-связи помогло бы допрашиваемым лицам находится в комфортной для них обстановке для дачи показаний;
- использование данных систем видеоконференц-связи способствовало бы получению наиболее полных, достоверных, информативных показаний со стороны допрашиваемого лица;
- полученные с помощью системы видеоконференц-связи показания помогут следователю в составлении не только процессуальных документов (протокол допроса), но и также будут фиксироваться посредством записи произведенного допроса. В свою очередь, запись отражала бы все действия со стороны следователя и допрашиваемого лица. Также данная запись исключала бы возможность подачи жалобы на неправомерные действия следователя при производстве следственного действия. Ведь на записи отражались бы все этапы производимого следственного действия (допроса лица).

Не следует забывать, что в данном случае также видеоконференц-связь имеет место быть при допросе лица, который болеет коронавирусной инфекцией. Участие в допросе в период пандемии может быть сопряжено с угрозой за-

ражения COVID-19 других участников уголовного судопроизводства, поскольку допрашиваемому потребуется нарушить режим самоизоляции, добраться до следственного отдела, длительное время присутствовать на допросе в замкнутом пространстве, а затем возвращаться домой. Проблема становится еще более актуальной, когда допрашиваемое лицо относится к группе риска по коронавирусной инфекции (возраст старше 65 лет, наличие ряда хронических заболеваний). В данной ситуации представляется разумным заявить ходатайство об отложении допроса до окончания действия ограничительных мер по распространению коронавирусной инфекции, либо проводить допрос посредством видеоконференц-связи, если самочувствие допрашиваемого лица позволит провести данное следственное действие.

На основании всего вышесказанного следует учесть, что со временем мир прогрессирует и растет в сфере компьютерных технологий, правда, касается этот прогресс не всех сторон жизни человечества. Настоящее законодательство бы сильно пострадало от внесения постоянных новшеств в законодательство на фоне прогрессирования общества и мира в целом. Уголовно-процессуальное законодательство также меняется на фоне развития общества, но следует сказать, что пробелы в нормах остаются и по сей день, также возможны противоречия в нормах. Одним из противоречий как раз и выступает видеоконференц-связь, так как данное понятие введено в УПК РФ, правда используется не в отношении всех участников уголовного судопроизводства и не на всех стадиях. Например, видеоконференц-связь чаще всего применяют на станциях апелляционного производства и в нормах УПК РФ об этом сказано. Почему же нельзя ввести данный процесс в настоящее время на всех стадиях уголовного судопроизводства во время пандемии коронавирусной инфекции? Ответ на данный вопрос пока невозможно дать в связи с малым процентным соотношением таких ситуаций с лицами, участвующими в уголовном судопроизводстве с диагнозом коронавирусной инфекции.

Следует отметить, законопроект о возможности производства допроса по видеоконференц-связи несет в себе действительно позитивный мотив, данное новшество помогло бы следователям (дознавателям) в производстве след-

ственного действия. Следует сказать, что видеосвязь существовала и раньше, например, иной раз она помогала в построении диалога с лицом, находящимся в местах лишения свободы, который не имеет возможности присутствовать в зале суда. Данное новшество позволит допрашивать свидетелей посредством видеоконференц-связи на стадии предварительного следствия с соблюдением основных правил и требований производства расследования по уголовному делу и с учетом особенностей допроса несовершеннолетних лиц [6, с. 4].

Видеодопрос свидетеля сократил бы срок предварительного расследования, так как существуют ситуации, когда свидетель может находиться на большом удалении от органа предварительного следствия, а это в свою очередь может служить поводом для продления разумного срока. Став очевидцем преступления в одном регионе Российской Федерации, лицо по личным обстоятельствам может его покинуть (возвращение в место постоянного проживания, переезд на постоянное место жительства, командировка, отбывание наказания и др.), что делает достаточно затруднительным обеспечение явки свидетеля к следователю для допроса. Выезд следователя в местонахождение свидетеля требует дополнительных временных и материальных затрат. При этом не стоит забывать, что у следователя в производстве находится не одно уголовное дело, и его выезд для допроса одного свидетеля будет также затягивать сроки расследования по другим уголовным делам.

Несомненно, следует указать о полезности использования видеоконференц-связи при заболевании коронавирусной инфекцией, так как данная пандемия поработила большую часть населения и поставила некоторые сферы деятельности в состояние регресса. В данном случае видеоконференц-связь помогла бы помочь следователю взаимодействовать со всеми участниками уголовного судопроизводства, которые находятся на самоизоляции с диагнозом коронавирусной инфекции.

Таким образом, данная норма является актуальным средством получения криминалистически значимой информации от свидетеля в ситуации, когда он находится на самоизоляции в условиях пандемии инфекции COVID-19, вызванной коронавирусом SARS-CoV-2. Законодательная норма, предусматрива-

ющая введение новой статьи в УПК РФ — ст. 189.1 «Особенности допроса свидетеля посредством видеоконференц-связи», является правильным решением в период пандемии коронавирусной инфекции. Помимо этого, допрос свидетеля стал бы проводиться намного экономичнее как с точки зрения финансовой составляющей, так и времени следователя.

## Список литературы


1. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 20 марта 2011 г. № 39-ФЗ // Собр. законодательства Рос. Федерации. 28.03.2011. № 13. Ст. 1686.
2. Поддубняк А.А., Евдокимова И.С. Допрос свидетеля посредством видеоконференц-связи на стадии предварительного расследования как новелла Российского законодательства // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2018. Т. 4 (70). № 3. С. 159–165.
3. Адвокатская газета // Проект поправок в УПК, предусматривающих онлайн-допросы свидетелей и потерпевших, доработан [Электронный ресурс]. URL: https://www.advgazeta.ru/novosti/proekt-popravok-v-upk-predusmatrivayus05%20УПК%20предлагается%20дополнить,и%20изображения%20в%20реальном%20времени» (дата обращения: 24.05.2021 г.).
4. Коллегия адвокатов Таможенный адвокат // Проект поправок в УПК, предусматривающих онлайн-допросы свидетелей и потерпевших, доработан [Электронный ресурс]. URL: http://www.customs-advocate.ru/ru/news/sendvalues/hchikh-onlayn-doprosy-svideteley-i-poterpevshikhdorabotan/#:~:text=Статью%2more/2582/#:~:text=По%20мнению%20статссекретаря%20ФПА%20Константина,и%20потерпевших%20по%20уголовным%20дела» (дата обращения: 27.05.2021 г.).
5. Российская газета // Предлагается разрешить следствию проводить допросы свидетелей по видео [Электронный ресурс]. URL: https://rg.ru/2020/10/29/sledstviiu-mogut-razreshit-provodit-doprosy-svidetelej-po-videosviazi.html (дата обращения: 28.05.2021 г.).

6. Новиков С.А. Допрос с использованием систем видеоконференц-связи: завтрашний день российского предварительного расследования // Российский следователь. 2014. № 1. С. 2–6.

***А.В. Казакова,*** *к.ю.н., доцент кафедры судебной деятельности и уголовного процесса Уральского государственного юридического университета, г. Екатеринбург*

## ВОПРОСЫ ПРИМЕНЕНИЯ СИСТЕМЫ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ ПРИ ПРОИЗВОДСТВЕ ДОПРОСА

Развитие информационных технологий приводит к постепенному их внедрению в деятельность государственных, в том числе правоохранительных органов и судов с целью упрощения работы и повышения ее эффективности.

В 2011 г. в Уголовно-процессуальный кодекс Российской Федерации (далее — УПК РФ) была введена ст. 278.1, которая позволяет допрашивать во время судебного заседания свидетеля, находящегося на территории другого региона посредством системы видеоконференц-связи (далее — ВКС)[13]. Обоснованием новеллы явилась попытка по снижению судебных издержек (прежде всего связанных с проездом до места разбирательства, проживанием и т.д.) и облегчению работы судебного аппарата.

Анализируемая норма права повлекла дискуссии среди теоретиков и практиков, что повлекло фундаментальные теоретические исследования [1].

УПК РФ не содержит разрешения на применение ст. 278.1 УПК РФ к лицам, находящихся за границей (вне территории РФ). Это является защитой российского суверенитета, так как не во всех государствах законодательно закреплено использование ВКС. При допросе свидетеля на территории иностранного

[13] Федеральный закон №39-ФЗ от 20.03.2011 г. «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2011. 25 марта.

государства обязательно возникнет вопрос о применении иностранного процессуального права к следственному действию.

Схематично применение ВКС в судебном заседании выглядит следующим образом.

Решение о применении ВКС фиксируется в постановлении о назначении судебного заседания. Если этот вопрос возник в ходе судебного разбирательства, то суд принимает его в совещательной комнате и оформляет в виде отдельного постановления [2, с. 27], несмотря на то, что правила ст. 256 УПК РФ не содержат такого требования.

Суд, рассматривающий дело по существу, передает поручение об организации допроса свидетеля суду по месту нахождения последнего. Председатель получившего данный документ суда передает его для исполнения одному из судей, который обязан выполнить ряд действий:

1) поручить техническому персоналу данного суда включить и настроить систему ВКС;

2) если есть необходимость, то обеспечить участие переводчика;

3) информировать суд, рассматривающий дело, о явке свидетеля;

4) удостоверить личность свидетеля, после чего отобрать подписку о разъяснении прав/обязанностей/ответственности;

5) после окончания следственного действий направить подписку, копию паспорта, протокол допроса и документы, предоставленные свидетелем по почте в суд, рассматривающий дело.

Сам допрос осуществляет суд, рассматривающий дело. Как правило, этот же суд вызывает свидетеля на допрос повесткой, а в случае неявки по неуважительным причинам принимает решение о приводе и направляет его в службу судебных приставов по месту проведения допроса.

Допрос проводится по общим правилам. Примечательно, что стороны не вправе заявить отвод судье-исполнителю. Это положение представляется логичным, поскольку судья-исполнитель выполняет исключительно организаци-

онную (техническую) функцию и не вправе принимать какие-либо решения по уголовному делу.

Если ввиду технических неполадок невозможно провести трансляцию, то суду целесообразно исследовать другие доказательства, а допрос провести позже.

Следует указать на препятствия применения ВКС при допросе:

1. Недостаточное техническое обеспечение, так как необходимым оборудованием оснащены только суды субъектов РФ и Верховный Суд РФ. В ряде районных судов и у мировых судей отсутствует необходимое оборудование.

2. Использование неспециализированных систем (например, Skype) нежелательно, но напрямую и не запрещено.

3. Отсутствует нормативная регламентация по вопросу возможности допроса с использованием ВКС других участников процесса (эксперта, специалиста, потерпевшего, гражданского истца, ответчика и т.д.). Данное положение представляется существенным пробелом в уголовно-процессуальном законодательстве.

4. Потенциальная возможность технических сбоев в виде некачественного изображения или звука и т.д. Так, при рассмотрении апелляционной жалобу по делу № 19-9/2018 в отношении С., который обвинялся в совершении преступления, предусмотренного ч. 1 ст. 291.2 УК РФ в феврале 2018 г. возникла проблема технического характера: на мониторе не было видно подсудимого; шел только звук [3, с. 6].

5. Невозможность использования ВКС на досудебных стадиях.

Несмотря на массу плюсов, не все участники уголовного судопроизводства настроены на онлайн-заседание. Например, адвокат Центральной коллегии адвокатов г. Владимира М.А. Никонов приводит интересный пример: суд обязал стороны участвовать в судебном заседании посредством ВКС. Технических проблем не возникло, стороны донесли свои позиции. Первый кассационный суд общей юрисдикции удовлетворил кассационную жалобу защитника, отменил обвинительный приговор и апелляционное постановление и направил уголовное дело в отношении осужденного на новое рассмотрение в суд первой ин-

станции. Как отмечает адвокат, возможность использования ВКС не должна реализовываться в приказном порядке — подобно тому, как сейчас это происходит с участием обвиняемых вне зависимости от их ходатайств о личном присутствии в суде. Выбор из двух опций участия (лично или по видео) должна делать именно сторона защиты — необходимо согласие защитника и его доверителя на это [11, с. 10].

Ю.С. Курочкина полагает, что для использования ВКС на досудебных стадиях нет необходимости вносить изменения в закон, так как УПК РФ позволяет использовать любые технические средства, а поскольку использование ВКС допустимо на этапе судебного производства, то применима аналогия закона [4, с. 306].

Первое использование системы ВКС датировано 1999 г., за 20 лет с ее помощью было разрешено более 350 000 уголовных дел [5].

Полагается, что хорошие результаты использования ВКС во время судебного разбирательства привело к внесению в Государственную Думу законопроекта №434998-7, в котором предлагается установить возможность использования ВКС в досудебном производстве при допросе свидетеля[14]. По проекту: следователь, в производстве которого находится уголовное дело, вправе направить специальное постановление в орган предварительного расследования по месту нахождения свидетеля. Допрос будет производить следователь, в производстве которого находится уголовное дело, а вопросы по организации связи, удостоверению личности свидетеля и составлению протокола передаются в ведение следователя, который находится рядом с допрашиваемым. Протокол и иные документы должны быть направлены следователю, который ведет дело. Имеется требование о подписях обоих следователей в протоколе допроса. Однако данный законопроект не был одобрен.

Своеобразное объяснение этому положению содержится, предположительно, в мнении ряда ученых о том, что проведение следственного действия с си-

[14] Консультант Плюс: справ.-правовая система. [Электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=170953#022543185550200584 (дата обращения: 28.05.2021). Код доступа: по паролю.

стемой ВКС противоречит ч. 1 ст. 187 УПК РФ, содержащей требование о проведении допроса по месту производства предварительного следствия [6, с. 125].

Небезынтересной представляется точка зрения О.В. Мичуриной: научно-технический прогресс прошел мимо УПК РФ, особенно это касается досудебной части отечественного уголовного процесса, хотя все предпосылки к нормативному совершенствованию в этом направлении имеются. Так, несмотря на активное применение видеоконференц-связи при рассмотрении уголовных дел в судах, она не может использоваться в процедуре досудебного производства [7, с. 230]. Ученый полагает, что уже давно назрела необходимость перехода на более современную форму уголовно-процессуальной деятельности, что особенно актуально в условиях распространения новой коронавирусной инфекции [7, с. 231].

Н.В. Калужская также отмечает, что онлайн-допросы также невозможны и при проведении доследственных проверок в порядке ст. 144-145 УПК РФ [8, с. 143].

О.А. Машовец и Е.Ю. Никифорова полагают, что «имеются предпосылки к переходу от формального к материальному стандарту допустимости доказательства как средства удостоверения истины по уголовному делу, в основе которого должна быть верифицируемость представленной стороной информации» [10, с. 122].

При подготовке настоящих тезисов была обнаружена информация о том, что примерно с декабря 2015 г. в подразделениях Следственного управления МВД России по Хабаровскому краю при проведении очной ставки применяется ВКС [9, с. 47-49].

Процедура выглядит следующим образом: используется ВКС при применении сервиса СВКС-М, который находится в системе электронного документооборота ИСОД МВД России. Следователь на основании п. 4 ст. 38 и ч. 1 ст. 152 УПК РФ направляет поручение следователю по месту нахождения второго участника очной ставки. В назначенное время оба следователя обеспечивают явку необходимых участников к рабочим местам с компьютерами, на ко-

торых имеется выход в ИСОД МВД России. Включается электронная система, проводится очная ставка по общим правилам, установленным ст. 192 УПК РФ, при этом участникам следователь разъясняет права и обязанности, порядок производства следственного действия, а также предупреждают об использовании технических средств (компьютера, принтера, сканера) и производства видеозаписи, которая будет приобщена к делу.

Следователь, ведущий расследование, составляет протокол по ст. 166 УПК РФ.

После завершения очной ставки с протоколом допрошенного знакомит следователь, производящий следствие. После чего протокол сканируется и с использованием системы электронного документооборота ИСОД МВД России направляется на электронный адрес следователя, находящегося со вторым участником. Второй следователь распечатывает и предъявляет протокол другому допрошенному; после ознакомления подписывает, после чего протокол снова сканируется и направляется на электронный адрес первого следователя. Оба протокола приобщаются к материалам уголовного дела.

Интересная практика, поскольку, с одной стороны, следователи Хабаровского края уже имеют практический опыт по использованию ВКС, с другой — показательно, что эта система применяется только при производстве одного следственного действия — очной ставки.

Примечательно, что подобная практика распространилась и на территорию Свердловской области: в ходе расследования уголовного дела следователем СУ СКР по Свердловской области М. было принято решение о проведении очной ставки между свидетелями с использованием связи по Skype через Интернет. Возникла проблема подписания протокола с учётом положений ч. 7 ст. 166 УПК РФ. Протокол подписали по ту сторону экрана после оглашения текста вслух с последующей пересылкой (почтой) по месту производства предварительного расследования для подписания следователем и вторым свидетелем.

О.А. Машовец и Е.Ю. Никифорова отмечают, что временного разрыва в подписании протокола очной ставки (и, соответственно, пересылки почтовой

связью) можно было избежать, легализовав электронный образ процессуального документа с последующей его передачей по компьютерным сетям [10, с. 123].

Получается, что на одной чаше весов — публичный интерес, связанный с эффективным и быстрым судопроизводством, с другой — незыблемые постулаты процесса. Хотелось бы выразить надежду, что в условиях дальнейшего развития компьютерной техники возможно осуществление следственных действий посредством информационных технологий без ущерба для неукоснительного соблюдения процессуальной формы. Н.В. Калужская отмечает, что многие страны в сфере применения цифровых технологий ушли далеко вперед. Например, в Саудовской Аравии расследование большинства дел заканчивается в течение двух дней. В этой стране перешли на электронные уголовные дела 9 лет назад, активно используются онлайн-допросы на всех стадиях судопроизводства, при этом сократились сроки расследования до 80% [8, с. 143-144].

**Список литературы**

1. Архипова Е.А. Применение видеоконференц-связи в уголовном судопроизводстве России и зарубежных стран (сравнительно-правовое исследование): дисс. … канд. юрид. наук: 12.00.09. М., 2013. 198 с.

2. Долгополов Д.В. Допрос свидетеля по видеоконференц-связи: ответы на вопросы судей // Уголовный процесс. 2017. № 7. С. 26-28.

3. Новиков С.А. Допрос с использованием систем видеоконференц-связи: завтрашний день российского предварительного расследования // Российский следователь. 2014. № 1. С. 2-6.

4. Курочкина Ю.С. Проблемы проведения судебных действий следственного характера с использованием видеоконференцсвязи // Вестник КГУ. 2018. № 2. С. 305-308.

5. Кравец Е.Г., Казначей И.В. Результаты анализа проекта федерального закона «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации (в части производства предварительного расследования с примене-

нием систем видеоконференц-связи)». [Электронный ресурс]. URL: science-education.ru/pdf/2015/2/479.pdf.

6. Долгополов Д.В. Допрос свидетеля по видеоконференц-связи: ответы на вопросы судей // Уголовный процесс. 2017. № 7. С. 26-28.

7. Мичурина О.В. Оценка эффективности процедур досудебного производства зарубежных сран и возможности их имплементации в уголовный процесс России // Уголовное судопроизводство России: проблемы и перспективы развития: материалы Всероссийской научно-практической конференции. СПб., 2020. С. 228-232.

8. Калужская Н.В. Возмещение ущерба, причиненного преступлением как способ реализации конституционного права граждан в условиях развития цифровых технологий // Трансформация права и правоохранительной деятельности в условиях развития цифровых технологий в России, странах СНГ и Европейского Союза: проблемы законодательства и социальной эффективности: материалы VI Международной научно-практической конференции преподавателей, практических сотрудников, студентов, магистрантов, аспирантов (СГУ им. Н.Г. Чернышевского). Пенза, 2019. С. 142-144.

9. Авдонин К.В., Черкасов В.С. Видеоконференц-связь в следственных действиях: как правильно использовать и что поменять в УПК // Уголовный процесс. 2018. № 7. С. 46-53.

10. Машовец О.А., Никифорова Е.Ю. Вопросы теории и практики доказывания в аспекте цифровых технологий // Университетские правовые диалоги: материалы Международной научно-практической конференции, посвященной 90-летию со дня рождения профессора, доктора юридических наук, Заслуженного деятеля Высшей школы Юрия Даниловича Лившица, 29-30 марта 2019 г. / под ред. С.М. Даровских, Г.С. Русман. Челябинск: Изд. центр ЮУрГУ, 2019. С. 120-125.

11. Никонов М.А. Отмена приговора по видеоконференц-связи // Уголовный процесс. 2020. № 6. С. 10.

***В.С. Калашников,*** *к.ю.н., доцент кафедры уголовного процесса и криминалистики Кемеровского государственного университета, г. Кемерово*

# ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ СЛЕДОВ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

Представить себе современного человека, не пользующегося средствами передачи цифровых данных, в настоящее время достаточно сложно. Технический прогресс активно распространяет свои результаты во все сферы жизни и деятельности как отдельных граждан, так и различных групп. Электронный документооборот постепенно вытесняет документы на бумажном носителе, целые библиотеки помещаются на микроскопическом носителе информации, банковские и правительственные структуры осваивают блокчейн-технологии, различного рода токены участвуют в финансовом обороте наряду с ценными бумагами, выступая в ряде случаев их аналогом, вводятся и создаются цифровые валюты.

Криминалистика всегда внедряла достижения научно-технического прогресса в оперативно-розыскную и процессуальную деятельность правоохранительных органов после соответствующей адаптации. В настоящее время достаточно большое количество оперативно-значимой информации о человеке, его связях и интересах можно получить без выхода в оперативное пространство, просто с рабочего компьютера или смартфона. Некоторые люди даже не представляют, сколько следов они оставляют, используя социальные сети, мессенджеры, приложения. Разумеется, что доказательственное значение такая информация приобретает редко, однако для деятельности органов, осуществляющих оперативно-розыскную деятельность, может носить ориентирующий характер или служить основанием для получения более значимых сведений.

Естественно, что существует и оборотная сторона данной медали, так как достижения прогресса используются и в преступной деятельности. При этом органы предварительного расследования сталкиваются с проблемой обнаружения, а главное, изъятия и фиксации цифровых следов, поскольку действующее

уголовно-процессуальное законодательство существенно отстает в вопросах урегулирования использования цифровой информации в доказывании.

Криминалистические характеристики цифровой информации активно исследуются в научной юридической среде [19].

Обоснованно отмечено, что цифровые следы нельзя отнести ни к материальным, ни к идеальным следам [10]. В настоящее время внимание уделяется следующим видам цифровых следов:

- сведения с камер видеозаписи (съемка с звуковым сопровождением либо без такового может производиться как самими преступниками, так и помимо их воли) подготовки, совершения, сокрытия преступлений;
- биллинговая информация о соединениях между абонентами (абонентскими устройствами);
- информация, содержащаяся в памяти смартфона, телефона участника уголовного судопроизводства;
- криминалистически значимая информация, находящаяся в памяти домашнего (рабочего) компьютера (ноутбука, планшета, моноблока) участника;
- метаданные и иная цифровая информация различных устройств, позволяющая определить местонахождение гаджета и его владельца в интересующее следствие время;
- социальные сети как источник криминалистически значимой информации;
- сведения об истории журналов браузеров пользователя (программ просмотра содержимого сайтов);
- данные дистанционного зондирования поверхности Земли;
- цифровые данные компьютерных систем авто-, мототранспорта в раскрытии и расследовании преступлений (датчики EDR и IV) [11].

Однако указанные выше следы содержатся на конкретных устройствах. Действующее российское законодательство также пока урегулировало лишь вопросы изъятия информации, хранящейся на цифровых носителях [12], в том числе путем ее копирования [13].

Между тем современные технологии, такие как блокчейн, позволяют хранить информацию одновременно на нескольких, не связанных между собой устройствах. В технологиях распределенного реестра информация не интегрируется, а хранится блоками в информационной цепи, что обеспечивает эффективную защиту информации, так как каждая копия хранится на разных компьютерах, такая технология децентрализована и характеризуется отсутствием посредников [14]. Указанное позволяет сохранять информацию в сети даже в случае выхода из строя или вывода из цепочки нескольких носителей. Кроме того, децентрализованность позволяет изменять хранящуюся таким образом информацию с других устройств, что может повлечь вопросы с допустимостью и достоверностью доказательств, содержащихся на изъятом устройстве. Таким образом, цифровой след может и не иметь конкретного носителя, что входит в противоречие с устоявшимся в науке представлении о единстве информации и ее носителя [15].

Кроме того, активно используются при совершении преступлений, например, связанных с незаконным распространением наркотических средств, расчеты в криптовалюте, что обусловливается ее относительной анонимностью и неподконтрольностью в настоящее время государственным финансовым и контролирующим структурам. Между тем виртуальные денежные средства могут быть предметом преступного посягательства, например, хищения.

В настоящее время уголовное законодательство защищает виртуальные денежные средства, хранящиеся на банковских счетах. По сути, при использовании различного рода информационных технологий, при помощи которых происходит проникновение в базу данных банковских учреждений, равно как и при получении от владельцев счетов средств доступа к ним, осуществляется не физическое изъятие денежных средств, а изменение информации о состоянии счетов. Таким образом, до момента обналичивания хищение происходит без участия реальных денежных средств, однако законодателем и правоприменителем такие манипуляции расцениваются как преступление, наряду с хищением кошелька из кармана потерпевшего.

Известны случаи обращений граждан в правоохранительные органы в связи мошенническими действиями в отношении виртуальных объектов, имеющих для граждан определенную ценность, например, артефактов компьютерных игр. Отсюда следует, что криптовалюта, независимо от признания или непризнания ее платежным средством, может быть признана объектом преступного посягательства, поскольку представляет ценность для пострадавшего, который приобрел ее за реальные денежные средства или понес затраты в процессе так называемого «майнинга».

Кроме того, при использовании криптовалюты в наркопреступлениях или финансировании террористической деятельности она становится имуществом, подлежащим конфискации. Действующее уголовно-процессуальное законодательство не регулирует вопросы наложения ареста на криптокошельки, на которых оказалась похищенная или полученная в результате преступной деятельности цифровая валюта, изъятия средств с этих кошельков, их хранения. Не регламентирован процесс возможной реализации и обращения в доход государства криптовалюты, хотя он и является второстепенным.

На основании изложенного напрашивается вывод, что необходимо пересматривать представления криминалистики и уголовного процесса о видах следов, их характеристиках, а самое главное, искать и разрабатывать универсальные способы фиксации и изъятия цифровых следов, обеспечивающих возможность их использования в доказывании по уголовным делам. Однако для решения этих вопросов одних юридических знаний недостаточно, поскольку в первую очередь решать проблемы необходимо техническим путем, а именно, разработать с последующим внедрением в деятельность правоохранительных органов технологии, позволяющие блокировать виртуальные транзакции между криптокошельками, отслеживать движение виртуальных средств и устанавливать принадлежность виртуальных адресов конкретным физическим устройствам, при помощи которых осуществляется доступ к ним и т.п. А пока лицу, в производстве которого находится уголовное дело, при обнаружении на просторах Интернета доказательственной информации необходимо при помощи

компьютера, фотоаппарата, смартфона и иных научно-технических средств, желательно с участием понятых и видеосъемки, создавать производные доказательства в виде иных документов, что хотя и трудозатратно, но в настоящее время не вызывает сомнений у суда в их достоверности.

## Список литературы


1. Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: дис. ... д-ра юрид. наук. Волгоград, 2008.
2. Воскобитова Л.А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex Russica. 2019. N 5.
3. Гриб В.Г., Тюнис И.О. Криминалистика и цифровые технологии // Российский следователь. 2019. N 4.
4. Зазулин А.И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2018.
5. Мещеряков В.А. Цифровая криминалистика // Библиотека криминалиста. 2014. N 4.
6. Пастухов П.С. Роль и значение специальных знаний в информационно-технологическом обеспечении уголовно-процессуального доказывания // Вестник Пермского университета. Юридические науки. 2014. N 1.
7. Романенко М.А. Новый подход к содержанию криминалистической системы криминалистической техники // Вестник Пермского университета. 2008. N 2.
8. Чернышов В.Н., Лоскутова Е.С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т. 12. N 5.
9. Шелегов Ю.В., Шелегов В.Г. К вопросу о классификации электронных (цифровых) доказательств // Криминалистика: вчера, сегодня, завтра. 2019. N 2.

10. Бахтеев Д.В., Смахтин Е.В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2019. № 6. С. 61-68.

11. Скобелин С.Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. 2020. № 4. С. 42-44.

12. Гаврилин Ю.В. Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России // Труды Академии МВД России. 2018. № 3.

13. Овсянников Д.В. Копирование электронной информации как средство уголовно-процессуального доказывания: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2018.

14. Кириллова Е.А. Правовой статус и принципы использования технологии больших данных (Big Data) // Российская юстиция. 2021. № 2. С. 68-69.

15. Балакшин В.С. Оценка допустимости доказательств в российском уголовном процессе: монография. М., 2016. С. 109.

***А.Н. Калюжный**, к.ю.н., доцент, сотрудник Академии ФСО России, г. Орел*

## ОТДЕЛЬНЫЕ АСПЕКТЫ ПРОВЕДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ, НАПРАВЛЕННЫХ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ТЕХНИЧЕСКИМ КАНАЛАМ СВЯЗИ В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ СВОБОДЫ ЛИЧНОСТИ

В настоящее время получили широкое распространение различные коммуникационные средства: Интернет, устройства мобильной связи, социальные сети, мессенджеры и другие — выступают неотъемлемыми частями повседневной жизнедеятельности граждан. Техническое развитие общества активно используется преступниками в ходе совершения преступлений против свободы личности: для связи между соучастниками; общения с жертвами преступлений и их

родственниками (предъявления требований о выкупе, выполнения определенных условий и т.п.); поиска потенциальных клиентов «услуг», оказываемых потерпевшими; установления третьих лиц, желающих купить человека.

Криминалистически значимая информация, передаваемая по современным коммуникационным средствам, предопределяет необходимость субъектов расследования использовать возможности оперативно-розыскных мероприятий для отслеживания и документирования преступных действий виновных, осуществления оперативного контроля за деятельностью преступников, поддерживания с фигурантами определенных контактов и в конечном итоге — изобличения преступной деятельности.

Проведение оперативно-розыскных мероприятий позволяет выявить данные, отражаемые при использовании коммуникационных средств, установить местонахождение потерпевших, выявить лиц, совершивших посягательства на свободу личности, зафиксировать их преступную деятельность. Одними из наиболее информативных оперативно-розыскных мероприятий, устанавливающих многоплановую криминалистически значимую информацию, используемую в дальнейшем в расследовании преступлений, являются снятие информации с технических каналов связи (78,2% уголовных дел, где проводились ОРМ) и прослушивание телефонных переговоров (45,6% дел, где проводились ОРМ).

Учитывая особенности предмета исследования рассматриваемой нами тематики, ее объем и изученность другими авторами, не будем останавливаться на специфике и технологиях легализации и использования результатов оперативно-розыскной деятельности в уголовном судопроизводстве. Несмотря на имеющиеся до настоящего времени дискуссии [1, с. 120-125; 2, с. 78-80; 3, с. 1248] о возможности и порядке интерпретации результатов оперативно-розыскной деятельности, отметим справедливость высказывания профессора Е.А. Доля: «…результаты оперативно-розыскной деятельности могут послужить лишь основой для формирования доказательств в уголовном процессе»

[4, с. 25], поскольку должны быть оформлены и представлены в соответствии с требованиями уголовно-процессуального законодательства[15].

Одним из наиболее криминалистически информативных оперативно-розыскных мероприятий, восполняющих дефицит информации по поступившему сообщению о совершении посягательства на свободу личности, а также возбужденному уголовному делу по данному факту, является снятие информации с технических каналов связи. Рассматриваемое мероприятие осуществляется на основании судебного решения, посредством использования специальных технических средств, с помощью которых проводится негласный контроль и фиксация данных, передаваемых фигурантами по техническим каналам связи [5, с. 353].

При обращении к субъектам расследования родственников похищенного у последних выясняется номер мобильного телефона жертвы, после чего в ходе реализации оперативно-розыскного мероприятия снятие информации с технических каналов связи может быть получена следующая криминалистически значимая информация: номер SIM-карты абонента, IMEI мобильного телефона, дата, время и продолжительность соединения, номера и места расположения базовых станций. Возможности исследуемого оперативно-розыскного мероприятия позволяют осуществить позиционирование мобильного телефона потерпевшего на местности, тем самым установить его (жертвы) местонахождение [6, с. 94]. С помощью данного мероприятия можно отследить и переписку фигурантов и жертвы посредством электронной почты, а также выявить текстовую и графическую информацию, передаваемую ими с использованием мессенджеров [7, с. 87].

Положения ст. 8 ФЗ «Об оперативно-розыскной деятельности» определяют реализацию снятия информации с технических каналов связи лишь по судебному решению, поскольку в ходе его проведения субъекты расследования получают доступ к гарантированным Конституцией Российской Федерации правам человека и гражданина на тайну переписки, телефонных переговоров

[15] См., например, Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд // Российская газета. 13.12.2013. № 282.

и иных сообщений, передаваемых по сетям связи. Вместе с тем в случаях, не терпящих отлагательств или наличия возможности совершения тяжкого или особо тяжкого преступления, анализируемое оперативно-розыскное мероприятие может быть проведено и без судебного решения, с последующим уведомлением (в течение 24 часов с начала его проведения) суда и получения разрешения на его проведения в течение 48 часов.

Как правило, получаемая при реализации данного оперативно-розыскного мероприятия информация является массивной в связи с тем, что по требованию субъектов расследования предоставляются не только данные биллинга жертвы, но и иных лиц, находящихся в запрашиваемый период времени в зоне базовой станции совместно с потерпевшим. Объем полученных данных обусловливает для их осмотра и обработки привлекать специалистов-криминалистов, которые, применяя специальную криминалистическую технику [8, с. 33], могут установить: а) где была и с кем встречалась жертва; б) длительность общения фигурантов; в) лица, находящиеся вблизи места преступления, в момент похищения жертвы и в другое время, до тех пор, пока мобильный телефон похищенного не был выключен. Выясняются абонентские номера, с которых звонили или писали жертве до совершения преступления, перемещавшиеся вместе с ней в ходе преступления в зону действия других базовых станций и определяется принадлежность интересующих абонентских номеров или IMEI телефонов конкретным лицам, после чего они проверяются на причастность к совершенному преступлению.

Использование специальной криминалистической техники дает возможность систематизации криминалистически значимой информации, полученной в ходе проведения снятия информации с технических каналов связи: по номеру абонента, IMEI мобильного телефона, времени сеансов связи и другим параметрам. Специфика обработки биллинговой информации способствует определению IMEI мобильного телефона, который остается неизменным, даже если преступники используют несколько SIM-карт, меняя их в телефоне.

Так, М. использовала для связи телефон потерпевшего В., похищенного с целью выкупа ее сожителем Ш., вставив в него свою SIM-карту. В ходе проведения оперативно-розыскного мероприятия — снятие информации с технических каналов связи — было установлено, что IMEI мобильного телефона, принадлежавшего ранее потерпевшему В., определяется с SIM-картой, зарегистрированной на М. В ходе последующего опроса М. указала на Ш., как на лицо, совершившее похищение потерпевшего[16].

Результаты снятия информации с технических каналов связи находят отражение в рапорте оперативного сотрудника, составленного на имя начальника оперативного подразделения. При необходимости часть полученных в ходе проведения оперативно-розыскных мероприятий данных или их в полном объеме, могут быть рассекречены и предоставлены в следственные подразделения для решения вопроса о возбуждении уголовного дела или использования в процессе расследования анализируемых преступлений. Для преобразования полученных результатов в доказательства по уголовному делу проводится ряд следственных и процессуальных действий: проведение осмотра предметов (CD-диска с полученной информацией); признание и приобщение данного CD-диска в качестве доказательств к материалам уголовного дела; допрос специалиста, участвующего в ходе осмотра и проведения выборки полученных данных и других. В дальнейшем исследование, проверка и оценка полученных доказательств осуществляется в соответствии с требованиями уголовно-процессуального законодательства.

Снятие информации с технических каналов связи обладает большим практическим потенциалом, позволяя получить существенную криминалистически значимую информацию, однако не позволяет осуществлять негласную аудиозапись и прослушивание переговоров проверяемых лиц, ведущихся по телефонным линиям связи [9, с. 118]. Указанное обусловливает применение иных средств оперативно-розыскной деятельности, в числе которых прослушивание телефонных переговоров близких и родственников жертвы. Актуальность

[16] Архив Московского городского суда // Уголовное дело № 2-62/2006.

и значимость данного оперативно-розыскного мероприятия вызвана тем, что именно родственникам и близким жертвы чаще всего адресовано требование о выкупе похищенного лица.

Требования ст. 8 ФЗ «Об оперативно-розыскной деятельности» закрепляют, что в случае возникновения угрозы жизни, здоровью или собственности отдельных лиц, по их письменному заявлению или с их согласия в письменной форме разрешается прослушивание телефонных переговоров, ведущихся с их телефонов на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность. С целью быстроты реализации указанного оперативно-розыскного мероприятия, максимальной фиксации преступных намерений виновных, родственники похищенного, выступающими заявителями о преступлении, пишут заявление на имя начальника оперативного подразделения, в котором разрешают поставить свой телефон на прослушивание, указывают имеющиеся для этого основания и срок (не более 180 дней).

В ходе реализации анализируемого оперативно-розыскного мероприятия будет получена информация о подозреваемых в совершении посягательств на свободу личности, а их абонентские номера могут быть поставлены на прослушивание телефонных переговоров. Поскольку действиями субъектов расследования будут затронуты конституционные права и свободы фигурантов, прослушивание телефонных переговоров осуществляется на основании судебного решения, которое должно быть получено в течение 48 часов с момента начала его осуществления (ст. 8 ФЗ «Об оперативно-розыскной деятельности»).

Например, в начале 2014 г. в 4 ОРЧ УУР МВД России по г. Москве поступила оперативная информация о том, что в Москве действует преступная группа, занимающаяся похищением людей и квартирным мошенничеством. По заданию сотрудников 4 ОРЧ УУР МВД России по г. Москве проводилось прослушивание телефонных переговоров Ч.Л.И., согласно данным которых, в августе 2014 г. был установлен факт похищения гражданина Н.В.Ф. с целью прода-

жи его квартиры. Поскольку возникла угроза жизни и здоровью похищенного, было проведено задержание виновных[17].

Значимость и результативность прослушивания телефонных переговоров заключается в том, что позволяет зафиксировать факты получения угроз, причинения насилия к жертвам, вымогательства денежных средств у родственников и близких похищенного, установить дату и время «выкупа», дать оценку объективности и полноты данных, изложенных в сообщениях о совершении преступлений против свободы личности, а также использовать полученные результаты в доказывании.

По результатам прослушивания телефонных переговоров инициатору оперативно-розыскного мероприятия предоставляется CD (DVD)-диск аудиозаписи состоявшихся фонограмм, редко — распечатка полученных данных. Оперативный сотрудник по полученным материалам докладывает рапортом начальнику оперативного подразделения, решая вопрос о рассекречивании результатов оперативно-розыскной деятельности и ее предоставления органам предварительного следствия.

Для перевода полученных фонограмм в текстовую информацию, наиболее целесообразно реализовывать организационно-процессуальное мероприятие — привлечение специалиста, который посредством применения цифрового транскрайбера преобразует аудиозапись в текстовый формат [10, с. 36]. Данные устройства сочетают возможности текстового редактора и цифрового магнитофона [11, с. 133].

Полученные в ходе проведения данного оперативно-розыскного мероприятия результаты используются в качестве доказательств по уголовному делу путем: проведения осмотра предметов (CD или DVD-диска с полученной информацией); проведения осмотра документов (в случае предоставления распечатки полученных данных); признания и приобщения данного CD (DVD)-диска или распечатки в качестве доказательств к материалам уголовного дела; допроса специалиста, участвующего в ходе осмотра полученных данных; назначения

[17] Архив Бутырского районного суда г. Москвы // Уголовное дело № 01-0060/2016.

и проведения фоноскопической экспертизы; последующего исследования, проверки и оценки полученных доказательств требованиям уголовно-процессуального законодательства.

Подводя итог изложенному, отметим, что современные коммуникативные средства не только стали неотъемлемым атрибутом нашей объективной действительности, но и активно используются преступниками в ходе подготовки и совершения посягательств на свободу личности. Передаваемые с помощью указанных технических средств данные являются криминалистически значимыми, обусловливая субъектов расследования их выявлять, фиксировать и использовать в процессе доказывания преступной деятельности виновных. Снятие информации с технических каналов связи и прослушивание телефонных переговоров выступают одними из наиболее распространенных оперативно-розыскных мероприятий, позволяющих выявить преступления против свободы личности, организовать их раскрытие и расследование, а также установить и изобличить виновных.

**Список литературы**

1. Зажицкий В.И. Результаты оперативно-розыскной деятельности в уголовном судопроизводстве: теория и практика. СПб., 2006. 449 с.

2. Доля Е.А. Использование в доказывании результатов оперативно-розыскной деятельности. М., 1996. 111 с.

3. Меретуков Г.М. Использование материалов оперативно-розыскной деятельности в расследовании // Политематический сетевой электронный журнал Кубанского государственного аграрного университета. 2013. № 92. С. 1248-1259.

4. Доля Е.А. Результаты оперативно-розыскной деятельности не могут стать содержанием доказательств в уголовном процессе // Государство и право. 2013. № 5. С. 24-39.

5. Оперативно-розыскная деятельность: учебник. 2-е изд., доп. и перераб. / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: Инфра-М, 2004. С. 353.

6. Ковалев С.Д., Курысев К.Н., Полуянова Е.В. Позиционирование мобильных телефонов в сотовых сетях связи при реализации оперативно-розыскного мероприятия «снятие информации с технических каналов связи» // Вестник Владимирского юридического института. 2017. № 2 (43). С. 93-97.

7. Осипенко А.Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации: содержание и основы осуществления // Вестник Воронежского института МВД России. 2016. № 3. С. 83-90.

8. Дерюгин Р.А. Специализированная криминалистическая техника, предназначенная для анализа и обработки информации о соединениях между абонентами и (или) абонентскими устройствами // Полицейская и следственная деятельность. 2016. № 3. С. 32-35.

9. Шматов М.А., Шматов В.М. Контроль и запись телефонных переговоров как следственное действие в соотношении с оперативно-разыскным мероприятием — прослушивание телефонных переговоров // Вестник Волгоградской академии МВД России. 2017. № 1 (40). С. 117-121.

10. Шурухнов Н.Г. Перспективные направления развития российской криминалистики и практики расследования отдельных видов и групп преступлений // Криминалистика как наука и учебная дисциплина: история, настоящее и перспективы развития: материалы Междунар. науч.-практ. конф., посвященной 35-летию кафедры криминалистики Института права БашГУ. Уфа: Изд-во Башкирского гос. ун-та, 2017. С. 34-45.

11. Просвирин Е.В. Использование транскрайбера при описании в ходе следственных действий // Криминалистика. Экспертиза. Розыск: сб. науч. статей. Саратов, 2008. С. 129-135.

***А.С. Каменев,*** *адвокат Адвокатской палаты Челябинской области,*
*г. Челябинск*

# СОБИРАНИЕ ДОКАЗАТЕЛЬСТВ В ЭЛЕКТРОННОМ ВИДЕ СТОРОНОЙ ЗАЩИТЫ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

В соответствии с ч. 3 ст. 86 УПК РФ защитник праве собирать доказательства путем: получения предметов, документов и иных сведений; опроса лиц с их согласия; истребования справок, характеристик, иных документов от органов государственной власти, органов местного самоуправления, общественных объединений и организаций, которые обязаны предоставлять запрашиваемые документы или их копии. Кроме того, обвиняемый, гражданский ответчик и его представитель как участники стороны защиты вправе собирать и представлять письменные документы и предметы для приобщения их к уголовному делу в качестве доказательств (ч. 2 той же статьи). В электронном виде реализовать указанные в законе возможности можно таким образом:

1) предметы и документы могут быть получены и представлены следователю, дознавателю, органу дознанию в суд в электронном виде.

2) опрос лиц может проводить с использованием цифровых информационно-телекоммуникационных средств (с применением видеоконференц-связи смартфонов, компьютеров, ноутбуков через программы и приложения, поддерживающие видеосвязь).

3) запросы на получение справок, характеристик и иных документов в органы государственной власти и организации различных форм собственности могут быть направлены посредством сети «Интернет».

Однако для того чтобы предметы и документы, обнаруженные стороной защиты, стали доказательствами по делу, необходимо их процессуальное закрепление [2, с. 40]. Такие возможности имеются лишь у властных участников процесса, в производстве которых находится уголовное дело. Примерно о том же пишет А.Н. Калюжный: обнаруженные адвокатом данные являются сведе-

ниями об источниках тех фактов, которые могут стать доказательствами после их закрепления надлежащим процессуальным путем [3, с. 45]. Поэтому даже если защитник обнаружит материалы, которые могут устанавливать обстоятельства, подлежащие доказыванию, он должен представить их для решения вопроса о приобщении их к уголовному делу. При этом электронные доказательства, как правило, нуждаются в подтверждающих сведениях на бумажных носителях.

Так, по одному уголовному делу лицо обвинялось в создании организованной преступной группы, занимающейся сбытом наркотических средств через сеть «Интернет». В суд были представлены доказательства того, что на момент инкриминируемых покушений на сбыт наркотического средства страница интернет-магазина была закрыта. Тем самым утверждалось, что подзащитный не занимался преступной деятельностью на тот момент времени. К делу были приобщены распечатки интернет-страниц (скриншоты), защита сослалась на позицию Верховного Суда РФ, выраженную в Постановлении Пленума от 23.04.2019 № 10, согласно которой допустимыми доказательствами являются, в том числе сделанные и заверенные лицами, участвующими в деле, распечатки материалов, размещенных в информационно-телекоммуникационной сети (скриншот), с указанием адреса интернет-страницы, с которой сделана распечатка, а также точного времени ее получения. Дело закончилось оправданием по одному из эпизодов, исключением ряда квалифицирующих признаков и назначением достаточно мягкого наказания с учетом всего объема обвинения[18].

Можно прийти к выводу, что защитник, как и другой участник стороны защиты, не является в полной мере субъектом уголовно-процессуального доказывания. На сегодня закон не позволяет решить эту проблему. Порядок представления доказательств стороной защиты также не находит нормативного отражения [7, с. 91].

[18] [Электронный ресурс]. URL: https://u.to/dCo-Gw.

О.В. Овчинникова справедливо обращает внимание на решения высших судов по данному вопросу, что, по сути, является своего рода препятствием к дальнейшему развитию ситуации [5, с. 327-328].

Конституционный Суд РФ указывает, что право защитника собирать и представлять доказательства может быть реализовано только во взаимосвязи с обязанностью дознавателя, следователя и прокурора рассмотреть каждое заявленное в связи с исследованием доказательств ходатайство[19].

Верховный Суд РФ в кассационном определении от 8.12.2004 № 3-О04-42 приходит к выводу о том, что исходя из смысла ст. 84 и 86 УПК РФ, следует, что относимые к делу сведения, полученные защитником в результате опроса частных лиц, изложенные им или опрошенными лицами в письменном виде, нельзя рассматривать в качестве показаний свидетеля или потерпевшего. Они получены в условиях отсутствия предусмотренных уголовно-процессуальным законом гарантий их доброкачественности и поэтому могут рассматриваться как основания для вызова и допроса указанных лиц в качестве свидетелей, потерпевшего или для производства других следственных действий по собиранию доказательств, а не как доказательства по делу[20].

Другой проблемой является и то, что так называемые электронные доказательства, обнаруженные стороной защиты, не всегда приобщаются к материалам уголовного дела. В данном случае легко просматривается не только обвинительный уклон, но и явное преимущество стороны обвинения в ходе предварительного расследования. В таком случае стороне защите удобнее представлять доказательства непосредственно в суде или «изобретать» тактические ходы, чтобы информация попала к следователю, например, сохранение ее на телефоне подзащитного, у которого тот будет в дальнейшем изъят и осмотрен [5, с. 333].

Электронная информация может находиться на материальных носителях, которые в дальнейшем по ходатайству стороны защиты могут быть приобщены

---

[19] [Электронный ресурс]. URL: https://legalacts.ru/doc/opredelenie-konstitutsionnogo-suda-rf-ot-21122004-n-467-o-po/

[20] [Электронный ресурс]. URL: http://www.sudbiblioteka.ru/vs/text_big2/verhsud_big_31053.htm

к материалам уголовного дела. Совсем другое дело, когда такого рода информация находится на сайтах сети «Интернет», на личных аккаунтах ее пользователей. В этом случае есть несколько вариантов действий: 1) обратиться к следователю для осмотра интернет-ресурса; 2) с той же просьбой обратиться к суду во время слушания дела; 3) удостоверить наличие информации у нотариуса и результаты представить в любой момент производства по уголовному делу лицу, в чьем производстве находится уголовное дело.

Риск утраты информации в сети «Интернет» достаточно велик, поэтому решения при обращении участников стороны защиты надо принимать безотлагательно. Какой статус приобретет доказательство в электронном виде: вещественное доказательств или иной документ, не имеет принципиального значения и на доказывание не влияет. Хотя и этот вопрос заслуживает отдельного рассмотрения.

О.В. Овчинникова справедливо предлагает в целях сохранения электронной информации в сети «Интернет» возложить на следователя обязанность рассмотрения ходатайств о получении такого рода информации, дополнить ст. 159 УПК РФ «Обязательность рассмотрения ходатайств» частью 2.3. следующего содержания: «Стороне защиты не может быть отказано в удовлетворении ходатайства об осмотре и копировании электронной информации, находящейся в глобальной сети Интернет, если они заявляют, что эта информация подтверждает обстоятельства, подлежащие доказыванию по уголовному делу». Указанные дополнения, по мнению автора, защитят электронные доказательства, обнаруженных стороной защиты от возможности уничтожения, предоставят гарантии их исследования и оценки субъектами доказывания, устранят препятствия и ограничения права защитника на собирание доказательств по уголовному делу [4, с. 33].

Кроме того, представляется важным закрепить в законе право защитника собирать доказательства путем получения компьютерной информации, а также информации, передаваемой посредством телефонной связи. Первый способ получения информации предусмотрен п. 15 ч. 1 ст. 6 Федеральным законом

«Об оперативно-розыскной деятельности». Однако для стороны защиты ни в том, ни в другом случае нет необходимости в получении судебного решения. Во-первых, компьютерная информация может быть получена стороной защиты только с согласия обладателя сведений или собственника электронного носителя информации. Во-вторых, принудительные меры в принципе не являются частью средств защиты, и требования закона о получении судебного решения распространяются исключительно на действия должностных лиц.

Интерес представляет позиция Конституционного Суда Республики Армения, выраженная в последних решениях, касающихся данного вопроса.

При определении возможности использования записи телефонного разговора в качестве доказательства, произведенной частным лицом, нужно, прежде всего, оценить цель произведения записи. Таким образом, запись должна преследовать правомерную цель, а именно: защищать права и законные интересы лица, предотвращать противоправное поведение, раскрывать и защищать значимые частные интересы («significant private interest»). В то же время следует отметить, что в качестве правомерного поведения можно рассмотреть также запись телефонного разговора, произведенную со стороны частного лица в качества доказательства его невиновности. Другими словами, запись телефонного разговора может быть оправдана, если она предназначена для обеспечения правовой защиты лица [1, с. 11].

Верховный суд РФ, по сути, разрешает поводить запись телефонных переговоров без согласия собеседников. Для признания аудио- или видеозаписи допустимым доказательством согласия на проведение аудиозаписи или видеосъемки того лица, в отношении которого они производятся, не требуется[21]. Адвокат, председатель комиссии защиты прав адвокатов А. Иванов указывает на то, что доказательствами могут быть также данные с видеорегистраторов, записи уличных камер и тому подобное[22].

---

[21] П. 55 постановления Пленума Верховного Суда РФ от 23 апреля 2019 г. № 10 «О применении части четвертой Гражданского кодекса Российской Федерации». [Электронный ресурс]. URL: https://rg.ru/2019/05/06/postanovlenie-dok.html

[22] [Электронный ресурс]. URL: https://pravo.ru/review/view/137811/

Таким образом, собирание доказательств в электронном виде стороной защиты в уголовном судопроизводстве является достаточно проблемным вопросом и его дальнейшее развитие во многом зависит от законодательной регламентации. Соответствующие изменения и дополнения должны, прежде всего, найти отражения в Уголовно-процессуальном кодексе РФ. Кроме того, зависимость активности стороны защиты от органов расследования необходимо пересматривать с учетом потребностей практики правоприменения в стремлении к справедливости и установления правового государства.

**Список литературы**


1. Гамбарян А.С., Бегларян К.С. Правовая позиция Кассационного суда РА по поводу допустимости тайной записи частным лицом // Судебная власть и уголовный процесс. 2020. № 3. С. 7-13.
2. Жунусканов Т.Ж. Проблемы адвокатского расследования в процессе осуществления защиты по уголовному делу // Адвокатская практика. 2010. № 3. С. 40-42.
3. Калюжный А.Н. Трансформация форм адвокатского расследования в уголовном процессе: проблемы правовой конструкции и практики реализации // Адвокатская практика. 2017. № 2. С. 44-49.
4. Овчинникова О.В. Проблемы собирания электронных доказательств стороной защиты // Вестник ЮУрГУ. Серия «Право». Т. 18. № 3. 2018. С. 27-33.
5. Основы теории электронных доказательств: монография / под ред. докт. юрид. наук С.В. Зуева. М., 2019. 400 с.
6. Петрухин И.Л. Теоретические основы реформы уголовного процесса в России: в 2 т. Т. 1. М., 2005. 220 с.
7. Шейфер С.А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования. М., 2008. 240 с.

***А.В. Караваева,*** *преподаватель кафедры «Цифровая криминалистика» Московского государственного технического университета имени Н.Э. Баумана, г. Москва*

***В.С. Федосеева,*** *студентка кафедры «Цифровая криминалистика» Московского государственного технического университета имени Н.Э. Баумана, г. Москва*

# МЕТОДЫ И СРЕДСТВА СУДЕБНЫХ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ИССЛЕДОВАНИЙ ПРЕДПОЛОЖИТЕЛЬНО ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В последние годы ввиду внедрения информационных технологий широко распространились новые компьютерные преступления. Их основные следы, существующие в виртуальном пространстве, являются недоступными для непосредственного представления участникам судопроизводства без применения специальных программно-технических средств. Без использования специальных знаний из области информационных технологий, какими и обладает судебный эксперт, прошедший соответствующую подготовку в области судебной компьютерно-технической экспертизы (далее — СКТЭ), раскрытие и расследование подобных преступлений представляется невозможным.

Перед судебными экспертами в области СКТЭ часто ставятся задачи по нахождению предположительно вредоносных программ. Они отвечают на вопросы о наличии либо отсутствии предположительно вредоносных программ на конкретном устройстве (компьютере, ноутбуке, мобильном устройстве) при использовании какого-либо программного обеспечения. Довольно часто лица, запрашивающие экспертизы, не понимают различия между терминами «вирус» и «вредоносная программа», из-за чего возникают противоречия. Согласно ГОСТ Р 54429 — 2017 «Судебная компьютерно-техническая экспертиза. Термины и определения», компьютерный вирус — это программа, способная к самостоятельному распространению по локальным сетям, средствам вычислительной техники, не использующая сетевые сервисы [1].

Под вредоносным программным обеспечением (далее — ПО) принято считать программное средство, созданное в целях совершения неразрешенных владельцем информации действий. При этом такими действиями могут выступать как полное уничтожение информации или системы ее защиты, так и ее блокирование, модификация либо копирование.

Несмотря на значимость проблемы, в уголовно-правовой науке так и не сложилось единообразного понимания вредоносной программы как конструктивного признака. Один из признаков состава преступления, предусмотренного ст.273 Уголовным кодексом Российской Федерации (далее — УК РФ), является вредоносная программа и согласно этой статье установлена ответственность за создание, использование и распространение вредоносных компьютерных программ. Исходя из этого, вредоносное программное обеспечение — это компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации [2].

В науке уголовного права отмечается, что квалификация преступлений, совершаемых в сфере компьютерной информации, представляет определенные трудности. М.М. Малыковцев пишет, что «вредоносная программа — это программа, специально написанная на любом языке программирования, использование и распространение которой в информационном системе либо в информационно-телекоммуникационной сети приводит к неправомерному воздействию на информацию и на средства компьютерной техники и связи, выражающемуся в незаконном уничтожении, копировании, повреждении, блокировании, искажении информации, и иному нарушению установленного законным владельцем порядка работы указанных устройств» [3].

В свою очередь, М.Ф. Ефремова подчеркивает, что основное отличие вредоносных программ от иных, которые также могут производить копирование, уничтожение, модификацию информации, определяет тем, что все действия

производятся без уведомления пользователя, скрытно от него, а сам пользователь зачастую и не подозревает о наличии такой программы на его компьютере.

По мнению В.Б. Вехова, для того чтобы признать компьютерную программу вредоносной, необходимо доказать наличие совокупности следующих обстоятельств: 1) программа способна уничтожать, блокировать, модифицировать либо копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации; 2) программа не предлагает предварительного уведомления собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно — телекоммуникационной сети о характере своих действий; 3) программа не запрашивает согласия (санкции) у собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети на реализацию своего назначения [4, с. 10-12].

В настоящее время принято разделять следующие категории вирусов:

- по поражаемым объектам (файловые вирусы, поражающие исходный код загрузочные вирусы, соответственные макровирусы, сценарные вирусы, просто вирусы);
- файловые вирусы делят по механизму заражения: те, которые, добавляя себя в исполняемый файл, называются паразитирующими вирусами, те, которые невосстановимо портят зараженный файл, называются перезаписывающими, вирусы-«спутники» идут отдельным файлом;
- по поражаемым операционным системам и платформам (DOS, Windows, — Unix, Linux, Android);
- по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый — язык программирования, сценарный язык и др.);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.)

Для более эффективного расследования конкретного дела, в рамках которого была назначена экспертиза, судебному компьютерно-техническому эксперту следует провести комплексное исследование объектов, которое должно быть основано на определенном алгоритме действий с учетом специфики обстоятельств расследуемого дела. Поэтому различные государственные учреждения и иные экспертные организации разрабатывают определенные методические рекомендации и пособия, в которых прописывается алгоритм применения комплекса методов, приемов и технических средств в определенной последовательности для решения экспертной задачи. Так, Российским федеральным центром судебной экспертизы при Министерстве Юстиции РФ были разработаны методические рекомендации по проведению эксперимента для установления функций предположительно вредоносной программой.

При исследовании предположительно вредоносной программы необходимо определить:

1) характеристики программы, позволяющие отнести ее к разряду вредоносных, т.е. подпадающие под формулировку статьи 273 УК РФ;

2) компилятор, которым была создана программа. Данные, сопутствующие компиляции (сохранение даты и времени компиляции в заголовке файла);

3) персонализирующую информацию, хранящуюся в файле (имена, псевдонимы, сетевые адреса и идентификаторы);

4) адреса, с которыми осуществляется связь и взаимодействие (куда отправляется информация, с каких сайтов скачиваются файлы);

5) иные настройки программы [5, с. 23].

В некоторых случаях невозможно обойтись и без эксперимента — анализа вредоносных программ, целью которого является понимание работы вредоносных программ, а также определение методов обнаружения и устранения последствий их применения. Он включает в себя анализ подозрительного двоичного файла в безопасной среде для определения его характеристик и функциональных возможностей, чтобы можно было выстроить лучшую оборонительную стратегию для защиты.

Основной целью проведения исследования вредоносных программ является извлечение информации их образа вредоносного ПО, которая может помочь в реагировании на вредоносный инцидент.

Растущее количество вредоносных программ привело к разработке автоматизированных и более эффективных методов анализа вредоносных программ. Автоматический анализ использует различные методы для отслеживания поведения подозрительного файла и создания отчета, описывающего различные действия, выполняемые исполняемым файлом. Методы автоматизированного анализа подразделяются на две группы: статический анализ и динамический анализ.

Статический анализ вредоносных программ относится к методам, которые исследуют содержимое вредоносных файлов без их запуска, в то время как динамический анализ рассматривает поведение вредоносных файлов, выполняя их в контролируемой среде. Существует несколько методов, которые могут предоставить различную информацию о файле, которая зависит от цели контекста, окружающего подозрительный файл [6, с. 173]:

1. Определение типа файла. В ходе анализа определение типа подозрительного двоичного файла поможет идентифицировать операционную систему, на которую нацелено вредоносное ПО (Windows, Linux и т. Д.), и ее архитектуру (32- или 64-битные платформы). Например, если подозрительный бинарный файл имеет формат Portable Executable (PE), который является форматом исполняемых файлов Windows (.exe, .dll, .sys, .drv, .com, .ocx и т. Д.), можно сделать вывод, что файл предназначен для операционной системы Windows. Определение типа файла с использованием ручного метода. Ручной метод определения типа файла заключается в поиске его цифровой подписи, когда файл открывают в hex-редакторе. Определение типа файла с использованием инструментальных средств — определение типа файла с помощью Python.

2. Сличение информации с помощью цифровых отпечатков. Метод сличения информации с помощью цифровых отпечатков включает в себя генерацию значений хеш-сумм для подозрительного двоичного файла в зависимости от его содержимого. Алгоритмы криптографического хеширования, такие как

MD5, SHA1 или SHA256, считаются стандартом де-факто для генерации хеш-сумм образцов вредоносных программ

3. Многократное антивирусное сканирование. Сканирование подозрительного двоичного файла с помощью нескольких антивирусных сканеров помогает выявить наличие сигнатур вредоносного кода. Имя сигнатуры конкретного файла может предоставить дополнительную информацию о нем и его возможностях. Посещая веб-сайты соответствующих антивирусных компаний или занимаясь поиском сигнатуры в поисковых системах, можно найти более подробную информацию о подозрительном файле. Такая информация может помочь в последующем расследовании и сократить время анализа.

4. Извлечение строк. Строки — это последовательности печатных символов ASCII и Юникода, встроенные в файл. Извлечение строк может подсказать, как функционирует программа, и рассказать об индикаторах, указывающих на подозрительный двоичный код. Например, если вредоносная программа создает файл, имя файла сохраняется в виде строки в двоичном файле. Или если вредоносная программа разрешает доменное имя, контролируемое злоумышленником, это имя впоследствии хранится в виде строки. Строки, извлеченные из двоичного файла, могут содержать ссылки на имена файлов, URL-адреса, доменные имена, IP–адреса, команды атаки, ключи реестра и т.д.

5. Определение обфускации файла. Несмотря на то, что извлечение строк является отличным способом для сбора ценной информации, часто авторы вредоносных программ прячут или защищают свои вредоносные двоичные файлы. Обфускация используется ими для защиты внутренней работы вредоносного ПО от экспертов по безопасности, аналитиков вредоносного ПО и реверс-инженеров. Эти методы затрудняют обнаружение/анализ двоичного файла; Авторы вредоносных программ часто используют такие программы, как упаковщики и крипторы, чтобы скрыть свой файл и не дать антивирусу себя обнаружить, тем самым помешав анализу.

6. Проверка информации о PE-заголовке.

7. Сравнение и классификация вредоносных программ. В ходе изучения вредоносной программы, когда сталкиваются с образцом вредоносного ПО, ве-

роятно, захочется узнать, относится данный образец к определенному семейству вредоносных программ или имеет характеристики, которые соответствуют ранее проанализированным образцам. Сравнение подозрительного файла с ранее проанализированными образцами или образцами, хранящимися в публичном либо частном хранилище, может дать представление о семействе вредоносных программ, их характеристиках и сходстве с предварительно проанализированными образцами.

В то время как динамический анализ (поведенческий анализ) рассматривает поведение вредоносных файлов, путем выполнения его в изолированной среде в качестве мониторинга деятельности, а также анализа влияния на систему. Существует несколько этапов динамического анализа:

1. Возврат виртуальной машины в исходное состояние.
2. Запуск инструментов мониторинга / динамического анализа: на этом этапе запускаются инструменты мониторинга перед исполнением образца вредоносного ПО.
3. Выполнение образа вредоносного ПО: на этом этапе запускается образец вредоносного ПО с правами администратора.
4. Остановка инструментов мониторинга: включает в себя остановку инструментов мониторинга, после того как вредоносный файл исполняется в течение указанного времени.
5. Анализ результатов: включает в себя сбор данных/отчетов инструментов мониторинга и их анализ для определения поведения вредоносного ПО и его функциональности [6].

Таким образом, динамический анализ — отличный метод для понимания поведения вредоносных программ и определения их сетевых и хост-индикаторов. Динамический анализ удобно использовать для проверки результатов, полученных в ходе статического анализа. Сочетание статического и динамического анализов поможет лучше понять вредоносный код.

В целом можно представить следующий алгоритм действий судебного эксперта при исследовании обнаруженных вредоносных программ при производстве СКТЭ, которые можно подразделить на несколько стадий:

1. Подготовительное исследование вредоносных программ. Оно включает в себя подготовку устройства — компьютера, функциональность которого установлена достоверно. Анализ враждебной программы требует безопасной и надежной тестовой среды, поэтому чаще всего применяют виртуальные машины (например, VMware или VirtualBox). Преимуществом ее использования заключается в том, что, завершив анализ вредоносного ПО, можно с легкостью вернуть тестовую среду в чистое состояние.

2. Исследование вредоносных программ. На данной стадии необходимо извлечение ценной информации из образца вредоносного ПО, анализ образца путем выполнения его в изолированной среде и мониторинг его деятельности. При производстве СКТЭ следует иметь в виду, что непосредственно понятие «вредоносная программа» в своей структуре имеет правовые и технические составляющие, последние из которых и представляют собой объект экспертного исследования СКТЭ. Именно поэтому судебный эксперт в области СКТЭ уделяет особое внимание именно на определенные технические свойства и параметры программы, методам ее установки в систему, их несанкционированному использованию в последней либо определенным техническим дефектам и проблемам в функционировании существующих в системе программных продуктов [7, с. 6].

3. Ответы на вопросы о непосредственном наличии/отсутствии компьютерного вируса в системе устройства. В процессе проведения СКТЭ различного вида компьютерные вирусы и их влияние на взаимодействие являются непосредственно объектами изучения. В таком случае перед экспертом ставятся определенные вопросы (вышеупомянутые), при условии его существования рассматриваются также вопросы о его характеристиках и степени влияния на функционирование всей системы в целом.

В настоящее время компьютерные технологии внедряются во все сферы жизни общества, появляется все больше вредоносного программного обеспечения, которое содержит сложные механизмы защиты от обнаружения антивирусными средствами защиты. Растет объем оставляемых ими информационных

следов как в сети Интернет, так и вне ее пределов. Поиск этих следов является основной задачей судебной компьютерно-технической экспертизы.

## Список литературы


1. ГОСТ Р 57429-2017 Судебная компьютерно-техническая экспертиза. Термины и определения. М.: Стандартинформ, 2018. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200144960?section=text (дата обращения 26.05.2021).
2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации от 17 июня 1996 г. № 25. Ст. 2954 // Система ГАРАНТ. [Электронный ресурс]. URL: http://base.garant.ru/ 10108000/#ixzz6vzCYTBFI (дата обращения 26.05.2021).
3. Русскевич Е.А. Понятие вредоносной компьютерной программы. Текст научной статьи по специальности «Право». [Электронный ресурс]. URL: https://cyberleninka.ru (дата обращения 03.03.2021).
4. Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием средств компьютерной техники: дисс. … канд. юрид. н. Волгоград: ВСШ МВД России, 1995. 283 с.
5. Усов А.И. Производство судебной компьютерно-технической экспертизы (IV актуальные комплексные экспертные задачи): методическое пособие. М., 2011. 249 с.
6. Монаппа К.А. Анализ вредоносных программ / пер. с англ. Д.А. Беликова. // ДМК Пресс. 2019. 452 с.
7. Баюш А.А. Методические основы исследования предположительно вредоносного программного обеспечения в рамках судебной компьютерно-технической экспертизы // Политехнический молодежный журнал. 2019. № 5 (34). С. 1-10.

***Н.В. Карепанов,*** *к.ю.н., доцент, доцент кафедры криминалистики Уральского государственного юридического университета, г. Екатеринбург*

# НЕКОТОРЫЕ ОСОБЕННОСТИ ПОИСКА И ИССЛЕДОВАНИЯ СЛЕДОВ ПРЕСТУПЛЕНИЙ В КИБЕРПРОСТРАНСТВЕ

Рожденное в романе фантаста Уильяма Гибсона «Нейроман» слово «киберпространство» (cyberspace) описано в виде замены реального мира компьютерными системами, существующими только в умах пользователей. Своего рода — виртуальная реальность, которая представлена не в виде физической среды, которая воспринимается через органы чувств, а в форме цифровой конструкции (компьютерная разработка). Одновременно следует заметить, что основа исследуемого понятия происходит от термина «кибернетика» (предложенного Норбертом Винером в 1940-х гг. для речевого обозначения познания процессов, происходящих между системами связи, управления машинами и живыми существами). Сегодня это понятие характеризуется в качестве электронной связи (коммуникационные сети, передача сигналов, взаимодействия компьютеров) [1, с. 28], науки о процессах управления, передачи информации и коммуникациях в сложных динамических системах (технических, компьютерных, биологических, нейронных, социальных). Развитие кибердискурса обогатило науку целым рядом новых терминов, связанных с технологиями и компьютерно-опосредованных коммуникаций (computermediated communication, CMC).

Понятие «киберпространство» (англ. cyberspace) можно рассматривать и как греко-латинскую комбинацию, состоящую из двух частей: «кибер» (cyber) и «пространство» (space) [2, с. 42; 3, с. 18; 4, с. 15].

Вокруг киберпространства дискуссии ведутся десятилетиями, но до настоящего времени единого понимания этого понятия нет. Множественность суждений объясняется двумя основными причинами. Отождествление киберпространства и пространство интернета; киберпространства и виртуальной реальности.

В научной литературе авторитетным суждением о месте киберпространства в Интернете является мнение Майкла Бэтти — британского специалиста

по пространственным данным, а также председателя Центра расширенного пространственного анализа. Он выделял в «географии Интернета» четыре уровня: место (place) в традиционном научном понимании пространства; виртуальное пространство (virtual space), смоделированное на конкретном компьютере в реальном мире места (place: qeo-data); киберпространство (cyberspace) в компьютерных сетях; мир киберместа (a world of cyber-place) как посредник связи с конкретным географическим местом киберпространства [5, с. 46-52].

Из такого контекста можно сделать вывод, что киберпространство, как и его географический аналог, соединяет в себе все пространства в единое целое. Это достаточно широкое понятие, в которое кроме Интернета можно включать любые места встречи пользователей: социальные сети, интернет-форумы, игры и т.п. В характеристике сущности киберпространства можно выделить основные элементы: Интернет с его ресурсами и услугами; его пользователи; виртуальная реальность, создаваемая компьютером, сетью, Интернетом; социальная мегасеть (сеть сетей) как использование глобальных ресурсов через Интернет; эволюционирующая сложная динамическая система (system of systems). Можно определить киберпространство как пространство, не сводимое к физическому пространству, в котором агенты вступают во взаимодействие в условиях функционирования множества технически сконфигурированных сред [6, с. 13; 7, с. 5].

*Киберпространство определяется как виртуальное пространство, в котором коммуницируют подключенные к сети компьютеры или другие цифровые средства (мобильные устройства) чаще посредством Интернета (информационное пространство) и встречаются пользователи Интернета (социальное пространство).*

Виртуальность — самый значимый элемент киберпространства. Она является своеобразной реабилитацией иллюзии, особой парадигмой мимикрии (подражания). В физическом смысле это цифровая конструкция, разработанная с помощью компьютеров. По существу включает в себя чувственные ощущения человека в результате использования технических электронных устройств, имитирующих действия реального мира, создающих искусственную среду. Киберпространство в чистом виде не является иллюзией реальности, в нем отра-

жается существующая действительность преимущественно через простое (относительно простое) текстовое общение. Кроме того, в настоящее время современные технологии порождают бесчисленные социальные отношения, наложенные на киберпространство. Число, уровень и разнообразия проявлений социальной жизни здесь постоянно растет, скорость технологических новаций беспрецедентна. Киберпространство (цифровая среда) едино, представляет собой бесконечные возможности для коммуникации, характеризуется высокой пластичностью, текучестью, гипертекстуальностью, интерактивностью, а главное — точностью измерений в режиме реального времени. Его границы несводимы к границам физического пространства (не отображается на картах мира, неделимы границами национальных государств), они подвижны и изменчивы. Киберпространство представлено в сознании разных людей в виде некоего гибридного мира с определенной протяженностью и метрикой [8, с. 44-45].

Кроме границ и других характеристик в киберпространстве можно выделить четыре материальных слоя пространства потоков: технологическая инфраструктура информационных систем, телекоммуникационных систем и транспортных линий (микроэлектроника, телекоммуникации, компьютерная обработка, системы вещания и высокоскоростного транспорта и т.д.); узлы, хабы и коммуникационные центры; пространственная организация властвующих менеджерских элит; электронные пространства, такие как сайты в Интернете, мессенджеры и т.п. (это могут быть как однонаправленные, так и интерактивные потоки) [9, с. 386].

Расстояния в киберпространстве измеряются щелчком компьютерной мыши. Средством коммуникации является сообщение, в современном мире оно похоже на байты. Единая сеть электронной коммуникации касается всех сфер людского опыта в режиме реального времени и независимо от места расположения человека. Не имеет значения и IP-адрес, геополитическое нахождение сервера, поскольку коммуникационное поле одинаково для всех, одномерно и сжато. Отсюда определение киберпространства раскрывается в трех перспективах: физическом, информационном и социальном аспектах.

Из-за таких характеристик киберпространства правовое регулирование его крайне затруднено. Неминуемые столкновения разных законов приводят к осложнениям в преследовании за совершенные преступления в таких условиях. Компьютеры, цифровые технологии, искусственный интеллект стали фактически контролировать многие системы, необходимые для выживания (такие как Системы прогнозирования и диагностики). Такие обстоятельства требуют создания набора обязательных стандартов (концепция киберэтики).

Киберпреступление — это общественно опасное деяние, совершаемое в киберпространстве, посягающее на общественную безопасность, собственность, права человека, другие охраняемые законом отношения, необходимым элементом механизма подготовки, совершения, сокрытия и отражения которого является компьютерная информация, выступающая в роли предмета или средства преступления [10, с. 29-32].

Киберпреступления характеризуются особой картиной цифровых следов, находящиеся в памяти электронных устройств (следы совершения любых действий в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей. Цифровые следы выражаются в любом изменении состояния автоматизированной информационной системы, которое связано с событием преступления и принимает форму компьютерных сведений или данных [11, с. 265-269]. В результате электронно-цифрового отражения на материальном носителе фиксируется образ из цифровых значений параметров формальной математической модели наблюдаемого реального физического явления. Носителями таких следов обычно выступают: жесткие и оптические диски, магнитные ленты, дискеты, оперативно запоминающие устройства ЭВМ, периферийные и сетевые устройства, компьютерные устройства связи, проводные и другие электромагнитные системы и сети связи [12, с. 159-160]. Сами следы могут быть первичными (непосредственное воздействие на носителей информации) и вторичными (воздействие технологических процессов без участия человека) [13, с. 17]. Наиболее явными цифровыми следами являются следы в памяти высокоточных устройств: включения и выключения, различные

операции с содержимым памяти, действия с программами и сведения о работе сети Интернет, локальных и иных сетях.

Обнаружение цифровых следов в киберпространстве фиксируется описанием этих фактов в протоколе, где записываются: сведения об устройстве, в памяти которого они выявлены; кому принадлежит устройство; имеется ли связь с Интернетом, локальными или иными сетями; характеристика ее оперативной системы; локация, создание и изменение файлов; описание следов. После фотографирования экрана с демонстрацией свойств файлов, журналов администрации происходит изъятие самого объекта с последующим его исследованием [14, с. 23].

Поиск следов преступлений в киберпространстве осуществляется в основном при проведении следственного осмотра, который имеет свои особенности. Немаловажное значение при производстве осмотра имеет исключение риска обнаружения преступниками (зачастую опытных пользователей с высоким интеллектуальным уровнем) вмешательства в их деятельность. Для этого следует: ограничить или прекратить вход и выход с компьютеров; продолжить деятельность в глобальной сети; определить грамотную последовательность действий для сохранения тайны вмешательства; проводить все действия скрыто от возможных нежелательных очевидцев; осуществлять непрерывный контроль всех исходящих и входящих сообщений; выявить дефекты в системе защиты информации в устройстве, скрытые угрозы [15, с. 19]. Эффективный поиск невозможен без тщательной подготовки, в которую следует включить такие действия, как изучение схемы расположения удаленных устройств и связи между ними; выяснение наличия электронных охранных средств; извлечение необходимой поисковой информации; расшифровка файлов, которые содержат доказательственную базу данных. Понятые, привлекаемые для осмотра киберпространства, должны обладать специальными в этой области знаниями и являться сами пользователями компьютерной техники.

В основной части следственного осмотра киберпространства следует применить некоторые средства, приемы и методы, в частности, использование спе-

циальных программ и технических средств; программно-аппаратных средств для криминалистического исследования компьютерных носителей информации «EnCase Forensic Edition». Осмотр компьютера и киберпространства осуществляется после обнаружения, фиксации и изъятия материально фиксированных следов. Фиксируется состояние компьютера (выключенный компьютер во избежание уничтожения информации не включается): общий вид; наличие механических повреждений, пометок, специальных знаков, печатей, пломб; вид, назначение и технические возможности. При работающем компьютере последовательно производится осмотр дисплея, устанавливается программа, которая относится к расследуемому киберпреступлению, выясняется, какая операционная система установлена на устройстве, какие используются протоколы связи, службы доступа к файлам и сети (локальной или Интернет). Специалист исследует обнаруженную информацию (сведения) в той части киберпространства, которая была задействована в совершении преступного события. Выявленные цифровые следы, электронные документы и иные данные фиксируются и изымаются.

Исследование цифровых следов, изъятых в ходе следственного осмотра киберпространства, осуществляется в рамках судебной экспертизы, которая может проводиться как в лабораторных условиях, так и на месте следственного осмотра киберпространства. Особенности объекта и предмета рассматриваемого вида экспертизы предполагают применения интегрированных методов экспертного исследования и частных экспертных методов. Методика проведения экспертного исследования киберпространства должна воплощать в себе общетеоретическое понимание того факта, что преступная деятельность изобретательна и многовекторна. Методикой такой экспертизы обеспечивается проведение различных исследований на разных структурных уровнях. Ею могут быть исследованы как отдельные объекты, так и их совокупности, в том числе материальные отображения вещной обстановки места происшествия в целом.

Таким образом, особенности поиска и исследования следов в киберпространстве направлены: на получение цифровой информации, ее распознании

с помощью специального аппаратного или программного обеспечения; необходимость привлечения надлежащего специалиста на каждом этапе следственных или иных действий; подбор понятых, обладающих навыками работы с компьютерной техникой и телекоммуникационными сетями, владеющих знаниями в сфере компьютерной технологии.

В заключение на основании проведенного исследования можно сделать вывод о том, что особенности расследования киберпреступлений сопряжены с грамотным следственным осмотром киберпространства, фиксацией, выемкой и исследованием цифровых следов, а также с информационным взаимодействием с экспертом и специалистом.

**Список литературы**

1. Sitarski P. Rozmowa z cyfrowym cieniem model komunikacyjny rzeczywisto^ciwirtualnej. Krakow: RABID, 2002. S. 87.

2. Полякова Н.Л. Новые теоретические перспективы в социологии начала XXI в. // Вестник Московского университета. Серия 18. Социология и политология. 2015. № 2. С. 42.

3. Осипова Н.Г. Прошлое, настоящее и будущее социологической теории в России // Вестник Московского университета. Серия 18. Социология и политология. 2015. № 2. С. 18.

4. Lash S. Critique of information. L., 2002. P. 15.

5. Culture in the Cyber-Age: report from the Asia-Europe Forum. Kyongju, SouthKorea, October 23-25 / ed. by M. le Sourd [et al.]. Singapore: Asia-Europe Foundation, 2001. S. 59.

6. Вершинина И.А. Социальное неравенство в современных городах: перспективы урбанистической революции // Социология города. 2017. № 1. С. 13.

7. Маклюэн М. Понимание медиа: внешние расширения человека. М., 2003. с. 400.

8. Holmes D. Communication theory: media, technology, society. L., 2005. P. 44-45.

9. Кастельс М. Информационная эпоха: экономика, общество и культура. М., 2000. С. 386.

10. Шевченко Е.С. О криминалистической трактовке понятия «киберпреступность» // Информационное право. 2014. № 3 (39). С. 29-32.

11. Мещеряков В.А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. 2013. № 5 (10). С. 265-269.

12. Волеводз А.Г. Противодействие компьютерным преступлениям. М., 2002. С. 159-160.

13. Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. … канд. юрид. наук. Воронеж, 2005. С. 17.

14. Смушкин А.Б. Виртуальные следы в криминалистике // Законность. 2012. № 8.

15. Косынкин А.А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования // Российский следователь. 2012. № 2.

***Л.Ю. Кирюшина,*** *к.ю.н., доцент кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*
***А.С. Соколов,*** *старший преподаватель кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*
***И.В. Кирюшина,*** *к.ю.н., доцент кафедры гражданского права Алтайского государственного университета, г. Барнаул*

## ПСИХОЛОГИЧЕСКИЕ ПРЕДПОСЫЛКИ ВИКТИМНОГО ПОВЕДЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ ПОТЕРПЕВШИХ

Как показывает практика, несовершеннолетние становятся потерпевшими от самых разных видов преступлений, совершаемых с использованием информационных технологий. Это могут быть и мошенничество, и преступления сек-

суальной направленности, и другие преступления, которые затрагивают личные права и свободы подростков, а также причиняют им глубокие нравственные страдания.

Анализ уголовно-правовой статистики, материалов судебно-следственной практики и сообщений СМИ позволяет выявить психологические предпосылки и составить определенный психологический портрет несовершеннолетнего потерпевшего, который становится жертвой преступлений, совершаемых с использованием сети Интернет либо посредством иных информационных и компьютерных технологий.

Полагаем целесообразным в рамках данной статьи остановиться на выявлении и обобщении психологических предпосылок, которые создают условия для формирования виктимного поведения несовершеннолетних потерпевших.

В научной литературе довольно часто используется термин «виктимность», наряду с таким понятием, как виктимология. При этом виктимность традиционно рассматривается в двух аспектах. Во-первых, как предрасположенность отдельных людей стать жертвой преступления. Во-вторых, как неспособность общества и государства защитить своих граждан от преступного посягательства.

Также в отношении потерпевших используется понятие «виктимное поведение», что означает «поведение жертвы». Данный термин используется для обозначения неправильного, неосторожного, аморального, провоцирующего и иного поведения, которое может способствовать совершению преступления. Виктимной нередко именуют и саму личность, имея в виду, что в силу своих психологических и социальных характеристик индивид может стать жертвой. Как справедливо отмечает Е.Е. Центров, «отдельные лица приобретают некоторые виктимогенные качества в силу своего аморального поведения, совершения правонарушений, участия в преступлении» [1, с. 69].

Как показывает практика, нередко жертва преступления является активным элементом в предпреступной ситуации и в самой динамике преступного деяния, выступая активным элементом ситуации [2, с. 97]. Именно такое вик-

тимное поведение можно увидеть в действиях несовершеннолетних, которые становятся жертвами преступлений, совершенных с использованием информационных технологий. Полагаем, что такое виктимное поведение связано с психологическими особенностями, обусловленными возрастными особенностями психики. «Возрастные особенности» — это научный термин, используемый в физиологии и медицине, психологии и педагогике, в криминологии и уголовном праве и ряде других наук [3, с. 69].

В рамках данной статьи представляется целесообразным остановиться на некоторых психологических предпосылках, которые способствуют возникновению отдельных виктимных форм поведения несовершеннолетних потерпевших, при совершении преступлений с использованием информационных технологий:

Общение подростков со сверстниками, по справедливому мнению исследователей, приобретает в подростковый период чрезвычайную значимость [3, с. 473]. Кроме того, именно в этот период потребность в общении со сверстниками становится одной из центральных, а ведущей деятельностью является интимно-личностное общение.

Как отмечают психологи, спецификой интересов в 10-14-летнем возрасте является то, что они во многом реализуют потребность в общении со сверстниками: общие интересы дают повод, содержание, средства общения. Подросток зачастую интересуется тем, чем увлекаются его друзья или одноклассники, этим определяется характерная для подростков «мода на интересы», когда весь класс или даже всю школу охватывает какое-либо увлечение [3, с. 468]. Если эта острая для данного возраста потребность не удовлетворяется в рамках семьи, школы и т.д., то подросток начинает активный поиск круга общения и тех лиц, которые разделяли бы его интересы в рамках интернет-пространства, создавая тем самым условия для возникновения и развития криминальной ситуации. В ряде случаев мы можем даже говорить о таких формах виктимного поведения, как провокация, когда подросток, особенно девушки, проявляют излишнюю активность в общении с более взрослыми по возрасту лицами проти-

воположного пола. Низкий уровень правовой культуры и правовая безграмотность подростков не позволяет дать правильную оценку тому общению, которое возникает в Интернете, и тем последствиям, которые могут наступить.

Своеобразной чертой подростковых интересов, которая влияет на создание криминальной ситуации и создает условия для совершения преступлений в отношении несовершеннолетних с использованием информационных технологий, является безоглядность увлечений, когда они приобретают чрезмерный характер. В попытках удовлетворить свои потребности и реализовать свои увлечения подростки передают информацию, которая относится к персональным данным и защищается законодательством РФ, лицам, которые в дальнейшем используют ее для совершения мошенничества с использованием информационных технологий.

Эмоциональное принятие и непринятие ребенка в семье, как одна из предпосылок виктимного поведения, тесно связана с двумя предыдущими особенностями, поскольку именно в попытке компенсировать и заменить внимание своих родителей подросток начинает активный поиск для общения в Интернете. Учитывая огромную роль семьи в формировании личности, исследователи придают большое значение изучению особенностей семейного воспитания лиц, совершивших преступление. При этом справедливо отмечается, что решающее значение имеет не просто состав семьи (отношения между родителями, даже не их объективно неблаговидное, пусть и противоправное поведение), а главным образом, их эмоциональное отношение к ребенку. Это проявляется в его принятии или, напротив, отвергании [5, с. 40-41]. Крайне важным является неприятие своего ребенка, которое, по справедливому мнению Ю.М. Антоняна, В.Н. Кудрявцева, В.Е. Эминова, может быть и скрытым [5, с. 40-41]. При этом отношения между родителями и детьми в подобных случаях по своей сути нейтральны, а эмоционально никак не окрашены. Особая опасность состоит в том, что каждый живет по-своему и мало интересуется жизнью другого. Поэтому в будущем любому взрослому человеку очень травматично признать, да еще открыто, что родители его не любили, что он был им в тягость. Другую

особую группу риска составляют так называемые «нелюбимые» дети. Отметим, что ежегодно около 500 тыс. детей остаются без одного из родителей, 16% детей рождаются вне зарегистрированного брака, около 100 тыс. воспитываются в государственных учреждениях, среди них — и отказные дети, и дети родителей, лишенных родительских прав, так называемые «социальные сироты» [6, с. 229]. При этом не следует забывать, что еще также группу риска составляют несовершеннолетние потерпевшие из так называемых «внешне здоровых» и «благополучных семей». Основная проблема состоит в том, что в формально «здоровых» семьях, имеющих скрытые дефекты в воспитании, не выступающие в очевидных характеристиках формы поведения их членов, профилактика осложнена объективно [7, с. 40-41]. Актуальнейшей проблемой является деформация нравственных и семейных ценностей в обществе, что наиболее остро отражается на подростковой и молодежной среде. Поскольку в настоящее время многие семьи по разным причинам перестали выполнять свои позитивные воспитательные функции, это нередко прямо или косвенно способствует формированию у детей аморальных, а подчас и противоправных ориентаций, направленных, в том числе, и на близких людей, родственников, а главным образом — на сверстников. Вербальная агрессия проявляется в социальных сетях, группах WhatsApp, Telegram, ВКонтакте и других, и жертвами психического насилия становятся подростки, лишенные внимания и заботы со стороны родителей.

Особая форма проявления возрастного эгоцентризма несовершеннолетних — персональный миф, или миф о собственной исключительности, проявляющийся в убежденности в собственной неуязвимости, в особенности испытываемых чувств. Подростки убеждены в уникальности личных переживаний, поскольку им кажется, что никто другой не переживал и не будет переживать таких страданий или такого восторга, как они.

Общение является одной из важнейших составляющих личности, поскольку именно благодаря общению происходит социализация личности. Социализация подростков путем общения в сети Интернет довольно часто приводит к тому, что несовершеннолетний, становится потерпевшим от своих сверстников,

являющихся членами молодежной преступной группы. Как показывает практика, появляется все больше молодежных групп, в которых такие формы самореализации и самоутверждения, как совершение преступлений и правонарушений, употребление алкоголя и различных запрещенных веществ становится нормой. Оказавшись в криминальной группе, подросток (особенно девушка), вовлекается в совершение противоправных действий, которые не могли бы совершить без соучастников. Появляется уже иная социально психологическая атмосфера, поскольку группа несовершеннолетних оказывается прочно «спаянной» совершенным преступлением.

Освобождение от родительской опеки и стремление заменить ее доверительными, эмоционально окрашенными отношениями со сверстниками и друзьями является по наблюдениям психологов отличительной психологической особенностью присущей подросткам. Подросток стремится иметь близкого верного друга, с которым можно было бы поделиться своими переживаниями, тревогами, трудностями, сокровенными мыслями, который мог бы выслушать, понять и посочувствовать. Также несовершеннолетние все чаще обращаются по самым разным вопросам к близким друзьям, а не к родителям, поскольку именно друзья и приятели придают подростку сил и уверенности в себе, помогают в решении внутренних проблем и межличностных конфликтов [3, с. 474].

Практика показывает, что такое проявление агрессивного поведения, как вербальная агрессия, с улиц и школ шагнула в интернет-пространство и приобрела особые виртуальные формы. Насмешки, третирование, буллинг и другие формы вербальной агрессии в социальных сетях становятся частью повседневной жизни отдельных детей и подростков, поскольку так же, как и раньше есть «дети-обидчики» и «дети-жертвы».

Одним из важных аспектов проблемы агрессивности и психологического насилия в виртуальном пространстве, полагаем, является ее латентный характер. Такие формы насилия по отношению к несовершеннолетнему чаще всего скрыты от внимания родителей, лиц, их заменяющих, классного руководителя и учителей в школе.

Если раньше исследователями детской и подростковой психологии справедливо отмечалось, что круг общения подростков довольно ограничен и его, как правило, составляют, родственники, одноклассники, соседи, друзья и знакомые по кружкам, секциям и т.п., то современное интернет-пространство значительно расширило эти границы. Следовательно, расширился круг лиц, которые могут совершить различные преступные деяния в отношении детей и подростков.

Если раньше криминологи советского и постсоветского периода традиционно отмечали, что группу риска составляют подростки из материально необеспеченных и неполных семей, так называемых «неблагополучных семей», то в настоящее время все больше детей из «внешне здоровых» и «благополучных семей» оказываются вовлеченными в сферу уголовного судопроизводства. Основная проблема состоит в том, что в формально «здоровых» семьях, имеющих скрытые дефекты в воспитании, не выступающие в очевидных характеристиках поведения их членов, профилактика осложнена объективно.

Учитывая вышесказанное, можно сделать вывод, что страх быть непринятым среди сверстников, а также страх быть непонятым родителями, а также страх наказания или порицания со стороны взрослых могут стать предпосылками для формирования так называемой интернет-зависимости у детей и подростков. Кроме того, такие возрастные особенности, как неумение контролировать свои эмоции, выбирать средства общения, справляться со стрессовыми и конфликтными ситуациями, чаще всего приводит к проявлению отдельных форм виктимного поведения, создающих условия для возникновения криминальной ситуации и совершения преступлений в отношении детей и подростков с использованием информационных технологий.

**Список литературы**

1. Центров Е.Е. Криминалистическое учение о потерпевшем. М., 1988. С. 69.

2. Кирюшина Л.Ю. Юридическая психология: учебное пособие. Барнаул: Изд-во Алт. ун-та, 2011. С. 97.

3. Сапронова Н.А. Особенности преступности несовершеннолетних в сельской местности и ее предупреждение (региональный аспект). Барнаул, 2009. С. 58.

4. Психология: учебник для педагогических вузов / под ред. Б.А. Сосновского. М.: Юрайт-Издат, 2005.

5. Антонян Ю.М., Кудрявцев В.Н., Эминов В.Е. Личность преступника. СПб., 2004. С. 40-41.

6. Назарова Е.Н. Основы социальной медицины: учеб. пособие для студ. высш. учеб. заведений / Е.Н. Назарова, Ю.Д. Жилов. М., 2007. С. 229.

7. Кирюшина Л.Ю. Расследование преступлений, совершенных несовершеннолетними: учебное пособие. Барнаул: Изд-во Алт. ун-та, 2012. С. 10.

***Д.А. Книс,*** *адъюнкт Барнаульского юридического института МВД России, г. Барнаул*

## О ЗНАЧЕНИИ ОПЕРАТИВНО-РОЗЫСКНЫХ ХАРАКТЕРИСТИК ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СРЕДЕ, В ДЕЯТЕЛЬНОСТИ ПО ИХ ПРЕДУПРЕЖДЕНИЮ И РАСКРЫТИЮ

Одной из основополагающих тенденций в продолжающемся процессе повсеместной цифровой трансформации современного общества является разработка новых, совершенствование и внедрение имеющихся информационно-телекоммуникационных технологий, способствующих минимизации участия человека в той или иной деятельности. Не является исключением и преступная деятельность. Под воздействием информационно-телекоммуникационных технологий происходит не только изменение внешних проявлений криминальной

активности преступных элементов, но и видоизменяются механизмы самой преступной деятельности.

В контексте оперативно-розыскного познания криминальной деятельности, на наш взгляд, следует обратить внимание на интеграцию последних достижений информационно-телекоммуникационных технологий в такую деятельность, которые закономерно влекут за собой не только появление новых видов криминального поведения и способов совершения преступлений, но и эволюцию механизмов осуществления преступной деятельности, и трансформацию преступлений.

В настоящее время временные затраты преступников, связанные с планированием, совершением и сокрытием преступлений, в значительной степени сокращаются, при этом увеличиваются интеллектуальные затраты, связанные с такой деятельностью. Это требует от сотрудников подразделений уголовного розыска еще большей оперативности в осуществлении не только аналитического поиска, направленного на выявление, пресечение и раскрытие преступлений, но и своевременного оперативно-розыскного прогнозирования совершения преступлений, диагностики сетевого поведения и идентификации преступников в информационно-телекоммуникационных системах.

Для этого необходимо создание в рамках теории ОРД типологических характеристик преступлений, содержащих в своей структуре типичные информационные оперативно-значимые элементы криминальной деятельности, как в социальной, так и в информационно-телекоммуникационной среде. На основе данных характеристик должны быть разработаны частные методики выявления и документирования данных преступлений, ориентированные не только на деятельность специализированных субъектов в области информационно-аналитического обеспечения оперативных аппаратов, но и деятельность всех без исключения субъектов ОРД. Кроме того, необходимо создать систему получения первичной информации, в том числе с использованием программно-аппаратных комплексов и специализированных программ.

Знание о том, что выявленные в ходе осуществления оперативно-розыскной деятельности признаки взаимозависимы и являются частью одного преступного деяния, формируется посредством сопоставления оперативно-розыскной характеристики с реальной оперативно-розыскной ситуацией. Данное сопоставление происходит с применением общенаучных методов и приемов логического мышления, в результате чего оперативный сотрудник познает или изучает находящуюся в его распоряжении информацию с целью использования ее при выявлении преступлений в информационно-телекоммуникационной среде.

Обобщая вышеизложенное, представляется возможным сделать вывод, что система получения первичной информации должна строиться на основе анализа информации, характеризующей индивидуальные признаки криминальной активности криминальной среды, которые соподчинены общей картине оперативно-значимого поведения, и их возможно получить из оперативных источников в информационно-телекоммуникационной среде [1, с. 136].

В то же время сотрудники подразделений уголовного розыска в процессе познания в информационно-телекоммуникационной среде сталкиваются со следующими проблемами:

- выявления в инфотелекоммуникационной среде стабильных каналов получения значимой оперативно-розыскной информации;
- систематизации каналов получения значимой оперативно-розыскной информации;
- оптимизации поступающих из каналов информационных потоков и др.

Для оперативного решения данных актуальных проблем в рамках теории ОРД необходимо системное изучение закономерностей отражения значимой оперативно-розыскной информации в сетевых ресурсах, с выявлением особенностей применения оперативно-поисковых методов для ее обнаружения, получения, оценки, проверки и фиксации в информационно-телекоммуникационной среде. Изучение данных закономерностей, их обобщение и систематизация также входит в перечень задач, которые возможно решить в рамках оперативно-розыскной

науки на основе моделирования оперативно-розыскных характеристик преступлений, совершаемых в информационно-телекоммуникационной среде.

Кроме того, следует отметить, что преодоление указанных проблем возможно только с помощью создания условий для расширения практического использования научно обоснованных рекомендаций, выработанных в рамках теории оперативно-розыскной деятельности с учетом оперативно-розыскной характеристики преступлений.

Использование в деятельности оперативных подразделений комплексов практико-ориентированных, научно обоснованных рекомендаций на основе оперативно-розыскной характеристики, соотнесенной с постоянно пополняющимся массивом не только типовых оперативно-розыскных ситуаций, но и различных вариантов их развития, позволит также:

- определить оптимально возможные тактические варианты оперативного воздействия на сетевые сообщества и группы в социальных сетях, которые вызывают подозрение в организации и осуществлении противоправной деятельности в информационно-телекоммуникационной среде;
- улучшить качество комплексного планирования, подготовки оперативно-розыскных и оперативно-технических мероприятий с учетом различных разноплановых факторов, оказывающих негативное воздействие на развитие конкретной оперативно-розыскной ситуации в информационно-телекоммуникационной среде;
- обеспечивать оперативный сбор и систематизацию максимально полной значимой информации о сетевых объектах в инфотелекоммуникационной среде;
- выявлять и визуализировать латентные связи объектов в информационно-телекоммуникационной среде с иными объектами и событиями, как предкриминального, криминального, так и посткриминального характера;
- определять основные направления осуществления мониторинга появления в информационно-телекоммуникационном пространстве объектов с не-

обходимыми свойствами, указывающими на высокую вероятность подготовки, совершения, либо сокрытия действий криминального характера;

- создавать и дополнять социальные и сетевые поведенческие профили, характеризующие лиц, не только осуществляющих противоправную деятельность, но и совершающих определенные виды преступлений по средствам информационно-телекоммуникационной среды и др. [2, с. 18.]

Но несмотря на широкий спектр направлений использования, оперативно-розыскной характеристики и решаемых посредством ее моделирования задач, возложенных на оперативные подразделения органов внутренних дел, существует ряд проблем как теоретического, так и прикладного характера, требующих решения.

К числу таких проблем теоретического характера, по нашему мнению, следует отнести необходимость развития учения об оперативно-розыскной характеристики, как методологической основы мер предупреждения преступлений, совершаемых в том числе посредством информационно-телекоммуникационной среды, а также необходимости разработки новых эффективных методик оперативно-розыскного противодействия данному виду преступлений [3, с. 235].

К числу проблем практического характера следует отнести назревшую необходимость законодательного закрепления полномочий органов, осуществляющих оперативно-розыскную деятельность, на проведение систематического мониторинга опубликованных в различных социальных сетях или иных информационно-телекоммуникационных ресурсов материалов явно противоправного характера. При этом следует сделать акцент на возможность обеспечения в некоторых случаях проведения соответствующих оперативно-розыскных мероприятий с возможностью отслеживания сообщений, передаваемых по информационно-телекоммуникационным сетям в реальном времени, или получения необходимой значимой информации от провайдеров или Роскомнадзора напрямую без судебного разрешения (с последующей уведомительной процедурой) для своевременного принятия мер оперативного реагирования [4, с. 96.] Возможно, также обязать провайдеров и создателей и администраторов мессен-

джеров и интернет-ресурсов об обязательном немедленном уведомлении правоохранительных органов о выявлении и блокировке того или иного ресурса, нарушающего законы Российской Федерации.

Отметим, что распространение информационно-телекоммуникационных технологий в настоящее время проникает все больше в различные сферы, и практически ни одно преступление не обходится без оставления информационных следов в электронной среде. Поэтому одна лишь блокировка контента или группы в социальной сети не решит проблемы. В случае выявления того или иного сообщества считаем, что до его блокировки необходимо предварительно ограничить данную группу для вступления в нее новых членов и скрыть это сообщество от незарегистрированных пользователей, при этом дать возможность внедрения в данную группу оперативных сотрудников для выявления организаторов и основных членов. Оперативные работники должны составить профили каждого из членов сообщества, так как каждый из них может представлять не меньшую потенциальную опасность для общества, чем его организаторы.

## Список литературы


1. Родевич В.Ч., Войтихович С.А. Методы и модели комплексной оценки информации субъектами оперативно-розыскной деятельности при выявлении экономических преступлений // Вестник Полоцкого государственного университета. Серия D. Экономические и юридические науки. 2017. № 13. С. 135-141.
2. Осипенко А.Л. Новые технологии получения и анализа оперативно-розыскной информации: правовые проблемы и перспективы внедрения // Вестник Воронежского института МВД России. 2015. № 2. С. 13-19.
3. Давыдов С.И. Некоторые подходы к разработке частных оперативно-розыскных методик раскрытия преступлений в условиях цифровизации // Современные технологии и подходы в юридической науке и образовании: сборник материалов международного науч.-практ. форума. Калининград, 2021. С. 234-240.
4. Аносов А.В. Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий // Труды Академии управления МВД России. 2018. № 4 (48). С. 93-97.

***А.Б. Кокушев,*** *адъюнкт Волгоградской академии МВД РФ, г. Волгоград*

# ИДЕНТИФИКАЦИЯ СТРЕЛЯНЫХ ГИЛЬЗ ПРИ ПОМОЩИ АВТОМАТИЗИРОВАННОГО БАЛЛИСТИЧЕСКОГО ИНФОРМАЦИОННОГО КОМПЛЕКСА (АБИК) «EVOFINDER» (ПО МАТЕРИАЛАМ РЕСПУБЛИКИ КАЗАХСТАН)

Казахстан является исконно животноводческим государством с огромной территорией, на которой имеются десять государственных природных заповедников общей площадью 1 510 419 га[2] и более 30 заказников, где под охраной государства находится животный мир. Однако это не мешает браконьерам вести приступную деятельность по отстрелу животных, занесенных в «Красную книгу» и находящихся на охраняемой территории. Так, по ст. 337 Уголовного кодекса Республики Казахстан «Незаконная охота» в 2020 г. в единый реестр досудебного расследования было зарегистрировано 160 фактов, из которых по 45 уголовным делам были прерваны сроки досудебного расследования ввиду того, что лицо, его совершившее не установлено.

Преступления, совершенные с применением огнестрельного оружия на территории Республики Казахстан, относятся к категории тяжких и особо тяжких. На сегодняшний день в Республике Казахстан по статистическим данным, предоставленными Комитетом по правовой статистике, и специальным учетам Генеральной прокуратуры РК, за последние пять лет число совершенных преступлений с применением огнестрельного оружия сократилось более чем в два раза, с 488 в 2015 г. до 224 правонарушений в 2020 г. [1]. Этому способствовало проведение государством акции по выкупу у населения незаконно хранящегося огнестрельного оружия, которое осуществляется на основании приказа Министра внутренних дел РК от 27 марта 2015 г. № 266 «Об утверждении правил добровольно возмездной сдачи гражданами незаконно хранящегося огнестрельного оружия, боеприпасов и взрывчатых веществ» [2].

Для раскрытия и расследования преступлений, совершенных с применением нарезного огнестрельного оружия, на базе Оперативно-криминалисти-

ческого департамента МВД РК (далее — ОКД МВД РК) создана Республиканская пулегильзотека. В соответствии с п. 27 «Правил формирования Государственной пулегильзотеки», утвержденных Постановлением Правительства РК от 24 июня 2019 г. № 429, наряду с натурными ведомственными коллекциями не исключается возможность формирования электронного массива изображений контрольных пуль и гильз с использованием автоматизированных информационных баллистических систем (далее — АИБС) [3].

На вооружение криминалистических подразделений МВД в качестве АИБС взята система «Evofinder». Благодаря проверке по АИБС «Evofinder» ОКД МВД РК в 2020 г. было получено 30 положительных результатов идентификации нарезного огнестрельного оружия, способствовавших раскрытию и расследованию совершенных преступлений. Основным видом преступлений, по которым получена идентификация оружия, являются факты незаконной охоты на охраняемой территории, а также охоты на редких животных, занесенных в Красную книгу. Преступления по фактам незаконной охоты, совершенные с применением огнестрельного оружия, министр Внутренних дел РК взял на особый контроль, в этой связи было дано поручение руководству ОКД МВД РК для перевода в электронный формат контрольных пуль и гильз гражданского и служебного нарезного огнестрельного оружия.

На сегодняшний день криминалистическими подразделениями МВД РК ведется криминалистическая пулегильзотека по следующим видам:

1) коллекции пуль, гильз и патронов со следами оружия, изъятого с мест совершения преступления;

2) коллекции пуль и гильз, отстрелянных из изъятого, утраченного (похищенного), найденного и добровольно сданного гражданского, служебного и боевого нарезного огнестрельного оружия;

3) коллекции пуль и гильз, отстрелянных из самодельно изготовленного, в том числе атипичного или переделанного нарезного оружия;

4) натурной коллекции огнестрельного оружия и боеприпасов;

5) изображения контрольных пуль и гильз, отстрелянных из гражданского и служебного огнестрельного оружия, полученные системой «Evofinder».

АИБС, созданная на базе системы «Evofinder», сократила время проверок пуль и гильз, изъятых с мест происшествий, по криминалистической пулегильзотеке, так как вся информация с серверов региональных криминалистических подразделений по локальной сити автоматически передается в ОКД МВД РК.

Система «Evofinder» является передовой разработкой компании ScannBI Technology, где для получения 3D-изображений боковой поверхности пуль и донца гильз используется адаптированная технология динамической фокусировки «Focus Variation Microscopy», лазерная триангуляция и монофотограмметрия [4, с. 174]. В данной системе также внедрены инновационные технологии, такие как «Вертикальный сдвиг кадра», «Компенсация наклона поверхности», «Плавающий кадр», «Создание реальной поверхности», «Построение формы пули», «Многослойное освещение» и 100-кадровая технология. Сама система «Evofinder» состоит из трех основных интегрированных частей: станция анализа данных, станция ввода данных и рабочая станция эксперта, которые объединены в локальную или распределительную сеть. Станция ввода данных системы предназначена для получения цифровых изображений боковых поверхностей, а также дна (основания) цилиндрических объектов и сохранения их в памяти компьютера. Получение цифровых изображений осуществляется за счет сканирующего устройства, которое осуществляет цифровой покадрово-фрагментный ввод изображения исследуемого объекта [5].

Принцип работы системы «Evofinder» существенно не отличается от других систем, стоящих на вооружении ОКД МВД РК, таких как «Папилон», «Образ ++» и т.д. Поиск осуществляется по следам, указанным оператором. Из курса баллистики и судебно-баллистической экспертизы мы знаем, что к таковым относятся:

1) трассы на боковых поверхностях пуль, образованные от нарезов канала ствола:

– первичные следы;

– вторичные следы;

– следы дна нарезов.

2) на гильзах

– след бойка на капсюле гильзы;

– след выступа отражателя;

– след зацепа выбрасывателя;

– след патронного упора [6, с. 66].

В данной статье мы бы хотели по подробнее рассмотреть работу АИБС «Evofinder» с гильзами и идентификацию стреляных гильз. При влитии исследуемой гильзы для проверки по имеющейся гильзотеке оператор устанавливает гильзу в сканирующем устройстве, затем определяет «систему оружия», соответствующую установленной гильзе. Основные параметры выделенной системы оружия, необходимые для записи изображения поверхностей, отображаются в информационных окнах. Для гильзы это параметры установки в кассету для ее дальнейшего сканирования и параметры записи (диаметр следа бойка, количество дополнительных признаков, подлежащих записи). Общими параметрами являются наименование системы оружия и тип патрона, для которого разрабатывалась данная система оружия. Тип патрона определяет следующие значения, используемые системой для записи изображений:

– калибр, мм;

– диаметр дна гильзы, мм;

– диаметр капсюля, мм.

Далее для корректной работы функции записи дна выполняется определение координат плоскости дна гильзы по трем точкам, данная процедура может проходить как в автоматическом режиме, так и в ручном. После окончания записи изображения дна гильзы и его обработки оно загружается на экран монитора для просмотра и инициализации процедуры записи следа бойка и следа «Зуба» отражателя. Технология «Плавающего кадра» обеспечивает одинаковость условий записи каждого кадра, уменьшает влияние децентрирования объектов на качество изображения и повышает воспроизводимость изображений (см. рис. 1).

Рис. 1. Вид донца гильзы, отсканированного с помощью системы «Evofinder»

После проведения сканирования полученное изображение донной поверхности гильзы сохраняется с соответствующим заполнением необходимых идентификационных данных. При выборе конкретного изображения гильзы становится возможным назначить проверку по уже имеющимся в базе данных изображений гильз путем «автопоиска». Схожесть полученных совпадений подразделяется в системе на две группы:

1) совпадения по рельефу патронного упора с коэффициентов схожести от меньшего к большему;

2) совпадения по следу бойка с выведением среднего значения нескольких коэффициентов схожести.

Как и в случае с другими криминалистическими автоматизированными идентификационными базами данных, АИБС «Evofinder» дает лишь рекомендательный список пуль и гильз, отстрелянных из огнестрельного нарезного оружия, последнее же слово в идентификации объектов остается неизменно за оператором.

Рассматривая криминалистическую характеристику незаконной охоты, многие авторы выделяют такую характеристику, как сокрытие следов совершения преступления. После совершения любого вида преступления лицо, его совершившее, обычно предпринимает все необходимые меры к его сокрытию. Способ сокрытия преступления также, в свою очередь, можно разделить на несколько видов:

– сокрытие предмета преступления;
– сокрытие вещественных доказательств;
– сокрытие следов совершения преступления [7, с. 158].

Нами же рассмотрен еще один из способов сокрытия преступления — это видоизменение отдельных частей следообразующих деталей огнестрельного оружия.

В начале 2020 г. в Северо-Казахстанской области на территории одного из заказников при обходе территории егерем были обнаружены останки одиннадцати голов сибирской косули. На месте происшествия были обнаружены тринадцать гильз от нарезного огнестрельного оружия, четыре гильзы калибра 7,62х39 мм и девять гильз калибра 7,62х51 мм. При проверке стреляных гильз по АИБС «Evofinder» установлено, что четыре гильзы калибра 7,62х39 мм стреляны из одного карабина, принадлежащего одному из жителей районного центра. Оставшиеся девять гильз были стреляны из другого неустановленного карабина. Далее после формирования региональной базы данных через некоторое время и повторной проверки по пулегильзотеке карабин был установлен. Процесс идентификации оружия был затруднен тем, что подозреваемый внес существенные изменения в следообразующие детали оружия после совершения преступления, спилив боек (рис. 2). На данный факт указывает след бойка на контрольных гильзах, отстрелянных из карабина подозреваемого. Диагностическими признаками в данном случае являются (рис. 3):

- ровные, близкие к геометрическим края дна следа;
- наличие углублений линейной формы на дне следа.

Рис. 2. Вид бойка со следами механического воздействия

Рис. 3. Вид следа бойка на контрольных гильзах

Внесенные изменения в следообразующую поверхность (боек) огнестрельного оружия сделали следы бойка на гильзах, изъятых с ОМП, и контрольных гильзах несопоставимыми, соответственно, АИБС «Evofinder» не включает данные изображения гильз в рекомендательный список для проверки оператором, ввиду малого процента схожести следа бойка проверяемого объекта с другими.

В данном случае при изменении отдельных следообразующих деталей (боек, зуб отражателя) патронный упор менее остальных деталей подвержен видоизменениям и является более информативным с большим идентификационным периодом. Соответственно, оператором был выбран след патронного упора для проверки по АИБС «Evofinder», по которому и был установлен карабин подозреваемого (рис. 4).

Рис. 4. Сопоставление изображений патронного упора гильз
(слева — изъятая с ОМП, справа — контрольная)

Изменения, вносимые в следообразующие детали огнестрельного оружия, затрудняют его идентификацию. Однако ввиду неосведомленности преступники видоизменяют не все следообразующие детали, а лишь часть из них. Следообразующие детали огнестрельного оружия создают идентификационное поле, изменение части из них не лишает систему «Evofinder» для его идентификации. Нами предлагается разработать алгоритм действий оператора АИБС «Evofinder» по идентификации нарезного огнестрельного оружия по стреляным гильзам с признаками изменения следообразующих деталей оружия.

## Список литературы

1. Информационный сервис Комитет по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан. [Электронный ресурс]. URL: https://www.qamqor.gov.kz/portal/page/portal/POPageGroup/Services/Pravstat?_piref36_258157_36_223082_223082.__ora_navigState=eventSubmit_doSearch%3D%25D0%259F%25D0%25BE%25D0%25B8%25D1%2581%25D0%25BA%26p_YEAR%3D2016%26p_MONTH%3D12%26p_AREA%3

D190000%26p_REG%3D1900__%26p_DEP%3D000%26page%3Dmode_report%26currPage%3D1&_piref36_258157_36_223082_223082.__ora_navigValues=.

2. Приказ Министра внутренних дел РК от 27 марта 2015 года № 266 «Об утверждении правил добровольно возмездной сдачи гражданами незаконно хранящегося огнестрельного оружия, боеприпасов и взрывчатых веществ». [Электронный ресурс]. URL: https://online.zakon.kz/document/?doc_id=34330761#pos=5;-106.

3. «Әділет» информационно-правовая система нормативно-правовых актов Республики Казахстан. [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/P1900000429.

4. Юматов В.А., Полякова А.В. Возможности идентификации нарезного огнестрельного оружия по следам на деформированных пулях. Н. Новгород: Нижегородский государственный университет им. Н.И. Лобачевского, 2018.

5. Официальный сайт компании ScannBI Technology Europe GmbH. [Электронный ресурс]. URL: http://evofinder.com/contact-us/.

6. Стальмахов А.В., Сумарока А.М., Егоров А.Г., Сухарев А.Г. Судебная баллистика и судебно-баллистическая экспертиза. Саратов, 1998. С. 113.

7. Чаплыгина В.Н. Структурные элементы криминалистической характеристики незаконной охоты. Иркутск, 2021. С. 155-162.

***А.А. Количенко,*** *адъюнкт Нижегородской академии МВД России, г. Нижний Новгород*

## ИСТОКИ НОВОЙ ТЕОРИИ ОЦЕНКИ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В РОССИЙСКОМ УГОЛОВНОМ ПРОЦЕССЕ

Проблема доказательств и доказывания в уголовном судопроизводстве исторически относится к числу наиболее актуальных проблем, как в теоретическом, так и практическом смысле. Проблемным является и само понятие дока-

зательств, включающее в себя целую систему элементов, так и не получивших однозначной теоретико-методологической оценки. В числе этих загадочных элементов по-прежнему находятся источники доказательств, которые современный законодатель позиционирует как виды доказательств.

Статья 74 УПК РФ определяет семь видов доказательств. Казалось бы, что в этой норме сформулирована универсальная исторически сложившаяся система источников доказательственной информации, к которой уже просто невозможно добавить ничего нового. Однако в последние годы в научной доктрине и правоприменительной практике все острее развивается дискуссия о необходимости введения в эту систему нового элемента — электронных доказательств.

С одной стороны, для этого есть материальные предпосылки. Для начала можно привести статистку количества совершаемых преступлений с использованием электронной информации, электронных носителей информации. Согласно официальной статистике МВД России о состоянии преступности в России за январь-сентябрь 2020 г., наблюдается рост числа преступлений в интернет-пространстве. В отчетном периоде преступлений с использованием IT-технологий совершено на 77% больше, чем год назад, в том числе с использованием сети «Интернет» — на 93,2%, при помощи средств мобильной связи — на 97,7% [3]. При этом необходимо понимать, что не только преступления в сфере компьютерной информации, предусмотренные ст. 272-274 Уголовного кодекса Российской Федерации, но и многие другие «традиционные» общественно опасные деяния оставляют после себя электронные следы в компьютерных сетях, на магнитных или оптических носителях, экранах мониторов [1, с. 7].

Но материальные предпосылки — не единственный стимул дискуссии о специфике электронных доказательств. Вопрос этот крайне актуален в самых разных процедурных плоскостях. Во всяком случае, он однозначно выходит далеко за рамки чисто теоретического любопытства. Вопрос об идеологических и методологических основаниях принципиально новой трактовки электронных доказательств, не вписывающейся в традиционные схемы, является крайне

важным и в прикладной плоскости, в практическом судопроизводстве на досудебном и судебном этапах.

От правильного научного понимания электронных доказательств, от глубокого обоснования унифицированного или дифференцированного подхода к их интерпретации зависит и такой прикладной элемент процесса доказывания, как оценка доказательств. Оценка доказательств, по справедливому заключению многих ученых, является самым сложным элементом процесса доказывания. Это только на первый взгляд принцип свободной оценки представляется делом легким и не стесненным никакими правилами. На самом же деле свободная оценка не может обойтись и без четких формальных критериев.

Оценка электронных доказательств в силу специфики самой электронной информации, ее содержательного и «материального» разнообразия требует разработки особого теоретического и практического инструментария. И для качественной научной разработки этого инструментария необходимо широко и непредвзято посмотреть на теоретическое наследие, связанное с оценкой доказательств. Посмотреть в самом широком историческом смысле.

Мы полагаем, что теория формальной оценки доказательств была необоснованно вынесена на теоретические «задворки». Эта теория была не только отвергнута, она была приговорена к забвению. Причем по чисто идеологическим причинам. Сегодня не только студенты юридических вузов, но даже и преподаватели не имеют глубокого представления об этой теории, о которой выдающийся русский процессуалист В.Д. Спасович очень душевно написал следующее. «На выработание этого процесса слагались целые века неутомимой работы. Тут есть и доля римского права времен дряхлеющей империи, и весьма многое из права канонического, и масса случайных средневековых наростов. Весь этот процесс направлен к тому, чтобы дойти до полнейшего раскрытия истины материальной. Весь он основан на отвлеченной теории вероятностей, на вере в безошибочность объективных правил, выведенных разумом из долговременного опыта и основанных на глубоком знании свойств человеческого ума и сердца, на вере в возможность разрешить посредством их всевозможные

случаи жизни практической. Отличительный характер этой системы заключается в том, что закон ничего решительно не предоставляет произволу судьи, но определяет *a priori,* какую силу должно иметь каждое доказательство, так что судье оставалось только механически взвешивать эти доказательства объективной, законом данной меркой и быть простым орудием и исполнителем закона, не принимая ничего на свою совесть» [2, с. 29].

Полагаем, что теория формальных доказательств является интересной не только в части идеи ограничения судейского произвола. Интересной является сама идея формализации оценки доказательства, но уже в новом технологическом контексте. Современная наука напрямую столкнулась с феноменом электронных доказательств, являющихся предвестником внедрения в уголовное судопроизводство искусственного интеллекта. И эти доказательства поставили на повестку дня вопрос об особых критериях этой оценки, в частности о критерии допустимости. В рамках этих вопросов встал вопрос и о новых элементах формальной оценки электронных доказательств. Уголовный процесс, несмотря на весь свой консерватизм, неизбежно стоит перед вопросом о внедрении искусственного интеллекта. А для этого уголовному процессу нужна новая теория оценки электронных доказательств и новая технология практического внедрения положения этой теории.

## Список литературы

1. Зуев С.В. и др. Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / отв. ред. С.В. Зуев. М.: Юрайт, 2020. 193 с.

2. Спасович В.Д. Избранные труды и речи / сост. И.В. Потапчук. Тула, 2000. 496 с.

3. Краткая характеристика состояния преступности в Российской Федерации за январь — сентябрь 2020 года. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/21551069/ (дата обращения: 10.04.2021).

***М.В. 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*

# О НЕКОТОРЫХ ОСОБЕННОСТЯХ МЕХАНИЗМА НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ, СОВЕРШАЕМОГО БЕСКОНТАКТНЫМ СПОСОБОМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Как было отмечено в выступлении Министра внутренних дел Российской Федерации генерала полиции В.А. Колокольцева на расширенном заседании Коллегии МВД России, преступления, совершенные с использованием информационно-телекоммуникационных технологий, составляют большую часть в общей структуре преступности (в 2020 г. — 25%). В последние несколько лет прослеживается устойчивая динамика ежегодного прироста. Кроме этого, в течение 2020 г. на территории Российской Федерации пресечена противоправная деятельность 256 подпольных нарколабораторий по изготовлению синтетических наркотиков. Активно проводилась работа по пресечению фактов сбыта наркотических средств с использованием информационно-телекоммуникационных технологий и внебанковских систем оплаты. Общее количество преступных деяний, совершенных указанным способом, в 2020 г. превысило 47 тысяч и составило 1/4 от общего числа зарегистрированных наркопреступлений[23].

В соответствии с п. 9 Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 г., утвержденной Указом Президента Российской Федерации от 23.11.2020 № 733, к основным угрозам национальной безопасности в сфере оборота наркотиков, а также в области

[23] Выступление Министра внутренних дел Российской Федерации генерала полиции В.А. Колокольцева на расширенном заседании коллегии Министерства внутренних дел Российской Федерации: официальный сайт МВД России. [Электронный ресурс]. URL: https: мвд.рф. (дата обращения: 28.04.2021).

противодействия их незаконному обороту относятся: появление новых форм противоправной деятельности организованных групп и преступных сообществ (преступных организаций), в том числе транснациональных, усиление ими конспирации каналов поставки и сбыта наркотиков с использованием инновационных коммуникационных и других новых технологий; применение новых способов оплаты приобретаемых наркотиков; масштабное использование сети «Интернет» для пропаганды незаконного наркопотребления.

Из этого следует, что отдельные сегменты информационно-телекоммуникационной сети «Интернет» являются благоприятными площадками для развития теневой деятельности, связанной с незаконным сбытом наркотических средств и психотропных веществ дистанционным способом на территории нашего государства, что способствует росту уровня преступности в сфере незаконного оборота наркотиков и ухудшению отдельных показателей наркоситуации.

Именно поэтому в целях совершенствования антинаркотической деятельности и государственного контроля за оборотом наркотиков в рамках реализации вышеуказанной Стратегии запланированы такие меры, как выявление и пресечение функционирования в сети «Интернет» ресурсов, используемых для пропаганды незаконных потребления и распространения наркотиков; развитие системы мониторинга наркоситуации, в том числе создание и внедрение единого цифрового контура этой системы с учетом национальных приоритетов в сфере информационных технологий, сбора и обработки статистических данных.

В свою очередь, сокращение преступлений, связанных с наркотиками, осуществляется путем развития механизмов выявления и пресечения наркопреступлений, совершаемых с использованием современных информационных технологий, в том числе организованными группами и преступными сообществами (преступными организациями)[24].

---

[24] Указ Президента Российской Федерации от 23.11.2020 № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года». [Электронный ресурс]. URL: http://www.consultant.ru (дата обращения: 28.04.2021).

Как пишет Н.Т. Кузьмин, 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 незнаком 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 наркопреступниками 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].

В основном незаконный сбыт наркотических средств бесконтактным способом с использованием информационных технологий осуществляется посредством использования так называемых «интернет-магазинов», для которых характерны определенные функционально-отличительные особенности и способы противоправной деятельности.

Так, С.И. Земцова выделяет следующие характерные черты таких интернет-магазинов:

- наличие самостоятельных структурных формирований;
- значительное количество участников;
- использование программ для обмена сообщениями и медиафайлами при общении между участниками преступного сообщества;

- применение комплекса мер, обеспечивающих высокий уровень конспирации;
- использование криптовалюты при осуществлении преступной деятельности;
- распространение наркотических средств на территории нескольких регионов нашей страны одновременно, а также в отдельных случаях и на территории других государств;
- наличие разработанных должностных инструкций, предусматривающих обязанности каждого из участников, систему поощрений и наказаний.

Руководствуясь всеми вышеуказанными признаками, характеризующими противоправную деятельность интернет-магазинов по продаже наркотиков, данный автор приходит к выводам, что в зависимости от масштаба преступной деятельности такие интернет-магазины можно разделить на: 1) функционирующие в одной местности, городе, крае, области, районе и относящиеся к небольшим; 2) осуществляющие преступную деятельность в различных городах России, а в отдельных случаях — в странах ближнего и дальнего зарубежья, имеющие филиалы (представительства) и относящиеся к крупным; 3) реализующие наркотические средства посредством объединения в межрегиональные преступные альянсы [2, с. 19-20].

Ранее нами уже было написано о том, что бесконтактный способ сбыта наркотиков заключается в подыскании злоумышленниками клиентов путем размещения объявлений о продаже наркотических средств. Покупатели производят оплату денежных средств за наркотики через электронные платежные системы, а последующее получение запрещенного товара осуществляется через тайники. В результате такого способа не происходит непосредственного личного контакта между сбытчиком и приобретателем наркотиков, что имеет важное криминалистическое значение [6, с. 84].

Среди наркосбытчиков, использующих бесконтактный способ совершения наркопреступлений с использованием инновационных технологий, имеет место конкретное распределение ролей при организации преступной деятельности. Одни осуществляют общее руководство, другие непосредственно заказывают

и получают вещества, предназначенные для наркопроизводства, или сами наркотики, третьи занимаются непосредственным производством или фасовкой наркотических средств, четвертые занимаются изучением спроса и предложения на наркотики на теневом рынке, в соответствии с которыми распределяют наркотические средства по мелкооптовым и розничным продавцам. В этой иерархической системе серьезное значение уделяется вопросу конспирации. Многие члены группы между собой не знакомы, так как лично не встречаются, а движение наркотиков почти на всех уровнях происходит посредством «закладок», т.е. тайников [6, с. 85].

При осуществлении незаконного сбыта наркотических средств с использованием информационных технологий широко используются системы мгновенного обмена сообщениями (мессенджеры) WhatsApp, Viber, Telegram и др.

Наркопотребителю достаточно найти контакт наркосбытчика в любом из мессенджеров, связаться с продавцом наркотиков в целях приобретения запрещенного товара и оплатить его, после чего «оператор» сообщит приобретателю место «закладки» (тайника) с наркотиками.

Как покупатель, так и продавец используют при этом анонимайзеры TOR или VPN, предназначенные для сокрытия информации о точке доступа и выхода в Интернет, об IP-адресе или пользователе в сети удаленного сервера. Производством тайников с наркотиками занимаются «закладчики» («кладмэны», или «минеры»), которые заранее выбирают место для размещения наркотических средств и отправляют сведения об их местоположении «оператору» [1, с. 187].

Учитывая все вышеизложенные особенности механизма совершения преступлений, связанных с незаконным сбытом наркотических средств с использованием информационно-телекоммуникационных технологий, бесспорно можно прийти к выводу, что выявление, пресечение и раскрытие преступлений рассматриваемой категории невозможно без использования потенциала оперативно-розыскной деятельности, о чем также свидетельствуют научные взгляды некоторых других авторов [5, с. 195-196].

В связи с этим полагаем, что основными способами противодействия наркосбыту в сети «Интернет» являются следующие виды оперативно-розыскных мероприятий (ОРМ):

- ОРМ «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;
- ОРМ «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;
- ОРМ «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;
- ОРМ «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;
- ОРМ «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;
- ОРМ «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;

- ОРМ «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.);
- ОРМ «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 [3, с. 111-112].

Считаем, что только посредством организации и проведения именно этих вышеуказанных ОРМ возможно осуществление наиболее оптимального и результативного противодействия незаконному обороту наркотических средств и психотропных веществ на территории нашего государства, особенно в условиях глобализации информационных технологий и роста цифровизации в современном обществе.

## Список литературы

1. Бертовский Л.В., Девяткин Г.С. Криминалистические аспекты расследования преступлений, связанных с незаконным оборотом наркотических средств (типовые способы совершения преступлений как элемент криминалистической характеристики) // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXIII Международной научно-практической конференции (2-3 апреля 2020 г.) в 2 ч. / отв. ред. Д.В. Ким; ФГКОУ ВО

«Сибирский юридический институт Министерства внутренних дел Российской Федерации». Красноярск: СибЮИ МВД России, 2020. Ч. 1. С. 187-189.

2. Земцова С.И. Бесконтактный сбыт наркотических средств с использованием интернет-магазинов: актуальные вопросы // Наркоконтроль. 2019. № 3. С. 17-22.

3. Кондратьев М.В. Некоторые особенности оперативно-розыскного выявления, пресечения и раскрытия незаконного сбыта наркотических средств, совершаемого с использованием информационно-телекоммуникационных технологий // 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 Алтайского университета, 2020. С. 107-112.

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.

5. Нугаева Э.Д., Имаева Ю.Б. О некоторых возможностях взаимодействия следователя с органами, осуществляющими оперативно-розыскную деятельность при выявлении, раскрытии и расследовании преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ, новых потенциально опасных психоактивных веществ, совершенных бесконтактным способом // Актуальные проблемы борьбы с преступностью на современном этапе: сборник статей по материалам Международной научно-практической конференции 28-30 октября 2020 г. и межведомственного круглого стола 23 июня 2020 г. Волгоград: Волгоградская академия МВД России, 2020. С. 192-197.

6. Поляков В.В., Кондратьев М.В. Криминалистические особенности бесконтактного способа совершения наркопреступлений // Известия Алтайского государственного университета. 2015. № 2/1 (86). С. 83-86.

***А.А. Корчагин,*** *к.ю.н., доцент, доцент кафедры уголовного права и таможенных расследований Санкт-Петербургского государственного университета аэрокосмического приборостроения, г. Санкт-Петербург*

## ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ДРУГИХ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ В ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОМ ОБЕСПЕЧЕНИИ ПРЕДВАРИТЕЛЬНОГО И СУДЕБНОГО СЛЕДСТВИЯ ПО УГОЛОВНЫМ ДЕЛАМ ОБ УБИЙСТВАХ

В настоящее время эффективная борьба с умышленными убийствами невозможна без активного использования современных достижений науки и техники. В этих условиях необходимо вести речь о разработке эффективного технико-криминалистического обеспечения предварительного расследования и судебного разбирательства по уголовным делам об убийствах.

Способы совершения некоторых видов убийств обусловливают необходимость применения для их расследования широкого спектра технических средств и других достижений естественных и технических наук. Так, при совершении убийств с применением огнестрельного оружия, взрывных устройств, взрывчатых веществ для обнаружения, фиксации, изъятия обусловливает использование широкого спектра технических средств, позволяющих обнаруживать как само оружие, так и следы его применения.

При совершении убийств убийцы используют технические средства в процессе подготовки, совершения, сокрытия убийств, особенно когда речь идет о таких видах убийств, как убийства по найму, убийства, совершенные органи-

зованными преступными группами, серийные убийства, убийства, совершенные с применением взрывных устройств, поджогов, убийства, инсценированные под ДТП, и т.п.

В таких условиях разработка и внедрение в практику современных технических средств как российского, так и иностранного производства, современной компьютерной техники, специально разработанных для правоохранительных органов (в том числе следственных органов) компьютерных программ могло бы существенно повысить эффективность деятельности по раскрытию и расследованию убийств.

Однако как показывает практика, современные технические средства в практической деятельности по раскрытию и расследованию убийств практически не используются, зачастую ввиду их отсутствия, следственные отделы районного уровня не имеют необходимых технических средств. В этих условиях значимость технико-криминалистического обеспечения предварительного расследования и судебного разбирательства убийств особенно актуальна. Ему уделено внимание в работах Р.С. Белкина, В.А. Волынского [1, с. 80], А.Ю. Краснобаевой, С.Б. Пазухина [2, с. 88], Х.М. Сабирова [3, с. 125], П.Т. Скорченко [4, с. 272], С.И. Соболевской [5, с. 65], А.С. Шаталова [6, с. 22] и др.

В.А. Волынский определяет технико-криминалистическое обеспечение как организационно-функциональную систему, направленную на создание условий постоянной готовности служб и подразделений органов внутренних дел к быстрому и эффективному решению технико-криминалистических задач и на практическую реализацию этих условий в целях получения, накопления, обработки криминалистически значимой информации и ее использования в процессе раскрытия и расследования преступлений [1, с. 16].

С.Б. Пазухин, А.Ю. Краснобаева, разделяя позицию ведущих ученых-криминалистов (Г.И. Грамовича, А.И. Винберга, С.И. Зернова, А.Ф. Волынского, А.С. Шаталова), определяют технико-криминалистическое обеспечение как своеобразный вид деятельности, содержание которой определяется направленностью, с одной стороны, на создание условий постоянной готовности право-

охранительных органов к применению научно-технических средств и методов в указанных целях, а с другой — на практическую реализацию таких условий в каждом конкретном случае раскрытия и расследования преступлений [2, с. 9].

Х.М. Сабиров, говоря о технико-криминалистическом обеспечении, пишет: «Под ТКО следует понимать комплексную организационно-функциональную систему, в своей деятельности направленную на собирание и исследование криминалистически значимой информации и реализующую свои возможности посредством применения технико-криминалистических методов и средств» [3, с. 5].

Во всех вышеприведенных определениях авторы ведут речь о технико-криминалистическом обеспечении только применительно к предварительному расследованию преступлений, о технико-криминалистическом обеспечении судебного разбирательства речи не идет.

По-нашему мнению, технико-криминалистическое обеспечение предварительного и судебного следствия по делам об умышленных убийствах можно определить как основанную на изучении преступной деятельности по совершению убийств и криминалистической деятельности по их выявлению, раскрытию, предварительному и судебному следствию уголовных дел об умышленных убийствах деятельность, направленную на создание и обеспечение правоохранительных органов знаниями, а также разработанной на основе изучения потребностей практики техникой, применяемых в целях осуществления успешной деятельности по выявлению, раскрытию, предварительному и судебному следствию по уголовным делам об умышленных убийствах в складывающихся доследственных ситуациях и ситуациях предварительного и судебного следствия.

Технико-криминалистическое обеспечение предварительного расследования и судебного разбирательства по уголовным делам об умышленных убийствах, безусловно, должно иметь серьезное научное обоснование. Специфика расследования дел об убийствах заключается в том, что успех их раскрытия и расследования зачастую зависит именно от результатов применения технических средств для обнаружения следов преступления и от результатов заключения назначенных по делу экспертиз, так как по делам об умышленных убий-

ствах нередки ситуации, когда свидетелей преступления нет или почти нет, либо есть только косвенные доказательства. Особенно роль применения технических средств велика при расследовании таких видов убийств, как убийства прошлых лет, убийства, связанные с безвестным исчезновением потерпевших, когда следственные органы испытывают трудности с формированием доказательственной базы по делу.

Анализ судебно-следственной практики показал, что технико-криминалистическое обеспечение предварительного расследования и судебного разбирательства по уголовным делам об умышленных убийствах должно основываться, с одной стороны, на разностороннем изучении преступной деятельности по совершению умышленных убийств, и деятельности по их выявлению раскрытию, предварительному расследованию и судебному разбирательству — с другой. Изучение деятельности по совершению убийств должно основываться на рассмотрении ее как системной структуры, включающей в себя в качестве составляющих структурных элементов личность убийцы, личность потерпевшего, обстановку совершения убийств, действия убийцы по подготовке, совершению, сокрытию убийства, механизм взаимодействия убийцы и жертвы, типичные следы преступной деятельности по совершению умышленных убийств.

Изучение личности убийцы должно осуществляться на научной основе, включающей в себя использование не только достижений криминалистики, но и психологии, медицины, психиатрии, социологии, биологии и других наук. Практическое значение имеет, по нашему мнению, составление типовых портретов, психологических портретов убийц и использование их для установления личности преступников в ситуациях совершения убийств.

В этой связи изучение личности потерпевших также должно осуществляться на научной основе, включающей всестороннее изучение личности потерпевших с точки зрения психологии, физиологии, медицины, биологии и т.д.

Важное практическое значение в деятельности по предварительному расследованию и судебному разбирательству по уголовным делам об убийствах имеет разработка и внедрение в практику современных научно-технических

средств, позволяющих эффективно исследовать обстановку места происшествия по делам об умышленных убийствах. Для достижения этой цели необходимо знать потребности практики расследования убийств, в частности практику проведения осмотров мест происшествий, типичную следовую картину по делам об убийствах. На этой основе должна производиться разработка соответствующих технических средств обнаружения, фиксации, изъятия и исследования следов по делам об убийствах.

Помимо осмотров мест происшествия должно осуществляться изучение практики проведения иных следственных действий по уголовным делам об убийствах с применением технических средств и участием в них экспертов и специалистов. На основании этого необходимо разрабатывать новые и совершенствовать существующие тактические приемы производства следственных действий с применением технических средств. Для практики расследования уголовных дел об умышленных убийствах большое практическое значение имеет разработка и применение технических средств, направленных на обнаружение скрытых, давностных следов преступлений, следов в микроколичествах, подвергавшихся воздействию, попыткам уничтожения.

Изучение действий убийцы по подготовке, совершению и сокрытию убийств также должно осуществляться с активным использованием технических средств, позволяющих выявлять следы преступной деятельности. Данные о подготовке, совершению, сокрытию убийств могут быть получены, например, в ходе осмотров мест, где убийца мог осуществлять подготовительные действия, где было совершено убийство, и где убийца совершал действия по сокрытию совершенного преступления.

Научное обоснование технико-криминалистического обеспечения включает в себя разработку и совершенствование на основании изучения практики борьбы с убийствами научно-технических средств, позволяющих выявлять, раскрывать, успешно расследовать, рассматривать в суде, а также предупреждать совершение убийств. В настоящее время в криминалистической литературе много говорится о необходимости активного внедрения в практику борьбы с преступностью со-

временных достижений науки и техники, достижений как естественных (математика, физика, химия, биология и др.), технических наук (например, материаловедение, нанотехнология, информатика и др.), так и гуманитарных (психология, социология, логика, этика, философия, история науки и др.).

Как показывает изучение следственно-судебной практики по уголовным делам об убийствах, а также личный опыт расследования таких преступлений, в том числе работа в составе следственной бригады при расследовании серийных убийств, значение использования технических средств существенно возрастает при расследовании подобных убийств, когда приходится решать вопросы об отыскании и исследовании следов биологического происхождения, в том числе давностных, когда убийцы предпринимают меры по сокрытию следов преступной деятельности, возникает необходимость проведения идентификации костных останков путем проведения ДНК-экспертизы, других видов экспертиз.

Например, по уголовному делу об исчезновении абитуриенток Алтайского политехнического университета в 2000 г., в расследовании которого в составе следственной бригады принимал автор, было проведено более 200 экспертиз. Благодаря современным достижениям ДНК-экспертизы оказалось возможным провести идентификацию костных останков потерпевших, установить их личность. Также активно в рамках дела привлекались эксперты-психологи, благодаря которым были составлены психологические портреты как потерпевших, так и возможного убийцы.

Изучение следственно-судебной практики показывает, что преступники в процессе совершения убийств применяют современные средства связи (мобильная связь, сеть Интернет, электронная почта), пользуются различными интернет-сервисами, создают и используют интернет-страницы и сайты, пользуются электронными носителями информации. Имеют место случаи, когда преступники используют сеть Интернет для сбора информации о будущей жертве (например, при совершении убийств по найму), создают сайты с целью склоне-

ния потерпевших к совершению самоубийства (различные так называемые группы смерти, например «Синий кит»).

В этих условиях речь можно вести о появлении информационных следов в виртуальном пространстве и о необходимости обнаружения, фиксации, изъятия и исследования информации, содержащейся на электронных носителях. Осуществить эту задачу самим следователем не всегда представляется возможным, так как требуется наличие специальных знаний в области информационных технологий, которыми следователи не обладают, требуется либо привлечение специалистов к участию в производстве следственных действий, либо назначение компьютерно-технических экспертиз.

В настоящее время по-прежнему является актуальным внедрение в следственную практику цифровых технологий, современной компьютерной техники, разработка, внедрение и использование следователями компьютерных программ, позволяющих анализировать исходные данные по уголовным делам об умышленных убийствах и предлагать следователям на основании этого рекомендации по определению наиболее оптимального пути расследования, алгоритмы разрешения складывающихся следственных ситуаций.

Актуальным также является создание автоматизированных рабочих мест для следователей, имеющих доступ к современным автоматизированным базам данных по уголовным делам и автоматизированным поисковым системам, а также базам данных не только правоохранительных органов, но и других организаций (например, многофункциональных центров). Это позволило бы следователям оперативно получать необходимую поисковую, справочную информацию по делу, информацию о возможном местонахождении лиц и т.д.

Как показывает изучение криминалистической литературы, отсутствуют рекомендации по применению в ходе расследования преступлений, в том числе уголовных дел об убийствах, средств сотовой связи для фиксации хода и результатов следственных действий. По этому поводу не проводилось исследований относительно того, целесообразно ли применять такие устройства, как альтернативу фото- и видеотехнике, не разработаны рекомендации по ее примене-

нию. Неясно, какими техническими характеристиками должны обладать данные устройства, чтобы их можно было использовать в следственной практике.

То же самое можно сказать об использовании в следственной практике современных компьютерных программ, позволяющих осуществлять коммуникацию в режиме реального времени на расстоянии (например, программы видеосвязи). Если в судебной практике видеоконференц-связь уже широко применяется, то в следственной практике вопрос о ее использовании не решен ни законодательно, ни с точки зрения криминалистических рекомендаций по ее применению в процессе расследования преступлений.

В настоящее время в связи с повсеместным распространением компьютерной техники, средств сотовой связи, цифровых носителей информации актуальной является разработка тактических приемов применения цифровой, компьютерной техники в расследовании убийств, а также получения доказательственной информации, содержащейся на электронных носителях, в памяти компьютеров, средств сотовой связи. В этих условиях актуально активное взаимодействие следователей, оперативных работников со специалистами в области информатики, программирования, сотовой связи. Информация об убийце, жертве, их взаимоотношениях, круге общения, местах возможного нахождения. В таких случаях актуальным является включение в состав следственно-оперативных групп специалистов в области компьютерной техники. В состав следственно-оперативной группы, в зависимости от конкретной ситуации, помимо следователя при осмотре месте происшествия должен входить специалист по средствам вычислительной техники [7, с. 44].

Большое практическое значение может иметь в настоящее время для розыска убийц, а также для розыска без вести пропавших лиц портретная экспертиза по фото- и видеоизображениям, полученным с камер видеонаблюдения, установленным в общественных местах, банкоматах, подъездах, на придомовых территориях.

*В настоящее время по-прежнему актуальной является информатизация следственной деятельности, внедрение в следственную практику расследования убийств современных информационных технологий.*

Современные цифровые технологии позволяют обрабатывать и хранить большие объемы информации. Актуальным в настоящее время является создание и внедрение в следственную практику по делам об умышленных убийствах технологии искусственного интеллекта.

Под искусственным интеллектом в криминалистике понимается как *производное* комплекса (системы), состоящего из компьютерной системы (сетевые, персональные и иные цифровые компьютеры), компьютерных программ (программное обеспечение), базы данных (криминалистически значимая информация о совершенном преступлении и его участниках) и искусственных нейронных сетей (выполняющие математические функции), который и обеспечивает формирование и функционирование данного интеллекта.

Данный искусственный интеллект способен не просто действовать (работать) по заранее заданному алгоритму (программе), но и реализовывать такие творческие функции человека, как принятие решений, прогнозирование, оценка рисков, работа с неполными данными и данными криминалистических учетов, предсказание последствий, учет и реагирование на дополнительную информацию и т.д.

В настоящее время наиболее эффективный способ организации искусственного интеллекта — искусственные нейронные сети. Они способны выявлять скрытые, неочевидные связи и закономерности обстоятельств совершения преступления и т.д. Для практики расследования корыстно-насильственных преступлений используются или, правильнее сказать, работают сверточные нейронные сети (для распознавания образов и классификации объектов) и рекуррентные сети (для работы с текстами, т.е. получить данные о чем-то или о ком-то).

Цифровые информационные технологии сегодня следователями (дознавателями) и экспертами используются при сборе, фиксации и обработке большого

количества данных о совершенном преступлении и его участниках, в получении и обработке оперативной информации и на этих результатах для принятия решений по оперативному управлению самим процессом расследования и т.д.

А.М. Кустов пишет, что на первом этапе работы с искусственным интеллектом сотрудники правоохранительных органов применяли его в трех направлениях:

выявление серийных и объявленных в розыск преступников, находящихся в общественных местах (в некоторых странах, например в Голландии, полиция использует данный интеллект для расследования сложных преступлений);

видеонаблюдение за поведением негативно настроенных граждан, находящихся в общественных местах, в целях обеспечения общественного порядка и безопасности;

анализ поведения пользователей компьютеров и Интернета на сайтах (в социальных сетях) и в мессенджерах (так, например, в 2018 г. китайским ученым удалось выявить более 20 тысяч потенциальных самоубийц и оказать им психологическую помощь).

Анализ судебно-следственной практики показал, что искусственный интеллект сегодня позволяет значительно упростить работу следователя (дознавателя) в части изучения юридических документов и материалов уголовного дела, анализа имеющихся прямых и косвенных улик, определения вероятного уровня сложности сложившейся следственной ситуации и сути дела, быстрой подготовки необходимой информационной цифровой базы для проверки полученных доказательств, формирования предложений по программе (алгоритму) действий, а по полученным результатам подготовить обвинительное заключение (обвинительный акт) по уголовному делу и т.д.

При этом следователь или эксперт может пользоваться интернет-ресурсами как дополнительным источником информации — это различная информация или предложения от пользователей данной социальной системой, данные из сотовых телефонов, компьютеров и автомобилей (видеорегистраторы, GPS, Bluetooth), которые позволяют получить информацию о его использовании, ме-

стонахождении, а также данные бытовых приборов, систем охраны объектов, видеонаблюдения на улицах городов, в общественном транспорте — позволяют с использованием искусственного интеллекта строить дополнительные связи между людьми, событиями и обогащать материалы следствия и т.д.

В настоящее время актуальным является использование искусственного интеллекта при расследовании серийных убийств.

Проблема заключается в том, что в настоящее время в науке не разработаны четкие критерии, позволяющие ограничивать серийного преступника от законопослушных граждан. На основании изучения уголовных дел о серийных убийствах учеными были выявлены определенные закономерности в поведении серийных преступников. На этой основе было предложено создавать компьютерные программы, позволяющие устанавливать серийных убийц.

Например, у виновного, совершившего ту или иную серию преступлений, присутствуют некоторые психологические черты, которые характеризуют определенный *порядок действий*; у маньяков-убийц возникают жизненные *периоды активности*, которые связаны с патологическими изменениями мозга, когда они наиболее склонны к совершению преступлений.

Учеными, проводившими исследование серийных убийц, было установлено, что в мозге некоторых из них присутствовала группа клеток, которые отвечали за желание совершить убийство. На основании этого учеными была разработана компьютерная программа, позволяющая имитировать циклы активности этих клеток, на основании чего можно делать предположения о циклах активности серийных убийц. Построив график колебаний предполагаемой активности нейронов в течение 12 виртуальных лет, они сопоставили его с реальным временем совершения убийств. Оказалось, что математическая модель и «график» убийств в реальности у А. Чикатило практически совпали.

Замечено, что серийные убийцы совершают преступления районе своего места жительства, но не в непосредственной близости от дома. Для одних убийц наличие у них детей является сдерживающим фактором, для других —

нет. Также по-разному влияют такие факторы, как социальный статус, степень психических отклонений, семенное положение и т.д.

На основании изучения этих данных учеными бала разработана компьютерная программа, которая на основании анализа введенных в нее вышеуказанных параметров составляет поисковый портрет серийного убийцы в каждом конкретном случае. Искусственный интеллект способен анализировать большой информации, но только те данные, которые были введены в память машины.

В практической деятельности следователи, оперативные работники, помимо информации из различных баз данных, используют еще и свой профессиональны и житейский опыт, в том числе свою интуицию. В совокупности с результатами анализа искусственного интеллекта это может значительно повышать эффективность раскрытия данных убийств.

Проблемой является то, что не всегда следственные работники своевременно распознают серийный характер убийств, уходит время, утрачиваются следы, преступники успевают совершить новые убийства. Повсеместное внедрение и использование в следственной практике искусственного интеллекта позволило бы избегать данных недостатков.

Таким образом, современные цифровые технологии, используемые следователями (дознавателями) и экспертами-криминалистами, позволяют автоматически выявлять признаки серийных, взаимосвязанных преступлений, в том числе и по полученному с мест преступлений биоматериалу, т.е. определять внешние анатомические признаки преступников (например, цвет глаз, волос, форму лица, голову и т.д.).

В настоящее время в связи с активным развитием 3D-технологий обсуждается вопрос о внедрении в деятельность по расследованию и судебному рассмотрению дел об умышленных убийствах 3D-моделирования. Например, К.В. Ярмак отмечает: «В настоящее время существует целый ряд программных продуктов, предназначенных для 3D-моделирования. Одно из наиболее известных в мире приложений в сфере фотограмметрического программного обеспечения — пакет Photo Modeler, предназначенный для получения трехмерных мо-

делей-эскизов на основе фотографий. Например, в судебной практике данное приложение очень активно используется для воссоздания картины места происшествия. Пакет позволяет работать с любым количеством фотографий, полученных при съемке самыми разными камерами, в том числе и одновременно в одном проекте. При необходимости можно создать модель даже по одной-единственной фотографии, однако в этом случае пострадает качество. Если в ходе работы над проектом появился новый исходный материал, то в любое время можно добавить новые снимки. В тех случаях, когда эксперт по каким-либо причинам не может или не должен работать с реальным объектом или следом (объект утрачен, разрушен, опасен), может прийти на выручку 3D-принтер. Технологии 3D-моделирования могут помочь воссоздать место преступления в зале суда. Для этого может использоваться технология трехмерного моделирования и анимации, широко применяемая в современной игростроительной индустрии и киноиндустрии. Так, например, инструментарий, разработанный специалистами из Управления мультимедийной судебно-медицинской экспертизы в Глазго, позволяет с высокой точностью реконструировать место преступления, а также моделировать тела жертв для демонстрации ранений, нанесенных огнестрельным или холодным оружием» [8, с. 60-64].

Повышению качества и оперативности расследования убийств способствовало бы внедрение в практику информационных рекомендующих систем, содержащих отдельные методики расследования отдельных видов умышленных убийств. В настоящее время в связи с повсеместным распространением цифровых технологий актуальным является проведение судебно-портретной экспертизы цифровых изображений, полученных с помощью цифровых средств видео- и фотофиксации, цифровых фото- и видеоизображений. В криминалистической литературе справедливо отмечается, что информация, полученная с таких устройств, может являться одним из важных средств документирования противоправной деятельности. Нередко лица, совершающие преступления, фиксируют на камеру мобильных телефонов свои действия, либо очевидцы снимают противоправные действия других лиц.

Изучение криминалистической литературы показало, что в настоящее время развитие нанотехнологий привело к появлению новых средств выявления следов преступления. Так, Е.В. Прокофьева отмечает: «Нанотехнологии находят свое применение в криминалистике при исследовании отпечатков пальцев. В частности, металлосодержащие наночастицы и наноструктурированные частицы используются для проявления отпечатков. Для контрастирования жирных следов пальцев использовали взвесь золотых наночастиц, обладающих гидрофобными свойствами, т.е. способных прилипать к поверхностям, покрытым жиром. Эти наночастицы, прилипая к жирным бороздкам отпечатков пальцев, формировали значительно более четкий рисунок, чем можно было бы получить с помощью традиционной техники.

В рамках криминалистической экспертизы материалов веществ и изделий при решении вопросов, касающихся индивидуализации веществ или изделий, определения их качественного и количественного состава, широко применяются современные физические методы исследования поверхности и анализа наноструктур, которые позволяют оперировать не просто малыми количествами веществ, а индивидуальными молекулами. В последние годы в экспертной практике стали шире использовать атомно-абсорбционный анализ и лазерный микроанализ. Высокая чувствительность эмиссионной спектроскопии позволяет получить данные об элементах основы и имеющихся в ней микропримесях на наноуровне.

Таким образом, современные цифровые технологии, используемые следователями (дознавателями) и экспертами-криминалистами, позволяют автоматически выявлять признаки серийных, взаимосвязанных преступлений, в том числе и по полученному с мест преступлений биоматериалу, т.е. определять внешние анатомические признаки преступников (например, цвет глаз, волос, форму лица, голову и т.д.). Используя искусственный интеллект, следователи (дознаватели), расследуя серийные преступления, осуществляют поиск особо опасных преступников — убийц, маньяков и др.

При помощи высоких цифровых технологий, криминалистических учетов и интернет-ресурсов (социальных сетей) следователи могут:

– по подробно описанному расследуемому криминальному событию определить аналогичные ранее раскрытые или нераскрытые преступления;

– по полученным с места происшествия биоматериалу (ДНК) определить с большей вероятностью внешние анатомические признаки лиц, совершивших серийные преступления, например, цвет глаз, относительную форму лица, цвет волос, относительную форму головы и тела, цвет кожи;

– составить психофизический портрет разыскиваемого преступника; распознать практически всех лиц, совершивших преступление;

– установить личность неопознанных жертв;

– с учетом извлеченных данных из сотового телефона определить лиц, учувствовавших в переговорах;

– произвести поиск людей, связанных с событием совершенного преступления;

– составить карты мест с возможной высокой преступностью в городе или районе;

– технологию искусственного интеллекта использовать для профилактики преступлений;

– позволяет усовершенствовать алгоритмы прогнозирования серийных преступлений (т.е. прогнозировать вероятность совершения очередного серийного преступления);

– осуществить оперативный поиск и идентификацию лица человека по фото-, видеоизображению;

– используя нейросети и выявляя совпадения при анализе описание места происшествия, показания свидетелей и потерпевших, составить фоторобот с внешностью преступника;

– используя созданных фотороботов, систему распознавания лиц в метро, уличных и подъездных видеокамерах, установить лиц, разыскиваемых за совершенные корыстно-насильственные преступления;

– по пыльцовым зернам и спорам растений, оставшихся на одежде преступника, вычислить убийц и место преступления (у биологов в базе данных компьютеров есть подробная карта ареала произрастания растений и времени цветения), а по пыльце на теле жертвы можно установить место расправы над ним;

– по полученным показаниям и сведениям о ранее совершенных серийных преступлениях описать субъективный портрет маньяка и др.

За последние годы в системе Следственного комитета на базе высоких технологий создано пять уникальных интерактивных баз данных. В них материалы большинства резонансных дел: серийные нападения с сексуальным мотивом; убийства, связанные с захватом жилья; экстремизм; преступления в сфере медицинских услуг; случаи исчезновения детей.

Анализируя вышесказанное, можно сделать следующий вывод о том, что использование искусственного интеллекта в следственной, оперативно-розыскной и экспертной деятельности сегодня определяется по следующим направлениям:

– оценка и анализ первичной информации о криминальном событии и его участниках;

– моделирование механизма преступления, его последствий и следов;

– вычленения из массива расследуемых дел признаков серийности, объединения преступлений по схожим признакам;

– выявление признаков серийности в совершенных преступных деяниях;

– оценка достаточности доказательств в материалах уголовного дела;

– анализа материалов уголовных дел для выявления следственных ошибок процессуального и тактического характера;

– планирование дальнейших следственных действий и оперативных мероприятий, описание оперативной обстановки и т.д.

## Список литературы

1. Волынский В.А. Технико-криминалистическое обеспечение раскрытия и расследования преступлений: пособие. М.: ВНИИ МВД РФ,1994. 80 с.

2. Пазухин С.Б., Краснобаева А.Ю. Технико-криминалистическое обеспечение расследования бандитизма: учеб.-метод. пособие. Волгоград: ВА МВД России, 2005 88 с.

3. Сабиров Х.М. Технико-криминалистическое обеспечение расследования преступлений: учеб. пособие. Краснодар: КубГАУ, 2013. 125с.

4. Скорченко П.Т. Криминалистика. Технико-криминалистическое обеспечение расследования преступлений: учебное пособие для вузов. М.: Былина, 1999. 272 с.

5. Соболевская С.И. Научно-техническое обеспечение расследования криминальных пожаров: учебное пособие. Тюмень: Тюменский юридический институт МВД РФ, 2005. 65 с.

6. Шаталов А.С. Технико-криминалистическое обеспечение раскрытия и расследования преступлений, совершенных в условиях массовых беспорядков: автореф. дисс. … канд. юрид. наук. М., 1993. 22 с.

7. Бутина Е.А. Особенности изъятия компьютерной техники и машинных носителей цифровой информации // Технико-криминалистическое обеспечение раскрытия и расследования преступлений: сборник тезисов и статей Международной научно-практической конференции (19 октября 2018 г.). Волгоград: Перископ Волга, 2018. С. 44.

8. Ярмак К.В. Применение 3D-технологий в криминалистике // Технико-криминалистическое обеспечение раскрытия и расследования преступлений: сб. науч. тр. / ред. кол.: А.А. Курин, Д.В. Кайргалиев, А.В. Кочубей. Волгоград: ВА МВД России, 2013. С. 60-64.

***Е.А. Кудайбергенова,*** *адъюнкт Волгоградской академии МВД России, г. Волгоград*

# ПРИМЕНЕНИЕ ИНСТИТУТА ПРОЦЕССУАЛЬНОГО СОГЛАШЕНИЯ В ФОРМЕ СДЕЛКИ О ПРИЗНАНИИ ВИНЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ НА ПРИМЕРЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВА (ПО МАТЕРИАЛАМ РЕСПУБЛИКИ КАЗАХСТАН)

Современный мир — информационный мир…

С развитием современного общества развиваются и информационные технологии, проникая во все сферы жизни человека. Основным этапом научно-технического прогресса является становление информационного общества, то есть люди с каждым днем все чаще используют услуги, предоставленные посредством сети Интернет. Однако необходимо учесть тот факт, что с глобализацией этого процесса развивается такое явление, как преступления в сфере информационных технологий.

Анализ статистических данных показал, что с каждым годом регистрация правонарушений в сфере информационных технологий только растет, при этом их большая часть остаются не раскрытыми. Наиболее распространенным видом такого рода правонарушений является мошенничество с использованием сети Интернет (п. 4 ч. 2 ст. 190 Уголовного кодекса Республики Казахстан (далее — УК РК) — «мошенничество, совершенное путем обмана и злоупотребления доверием пользователя информационной системы) [1].

Согласно данным Комитета по правовой статистике и специальных учетов Генеральной прокуратуры Республики Казахстан, в 2020 г. число зарегистрированных фактов интернет-мошенничеств на территории Республики Казахстан (далее — РК) составило 14138, в 2019 г. — 7733, а в 2018 г. — 516 фактов, то есть четко прослеживается рост данного вида правонарушений [2].

Расследование уголовных дел по преступлениям, совершенных в сфере предоставления услуг посредством сети Интернет, остается довольно сложной

задачей. При этом основные проблемы, на наш взгляд, заключаются в следующем:

1) слабая квалификация сотрудников, занимающихся расследованием преступлений данной категории;

2) отсутствие практики расследования интернет-мошенничеств;

3) недостаточная научно-теоретическая база.

Несмотря на имеющиеся проблемы при производстве досудебного расследования по правонарушениям, совершенным с использованием информационных систем, законодателями принимаются действенные меры к решению этих задач на законодательном уровне.

Необходимо помнить, что важнейшим гарантом прав личности, в том числе и субъектов уголовного процесса, является Конституция Республики Казахстан, провозглашающая, что права и свободы человека и гражданина являются высшей ценностью государства. В качестве основного направления развития и реформирования уголовной политики обозначено упрощение уголовно-процессуального права, в том числе и «порядка досудебного производства», согласно Концепции правовой политики Республики Казахстан в период с 2010 до 2020 г., утвержденной Указом Президента Республики Казахстан 24 августа 2009 г. Введение в уголовно-процессуальное законодательство института процессуального соглашения является главной целью упрощения и повышения эффективности уголовного процесса Республики Казахстан. Однако мнения юристов разделилось — одни утверждают, что данный институт не соответствует принципам правосудия, другие же, наоборот, поддерживают такие изменения в уголовно-процессуальном законодательстве.

Согласно ст. 612 УПК РК, имеется возможность заключения процессуального соглашения двух видов:

1) в форме сделки о признании вины — по преступлениям небольшой и средней тяжести, а также по тяжким преступлениям, но только с согласия подозреваемого, обвиняемого с предъявленным подозрением, обвинением;

2) в форме соглашения о сотрудничестве — по всем категориям преступлений при способствовании раскрытию и расследованию преступлений, совер-

шенных преступной группой, а также экстремистских и террористических преступлений [3].

В рамках данной статьи мы рассмотрим институт процессуального соглашения в форме сделки о признании вины как применяемую норму в ходе досудебного производства по преступлениям данной категории и рассмотрении дела в суде. Применение данной формы возможно лишь при добровольном волеизъявлении подозреваемого, обвиняемого на применение данного института в рамках расследования уголовного дела, а также с обязательного согласия потерпевшей стороны. Основными последствиями заключения такого соглашения являются:

1) применение сокращенного судебного разбирательства;

2) рассмотрение дела в порядке согласительной процедуры;

3) после подписания процессуального соглашения потерпевшей стороной, исключение возможности изменения суммы ущерба.

Порядок заключения сделки о признании вины состоит в следующем: подозреваемый, обвиняемый вправе заявить ходатайство о заключении процессуального соглашения в форме сделки о признании вины на любой стадии досудебного производства по уголовному делу, впрочем, как и отказаться от его применения, но до удаления суда в совещательную комнату для принятия решения.

Получив ходатайство от подозреваемого или его защитника о заключении сделки о признании вины, орган уголовного преследования в течение трех суток направляет его вместе с материалами уголовного дела прокурору. Прокурор, усмотрев в деле возможность заключения процессуального соглашения, предлагает стороне защиты обсудить вопрос о его заключении либо письменно сообщает об отказе в удовлетворении ходатайства, а также разъясняет последствия заключения соглашения и возможность отказаться от его заключения.

При рассмотрении вопроса о применении института процессуального соглашения прокурор обязан проверить:

1) подпадает ли деяние, совершенное лицом, под процессуальное соглашение в форме сделки о признании вины;

2) добровольность заявленного лицом ходатайства о заключении процессуального соглашения и осведомленность о его последствиях;

3) лицо не оспаривает собранные доказательства и квалификацию деяния;

4) соглашение лица с характером и размером причиненного им вреда и гражданским иском;

5) отсутствие в деле обстоятельств, влекущих прекращение уголовного

6) преследования.

Для выяснения указанных обстоятельств прокурор выясняет мнение не только стороны защиты подозреваемого, обвиняемого, но и потерпевшей стороны о возможности применения по данному уголовному делу института процессуального соглашения. Если после проведения процедуры подписания процессуального соглашения необходимо провести дополнительные следственные действия, прокурор вправе направить уголовное дело в орган уголовного преследования, но это происходит очень редко. После заключения процессуального соглашения досудебное расследование по делу считается оконченным, и прокурор направляет дело в суд без составления обвинительного акта с обязательным уведомлением потерпевшей стороны. Применение процессуального соглашения в форме сделки о признании вины при расследовании уголовного дела способствует сокращению по времени проведение досудебного производства и судебного разбирательства.

Несмотря на положительные моменты применения процессуального соглашения в форме сделки о признании вины, за пять лет данный институт широкого распространения по преступлениям совершенных посредством сети Интернет на территории Республики Казахстан не получил.

Так, в 2020 г. на стадии досудебного расследования уголовных правонарушений в виде интернет-мошенничеств институт процессуального соглашения в форме сделки о признании вины был применен лишь по 98 уголовным делам из 1676 дел, направленных в суд. В 2019 г. из направленных 662 уголовных дел в суд процессуальное соглашение было заключено только по 13 делам [2].

Проблемой применения со стороны органов уголовного преследования процессуального соглашения в форме сделки о признании вины является право

подозреваемого, обвиняемого отказаться от процессуального соглашения в ходе рассмотрения дела в суде, до удаления суда в совещательную комнату для принятия решения (ч. 2 ст. 614 УПК РК) [3]. Данное обстоятельство, в свою очередь, приводит к возвратам уголовных дел для производства дополнительного следствия и направления дела в суд в общем порядке, тем самым приводя к нарушению сроков расследования, волокиты, а также рождению жалоб со стороны потерпевших.

Для исключения фактов возвращения уголовных дел на дополнительное расследование по причине отказа подозреваемого, обвиняемого от заключенного ранее процессуального соглашения в форме сделки о признании вины, подписанного в ходе досудебного расследования, необходимо исключить возможность отказа подписанного соглашения на любой стадии досудебного расследования и рассмотрении дела в суде.

Институт согласительного производства является новеллой казахстанского уголовно-процессуального законодательства, и только применяя на практике данные нормы, мы сможем увидеть проблемы ее реализации, пути решения этих проблем через принятие действенных законодательных актов позволяющих упростить норму с учетом прав и свобод человека.

## Список литературы

1. Уголовный кодекс Республики Казахстан от 3 июля 2014 года. [Электронный ресурс]. URL: http://adilet.zan.kz/rus/docs/K1400000226

2. Информационный сервис Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан. [Электронный ресурс]. URL: https://qamqor.gov.kz/portal/page/portal/POPageGroup/ Services/Pravstat

3. Уголовно-процессуальный кодекс Республики Казахстан от 3 июля 2014 года. [Электронный ресурс]. URL: http://adilet.zan.kz/rus/docs/K1400000231

4. Канафин Д.К. К вопросу о внедрении в уголовное судопроизводство института соглашения о признании вины. [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=31204288

***А.А. Кузнецов,*** *к.ю.н., профессор, заслуженный юрист Российской Федерации, 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 Министерства внутренних дел Российской Федерации по городу Кургану, г. Курган*

# ДОПРОС ПОТЕРПЕВШЕГО ПРИ РАССЛЕДОВАНИИ ХИЩЕНИЙ С БАНКОВСКИХ КАРТ, СОВЕРШЕННЫХ ДИСТАНЦИОННО С ИСПОЛЬЗОВАНИЕМ IP-ТЕЛЕФОНИИ (SIP-ТЕЛЕФОНИИ)

Хищения с банковских карт, совершаемые дистанционно с использованием IP (SIP)-телефонии, являются абсолютно новым видом преступного посягательства и представляют особую сложность в раскрытии и расследовании. Органы внутренних дел столкнулись с очередным вызовом, поскольку своевременное выполнение стандартных (общих) первоначальных следственных действий и процессуальных мероприятий не гарантирует установление лица, совершившего преступление. Из всех следственных действий, проводимых на первоначальном этапе расследования дел данной категории, наиболее информативным и по сути основным источником доказательственной информации является допрос пострадавшего. Особенности проведения данного следственного действия всегда привлекали внимание ученых. Имеются работы как в области уголовного процесса, криминалистики, так и психологии, и все равно остается достаточно много нерешенных вопросов [1, с. 71-89; 2, с.160-171; 3, с. 247-264]. Применительно к хищениям, совершаемым дистанционно, достаточно важно как можно быстрее получить информацию о способе совершения преступления, об обстоятельствах, при которых произошло расследуемое событие. В пределах предварительной проверки поступившего материала, при достаточно широком спектре средств производства такой проверки, возникает необходимость в проведении следственных действий, которые фактически про-

водятся по возбужденному уголовному делу. В данном случае получение объяснения от пострадавшего об обстоятельствах совершения преступления необязательно, так как подобная информация достаточно полно может быть прописана в заявлении о преступлении. Вместе с тем говоря о допросе потерпевшего, прежде всего следует обратить внимание на знание следователем технологии совершения преступления дистанционно с использованием IP-телефонии (SIP-телефонии). Поэтому одним из основных элементов подготовки к допросу является получение дополнительных сведений следователем, позволяющих ориентироваться в условиях применения современных технологий [4, с. 31-64]. Тем более следует иметь в виду, что потерпевший, как показывает практика, редко представляет себе возможности интернет-пространства. Следователю при установлении психологического контакта нужно набраться терпения и уметь объяснить основные особенности таких технологий потерпевшему, чтобы правильно сформулировать вопрос и полученный ответ зафиксировать ответ в протоколе [5, с. 237-245].

Особенностью хищений с банковских карт, совершенных с использованием IP-телефонии (SIP-телефонии), отличающихся от иных дистанционных хищений, является тот факт, что номерные емкости звонков, поступающих на абонентские устройства пострадавших, выглядят как звонки от официальных организаций (банковских, коммерческих, государственных и т.д.), диалог злоумышленника и пострадавшего начинается с обращения к последнему по имени-отчеству, и зачастую после такого обращения пострадавшему называется часть номера его банковской карты и ее принадлежность, что создает полную уверенность у пострадавшего, что он разговаривает с официальным лицом банковской либо иной организации, от имени которой происходит звонок.

Ранее до появления средств интернет-телефонии и возможностей виртуальных переводов денежных средств действия злоумышленника по сокрытию рассматриваемых хищений, включали:

- приобретение сим-карт, оформленных на несуществующих либо третьих лиц;
- приобретение банковских карт, эмитированных на третьих лиц;

- открытие электронных кошельков, оформленных на несуществующих либо третьих лиц.

Сегодня ситуация изменилась в связи с использованием современных технологий. Коммуникация злоумышленника и пострадавшего полностью перешла в виртуальное интернет-пространство. Это относится как непосредственно к самому процессу совершения преступления — использование IP-телефонии (SIP-телефонии) в качестве средства общения с пострадавшим, так и к дальнейшим переводам похищенных денежных средств, для осуществления которых используются виртуальные банковские карты и виртуальные счета.

IP-телефония — это технология, позволяющая использовать Интернет или любую другую IP-сеть для ведения международных, междугородних телефонных разговоров в режиме реального времени. Сигнал передается через Интернет, а используемый при этом номер не является городским или абонентским номером операторов подвижной радиотелефонной (сотовой) связи. Регистрация на использование услуг IP-телефонии может осуществляться через Интернет, при этом документы, удостоверяющие личность пользователя услуги, не предоставляются. IP-телефония — это название технологии в целом, SIP-телефония — это одна из разновидностей IP-телефонии. IP-телефония — это протокол связи.

SIP-телефония — протокол передачи данных, при котором все звонки поступают на персональный компьютер или смартфон через специальное приложение, подобно звонку на сайт. Отличие от сотовой связи в том, что она не требует наличия сотового аппарата и подключения к базовой станции. Абонентский номер SIP-телефонии не имеет физического носителя (сим-карты), он виртуальный. При таких обстоятельствах получить информацию о расположении базовой станции, которой регистрировалось соединение телефонного звонка злоумышленника и пострадавшего, невозможно. В данном случае можно получить лишь сведения об IP-адресах, которые были использованы злоумышленником, для подключения к приложению (сайту) по работе с SIP провайдерами.

IP-адрес — это уникальный идентификационный номер, который присваивается каждому компьютерному устройству при входе в сеть Интернет.

Зачастую при совершении хищений с использованием IP (SIP)-телефонии с целью противодействия и сокрытия преступления на стадии его совершения используют программу по подмене абонентского номера. При этом абонентский номер подменяется на официальный номер организации, от имени которой происходит звонок (банковские, государственные, коммерческие организации, правоохранительные органы и т.д.). Факт подмены возможно установить только после истребования и приобщения статистики входящих и исходящих соединений (детализации) пострадавшего и злоумышленника. Если в детализации будет отсутствовать трафик соединений за интересующий период времени, то это свидетельствует о том, что была использована программа по подмене абонентского номера.

Наиболее типичной и представляющей наибольшую сложность следственной ситуацией является та, в которой исходная информация содержит данные о факте противоправного деяния, когда имеются сведения о пострадавшем, но нет сведений о движении денежных средств с момента их хищения, до их обналичивания, а также отсутствуют сведения о лице, совершившем преступление.

В таком случае следователь обязан убедиться, что в представленных материалах содержатся признаки состава преступления и незамедлительно вынести постановление о возбуждении уголовного дела. Зачастую в указанной следственной ситуации с целью экономии времени не требуется производить опрос заявителя, поскольку в заявлении о факте дистанционного хищения излагаются исчерпывающие обстоятельства, необходимые для принятия решения о возбуждении уголовного дела. Кроме того, выполнение всех возможных в рамках рассмотрения сообщения о преступлении следственных и процессуальных действий приведет к потере времени, поскольку не все следственные, процессуальные действия возможно провести в рамках доследственной проверки, а для проведения остальных требуется значительное время.

Следователь после вынесения постановления о возбуждении уголовного дела незамедлительно производит допрос потерпевшего.

По уголовным делам о дистанционных хищениях, совершенных с использованием IP-телефонии (SIP-телефонии), на первоначальном этапе расследования перед следователем стоят две основных задачи:

1. Определить местонахождение в пространстве злоумышленника (установить IP-адрес абонентского, либо иного технического устройства, с дальнейшей привязкой его к личности злоумышленника и месту его нахождения во время интернет-сессии, то есть в момент совершения преступления).

2. Отследить первоначальное и последующее звено (банковский счет, электронный кошелек и т.д.) движения похищенных денежных средств.

Сбор информации для решения этих неотложных задач начинается непосредственно во время допроса потерпевшего. При этом никто не отменял подготовку к такому допросу. В рамках проведения данного следственного действия подготовка сводится к стандартной процедуре с учетом дефицита времени для выяснения основных вопросов [6, с. 63-66]. В ходе допроса следователь должен выяснить:

- подробные обстоятельства хищения, в том числе количество банковских карт, имеющихся в пользовании у потерпевшего, наличие на них денежных средств и точные суммы остатков;
- описание особенностей голоса и устной речи злоумышленника;
- номерные емкости IP-телефонии (SIP-телефонии), с которых были осуществлены звонки;
- номера банковских счетов (карт), лицевых счетов банковских карт, номера электронных кошельков, на которые были переведены похищенные денежные средства;
- иные имеющие значение по уголовному делу обстоятельства.

Для этого следователь разъясняет потерпевшему последовательность своих действий по подготовке запросов, а также сроках предоставления ответов, адресуемых операторам сотовой связи, банковским организациям. Обращает внимание потерпевшего на особенности кратковременного использования злоумышленниками технических средств, для совершения дистанционных хищений. Рекомендуется разъяснять данные обстоятельства, чтобы наглядно пока-

зать потерпевшему, что любое промедление в истребовании информации, имеющей значение по уголовному делу, приведет не только к утрате доказательственной базы, но и существенно затруднит установление местонахождения похищенных денежных средств и их изъятие. Таким образом, следователь убеждает потерпевшего в необходимости скорейшего самостоятельного истребования у своего оператора связи статистики входящих и исходящих соединений (детализации), которую последний может получить, обратившись в свой личный кабинет, предоставляемый оператором связи, и информации о движении похищенных денежных средств, после их перевода на счета злоумышленника, которую потерпевший может получить путем личного обращению в банковскую организацию, либо через личный кабинет, предоставляемый банковской организацией (Банк-эмитент).

Информация, предоставляемая оператором связи, позволяет установить факт подмены абонентского номера, с которого был осуществлен звонок злоумышленником.

Информация, предоставляемая Банком-эмитентом (кредитная организация, участник платежной системы, осуществляет выпуск и обслуживание банковских карт), необходима с целью определения Банка-эквайера (это банк или финансовая организация, которая обрабатывает платежи, другими словами, это посредник между отправителем и получателем денежных средств, и которая предоставляет оборудование для эквайринга, то есть перевода денежных средств).

Подобное разъяснение необходимости самостоятельного обращения потерпевшего к оператору связи фактически является таким тактическим приемом допроса, как беседа. Помимо установления психологического контакта с допрашиваемым, следователь сокращает сроки проведения предварительной проверки, наиболее оптимально пытается получить весь объем необходимой доказательственной информации.

Сведения от оператора связи могут быть получены потерпевшим в течение нескольких часов, при этом у органов предварительного следствия для истребования аналогичной информации потребовалось бы не менее 15 суток.

Факт получения доказательственной информации от потерпевшего не освобождает следователя от подготовки и направления официальных запросов в адрес операторов связи и банковские организации.

Предоставляемая потерпевшим информация в виде выписок, квитанций, справок, чеков и т.д., если они приобщатся в оригиналах, подлежит изъятию с составлением протокола выемки, о чем выносится соответствующее постановление. Если потерпевший желает приобщить копии указанных документов, то производится дополнительный допрос потерпевшего, в ходе которого фиксируется факт приобщения к материалам уголовного дела соответствующих копий.

Также следователь после допроса потерпевшего в случае необходимости производит выемку у потерпевшего: абонентского устройства (иного технического устройства), содержащего записи телефонных переговоров (в случае если потерпевший записал разговор на диктофон), либо содержащего переписку злоумышленника и пострадавшего, с последующим их осмотром и признанием в качестве вещественных доказательств.

При допросе потерпевшего необходимо выяснить механизм хищения, поскольку данное обстоятельство будет существенно влиять на квалификацию преступления.

Потерпевший должен подробно описать все действия, которые он выполнял по указанию злоумышленника, а именно рассказать, в какой последовательности и какую именно информацию он предоставлял. Данные обстоятельства выясняются применительно к следующему:

- номер банковской карты;
- срок действия банковской карты;
- выяснение кода с оборотной стороны банковской карты;
- порядок предоставления кода из смс-сообщения, в подтверждение заявки на списание денежных средств.

Если потерпевший затрудняется ответить на отдельные вопросы, следует применять тактические приемы, направленные на восстановление в памяти забытого (допрос по ассоциации, проведение допроса в том месте, где произошло

преступное событие, демонстрация банковских карт, справок, чеков и т.п.). Подобные приемы используют при допросе в бесконфликтной ситуации.

При этом если потерпевший передает указанную информацию злоумышленнику, а последний в свою очередь использует ее для хищения (формирует заявку на перевод денежных средств от имени потерпевшего), действия злоумышленника необходимо квалифицировать по п. «г» ч. 3 с. 158 УК РФ — кража, то есть тайное хищение чужого имущества, совершенное с банковского счета.

Если же потерпевший сам лично вводит информацию по формированию заявки на перевод денежных средств, будучи введенным в заблуждение злоумышленником, то действия последнего подлежат квалификации по ст. 159 УК РФ — мошенничество, то есть хищение чужого имущества, путем обмана и злоупотребления доверием.

На практике встречаются случаи, когда в ходе допроса потерпевший может исказить информацию о механизме совершенного преступления, это может быть как добросовестным заблуждением, так и умышленным искажением некоторых обстоятельств хищения. Мотивы дачи ложных показаний потерпевшим могут быть самые различные [7, с. 57-58].

Удачную, на наш взгляд, классификацию мотивов предложила О.Г. Карнаухова, которая выделила следующие:

1. Корыстные мотивы (41,5%) — строятся на желании человека получить материальную выгоду путем совершения преступления.

2. Мотивы-страхи (33%) — основываются на негативных эмоциях человека.

3. Мотивы-оправдания (58%) — появляются у человека с желанием привести самому себе какие-либо доводы в пользу целесообразности тех или иных действий.

4. Мотивы-отрицания (26,5%) — возникают вследствие непринятия человеком каких-либо моральных или социальных норм поведения. Желание открыто воспрепятствовать следствию, убежденность в своей безнаказанности являются основой мотивов-отрицаний [7, с. 104-106].

Для потерпевших более характерны мотивы, связанные с сокрытием своего неблаговидного поведения (в том числе чувство стыда, так как позволил мошеннику себя обмануть); желание завысить (корысть, злоба, ревность) или уменьшить (скрыть незаконный источник обогащения) ущерб, а также скептическое отношение к возможности установления виновного в совершении преступления.

Зачастую потерпевшие в силу возраста, а также недостаточной финансовой грамотности и непонимания обстоятельств хищения, додумывают некоторые детали преступления. Им бывает стыдно, что в средствах массовой информации постоянно обращается внимание на возможность завладения мошенниками денежных средств у населения. И между тем потерпевший допускает в отношении себя совершение преступления. В таких ситуациях уместно применить тактические приемы, направленные на уточнение показаний, их детализацию или приемы, направленные на устранение противоречий в показаниях. В частности, необходимо предъявить выписки из банковских организаций, чеки, статистику входящих и исходящих соединений потерпевшего и злоумышленника, скриншоты переписки потерпевшего и злоумышленника, аудио-, видеозаписи и т.д.

В конфликтной ситуации, при умышленном искажении обстоятельств хищения, потерпевший обычно недоговаривает значимые детали преступления, либо, наоборот, описывает действия, которых в реальности не было. Потерпевший в такой ситуации представляет обстоятельства события в иной последовательности, либо вообще отрицает свое участие. В такой ситуации можно слышать заявления, что ни на какие звонки он не отвечал, банковские реквизиты никому не сообщал, никаких действий с банковской картой не осуществлял. В такой ситуации преступление совершено в отношении банковской организации, которая будет являться потерпевшей стороной.

При таких обстоятельствах после приобщения всех документов (ответов на запросы финансовых организаций, операторов мобильной связи, интернет-провайдеров) необходимо провести дополнительный допрос с предъявлением неоспоримых данных, свидетельствующих о том, что первоначальные показания потерпевшего не соответствовали объективной картине преступления.

В качестве дополнительных средств фиксации показаний потерпевшего следует рекомендовать применение видеозаписи хода и результатов допроса [9]. Необходимость применения технических средств следует оставить на усмотрение следователя, кроме случаев, прямо предусмотренных в законе (ст. 191 УПК РФ).

Таким образом, допрос потерпевшего является одним из основных следственных действий, выполняемых на первоначальном этапе расследования хищений, совершенных дистанционно с использованием IP-телефонии (SIP-телефонии). Качественное, всестороннее, последовательное производство допроса позволит получить доказательственную информацию в оптимальные сроки.

## Список литературы


1. Коновалова В.Е. Допрос: тактика и психология. Харьков: Консум, 1999. 157 с.
2. Порубов Н.И., Порубов А.Н. Допрос: процессуальные и криминалистические аспекты: монография. М.: Юрлитинформ, 2013. 304 с.
3. Юридическая психология: учебник и практикум для вузов / И.Н. Сорокотягин, Д.А. Сорокотягина. 4-е изд., перераб. и доп. М.: Юрайт, 2020. 360 с.
4. IT-справочник следователя / под ред. докт. юрид. наук С.В. Зуева. М.: Юрлитинформ, 2019. 232 с.
5. Баев О.Я. Тактика следственных действий: учебное пособие. М.: Юрлитинформ, 2013. 456 с.
6. Криминалистическая тактика: учеб. пособие для академического бакалавриата / под общ. ред. А.Г. Филиппова. М.: Юрайт, 2019. 207 с.
7. Карпенко О.А. Криминалистические средства и методы преодоления дачи заведомо ложных показаний свидетелями и потерпевшими: дисс. … канд. юрид. наук. М., 2018. 214 с.
8. Карнаухова О.Г. Тактика преодоления противодействия расследованию со стороны свидетелей и потерпевших: дис. … канд. юрид. наук. СПб., 2015. 225 с.

9. Балакшин В.С., Литвин И.И. Современные технические средства и проблемы их применения в доказывании на досудебных стадиях уголовного судопроизводства: монография. М.: Юрлитинформ, 2020. 168 с.

***В.Н. Кукарцев,*** *доцент кафедры оперативно-разыскной деятельности ОВД Барнаульского юридического института МВД России, г. Барнаул*

## ОРГАНИЗАЦИОННЫЕ ПРОБЛЕМЫ РАСКРЫТИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Министерством внутренних дел Российской Федерации отмечено в истекшем году существенное ухудшение оперативной обстановки по линии противодействия кражам и мошенничествам, совершенным с использованием средств мобильной связи и сети «Интернет».

Согласно статистическим сведениям, из зарегистрированных в январе-декабре 2020 г. 510,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, прирост которых составил 73,4%, больше половины (58,8%) осуществлены с использованием сети «Интернет»: 267,6 тыс. (прирост составил 87,5%), почти половина (42,9%) — средств мобильной связи: 218,7 тыс. (прирост составил 88,3%). Четыре из пяти таких преступлений (80,4%) составили кражи или мошенничества: 410,5 тыс. (прирост составил 74,3%).

При росте числа зарегистрированных киберпреступлений их раскрываемость продолжила снижаться: по IT-мошенничествам составила 9,8% (2019 г. — 11,4%), по IT-кражам — 16% (2019 г. — 23,7%), по преступлениям, квалифицированным по п. «г» ч. 3 ст. 158 УК РФ — 15,5% [3].

Похожая тенденция наблюдается в текущем году. В январе-мае 2021 г. зарегистрировано 227,0 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной

информации, что на 25,7% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 21,7% в январе-мае 2020 г. до 26,8%.

Две трети таких преступлений (66,8%) совершены с использованием сети «Интернет» (151,6 тыс.; +48,4%), более трети (40,1%) — средств мобильной связи (91,1 тыс.; +18,9%).

Почти три четверти таких преступлений (74,8%) совершается путем кражи или мошенничества: 169,7 тыс. (+18,7%) [4].

Между тем существенных сдвигов в совершенствовании организации работы правоохранителей в указанной сфере не происходит.

Во всех аппаратах уголовного розыска территориальных органов внутренних дел на региональном уровне функционируют подразделения, специально созданные для противодействия преступности в сфере информационно-телекоммуникационных технологий, однако штат указанных подразделений не соответствует нарастающему валу таких преступлений. В ОВД на районном уровне решение указанных задач возлагается на отдельных сотрудников уголовного розыска, которые не освобождаются от обязанностей раскрытия других общеуголовных преступлений. В настоящее время назрела необходимость создания в системе ОВД отдельных оперативных подразделений, в компетенцию которых необходимо включить раскрытие общеуголовных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, с подчинением их соответствующему главному управлению на уровне МВД России. Для этого имеются все необходимые предпосылки: противодействие таким преступлениям обладает рядом особенностей, требует от оперативных сотрудников соответствующей квалификации, наблюдается существенный прирост количества зарегистрированных и снижение числа раскрытых преступлений и т.д. Создать такие подразделения возможно без увеличения общего количества сотрудников ОВД за счет перераспределения части штата подразделений уголовного розыска и подразделений «К» бюро специальных технических мероприятий.

В работе указанных подразделений по-прежнему используется неэффективный для противодействия рассматриваемым преступлениям территориальный принцип работы и оценки деятельности, при котором сотрудники не заинтересованы в раскрытии (передаче информации, значимой для раскрытия) преступлений, совершенных в отношении потерпевших, находящихся за пределами обслуживаемой территории.

Согласно приказу МВД России от 31.12.2013 № 1040 «Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации», результаты противодействия дистанционным хищениям оцениваются по соотношению количества лиц, привлеченных к уголовной ответственности за данные преступления, к общему количеству сотрудников полиции и следственных подразделений. Следовательно, сотрудники ОВД заинтересованы в выявлении и скорейшем расследовании уголовных дел в отношении большего числа участников таких преступлений при этом о приоритете вменения виновным всех эпизодов их преступной деятельности речи не идет, что негативно сказывается на реализации принципа неотвратимости наказания.

В выгодном положении оказываются ОВД тех регионов, с территории которых преступники дистанционно совершают преступления, этому способствует исполнение требования приказа [2] о возбуждении уголовного дела по факту совершения рассматриваемого деяния в ОВД, в который поступило сообщение о преступлении, что приводит к нерациональным материальным и временным затратам, возникающим в связи с командировками сотрудников в другие регионы для раскрытия таких преступлений, а также к отсутствию заинтересованности в осуществлении профилактических, оперативно-розыскных и иных мероприятий органами внутренних дел, на территории которых находятся лица, совершающие преступления в отношении потерпевших из других субъектов РФ.

Не обеспечена оперативность в организации и проведении оперативно-розыскных мероприятий, направленных на раскрытие дистанционных хищений. Между ОВД и кредитными организациями, операторами связи, провайдерами не налажен надлежащий электронный документооборот и взаимообмен

информацией. Данные организации не заинтересованы в предоставлении информации в возможно короткие сроки, в итоге ускорению исполнения того или иного запроса ОВД могут способствовать лишь так называемые «личные контакты» оперативников с сотрудниками указанных организаций. Имеются примеры, когда сами оперативники заключают соглашения с кредитными организациями по установлению электронного документооборота и за счет личных средств оплачивают данную услугу.

Подразделения специальных технических мероприятий ОВД не составляют единой сети и действуют по территориальному принципу — каждое в своем регионе, в результате непосредственному проведению прослушивания телефонных переговоров, снятия информации с технических каналов связи предшествует работа по установлению региона, из которого преступником осуществлен звонок и направление в тот регион соответствующих документов, при этом сами мероприятия согласно п. 2 Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность [1], осуществляются только при посредничестве органов федеральной службы безопасности.

В современных условиях развития техники и технологий в БСТМ не хватает линий для удовлетворения потребностей сотрудников ОВД в проведении оперативно-технических мероприятий в результате формируется так называемая «очередь» на проведение мероприятий по освобождаемым линиям.

Все указанные проблемы умело учитываются преступниками при совершении преступлений и сокрытии их следов.

## Список литературы

1. Постановление Правительства РФ от 27.08.2005 № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность» (ред. от 17.04.2021) // Собрание законодательства РФ. 2005. № 36. Ст. 3704.

2. Приказ МВД России от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений».

3. Состояние преступности в Российской Федерации за январь-декабрь 2020 года. [Электронный ресурс]. URL: https://мвд.рф/reports/item/22678184/.

4. Состояние преступности в Российской Федерации за январь-май 2021 года. [Электронный ресурс]. URL: https://мвд.рф/reports/item/24742236/.

***Д.Р. Кязимова,*** *студент Донбасской юридической академии, г. Донецк, ДНР*
***Д.Ю. Ключёва,*** *студент Донбасской юридической академии, г. Донецк, ДНР*
***Б.Б. Шавыркин,*** *ст. преподаватель кафедры юридического менеджмента Донбасской юридической академии, г. Донецк, ДНР*

## ИСПОЛЬЗОВАНИЕ ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ

Актуальность данной темы исследования заключается в том, что цифровые технологии получают все более широкое распространение, активно внедряются в нашу жизнь, упрощая процессы коммуникации, оптимизируя бизнес-процессы, снижая издержки предприятий, организаций и компаний. Внедрение цифровых технологий является одним из приоритетных направлений развития России до 2024 г. [1].

Активное развитие цифровых технологий помимо явных положительных сторон сопровождается рядом негативных явлений, связанных с применением инновационных инструментов в преступной сфере (например, с потерей государством части налоговой базы, с совершением криминальных действий).

Информационно-коммуникационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [2].

В переводе с греческого технология означает «мастерство», «умение», и это не что иное, как процессы, поэтому информационная технология — это процесс, который использует средства и методы сбора, обработки и передачи данных (первичной информации) для получения новой качественной информации о состоянии объекта, процесса или явления (информационного продукта).

В первую очередь необходимо отметить, что информационные технологии в современном мире играют важную роль в жизни каждого человека. Сейчас мы не можем представить свою жизнь без Интернета, компьютера, телефона и т.д. Также информационно-компьютерный прогресс открыл большие возможности во многих сферах жизни, облегчил работу в ряде многих профессий.

Научно-технический прогресс и изменения, происходящие в современном мире, являются толчком для рождения новых, более современных способов совершения преступления. Существовавшие ранее способы уходят на второй план, при этом как бы уступая место уже более современным способам совершения преступления. Ведь стремительно быстро развиваются сферы высоких технологий, которые проникают почти во все области жизни общества. И данный аспект имеет как плюсы, так и свои минусы, поскольку такое стремительное развитие не обошло стороной и преступную деятельность.

Правоохранительные органы стали достаточно часто использовать информационные системы для своей работы, в том числе для защиты прав и свобод человека и гражданина. Результаты работы правоохранительных органов напрямую зависят от качества информационной поддержки, так как самые основные усилия работников непосредственно по расследованию, раскрытию и предупреждению преступлений связаны с получением нужной информации. Но, к сожалению, далеко не во всех отделах органов внутренних дел имеются современные технические средства и соответствующие информационные технологии. Этот факт очень снижает эффективность реализации права и раскрытие преступлений. В информационном обеспечении правоохранительных орга-

нов главную роль занимают учеты, которые в свою очередь используются для регистрации первичной информации о преступлениях и о лицах, совершивших их. Также учеты предназначены для получения информации, помогающей в предупреждении, раскрытии и расследовании преступлений, установлении личности неизвестных граждан и принадлежности изъятого имущества и розыске преступников.

В системе мер по нейтрализации и искоренению преступлений, разработанных в мировом сообществе, наиболее действенными в настоящее время являются информационные технологии, позволяющие использовать при раскрытии и расследовании преступлений самые современные достижения науки и техники. Многие из этих технологий апробированы в практике мировой полиции, обслуживающих ее научно-технических служб и судебной экспертизы.

Наибольшие резервы и перспективы в практике раскрытия и расследования преступлений имеют три типа информационных систем:

1. регистрационные;
2. справочно-информационные;
3. аналитические.

Регистрационные системы имеют наибольшее значение в борьбе с рецидивом, составляющим около трети всех совершаемых и при этом наиболее опасных преступлений. Основная проблема этих систем состоит в оптимизации их структуры, организации взаимодействия подсистем и автоматизации их эксплуатации на основе компьютерных технологий.

Справочно-информационные системы (нормативно-правовые, демографические, транспортных средств, вещественных доказательств и образцов для сравнительного исследования) существенно повышают оперативность и эффективность деятельности оперативно-следственных органов и экспертных служб за рубежом. У нас они находятся в зачаточном состоянии и требуют для своего развития государственной поддержки.

Учеты предназначены для получения информации, которая помогает в предупреждении, раскрытии и расследовании преступлений, установлении личности неизвестных граждан и принадлежности изъятого имущества, розыс-

ке преступников. Они формируются в ГУВД, ИЦ МВД, УВД по территориальному принципу и образуют федеральные учеты МВД России [3].

Использование накопленных массивов информации по горизонтали усложняется многообразием информационных баз, которые создаются разными ведомствами. При выполнении подразделениями ОВД своих функций есть определенные проблемы по оперативному доступу к информации, которая содержится в этих массивах. Порой даже не совсем ясно, из каких источников можно получить нужную информацию.

Составной частью процесса обеспечения государственной системы противодействия преступности является информационно-аналитическая деятельность.

Аналитические информационные системы позволяют на основе современных информационных технологий решить основную проблему раскрытия и расследования преступлений, проблему дефицита информации об обстоятельствах преступления и преступнике.

Как известно, основным источником информации о преступлении и преступнике являются следы преступления в обстановке ее совершения. Обнаружение, анализ и лабораторные исследования этих следов представляли собой до последнего времени основной источник сведений о преступлении и преступнике.

Положение существенно изменилось в связи с внедрением в структуру криминалистического анализа идей системно-деятельностного подхода на основе компьютерного моделирования и анализа статистических выборок, однородных по способу совершения преступлений. На основе анализа работы наиболее продвинутых полицейских служб (Скотленд-Ярд, ФБР и ряд университетских лабораторий), а также практики российских криминалистических служб разработана типовая информационная модель преступной деятельности, представляющая новый эффективный инструмент криминалистического исследования.

Типовые информационные модели преступной деятельности позволяют на основе выявленных статистических зависимостей между ее элементами получать информацию о личности преступника и других обстоятельствах совершенного преступления. Разработка типовых информационных моделей пре-

ступной деятельности представляет качественно новый этап в развитии криминалистики.

В оперативно-розыскной деятельности в области расследования компьютерных преступлений применяют криминологическое прогнозирование индивидуального и преступного группового поведения. Чтобы извлечь какую-либо информацию, можно проанализировать сетевой трафик локальных и региональных компьютерных сетей. Стоит анализировать платежи клиентов за телефонные услуги.

Вот простой, но очень эффективный в настоящее время пример использования информации органами внутренних дел: сотрудники правоохранительных органов при расследовании преступлений имеют право при получении разрешения (ордера) смотреть записи с камер видеонаблюдения, находящихся рядом с местом совершения преступления.

Внедрение новых информационных технологий в органы внутренних дел продолжается с помощью построения современных компьютерных локальных, региональных и общегосударственных отраслевых информационно-вычислительных сетей, способствующих дальнейшему совершенствованию информационного обеспечения органов внутренних дел.

В настоящее время существует программное обеспечение, позволяющее:

– контролировать процесс попыток взлома компьютерной системы или сети;

– определять индивидуальный почерк работы программиста и идентификационных характеристик разработанных им программ;

– определять перечень электронных адресов и сайтов Интернета, с которыми работал пользователь;

– негласно регистрировать перечень программ, с которыми работает пользователь;

– определять путь, а в некоторых случаях — и конкретный адрес исходящей угрозы для компьютерных систем;

– осуществлять негласный контроль над программистом, определяя характер разрабатываемых продуктов;

– обнаружить латентную и закодированную информацию в компьютерной системе;

– проводить идентификацию компьютерных систем по следам применения на различных материальных носителях информации;

– осуществлять исследование следов деятельности оператора в целях его идентификации;

– осуществлять диагностику устройств и систем телекоммуникаций на возможность осуществления несанкционированного доступа к ним;

– исследовать материальные носители с целью поиска заданной информации;

– осуществлять исследование компьютерных технологий для установления возможности решения конкретных преступных задач (крекинг, хакинг, фрикинг и т.п.);

– исследовать программы для ЭВМ и базы данных для определения их возможного предназначения для преступных действий (наличие программных закладок, подпрограмм класса «троянский конь» и т.п.).

Однако развитие информационных технологий в правоохранительной системе России сталкивается с рядом проблем и несовершенностью системы, используемой непосредственно для этих целей, от проблем которых существенно снижается эффективность оперативной деятельности правоохранительных органов. Например, дактилоскопическая регистрация является все еще независимым направлением в дактилоскопии и ее взаимодействие с судебной дактилоскопической экспертизой минимально.

Далее необходимо отметить, что органы внутренних дел используют информационные технологии не только для розыска и учета преступников и преступлений, но и для предоставления услуг населению. Например, в настоящее время граждане и любые организации могут воспользоваться некоторыми из государственных услуг, которые предоставляют правоохранительные органы, в электронном виде. Самой востребованной услугой среди граждан является получение информации об административных правонарушениях в сфере до-

рожного движения. Данная информация предоставляется на абсолютно безвозмездной основе.

Стоит сказать, что в условиях информационно-технического прогресса информационные технологии являются ключевым фактором оптимизации деятельности органов исполнительной власти. Но, несмотря на это, некоторые источники утверждают, что реальная информационная база используется только на 20-25%, и этот процент очень мал. Данный факт говорит о том, что розыскная работа реализовывается затруднительно и медленно, а сами сведения, которые содержатся в информационных центрах, играют лишь вспомогательную, то есть второстепенную роль.

Сегодня благодаря стремительному развитию информационных технологий, созданию новейших и усовершенствованию существующих технических средств, возникает проблема подготовки кадров с квалификацией, которая обеспечит эффективное использование в профессиональной деятельности указанных средств и технологий.

Решение этой проблемы невозможно без комплексного подхода к организации подготовки и переподготовки кадров системы ОВД соответствующего уровня, повышение уровня специальной компьютерной подготовки работников органов внутренних дел в специализированных учебных заведениях [4].

Подготовка работников ОВД пользователей информационных подсистем должна обеспечить уровень их квалификации, достаточный для:

– выполнения операций, необходимых для информационной поддержки своей служебной деятельности;

– правильного обращения с компьютерным и коммуникационным оборудованием;

– выполнения требований техники безопасности и защиты информации.

Информацией, которая используется различными подразделениями полиции, в значительной мере имеет конфиденциальный характер, имеет грифы ограничения доступа. А некоторая часть информации конституционно охраняется от разглашения и незаконного использования. Поэтому организационные мероприятия, осуществляемые подразделениями полиции, обязательно должны

предусматривать защиту информации на разных уровнях ее функционирования, особенно на этапе ее накопления в автоматизированных системах ОВД [5].

Нельзя забывать о том, что в последнее время активизируется противодействие криминальных элементов сбору и использованию информации о преступлениях. Это особенно проявляется в информационном обеспечении специальных подразделений. Часто оперативные подразделения встречаются с откровенным противодействием со стороны криминала, а иногда откровенными или скрытыми контрмерами.

Снижение уровня, объема и качества информационных учетов сегодня позволяет криминальным элементам избегать ответственности, находиться в тени, усиливать криминальное влияние на общество и существенно изменять отношения в государстве.

## Список литературы


1. Правительство России // Программа «Цифровая экономика Российской Федерации». [Электронный ресурс]. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 20.05.2021).
2. Об информации и информационных технологиях: закон ДНР от 24 августа 2015 г. № 71-IHC: принят Народным Советом ДНР 7 августа 2015 г. 2014. Дата обновления 20.10.2018. [Электронный ресурс]. URL: http://doc.dnr-online.ru / wp - content / uploads / 2015 / 03 / Zakon _ DNR _ Ob _ InformcInformTechology _ I _ 278P _ NS . pdf (дата обращения: 20.05.2021).
3. Колупаева Т.А. Использование информационных технологий в правоохранительной деятельности. // Молодой ученый. 2020. № 22 (312). С. 267-268. [Электронный ресурс]. URL: https://moluch.ru/archive/312/70742/ (дата обращения: 29.05.2021).
4. Шавиркін Б.Б., Петрачук Л.І. Застосування ЕОМ в ОВС: навчальний посібник. Донецьк: ДЮІ, 2007. 178 с.
5. Основы оперативно-розыскной деятельности: учебник для юридических вузов / под ред. В.Б. Рушайло. СПб., 2000. 720 с.

***О.В. Левченко,*** *к.ю.н., прокурор Троицкого и Новомосковского административных округов города Москвы, г. Москва*

# ПРОКУРОР В УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ ЦИФРОВОЙ ЭКОСРЕДЕ

Проблематика взаимодействия прокуратуры с органами предварительного следствия и другими правоохранительными органами при выявлении, раскрытии преступлений и проведения предварительного расследовании в свете цифровых технологий и конкретно в контексте понятия «уголовно-процессуальная цифровая экосреда» вызывает повышенный интерес со стороны ученых-исследователей.

Понятие «экосреда» с недавних пор стало активно использоваться в юридической литературе при освещении вопросов как цифровизации уголовного процесса, так и всей организационно-правовой системы противодействия преступности [1, с. 120, 121; 2, с. 115-120; 3, p. 1195-1203].

Представители научной общественности едины во мнении, что внедрение цифровых технологий окажет значительное влияние на уголовно-процессуальную систему в целом и отдельные ее элементы. Однако в своих оценках последствий цифровизации уголовного процесса позиции ведущих ученых разделились.

Наметилось два принципиальных подхода по вопросу о том, затронет ли цифровизация основы правовой организации современного уголовного процесса. Большинство ученых априори исключают возможность глобальных преобразований уголовно-процессуальной системы и сводят воздействие цифровых технологий к ее оптимизации [4; 5, с. 15-25; 6, с. 95-101]. О цифровой экосистеме взаимодействия субъектов уголовного процесса в таком случае, на наш взгляд, говорить не приходится, поскольку предполагается доминирование субъектов следственной власти над всеми прочими.

Между тем другие ученые полагают, что цифровая революция неизбежно повлечет за собой смену типа процесса: с современного — следственного типа на состязательный/обвинительный [7, с. 199-207; 8, с. 75-86].

Ключевой вопрос здесь в сохранении института предварительного следствия и следственной власти на формирование доказательств и выдвижение обвинения, что в условиях следственной формы досудебного производства равнозначно привлечению к уголовной ответственности, и принятию решения об освобождении от уголовной ответственности. Следственная модель, нагруженная процессуальными гарантиями прав личности участников процесса, заинтересованных в исходе дела с обеих сторон, имеет тенденцию к формализации и бюрократизации. При минимальных предпосылках к настоящему взаимодействию обвинения и защиты на принципе равенства сторон. Причем отмеченная негативная тенденция проявляет себя и в подсистеме органов обвинительно-следственной власти, а именно: в правоотношениях органа предварительного следствия и прокурора. Они также перегружены формальностями, усложнены и малоэффективны.

По нашему мнению, концепция процессуальной самостоятельности следователя, как наиболее последовательное, концентрированное воплощение следственной идеологии, идет вопреки не только состязательности, но рациональной правовой организации досудебного производства по уголовному делу.

В досудебном производстве должен быть один процессуальный субъект на стороне обвинения, который бы организовывал и руководил уголовным преследованием, осуществляемым правоохранительными органами. Речь идет о единстве обвинительной власти. Обвинительную власть представляет прокурор, который, выступая субъектом процессуального права на выдвижение и поддержание обвинения, должен руководить предварительным уголовным расследованием преступления, включая современную оперативно-розыскную деятельность.

Аргументами в пользу данной версии цифровой трансформации уголовного процесса выступают, во-первых, архаичность следственной документальной формы фиксации и передачи доказательственной, бюрократичность следствен-

ной формы взаимодействия прокурора с поднадзорными органами, прежде всего — с органом предварительного следствия. Вместо цифровизации бюрократической, формализованной следственной модели, которая по своему определению антигуманна и никогда не будет способна обеспечивать права личности, равно как и малоэффективна, предлагается вовсе отказаться от нее, как бесперспективной и не подлежащей модернизации. Более того, вполне обоснованы опасения, что в условиях доминирования следственной власти в области доказывания и неравенства стороны защиты, цифровые технологии станут угрозой прав личности [2, с. 350-356].

В проекте сторонников реформы предварительного расследования цифровая уголовно-процессуальная экосистема представляет сферу взаимодействия представителей стороны обвинения и защиты по выработке оптимального правового средства разрешения уголовно-правового спора. Всю деятельность по выявлению, раскрытию преступления, получения цифровой информации, полезной для принятия решения по делу, предлагается «депроцессулизировать» и сделать доступной для любых лиц [9, с. 9-18].

В качестве довода в пользу позиции, предполагающей реформирование уголовно-процессуального механизма, который регулирует отношения прокурора с другими субъектами досудебного уголовного расследования, можно привести опыт Республики Казахстан. Это государство входит в круг тех немногих стран, которые сохраняют с нами некоторые общие моменты в правовом развитии.

В частности, в свое время в этом государстве недолгое время действовал Государственный следственный комитет, аналогичный Следственному комитету России[25]. Однако наши казахстанские коллеги довольно быстро отказались от подобного органа, как и от идеи процессуальной самостоятельности следователя от прокурора. Она не вписывалась в стратегию преобразований уголовного процесса по наиболее распространенной в мире процессуальной модели.

---

[25] См.: О Государственном следственном комитете Республики Казахстан и его органах: Указ Президента Республики Казахстан от 21 декабря 1995 г. № 2706, имеющий силу Закона. Утратил силу — Законом РК от 9 декабря 1998 г. № 307 ~Z980307. [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/U950002706

После принятия нового Уголовно-процессуального кодекса, который закрепил руководящую роль прокурора в отношении субъектов досудебного уголовного расследования, но вместе с тем сохранил основы прежней — следственной технологии формирования уголовно-процессуальных доказательств, в Казахстане был предпринят в 2019 г. эксперимент по оцифровке производства по уголовным делам. Это и была попытка цифровой трансформации следственной модели доказывания.

Очевидно, результаты данного правового эксперимента подвинули руководство страны к принятию концепции решительной реформы досудебного производства и переходу во всех развитых уголовно-процессуальных порядках на трехзвенную уголовно-процессуальную модель с четким разделением полномочий между органами уголовного преследования, прокуратурой и судом на стадии досудебного расследования [10].

Согласно этой концепции, три ключевые задачи уголовного процесса будут выполняться разными органами: 1) выявление, пресечение преступления, установление причастных лиц, сбор и закрепление доказательств — органами досудебного расследования; 2) дача независимой оценки собранным доказательствам, принятие ключевых процессуальных решений, предъявление и поддержание обвинения в суде — прокуратурой; 3) назначение наказания, рассмотрение жалоб граждан — судом. При этом на прокурора будут возложены ключевые процессуальные функции, определяющие ход предварительного расследования и переход дела в судебную стадию. Такая организация прокурорского надзора, совмещенная с цифровизацией уголовного процесса, представляет собой эффективную площадку для дальнейшего разграничения полномочий между органами уголовного преследования[26].

Очевидно, Республика Казахстан вскоре встанет в круг стран, имеющих полицейскую модель досудебного уголовного расследования под руководством прокурора и с участием следственного судьи, осуществляющего уголовно-

[26] Концепция к проекту Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам внедрения трехзвенной модели с разграничением полномочий и зон ответственности между правоохранительными органами, прокуратурой и судом». [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=32781342#pos=5;-120

процессуальные функции контроля и депонирования уголовно-процессуальных доказательств сторон. Российская Федерация остается пока в числе тех немногих стран, которые сохраняют следственную модель досудебного производства по уголовным делам, причем с гипертрофированной следственной властью.

В заключение выскажемся в пользу перехода к новой модели досудебного производства и взаимодействия прокурора с субъектами обвинительной власти в лице полицейских органов при расследовании и раскрытии преступления. Именно такая уголовно-процессуальная модель подлежит переносу на цифровую платформу.

## Список литературы


1. Зуев С.В. Цифровая среда уголовного судопроизводства: проблемы и перспективы // Сибирский юридический вестник. 2018. № 4. С. 118-123.
2. Власова С.В. Теоретическая концепция правовой (уголовно-процессуальной) организации противодействия преступности в сфере экономики: монография. М.: Юрлитинформ, 2020. 440 с.
3. Aleksandrov A.S., Zaytsev O.A., Muraev P.P., Ruchkin V.A. The Institutional Basis for Implementing «Smart Technologies» in the Legal System of Fighting Crimes // «Smart Technologies» for Society, State and Economy. 2021: Springer Nature Switzerland AG. Pp. 1195-1203.
4. Зуев С.В. Стратегия развития уголовного судопроизводства в условиях цифровизации: авторская концепция. [Электронный ресурс]. URL: https://www.iuaj.net/node/2833 (дата обращения: 15.05.2021 г.).
5. Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15-25.
6. Качалова О.В., Цветков Ю.А. Электронное уголовное дело — инструмент модернизации уголовного судопроизводства // Российское правосудие. 2015. № 2. С. 95-101.

7. Александров А.С., Андреева О.И., Зайцев О.А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестн. Том. гос. ун-та. 2019. № 448. С. 199-207.

8. Александров А.С., Александрова И.А., Власова С.В. Теоретическая концепция государственно-правовой организации противодействия преступности в 21 веке// Государство и право. 2019. № 9. С. 75-86.

9. Власова С.В. К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. Научный журнал. 2018. № 1. С. 9-18.

10. Послание Главы государства Касым-Жомарта Токаева народу Казахстана. 1 сентября 2020 г. [Электронный ресурс]. URL: https://www.akorda.kz/ru/addresses/addresses_of_president/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-1-sentyabrya-2020-(дата обращения: 15.05.2021 г.).

***М.М. Льянов,*** *аспирант кафедры уголовного права и процесса Института государства и права Тюменского государственного университета, г. Тюмень*

## ПОРЯДОК ИЗЪЯТИЯ ВИРТУАЛЬНЫХ СЛЕДОВ

Одним из обязательных этапов в процессе работы с виртуальными следами является их изъятие. В настоящее время существует достаточно большое количество научных работ на данную тему [1, с. 14; 2, с. 54-57]. Тем не менее постоянно меняющееся уголовно-процессуальное законодательство, а также практика работы органов предварительного расследования, требует дополнительного исследования данной темы.

В связи с этим в рамках данной статьи будут рассмотрены особенности изъятия виртуальных следов с электронных носителей информации. Для структурирования данной статьи будут приведены общие правила проведения изъя-

тия виртуальных следов, отдельные способы изъятия виртуальных следов и порядок их проведения.

Статья 164.1 Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ) устанавливает правила проведения изъятия электронных носителей информации, на которых может храниться информация, имеющая значение для уголовного дела. Стоит отметить, что средой, в которой существует виртуальный след, является электронный носитель информации, поэтому использование именно этого термина является оправданным. Из анализа ст. 164.1 УПК РФ можно вынести ряд ключевых правил изъятия электронных носителей информации, содержащих виртуальные следы:

1) действующее уголовно-процессуальное законодательство предусматривает возможность как изъятия электронного носителя информации, содержащего виртуальные следы, так и их копии;

2) при этом ст. 164.1 УПК РФ установлены определенные ограничения, связанные с возможностью изъятия электронных носителей информации. При совершении отдельных преступлений индивидуальным предпринимателем или членом органа управления коммерческой организации не допускается изъятие электронных носителей информации, если данное изъятие может привести к приостановлению законной предпринимательской деятельности. Тем не менее из данного правила имеются исключения, которые указаны в п. 1 ч. 164.1 УПК РФ, а именно:

- назначена судебная экспертиза в отношении электронных носителей информации;
- имеется судебное решение, согласно которому изъятие электронного носителя информации допускается;
- имеется риск утраты или изменения криминалистически важной информации, которое может произойти в результате копирования информации с электронных носителей информации;

3) УПК РФ обязывает проводить изъятие электронных носителей информации в присутствии специалиста. На наш взгляд, формулировка, касающаяся копирования информации с электронного носителя информации, является

неоднозначной и может толковаться двояко, так как в тексте статьи указывается о том, что копирование производится специалистом, если о копировании информации поступило ходатайство владельца информации или электронного носителя информации. Тем не менее исходя из общего смысла статьи, можно предположить, что законодатель закладывал в ее текст смысл, исходя из которого участие специалиста в обоих случаях обязательно. По нашему мнению, данное противоречие необходимо устранить введением обязанного участия специалиста в следственном действии, в ходе которого изымается копия информации с электронного носителя информации с отражением первого предложения ч. 2 ст. 164.1 УПК РФ в следующей редакции: «Электронные носители информации, а также копии с электронных носителей информации изымаются в ходе производства следственных действий с участием специалиста». Также стоит отметить, что по данному вопросу не существует оптимального подхода, относящегося к порядку изъятия электронных носителей информации, которые не требуют специальных знаний (оптических носителей информации, флэш-накопители и т.д.) [3, с. 40-43]. На наш взгляд, необходимо внести изменения, позволяющие изымать портативные электронные носители информации следователем без участия специалиста. Данная мера будет способствовать упрощению порядка проведения следственного действия, а также подготовки к нему;

4) УПК РФ не ограничивает перечень следственных действий, в рамках которых могут быть изъяты электронные носители информации, что предоставляет большую свободу для действий при производстве предварительного расследования.

Стоит отметить, что при копировании информации с электронных носителей информации могут возникнуть ошибки, приводящие к утрате данных либо их некорректному копированию. Так, например, при копировании данных могут не сходиться контрольные суммы файлов. Контрольная сумма файлов является индикатором, который указывает на корректность передачи информации. Расчет контрольной суммы может производиться по одному из нескольких алгоритмов (MD5, CRC32 и др.) [4, с. 58-63]. В связи с ошибками при передаче данных у внешне схожих файлов могут отличаться контрольные суммы. Таким

образом, исходный файл и его копию нельзя назвать идентичными. В связи с этим более предпочтительным является изъятие всех электронных носителей информации с их дальнейшим исследованием без производства копирования информации.

Отдельно следует упомянуть изъятие виртуальных следов с оперативных запоминающих устройств, которые имеют свойство энергозависимости. Данное свойство предполагает сохранение информации до прекращения подачи электрического тока. Таким образом, данное свойство исключает изъятие самого электронного носителя информации для целей получения содержащейся на нем информации. В связи с этим с данного электронного носителя информации допускается только копирование информации, которое должен производить специалист с использованием специального программно-технического обеспечения.

Одним из способов, с помощью которого можно изъять виртуальные следы, является изъятие электронных носителей информации в ходе следственных действий (осмотра места происшествия, выемки, обыска). В ходе осмотра места происшествия необходимо указывать общую обстановку места, где производится осмотр, подробно описать место, где были обнаружены электронные носители информации, а также технические устройства, в структуру которого включены электронные носители информации. В протоколе осмотра места происшествия необходимо указывать технические характеристики изымаемого технического устройства либо электронного носителя информации, их марку и модель, а также способ упаковки.

В случае получения сотрудником, ведущим предварительное расследование, информации о местонахождении электронного носителя информации либо технического устройства, на которых содержатся данные, имеющие значение для уголовного дела, а также установление мест, в которых могут находиться данные устройства, необходимо произвести выемку либо обыск. В протоколе обыска (выемки) необходимо указывать основания обыска (выемки), ход следственного действия. В части описания изымаемых объектов необходимо указывать те же сведения, что и при составлении протокола осмотра места происшествия [5, с. 8-12].

Также виртуальные следы могут быть изъяты путем официальных запросов в организации. Для данного способа изъятия виртуальных следов первоначально требуется установить информацию, по которой будет производиться запрос. Такую информацию можно установить в ходе получения объяснений, допроса свидетеля, потерпевшего и т.п. К указанной информации можно отнести сведения об абонентских номерах, адресов сайтов, IP-адресов и т.д. Таким образом, например, можно направить запрос о получении сведений, содержащихся на электронных носителях информации организаций, предоставляющих услуги по обслуживанию сайтов в информационно-телекоммуникационной сети «Интернет».

Исходя из рассмотренных в данной статье вопросов, можно сделать вывод о том, что УПК РФ, хоть и не без противоречий, но достаточно подробно регламентирует условия изъятия виртуальных следов. Данные условия содержат в себе указания на возможность изъятия электронных носителей информации и копирования хранящейся на них информации. Тем не менее, на наш взгляд, нормы УПК РФ в данной части требуют доработок.

## Список литературы


1. Кирсанова С.О., Калинина А.А. Виртуальные следы: понятие, сущность, проблемы // Скиф. 2018. № 3 (19). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/virtualnye-sledy-ponyatie-suschnost-problemy (дата обращения: 11.04.2021).
2. Васюков В.Ф. Изъятие электронных носителей информации: нерешенные проблемы практики // Уголовный процесс. 2016. № 2 (134). С. 54-57.
3. Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации // Законность. 2019. № 5. С. 40-43.
4. Мальчуков А.Н., Осокин А.Н. Быстрое вычисление контрольной суммы CRC: Таблица против матрицы // Прикладная информатика. 2010. № 2. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/bystroe-vychislenie-kontrolnoy-summy-crc-tablitsa-protiv-matritsy (дата обращения: 12.04.2021).

5. Васюков В.Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. № 2 (10). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/osobennosti-izyatiya-elektronnyh-nositelei-informatsii-pri-proizvodstve-sledstvennyh-dei-stvii-novelly-zakonodatelstva-i-problemy (дата обращения: 12.04.2021).

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

## НЕКОТОРЫЕ ПРОБЛЕМНЫЕ АСПЕКТЫ СТЕПЕНИ ЗАЩИЩЕННОСТИ НАСЕЛЕНИЯ АЛТАЙСКОГО КРАЯ ОТ ТЕРРОРИСТИЧЕСКИХ АКТОВ И АКТОВ КИБЕРТЕРРОРИЗМА

В обоснование актуальности нашей темы, отметим, что объявленный в марте прошлого года локдаун породил всплеск преступности в киберпространстве. Почти на 41% возросло число совершенных преступлений экстремистской и террористической направленности. Причем, как показывает статистика, большинство из лиц, совершивших данные деяния, являются несовершеннолетними [1, с. 34].

В современном мире стремительно растет количество «умных» устройств, которые работают именно с помощью сети Интернет, стоит отметить, что многие организации стали использовать современные интернет-технологии, что позволяет им организовать эффективное управление внутренней деятельностью, автоматизировав документооборот и работу бухгалтерии, обеспечив взаимозаменяемость сотрудников, оперативность руководства и принятия управленческих решений, мониторинг состояния рынка, рациональные отношения

с партнерами [9, с. 188]. Но все эти технологии дают почву для целенаправленных атак с целью террора или шантажа. Так, киберпреступникам стало намного проще получить необходимые им данные, просто взломав определенную систему [7, с. 31]. Например, киберпреступникам не составит большого труда организовать вывод целого производственного цеха из строя или даже взрыв АЭС. Конечно, на данный момент таких атак замечено не было, однако кто даст гарантию, что они не случатся в будущем? В своих акциях преступники активно используют все возможности современных технологий, в том числе современные гаджеты и программные продукты, радиоэлектронные устройства, достижения в других областях (вплоть до микробиологии и генной инженерии) [4, с. 142].

Официально кибертерроризмом признаются акты, совершенные одним человеком или независимыми группами, состоящими из нескольких участников. Если в подпадающих под это определение действиях принимают участие представители правительств или иных государственных структур, это считается проявлениями кибервойны. Влияние подобных акций на экономические и геополитические процессы зачастую преувеличивается журналистами в СМИ и сценаристами голливудских блокбастеров, что может привести к неправильной оценке сложившейся ситуации. Как на самом деле осуществляются кибератаки и что можно сделать для противостояния им? [5, с. 99].

Для грамотного противостояния проявлениям терроризма и кибертерроризма в первую очередь необходимо, чтобы население было осведомлено в данных вопросах. Поэтому было решено провести исследование относительно осведомленности населения Алтайского края.

В первую очередь в конце февраля мы провели эмпирическое исследование — анонимное анкетирование респондентов относительно проблем профилактики терроризма и иных деструктивных идеологий в сети «Интернет». В анкетировании приняло участие как взрослое население, так и молодежь.

Данные этого исследования показали, что взрослая часть населения менее осведомлена в таких понятиях, как терроризм и кибертерроризм, что нас очень заинтересовало. Поэтому мы решили детально изучить вопрос по степени защищенности личности и персональных данных от актов терроризма и кибер-

терроризма именно людей среднего и старшего поколения. Количество опрошенных составило примерно 50 человек, 66% из них имеют постоянное место работы, 10% временно не работают, 10% являются самозанятыми.

В ходе нашего исследования мы увидели, что 50% опрошенных в основном чувствуют себя защищенными от террористических актов в месте своего проживания, 24% — чувствуют себя защищенными лишь частично и 12% — не чувствуют себя защищенными. 46% респондентов в основном чувствуют себя защищенными от террористических актов в месте своей работы, 32% — чувствуют себя полностью защищенными и 10% — не чувствуют себя защищенными на своем месте работы.

Это говорит о достаточно высоком уровне доверия населения к правоохранительным органам и службам безопасности организаций. Однако только 34% опрошенных показали высокую степень доверия к работе, проводимой охранными службами в местах их трудоустройства. 56% показали, что единственной мерой защиты является оборудование помещений и территории организации системой видеонаблюдения, что, по их мнению, является явно недостаточным. 58% сообщили, что в месте их трудоустройства действует пропускной режим, однако указали на его несовершенство, ведь очень часто пропускной режим действует лишь формально.

Касаемо степени защищенности себя и своих персональных данных в сети «Интернет», респонденты показали совершенно другую картину. При использовании информационных и телекоммуникационных сетей 80% опрошенных не чувствуют защищенными свои персональные данные. 58% респондентов считают, что информационные ресурсы, которые использует организация, где они работают защищены, однако 34% ответить затруднились. Это свидетельствует о недостаточной осведомленности сотрудников организаций о мерах своей защиты в сети «Интернет», а следовательно, о недостаточности проводимых в рабочей организации мер по информированию сотрудников о степени их защищенности [3, с. 37].

Из респондентов 68% согласились бы использовать блокировщик экстремистских материалов в сети «Интернет», но 24% — пока не готовы использовать блокировщик и 8% — категорически отрицают возможность использовать подобные средства. Это может говорить о низкой осведомленности респондентов о наличии блокировочных защитных программ и иных средствах защиты конфиденциальности информации в сети «Интернет» [10, с. 19].

Исходя из результатов исследования, можно сделать вывод о том, что скорее всего старшее поколение осведомлено меньше из-за того, что с молодежью все чаще стали проводить профилактические мероприятия в местах их обучения, чего нельзя сказать о взрослом поколении. Ведь сложнее проводить подобные мероприятия с уже состоявшимися взрослыми людьми ввиду их занятости (семья, работа) [8, с. 24]. Отсюда мы предлагаем провести серию обучающих семинаров для сотрудников организаций различного профиля по вопросу повышения их осведомленности о защищенной работе в сети «Интернет». Также мы предлагаем работодателям при трудоустройстве обязать работников проходить инструктаж по работе в защищенной информационной среде и также обеспечить гласность в организациях относительно мер защиты работников от возможных актов нападения [2, с. 69].

Также нужно как можно больше предпринимать мер по огласке такой важной проблемы современности, как терроризм и кибертерроризм с помощью СМИ: запускать рекламные ролики, размещать баннеры с информацией в общественных местах, ведь именно СМИ позволяют нашему старшему поколению узнавать все, что происходит вокруг, а также необходим постоянный мониторинг осведомленности среди населения [6, с. 23]. Мы уверены, что все эти меры способны поднять уровень осведомленности населения и тем самым снизить уровень данных преступлений.

## Список литературы

1. Абрамова Г.С. Практическая психология: учебное пособие. М.: Прометей, 2018. 538 с.

2. Аминов И.И. Юридическая психология: учебное пособие. М.: Юнити-Дана, 2014. 270 с.

3. Андронникова О.О. Гендерная дифференциация в психологии: учебное пособие. М.: Инфра-М, 2017. 262 с.

4. Поляков В.В. Профилактика экстремизма и терроризма, осуществляемого с помощью сети Интернет // Известия Алтайского государственного университета. 2016. № 3 (91). С. 142-144.

5. Поляков В.В., Мананников А.С. Особенности противодействия кибертерроризму // Информационное противодействие экстремизму и терроризму: сборник трудов II всероссийской научно-практической конференции (Краснодар, 21 мая 2015 г.). Краснодар: Краснодарский университет МВД России, 2015. С. 99-105.

6. Sieber U. International cooperation against terrorist use of the internet: Revue internationale de droit penal. 2006/3 (Vol. 77). Pp. 395-449. DOI: 10.3917 / ridp.773.0395. [Электронный ресурс]. URL: https://www.cairn.info/revue-revue-internationale-de-droit-penal-2006-3-page-395.htm

7. Sieber U. the Threat of Cybercrime // Council of Европа (ред.), Organized Crime in Europe. Strasbourg, 2005. Pp. 81-218 (173-175).

8. Sieber U. Punishment of Serious Crimes Vol. 1. Freiburg. 2004. P. 26 ff.

9. Polyakov V.V., Starodubtseva M.A. Factors influencing motivation for terrorist activities being implemented with the use of information technologies in transboundary regions. The role of transnational corporations in the globalization of the economy // Advances in Social Science, Education and Humanities Research. 2019. Vol. 364. Pp. 188-191.

10. Waddel K. 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, 2018.

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

# ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СОВРЕМЕННОГО УГОЛОВНОГО ПРОЦЕССА: СОСТОЯНИЕ И ОТДЕЛЬНЫЕ ПЕРСПЕКТИВЫ РАЗВИТИЯ

Выступая 04 декабря 2020 г. на Международной онлайн-конференции Artificial Intelligence «Искусственный интеллект — главная технология XXI века», Президент Российской Федерации В.В. Путин сообщил о необходимости проведения цифровой трансформации всей нашей страны в ближайшие 10 лет. В частности, он отметил, что «в наступающее десятилетие нам предстоит провести цифровую трансформацию всей страны, всей России, повсеместно внедрить технологии искусственного интеллекта, анализа больших данных. Цифровая трансформация в России затронет каждого человека и все уровни власти. Наша страна на разных этапах успешно решала амбициозные задачи технологического и пространственного развития, строила железные дороги уникальными темпами на рубеже XIX-XX веков, проводила электрификацию в двадцатых — тридцатых годах прошлого столетия, — заявил он. Но наши планы повсеместного внедрения искусственного интеллекта, цифровой трансформации по глубине изменений во всех сферах аналогов не имеют. Они действительно затронут каждого человека, каждую семью, каждую отрасль экономики и социальной сферы, каждую организацию и каждый уровень власти, всю систему государственного управления» [13].

Современный уголовный процесс как особый вид государственной деятельности по расследованию и раскрытию преступлений также начинает постепенно подвергаться цифровизации. Практика цифровизации действующего Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ [1]) опирается, прежде всего, на возможности достижения современной науки и техники, а также современного программного обеспечения. Это позволило в конечном итоге разработать и внедрить в повседневую жизнь различные новые и уникальные справочно-правовые системы (Гарант, Консультант и др.),

которые существенно облегчили юристам-правоведам быстрый и эффективный поиск необходимой информации при производстве по уголовным делам. Внедрение в судебную систему программного обеспечения ГАС «Правосудие» позволило систематизировать базу данных выносимых судебных решений по уголовным делам, сделать ее простой и доступной для правоприменителя. На официальных сайтах современных судов и правоохранительных органов можно обнаружить различные судебные решения апелляционной, кассационной или надзорной инстанций, статистические данные, помогающие формировать единообразную судебную практику по уголовным делам.

Широкое развитие доступных и эффективных в использовании современных цифровых технологий аудиозаписи и видеозаписи позволили их использовать и применять для обнаружения и фиксации любых процессуальных действий (ч. 2 ст. 166 УПК РФ), в том числе осуществлять без участия отдельных субъектов уголовного процесса (ч. 3 ст. 170 УПК РФ)[27]. Начиная с 2011 г. по настоящее время в современном уголовном судопроизводстве (ст. 240, 399 УПК РФ) получили широкое распространение и признание отдельных цифровых технологий в форме использования видеоконференц-связи, что весьма актуально для отдаленных территорий нашей необъятной страны в случаях, когда личное присутствие участника процесса в судебном заседании по определенным причинам затруднительно или невозможно по определению[28].

Вопросы современного доказывания по отдельным уголовным делам также подверглись цифровому трансформированию, что в конечном итоге потребовало установлению дополнительной процессуальной регламентации порядка получения, изъятия, хранения и исследования необходимой информации, полу-

[27] Введена Федеральным законом от 04.03.2013 года № 23-ФЗ «О внесении изменений в статьи 62 и 303 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // Собрание законодательства Российской Федерации от 4 марта 2013 г. № 9. Ст. 875.

[28] Введена Федеральным законом от 20.03.2011 года № 39-ФЗ. «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Собрание законодательства Российской Федерации от 28 марта 2011 г. № 13. Ст. 1686.

ченной с электронных носителей, а также процессуальных действий с самими носителями данной информации (п. 5 ч. 2 ст. 82 УПК РФ)[29].

С 2013 г. в современный уголовный процесс вводится новый способ коммуникации — электронное отправление участникам судопроизводства СМС-сообщений о необходимости явки в судебные и правоохранительные органы [6]. С 2015 г. устанавливается новая обязанность потерпевшего сообщать свой адрес электронной почты для обеспечения более эффективной и быстрой связи с ним (ч. 5.1 ст. 42 УПК РФ)[30].

С введением таких мер пресечения, как домашний арест и запрет определенных действий, законодатель установил цифровой контроль за соблюдением подозреваемым или обвиняемым установленных судом запретов. В частности, в целях осуществления непосредственного контроля могут использоваться аудиовизуальные, электронные и иные технические средства контроля, перечень и порядок применения которых определяются Правительством Российской Федерации [7].

С 2016 г. в современный уголовный процесс вводится отдельная процедура использования электронных документов и электронной цифровой подписи, в том числе появилась возможность заверения электронного документа усиленной электронной подписью (ст. 474, 474.1 УПК РФ)[31]. При этом законодатель разрешил составлять и оформлять отдельные процессуальные документы не только в рукописном или машинописном, но и в электронном виде. В частности, в электронном виде могут изготавливаться копии отдельных процессуальных документов, например, исполнительные листы (ст. 393 УПК РФ). Существенно расширились возможности подачи отдельных уголовно-процес-

---

[29] Введена Федеральным законом от 28.07.2011 года № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Собрание законодательства Российской Федерации от 30 июля 2012 г. № 31. Ст. 4332.

[30] Введена Федеральным законом от 30.03.2015 года № 62-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации и Уголовно-исполнительный кодекс Российской Федерации по вопросу участия потерпевших при рассмотрении судом вопросов, связанных с исполнением приговора» // Собрание законодательства Российской Федерации от 30 марта 2015 г. № 13. Ст. 1806.

[31] Введена Федеральным законом от 23.06.2016 года № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» // Собрание законодательства Российской Федерации от 27 июня 2016 г. № 26 (часть I) Ст. 3889.

суальных документов, в частности, заявления, жалобы, ходатайства или представление теперь можно направить в электронном виде, заполнив определенную форму.

Существенно изменился порядок приглашения, назначения и замены защитника. В частности, с 2017 г. разработана система электронного распределения уголовных дел между адвокатами в тех случаях, когда органы, ведущие уголовное судопроизводство по конкретному делу, обязаны назначить адвоката для участия в деле в качестве защитника в порядке ст. 51 УПК РФ [8, с. 1-2].

Как мы видим, цифровые технологии постепенно проникают в современный уголовный процесс и в свою очередь получают отклики в непосредственном законодательстве. Однако нельзя не согласиться, что в современном непростом уголовном процессе это лишь пока отдельные фрагменты так называемой цифровой трансформации, которые лежат на ее поверхности. Между тем, как мы видим, усиленными темпами и со значительным опережением накапливается зарубежный опыт применения цифровых технологий в уголовном процессе отдельных иностранных государств. В частности, они находят свое воплощение при приеме и регистрации заявлений о совершенных преступлениях (УПК Республики Казахстан [2]; при производстве предварительного расследования в виде оформления отдельного «электронного уголовного дела» (УПК Турции [3] и др.); при производстве отдельных (упрощенных) процедурах по незначительным преступлениям или проступкам (УПК Англии и Уэльса [9]); при электронном оформлении различных уголовно-процессуальных документов: протоколов следственных и процессуальных действий, процессуальных решений, в том числе и приговора и иных судебных решений по уголовному делу (п. 15 ст. 7, ст. 45-1, 58, 83, п. 5 ч. 3 ст. 122, ст. 137, 347, ч. 4 ст. 395 и др. УПК Республики Казахстан) [2].

Со значительным опережением накапливается опыт применения цифровых технологий в уголовном судопроизводстве США, в частности, использование киберсудьи и реконструкция события совершенного преступления в виртуальной реальности [11, с. 54-61].

Неизбежность цифровой трансформации в современном уголовном процессе с учетом анализа темпов его развития в зарубежном законодательстве

очевидна и обусловлена также Стратегией развития информационного общества в Российской Федерации на 2017-2030 гг., утвержденной Указом Президента РФ от 09.05.2017 № 203 [12].

Вместе с тем и в этой части мы солидарны с уважаемой Л.А. Воскобитовой: «Произвольная и безграничная цифровизация уголовно-процессуальной деятельности без учета ее природы, объективно присущих ей особенностей представляется недопустимой. Нельзя недооценивать весьма великий риск судебных и следственных ошибок, несправедливости разрешения дела и нарушения прав человека, если принятие решений и/ или совершение процессуальных действий будет осуществлять машина, запрограммированная и действующая на принципах предельного упрощения и формализации информации и однозначности вариантов решений» [10]. В данном контексте возможность применения или использования цифровых технологий в современном уголовном процессе требует детального анализа и обсуждения от наступления возможных рисков, способных нанести непоправимый вред тем или иным общественным отношениям. Подобные риски в виде последствий мы явно наблюдаем и в современном уголовном судопроизводстве, в частности, оно выражается в отсутствии или недостаточных специальных знаниях должностных лиц по использованию высоких технологий при проведении онлайн-правосудий по уголовным делам и производство отдельных процессуальных действий. В результате изменения традиционных уголовно-процессуальных форм и внедрения отдельных цифровых технологий существенно сказались на реализации принципа равноправия и состязательности сторон.

Таким образом, только изучив все возможные риски и возникшие последствия, с учетом системного анализа положительного отечественного и зарубежного опыта в данном контексте, можно сформировать общий порядок применения и использования отдельных цифровых технологий в современном уголовном процессе. В этой связи считаем правильным не отказываться от традиционных уголовно-процессуальных форм человеческой деятельности, а параллельно внедрять отдельные цифровые технологии с учетом мнения заинтересованных сторон в уголовном деле. Верным и правильным решением на получение согласия на производство по уголовным делам и использования цифровых

технологий, мы наблюдаем сегодня в п. 2.3 приказа Судебного департамента при Верховном Суде РФ от 25.12.2013 № 257 «Об утверждении Регламента организации извещения участников судопроизводства посредством СМС-сообщений». В частности, извещение о вызове сторон посредством СМС-сообщения осуществляется только с согласия участника судопроизводства, то есть исключительно на добровольной основе. Подобные параллели в виде сохранения традиционных уголовно-процессуальных форм и использование цифровых технологий имеются и в гл. 5 УПК Казахстана в ст. 42-1 «Формат уголовного судопроизводства», где прописано, что «уголовное судопроизводство в Республике Казахстан ведется в бумажном и (или) электронном форматах. Лицо, ведущее уголовный процесс, с учетом мнения участников уголовного процесса и технических возможностей вправе вести уголовное судопроизводство в электронном формате, о чем выносит мотивированное постановление. В случае невозможности дальнейшего ведения уголовного судопроизводства в электронном формате лицо, ведущее уголовный процесс, переходит на бумажный формат, о чем выносит мотивированное постановление» [2].

Целесообразно начать рассматривать вопрос о внедрении цифровых технологий на этапе возбуждения уголовного дела с целью систематизации и учета всех сообщений о преступлениях, поступающих в органы внутренних дел, а также эффективного осуществления должностными лицами уголовного преследования. Так, согласно приказу МВД России № 736 от 29 августа 2014 г. [5], для приема заявлений о преступлениях и происшествиях в электронной форме, направляемых посредством официальных сайтов, применяется программное обеспечение, предусматривающее обязательное заполнение заявителем реквизитов, необходимых для работы с заявлениями о преступлениях и происшествиях. После чего поступившие электронные заявления распечатываются на бумажном носителе и дальнейшая работа ведется с ними как с письменными заявлениями о преступлениях. На этом все заканчивается.

Между тем для современной стадии возбуждения уголовного дела принципиально важным является вопрос не только способа подачи заявления, но и его официального электронного принятия и немедленной регистрации, чтобы как минимум началась процессуальная проверка по поступившему заявлению

о преступлении. При этом необходимо отдельно предусмотреть электронный порядок, учет, а также цифровую форму подачи электронных заявлений о преступлении, где конкретно установить соответствующее программное обеспечение, позволяющие определить конкретные признаки состава преступления, а также лиц, полномочных рассматривать и принимать соответствующие процессуальные решения. Внедрение подобных цифровых технологий будет способствовать обеспечение доступа граждан к современному правосудию, а также защите потерпевших от преступлений, в том числе где бы они ни находились.

Что касается современного процесса доказывания, то в этом контексте считаем необходимым сохранить традиционную уголовно-процессуальную форму, поскольку все доказательства не имеют заранее установленной силы, оцениваются уполномоченным лицом по своему внутреннему убеждению с учетом относимости, допустимости, достоверности и достаточности, руководствуясь при этом законом и совестью. Подобными функциями цифровые технологии не обладают. В этой связи, считаем, важно отметить, что цифровые технологии должны не заменять человеческий разум, а наоборот, помогать (подсказывать) должностному лицу находить различные варианты решения возникшей проблемы, а также оказывать необходимую помощь в поиске и принятии конкретного решения по уголовному делу.

Взвешенный подход к применению и использованию цифровых технологий в современный уголовный процесс, строящийся на общепризнанном принципе безопасности «не навреди», позволит усовершенствовать традиционный и классический процесс производства по уголовному делу. Сделать современный уголовный процесс максимально цифровым и эффективным, не создающим никаких угроз и рисков как для самого себя, так и для обеспечения прав и свобод человека в этой сфере, что в конечном итоге позволит реализовать в полном объеме все наставления главы Российского государства.

## Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства Российской Федерации от 24 декабря 2001 г. № 52 (часть I) ст. 4921.

2. Уголовно-процессуальный кодекс Республики Казахстан в ред. Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам модернизации процессуальных основ правоохранительной деятельности» от 21 декабря 2017 г. № 118-VI ЗРК — Текст электронный // Интернет-портал. [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=35167041 (дата обращения: 23.03.2021).

3. Уголовно-процессуальный кодекс Турецкой Республики / М-во образования и науки Российской Федерации, Дальневосточный федеральный ун-т; науч. ред. В.А. Оровер; пер. с тур. Рамин Садай Багирзаде. Владивосток: Изд-во Дальневосточного ун-та, 2015. 222 с.

4. Указ Президента РФ от 09 мая 2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы». Текст электронный // Интернет-портал. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 23.03.2021).

5. Приказ МВД России от 29 августа 2014 г. № 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях». Зарегистрировано в Минюсте РФ 6 ноября 2014 г. Регистрационный № 34570.

6. Приказ Судебного департамента при Верховном Суде РФ от 25 декабря 2013 г. № 257 «Об утверждении Регламента организации извещения участников судопроизводства посредством СМС-сообщений» // Бюллетень актов по судебной системе. 2014. № 2.

7. Приказ Минюста России № 189, МВД России № 603, СК России № 87, ФСБ России № 371 от 31.08.2020 «Об утверждении Порядка осуществления контроля за нахождением подозреваемых или обвиняемых в месте исполнения меры пресечения в виде домашнего ареста и за соблюдением возложенных судом запретов подозреваемыми или обвиняемыми, в отношении которых в качестве меры пресечения избран запрет определенных действий, домашний арест или залог» // Зарегистрировано в Минюсте России 03.09.2020 № 59635.

8. Ближайшие задачи адвокатуры // Адвокатская газета. 2019. № 1 (282). 1-15 января. С. 1-2.

9. Digitising the World's Courts — England & Wales [Переход в цифровое пространство мировых судов — Англия и Уэльс]. Текст электронный // Интернет-портал. [Электронный ресурс]. URL: https://www.geldards.com/digitising-the-worlds-courts.aspx (дата обращения: 23.03.2021).

10. Воскобитова Л.А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lex russica (Русский закон). 2019. № 5 (150). С. 91-104.

11. Юркевич М.А. Цифровое уголовное судопроизводство: какой процесс нас ждет в ближайшем будущем, и о чем нельзя забывать в погоне за всеобщей диджитализацией // Вопросы российского и международного права. 2020. Т. 10. № 5-1. С. 54-61.

12. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы. Указ Президента РФ от 09 мая 2017 года № 203. Текст электронный // Интернет-портал. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 23.03.2021).

13. В.В. Путин заявил о необходимости цифровой трансформации России. Текст электронный // Интернет-портал. [Электронный ресурс]. URL: https://tass.ru/ekonomika/10172635 (дата обращения: 24.03.2021).

***И.Д. Милич,*** *Ph.D., ассистент кафедры уголовного права Юридического факультета Новосадского университета, г. Нови-Сад, Республика Сербия*

## ОБ ОДНОЙ ВОЗМОЖНОСТИ УЛУЧШЕНИЯ ОСУЩЕСТВЛЕНИЯ ПРАВА НА УСЛОВНО-ДОСРОЧНОЕ ОСВОБОЖДЕНИЕ

Во время чрезвычайного положения, объявленного в связи с эпидемией инфекционного заболевания COVID 19, в Республике Сербия была введена возможность судить обвиняемое лицо, в отношении которого избрана мера пресечения в виде содержания под стражей (и который содержится в пенитен-

циарном учреждении), без его личного присутствия в зале суда. Его присутствие обеспечивалось путем видеосвязи для передачи звука и изображения (так называемый суд по скайпу). Такое решение было предусмотрено подзаконным актом, но оно не соответствовало Уголовно-процессуальному кодексу. Согласно УПК, только в определенных случаях подсудимого можно судить таким образом, при его отсутствии в зале суда, а будет иметь возможность наблюдать за основным судебным разбирательством с помощью технических средств передачи звука и изображения (например, если обвиняемый нарушает правила поведения в судебном заседании). Однако так как этот вопрос до сих пор мало обсуждался в научной и профессиональной общественности, мы хотим отметить, что в одном случае такой способ обеспечения присутствия осужденного может быть полезным. Это тот случай, когда принимается решение об условно-досрочном освобождении осужденного.

В Республики Сербия при определенных условиях осужденный по правилу может быть освобожден условно-досрочно, но есть несколько категорий осужденных, которые не имеют права на условно-досрочное освобождение. Условное освобождение — «мечта» каждого осужденного. В Республике Сербия решение об условном освобождении принимает суд. Чтобы реализовать это право, осужденным необходимо провести определенное время отбывания тюремного заключения. Они должны отбыть 2/3 своего срока, отбывая наказание в виде тюремного заключения, за исключением людей, приговоренных к пожизненному заключению, так как они должны провести 27 лет, отбывая наказание в виде тюремного заключения [1]. Этот срок является объективным условием условного освобождения осужденных. По истечении этого срока осужденный или его защитник может ходатайствовать об условно-досрочном освобождении [2]. Однако кроме времени, затраченного на отбытие тюремного заключения, для условно-досрочного освобождения осужденного должны быть соблюдены и другие условия. Необходимо установить, не получал ли осужденный дисциплинарные взыскания, и можно ли ожидать, что он не будет совершать уголовные правонарушения после условного освобождения. В суде проводится специальная процедура, на которой решается, будет ли осужденный освобожден условно-досрочно или нет [3]. У этой процедуры в Сербии есть

определенные недостатки, и один из них, безусловно, заключается в том, что присутствие осужденного на слушании дела не обязательно, а зависит от решения суда. Именно суд решает, вызывать осужденного или нет, и вызывает его, если он считает, что его присутствие необходимо. По оценке законодателя, правило состоит в том, что осужденный не присутствует на слушании, и исключение составляет то, что он может присутствовать. Итак, суд может принять решение об условно-досрочном освобождении, даже если осужденный не сделал никаких «заявлений» относительно своего права на условно-досрочное освобождение. Такое решение оправдано с точки зрения государства. Также не оспаривается экономичность такого решения. В Республике Сербия есть более тридцати пенитенциарных учреждений, в которых осужденные отбывают наказание [4]. Принимая во внимание правила о территориальной юрисдикции суда, принимающего решение об условном освобождении, а также правила о том, где осужденный отбывает наказание в виде лишения свободы, суд на территории, на которой находится пенитенциарное учреждение, не всегда имеет юрисдикцию проводить процедуру условного освобождения. Это означает, что передвижение осужденного (если его сопровождают на слушание) должно быть обеспечено службой безопасности на служебном автомобиле, что требует определенных затрат (размер затрат в первую очередь зависит от того, насколько далеко пенитенциарное учреждение находится от суда). Например, в Республике Сербия в течение 2006 г. из пенитенциарных учреждений освобождено условно-досрочно от отбывания наказания 1,561 осужденных лиц [5]. Такое передвижение осужденных также приводит к определенному риску, зависящему от того, насколько осужденный опасен, например, риск побега. Возможно, это одна из причин, по которой законодатель предписал вызывать осужденного на слушание только в исключительных случаях. С другой стороны, прокурор всегда присутствует на слушании, а представитель пенитенциарного учреждения, в котором осужденный отбывает наказание в виде лишения свободы, присутствует только в том случае, если характеристика на осужденного положительная. Если у осужденного есть защитник, он также может присутствовать на слушании. Принимая во внимание это решение УПК, при вынесении решения об условно-досрочном освобождении суд отдает предпочтение

характеристике осужденного, документу о поведении осужденного, который предоставляет в суд пенитенциарное учреждение. Этот документ может быть «написан» таким образом, что может принести как пользу, так и вред осужденному. Если документ содержит негативную информацию об осужденном и он не присутствует на слушании, то не имеет возможности указать на недостатки такого документа. Он не имеет возможности опровергнуть информацию, не соответствующую правде. Осужденный в данном случае находится в неравном положении. Мы считаем, что на слушании, в котором осужденный не участвует, суд не может правильно оценить все обстоятельства, имеющие значение для принятия решения об условно-досрочном освобождении. Полагаем, что для осужденных было бы справедливее присутствовать в зале суда на слушании, на котором решается их право на условно-досрочное освобождение. Однако если законодатель все-таки считает его присутствие «неважным», то для осужденного было бы более благоприятным решением, если бы его присутствие было обеспечено с помощью технических средств передачи звука и изображения. Это можно сделать таким образом, чтобы в пенитенциарном учреждении было специальное помещение, технически оборудованное для передачи звука и изображения. Конечно, таким образом присутствие осужденного могло бы быть обеспечено в некоторых других судебных процессах, в которых такой способ присутствия разрешен и оправдан. Таким образом, хотя и в ограниченном объеме, осужденный сможет указать суду, что он не нарушал дисциплину во время отбывания тюремного заключения и указать на определенные доказательства, подтверждающие его показание. Осужденный также мог бы указать на определенные недостатки документа (характеристики) о его поведении, выданного пенитенциарным учреждением. Такое решение, безусловно, помогло бы суду, это было бы способом для судей «увидеть осужденного», задать ему определенные вопросы, которые важны для принятия решения. Судьи, которые принимают решение об условно-досрочном освобождении, не могут быть судьями, осудившими осужденного. Они должны быть судьями, которые ранее не участвовали в этом судебном процессе. Это означает, что судьи принимают решение на основе характеристики на осужденного, выданной пенитенциарным учреждением. Таким образом, суд мог бы сравнить заявление осужденного

с документом о его поведении. Такой способ присутствия осужденного повлиял бы также на «качество» документа о его поведении, так как в данном случае руководство пенитенциарного учреждения было бы более осторожным при написании характеристики на осужденного. Прокурор всегда излагает свое мнение по ходатайству осужденного. Проблема возникает, если он тоже не видит и не слышит осужденного. Вероятно, что он также будет в основном руководствоваться документом о поведении осужденного при принятии решения по ходатайству (он излагает свое мнение об удовлетворении заявленного ходатайства или о его отказе, но его заявление не является обязательным для суда). В связи с этим в какой-то мере можно сделать вывод о том, что если осужденный не присутствует в судебном заседании, суд принимает решение на основе документа о поведении осужденного, что неоправданно.

В Республике Сербия осужденный имеет возможность отбывать наказание в виде лишения свободы в помещениях, где он проживает (в Республике Сербия есть так называемый домашний арест). Это модель лишения свободы, которая может быть определена только в том случае, если осужденный приговорен к лишению свободы на срок до одного года. Однако осужденные, отбывающие тюремное заключение в своей квартире или в доме, также имеют право на условно-досрочное освобождение. От суда зависит, вызовут ли осужденного на слушание дела об условном освобождении или нет. Принимая во внимание, что осужденный имеет право покинуть квартиру в течение дня на определенный период времени, мы считаем, что было бы действительно оправданным, если суд всегда вызывает осужденных присутствовать в судебном заседании. Также мы полагаем, что для данной категории осужденных нецелесообразно обеспечивать их присутствие с помощью технических средств передачи звука и изображения. Для этого есть несколько причин, и одна из них заключается в том, что они свободны прийти в зал суда. Они не сопровождаются уполномоченными лицами, поэтому государство не несет никаких расходов в связи с их передвижением в суд.

Действительно, необходимо условно освободить осужденного, который этого заслуживает, но мы считаем, это трудно определить, если он не присутствует на слушании. Если бы законодатель изменил свое решение и предписал

осужденным присутствовать на слушании посредством передачи звука и изображения, это было бы прогрессом в осуществлении права на условно-досрочное освобождение. Таким образом, было бы возможно условно не освобождать осужденного, не заслуживающего этого права.

**Список литературы**

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

2. Милич И. Индивидуализация тюремного заключения — криминологические, уголовно-правовые аспекты и аспекты наказания: докторская диссертация. Нови-Сад, 2017. С. 404-477.

3. Уголовно-процессуальный кодекс РС // Служебный вестник РС». № 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019; ст. 563-568.

4. Милич И. Где исполняется наказание в виде лишения свободы в Республике Сербия? // Союз криминалистов и криминологов. 2020. № 3. С. 168-174.

5. Годовой отчет о работе Управления исполнения санкций институционального характера за 2006 г. [Электронный ресурс]. URL: https://npm.rs/attachments/Izvestaj%202006.pdf

***С.А. Мужчиль,*** *магистр юридических наук, преподаватель Высшего колледжа Восточно-Казахстанского университета имени С. Аманжолова, г. Усть-Каменогорск*

***О.А. Чакилева,*** *и.о. начальника отдела организационно-аналитической работы следственного отдела Управления полиции г. Усть-Каменогорска, подполковник полиции, г. Усть-Каменогорск*

## УГОЛОВНЫЕ ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В ВОСТОЧНО-КАЗАХСТАНСКОЙ ОБЛАСТИ

Информационные технологии на данный момент стремительно развиваются во всем мире. Однако не всегда это приводит только к положительным по-

следствиям. К негативным результатам этого прогресса можно отнести то, что совершается все больше преступлений в сфере киберпространства.

В 2000 г. американские ученые провели глобальное исследование уголовного законодательства 52 стран и пришли к выводу, что в тех странах, в которых предусмотрены преступления, совершаемые в «информационном пространстве», можно выделить 10 видов таких преступлений, объединенных в четыре категории:

- преступления, связанные с информацией, включая ее перехват, модификацию и кражу;
- преступления, связанные с компьютерными сетями, включая вмешательство в их работу и саботаж;
- преступления, связанные с доступом, включая хакерство и распространение вирусов;
- преступления, связанные с использованием компьютеров, включая оказание помощи и соучастие в преступлении, компьютерное мошенничество и компьютерный подлог [1, с. 30].

Стоит отметить, что в Уголовном кодексе Республики Казахстан предусмотрены следующие составы уголовных правонарушений, совершаемых в информационном пространстве. Это кража, совершенная путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций (ст. 188, ч. 2, п. 4 УК РК), мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы (ст. 190, ч. 2, п. 4 УК РК) в главе 6 УК РК под названием «Уголовные правонарушения против собственности». Также в УК РК имеется глава 7 «Уголовные правонарушения в сфере информатизации и связи», в которой содержатся следующие статьи. Это статья 205 УК РК «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций», ст. 206 УК РК «Неправомерные уничтожение или модификация информации», ст. 207 УК РК «Нарушение работы информационной системы или сетей телекоммуникаций», ст. 208 УК РК «Неправомерное завладение информацией»,

ст. 209 УК РК «Принуждение к передаче информации», ст. 210 УК РК «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов», ст. 211 УК РК «Неправомерное распространение электронных информационных ресурсов ограниченного доступа», ст. 212 УК РК «Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели», ст. 213 УК РК «Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства» [2].

Нами было проведено исследование количества данных уголовных правонарушений по Восточно-Казахстанской области за период с 2018 г. по май 2021 г. Было выявлено, что наибольшее количество уголовных правонарушений зарегистрировано по ст. 190 ч. 2 п. 4 УК РК (2018 г. — 592 случая, 2019 г. — 823, 2020 г. — 1348, 5 месяцев 2021 г. — 592 случая). При этом с 2018 по 2020 г. происходит увеличение количества данных преступлений.

На втором месте по количеству идет ст. 188 ч. 2 п.4 УК РК. Так, в 2018 г. зарегистрировано 10 подобных преступлений. В 2019 г. зарегистрировано 35 преступлений, а в 2020 — 81. За 5 месяцев 2021 г. зарегистрировано 33 преступления. С 2018 по 2020 г. наблюдается динамика в сторону увеличения количества данных преступлений.

На третьем месте следует ст. 205 УК РК. По данной статье в 2018 г. зарегистрировано 1 преступление. В 2019 г. зарегистрировано 17 преступлений. В 2020 г. — 5 зарегистрированных преступлений. За 5 месяцев 2021 г. отмечено 4 подобных преступления.

По ст. 206 УК РК в Восточно-Казахстанской области в 2018 г. зарегистрирован 1 случай, в 2019 г. — также 1. По ст. 207 УК РК в 2018 г. зарегистрировано 1 преступление. По ст. 209 УК РК в 2018 г. зарегистрировано 1 преступление. По ст. 210 УК РК в 2018 г. зарегистрировано 1 преступление, в 2020 г. — также 1 преступление.

При этом отметим, что по ст. 208, 211, 212, 213 УК РК в Восточно-Казахстанской области в период с 2018 г. по май 2021 г. не было зарегистрировано уголовных правонарушений.

Для того чтобы предупредить компьютерные преступления, следует осуществить следующие меры:

- организовать взаимодействие правоохранительных органов и судов по вопросам киберпреступлений;
- организовать сотрудничество правоохранительных органов Республики Казахстан с правоохранительными органами зарубежных стран;
- постоянно работать над повышением квалификации юристов в сфере киберпреступности, регулярно организовывать для них специальные курсы повышения квалификации;
- организовать подготовку специалистов по направлению «Киберпреступность»;
- создать глобальный реестр киберпреступлений.

Таким образом, на данный момент преступления в сфере информационного пространства представляют собой повышенную общественную опасность. Еще не все граждане имеют познания в сфере информационно-коммуникационной деятельности, а потому для современного общества очень важна защита граждан от подобных преступлений со стороны правоохранительных органов.

**Список литературы**

1. Чекунов И.Г. Компьютерная преступность: законодательная и правоприменительная проблемы компьютерного мошенничества // Российский следователь. 2015. № 17. С. 30-32.
2. Уголовный кодекс Республики Казахстан от 3 июля 2014 года.

***В.Р. Набиуллина,*** *старший преподаватель кафедры техносферной безопасности Государственного аграрного университета Северного Зауралья, аспирант кафедры уголовного права и процесса Тюменского государственного университета, г. Тюмень*

# УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ ПУБЛИЧНОМУ РАСПРОСТРАНЕНИЮ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ, СОВЕРШАЕМОМУ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Увеличение числа случаев публичного распространения заведомо ложной информации с применением информационных технологий обусловливает актуальность рассматриваемой темы. В частности, в связи с появлением новой вирусной инфекции Роскомнадзор выявил более 1 тысячи ложных материалов о коронавирусе за 2020 г., однако, по мнению члена Общественной палаты, директора Ассоциации участников рынка интернет-индустрии «Лига безопасного интернета» Екатерины Мизулиной, реальная цифра выше — около 14,5 тыс. ложных сообщений, причиной распространения которых является «плохая работа социальных сетей по блокировке недостоверной информации на своих площадках» [1]. Переход на дистанционный формат работы способствовал увеличению числа преступлений, совершенных с использованием информационных технологий [2]. Так, по данным МВД России, рост числа преступлений в названной категории в 2020 г. по сравнению с предыдущим годом составил 73,4%, в том числе с использованием Интернета — на 91,3%, при помощи средств мобильной связи — на 88,3%.

В Уголовном кодексе РФ (далее — УК РФ) несколько статей особенной части регулируют уголовную ответственность за публичное распространение заведомо ложной информации. К ним относятся ст. 128.1, 197, 207.1, 207.2, 354.1 УК РФ. Выборка статей УК РФ произведена нами по признаку публичности распространения заведомо ложной информации. В связи с применением в различных статьях УК РФ разных характеристик относительно информации, а именно «ложности» и «недостоверности», как следствие, возможной их зако-

нодательной нетождественности, в качестве объекта настоящего исследования выбрана ложная информация.

Рост числа преступлений с использованием информационных технологий влечет совершенствование уголовного законодательства, в частности, за последнее время приняты новые ст. 207.1 и 207.2 УК РФ, внесены изменения в существующие ст. 128.1, 354.1 УК РФ. В целях обозначения разнообразных способов совершения преступлений законодателем используется в УК РФ характеристика публичности информации. Признак публичности информации, предусмотренный в ч. 2 ст. 128.1, ст. 197, 207.1, 207.2, 354.1 УК РФ, раскрывается в правовых нормах и правоприменительной практике по-разному. Например, ч. 2 ст. 128.1 УК РФ регламентировала ответственность за клевету, содержащуюся в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации. В связи со стремительным развитием информационных технологий и с учетом степени общественной опасности преступлений, совершаемых с применением указанных технологий, законодателем внесены дополнения в ч. 2 ст. 128.1 УК РФ [3], касающиеся установления новых квалифицирующих признаков клеветы, а именно совершение преступления публично с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», либо в отношении нескольких лиц, в том числе индивидуально не определенных. Более того, санкция рассматриваемой ч. 2 ст. 128.1 УК РФ дополнена новыми видами наказаний — принудительные работы, арест и лишение свободы. Учитывая специфику предмета преступления (заведомо ложная информация), в целях уголовно-правового противодействия распространению клеветы видится необходимым междисциплинарный анализ причин и условий публичного распространения человеком заведомо ложной информации, который позволит разработать методы, способствующие предупреждению совершения преступлений. В связи с тем, что распространение заведомо ложной информации является глобальной проблемой, необходимо принимать во внимание опыт зарубежных исследователей.

Публичность по ст. 197 УК РФ означает совершение уголовно наказуемого деяния (заведомо ложное объявление о несостоятельности) устным или пись-

менным сообщением в публичном месте (например, в средствах массовой информации, в арбитражном суде) [4]. По мнению П.Н. Семенцова, обращение должника в суд с заявлением о признании себя банкротом должно рассматриваться публичным объявлением о несостоятельности в силу общедоступности картотеки арбитражных дел и открытости судебных заседаний [5]. Таким образом, субъектом преступления по ст. 197 УК РФ может быть признано лицо, в действиях которого отсутствует общепризнанное понимание публичного распространения информации (в СМИ, в Интернете и т.д.), но его действия квалифицируются как публичные в силу дальнейшей общедоступности заявленной заведомо ложной информации. То есть непосредственное применение виновным лицом информационных технологий для распространения заведомо ложной информации о несостоятельности не требуется для признания его противоправных действий публичными. В качестве примера можно привести приговор Менделеевского районного суда Республики Татарстан по делу № 1-1/2017 от 19 февраля 2018 г. [6]. Генеральный директор в целях фиктивного банкротства компании подписал финансовые документы (оформил крупные денежные займы), увеличившие кредиторскую задолженность компании на сумму 2 280 592 руб., хотя заведомо знал о ее отсутствии перед кредиторами, чем создал видимость неплатежеспособности компании. Далее он обратился в арбитражный суд с заявлением о признании компании несостоятельной (банкротом), представил фиктивные документы о неплатежеспособности, тем самым публично объявил компанию банкротом. В рамках процедуры банкротства удовлетворены незаконные и необоснованные требования кредиторов в размере 4 360 592 руб., что является крупным размером. В результате противоправных действий генерального директора единственному акционеру компании причинен крупный ущерб в размере 23 294 484 руб., компания ликвидирована. Суд, учитывая обстоятельства, смягчающие наказание: положительные характеристики с места жительства и с места работы, ранее не судим, на учете у нарколога и психиатра не состоит, состояние здоровья и имеющиеся заболевания, инвалидность 2 группы, престарелый возраст, признал генерального директора виновным в совершении преступления по ст. 197 УК РФ, назначил наказание в виде штрафа

в размере 250 000 руб. Соразмерны ли в рассмотренном уголовном деле назначенное наказание и причиненный вред компании и единственному акционеру — навряд ли. В силу единичности случаев привлечения к ответственности по ст. 197 УК РФ законодателем последний раз вносились изменения в санкцию рассматриваемой статьи в 2011 г. Для квалификации деяний преступными по ст. 197 УК РФ необходимо совершение преступления лицом, непосредственно объявляющим себя несостоятельным (руководитель или учредители юридического лица, гражданин, индивидуальный предприниматель). В случае если иное лицо заведомо ложно объявит о банкротстве компании, его деяния подлежат квалификации по ст. 128.1 УК РФ.

Под публичностью в ст. 207.1 и 207.2 УК РФ признается распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и заведомо ложной общественно значимой информации, повлекшей тяжкие последствия, в любой форме (например, в устной, письменной, с использованием технических средств) в группе или неограниченном кругу лиц с использованием средств массовой информации, информационно-телекоммуникационных сетей, в том числе мессенджеров (WhatsApp, Viber и других), в массовой рассылке электронных сообщений абонентам мобильной связи, распространении такой информации путем выступления на собрании, митинге, распространения листовок, вывешивания плакатов и т.п. [7]. Таким образом, признак публичности информации включает в себя применение всевозможных способов распространения ложной информации, в том числе с использованием информационных технологий. Виновным может быть признано не только лицо, создавшее и разместившее ложную информацию, но и другое лицо, осуществившее репост информации. Автором статьи в текущем году проведен опрос среди студентов заочной формы обучения Государственного аграрного университета Северного Зауралья[32]. На вопрос о том, знали ли Вы ранее о наличии уголовной ответственности, предусмотренной ст. 207.1 и 207.2 УК РФ, из 77 респондентов положительно ответили 66,2%, отрицатель-

[32] С опросом можно ознакомиться по ссылке: [Электронный ресурс]. URL: https://sites.google.com/view/nvictoria/

но — 33,8%. На вопрос, знаете ли Вы, что клевета о том, что лицо болеет коронавирусом, влечет уголовную ответственность (ч. 4 ст. 128.1 УК РФ), 35,1% ответили да, 64,9% — нет. Незнание уголовно-правовых запретов является одним из условий совершения преступлений. В этой связи необходимо больше внимания уделять правовому просвещению населения в различных источниках информации.

В ст. 354.1 УК РФ (реабилитация нацизма) наряду с признаком публичности информации обозначены квалифицирующие признаки преступления: с использованием средств массовой информации, недавно законодателем добавлены информационно-телекоммуникационные сети, в том числе сеть «Интернет» [8]. Кроме того, увеличены размеры санкций статьи, дополнены виды наказания, квалифицирующие признаки преступления. Указанное свидетельствует о высокой степени общественной опасности деяний, совершаемых с применением информационных технологий. Несмотря на то, что признак публичности информации включает в себя распространение ложной информации в сети «Интернет» [9, с. 23-24], законодателем указанный способ распространения информации выделен в ст. 354.1 УК РФ в качестве квалифицирующих и особо квалифицирующих признаков преступления. Примером судебной практики является приговор Нижегородского областного суда по делу № 2-34/2019 от 6 ноября 2019 г. [10]. Виновное лицо создало и администрировало персональную общедоступную интернет-страницу, на которой разместило информацию, содержащую признаки оправдания идеологии фашизма (нацизма). Суд назначил наказание, предусмотренное ч. 1 ст. 354.1 УК РФ, в виде штрафа в размере 120 тыс. руб. с рассрочкой выплаты.

Учитывая изложенное, в целях уголовно-правового противодействия публичному распространению заведомо ложной информации с применением информационных технологий необходимы следующие меры: своевременное или опережающее совершенствование уголовного законодательства, ужесточение санкций, правовое просвещение населения в различных источниках информации.

## Список литературы

1. Роскомнадзор заявил о выявлении более тысячи коронафейков в 2020 году. [Электронный ресурс]. URL: https://roskomsvoboda.org/67656/ (дата обращения: 23.05.2021).

2. Уголовно-правовые риски в условиях цифровизации: способы противодействия. [Электронный ресурс]. URL: https://www.garant.ru/news/1443692/#sdfootnote1sym (дата обращения: 23.05.2021).

3. Федеральный закон от 30.12.2020 № 538-ФЗ «О внесении изменения в статью 128-1 Уголовного кодекса Российской Федерации». [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202012300058?index=0&rangeSize=1 (дата обращения: 23.05.2021).

4. Методические рекомендации по выявлению и пресечению преступлений в сфере экономики и против порядка управления, совершенных сторонами исполнительного производства (утв. ФССП России 15.04.2013 № 04-4) // СПС КонсультантПлюс (дата обращения: 23.05.2021).

5. Семенцов П.Н. Размышления о фиктивном банкротстве (ст. 197 Уголовного кодекса РФ). [Электронный ресурс]. URL: https://zakon.ru/blog/2018/1/11/razmyshleniya_o_fiktivnom_bankrotstve_st197_ugolovnogo_kodeksa_rf (дата обращения: 23.05.2021).

6. Приговор Менделеевского районного суда Республики Татарстан по делу № 1-1/2017 от 19 февраля 2018 г. [Электронный ресурс]. URL: //sudact.ru/regular/doc/HCQzDutckmbt/ (дата обращения: 23.05.2021).

7. Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2 (утв. Президиумом Верховного Суда РФ 30.04.2020) // СПС КонсультантПлюс (дата обращения: 23.05.2021).

8. Федеральный закон от 5 апреля 2021 г. № 59-ФЗ «О внесении изменений в статью 354.1 Уголовного кодекса Российской Федерации. [Электронный ресурс]. URL: https://www.garant.ru/hotlaw/federal/1454791/ (дата обращения: 23.05.2021).

9. Червонных Е.В. Уголовно-правовая характеристика преступлений, предусмотренных статьей 354.1 «Реабилитация нацизма» УК РФ, и отдельные проблемы её правоприменения // Проблемы правоохранительной деятельности. 2015. № 4. С. 21-27. С. 23-24

10. Приговор Нижегородского областного суда по делу № 2-34/2019 от 6 ноября 2019 г. [Электронный ресурс]. URL: //sudact.ru/regular/doc/Wlg9rDxsrvJ/ (дата обращения: 24.05.2021).

***А.П. Пинчук,*** *преподаватель Колледжа Алтайского государственного университета, аспирант Юридического института Алтайского государственного университета, г. Барнаул*

## ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ ОПЕРАТИВНО-РОЗЫСКНОГО ОБЕСПЕЧЕНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Преступность как остросоциальное явление обусловливается развитием общества. Данная ячейка социума также состоит из людей, хотя и имеющих другие целевые установки. Это диктует особую сложность и трудоемкость борьбы с криминальным сектором, поскольку противостояние здесь «субъект-субъект», а следовательно, «по ту сторону баррикад» будут делать все возможное, чтобы не только не стать жертвами правоохранительной деятельности компетентных органов, но и воспользоваться дарами времени, чтобы нарастить преступные обороты, приумножить противозаконные блага.

Современные возможности позволяют оцифровать жизнь общества. Пилотное использование различных гаджетов более десятилетия назад показало их удобство. Прошло чуть более десятка лет, а современный человек не видит свою жизнь без компьютера, планшета, телефона. Компьютеризация буквально всех сфер жизнедеятельности — учебы, работы, досуга — без излишних намеков создала условия для преступного промысла.

Современное состояние правоохранительных органов таково, что при казалось бы бюджетной государственной поддержке арсенал для борьбы с компьютерными преступлениями не соответствует уровню развития такой преступности.

В 2020 г. 25% преступлений совершалось с использованием информационных технологий [7]. При этом в суд направляется сравнительно небольшое количество таких уголовных дел (16% в прошлом году) [9]. Отделы полиции, прокуратуры буквально переполнены приостановленными уголовными делами по преступлениям такого характера (например, компьютерным мошенничествам). Такая статистика дала понять — имеющийся оперативно-розыскной инструментарий не в достаточной мере эффективен.

Компьютерные преступления отличаются своей латентностью, совершаются зачастую в условиях неочевидности. Это предопределило необходимость для правоохранительных органов принять отдельные меры для борьбы именно с такими преступлениями. Например, 10 сентября 2020 г. стало известно о создании Генеральной прокуратурой РФ межведомственной рабочей группы для борьбы с киберпреступлениями. В нее, помимо прокуроров, вошли представители МИДа, МВД, ФСБ, Следственного комитета и Минюста России [8]. В области оперативно-розыскной деятельности уже давно действует и зарекомендовал себя отдел «К» МВД РФ. Сама специфика компьютерных преступлений говорит о возможности борьбы с ними преимущественно оперативно-розыскными методами.

Оперативно-розыскное право закрепляет перечень оперативно-розыскных мероприятий (далее — ОРМ), некоторые из них направлены как раз на преступления с компьютерной спецификой (например, введенное в 2016 г. ОРМ «Получение компьютерной информации»).

Несмотря на преимущественно ограниченное для широких масс правовое регулирование ОРД, оперативно-розыскное право в базовом Федеральном законе «Об оперативно-розыскной деятельности» (далее — Закон об ОРД) закрепило определенные организационно-правовые средства борьбы с компьютерной преступностью. Однако говорить о совершенстве такого обеспечения дея-

тельности оперативно-розыскных органов преждевременно, вспоминая ту же статистику с четвертью совершенных в 2020 г. компьютерных преступлений.

В целом же имеется ряд проблем, в частности которыми можно объяснить неутешительную статистику раскрываемости компьютерной преступности. Рассмотрим некоторые из них.

Во-первых, изъятие электронных носителей информации при проведении гласных ОРМ (например, при обследовании помещений, зданий, сооружений, участков местности и транспортных средств). Статья 15 Закона об ОРД закрепляет такую возможность для оперативно-розыскных органов [1].

Отметим, что такое изъятие не уникально. Аналог встречается в Уголовно-процессуальном кодексе РФ — ст. 164.1 «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий». Однако имеются различия. Основное, как мы считаем, заключается в необходимости участия специалиста в изъятии электронных носителей при производстве следственного действия. Согласно ч. 2 ст. 164.1 УПК РФ, «электронные носители информации изымаются в ходе производства следственных действий с участием специалиста» [2]. При этом Закон об ОРД не вменяет в обязанность оперативно-розыскным органам привлекать в таких случаях специалиста, оставляя ситуацию на усмотрение конкретных должностных лиц.

Считаем, что возможность дискреции со стороны оперативных сотрудников может породить риск утраты уникальной информации, необходимой для дальнейшего расследования преступления. Отсутствие, на первый взгляд, необходимости в привлечении специалиста (например, когда изымается носитель информации целиком и изъятие производится без копирования содержащейся на нем информации), может повлечь возникновение нештатных ситуаций, вызванных заранее предусмотренными злоумышленниками мерами (стирание информации при обесточивании компьютера, при демонтаже устройства либо при выбытии техники с места дислокации, отслеженное через GPS, и др.). Закрепление в Законе об ОРД положения об обязательном участии специалиста в таких случаях

послужит страховкой для оперативно-розыскных органов при изъятии ценной для дальнейшего формирования доказательственной базы информации.

Безусловно, необходимо разработать исключения, когда участие специалиста не будет обязательным (например, наличие у оперативного сотрудника соответствующего образования в сфере информационных технологий; при изъятии отдельных жестких дисков, флэш-накопителей и т.д.), поскольку распространенность электронных носителей информации среди граждан при безоговорочном положении о необходимости привлечении специалиста повлечет отвлечение экспертов от производства, например, компьютерных экспертиз, что приведет к не менее вредным последствиям. В уголовном процессе это называется принципом процессуальной экономии. В оперативно-розыскном праве, полагаем, такая экономия также нелишняя.

Во-вторых, обратим внимание на ОРМ «Получение компьютерной информации». Данное оперативно-розыскное мероприятие было введено поправкой от 06.07.2016 г. на фоне наращивания оборотов компьютерной преступностью. Как отмечают Н.Г. Корнаухова и С.В. Катков, несмотря на то что это ОРМ уже существует относительно продолжительное время, фактически отсутствует нормативно-правовая регламентация, позволяющая четко определить варианты его документального оформления, обеспечивающих максимально эффективное использование полученных результатов, например, в рамках уголовного судопроизводства [5, с. 185]. К тому же проблемным видится отсутствие единства в науке относительно определения данного ОРМ. Отсутствует таковое и в нормативных правовых актах. Такое положение вещей, наряду с отсутствием достаточной материально-технической и кадровой базы у оперативно-розыскных органов, влечет затруднения в полноценном использовании данного ОРМ на практике. Более того, имеются вопросы и по разграничению данного ОРМ с таким как «Снятие информации с технических каналов связи».

В-третьих, недостаточное правовое регулирование в области предупреждения компьютерных преступлений. К мерам предупреждения преступлений, совершаемых с использованием высоких технологий, также относится разработка новых методик противодействия данному виду преступлений, в том чис-

ле в процессе оперативно-розыскной деятельности. Так, отмечается в литературе, представляется необходимым законодательно закрепить полномочия правоохранительных органов на осуществление мониторинга опубликованных в социальных сетях или иных ресурсах материалов противоправного характера, а в некоторых случаях обеспечить проведение соответствующих надзорных, оперативно-розыскных, следственных мероприятий с возможностью получения необходимой информации от провайдеров или Роскомнадзора напрямую без судебного разрешения [4, с. 65].

В-четвертых, допускаются тактические ошибки и в процессе изъятия компьютерной информации в условиях активного противодействия расследованию. Основным недостатком при этом является то, что с момента начала следственного действия (либо оперативно-розыскного мероприятия) до момента изъятия компьютерной информации проходит время, достаточное для уничтожения искомой информации и/или содержащих ее объектов.

В целях недопущения указанных негативных последствий необходимо обеспечить максимально эффективное использование фактора внезапности при производстве следственного действия (ОРМ), а именно: использование возможностей оперативно-розыскной деятельности для предварительного установления состава и конфигурации информационной системы, расположения ее основных элементов и узлов; обеспечение достаточного количества привлеченных сил и средств, обеспечивающих блокирование ключевых элементов информационной системы; неожиданное вхождение в обыскиваемое помещение; исключение доступа кого бы то ни было к основным элементам информационной системы [4, с. 131].

В-пятых, это специфика компьютерных преступлений, которые зачастую имеют трансграничный характер. При совершении таких преступлений субъект может находиться далеко за пределами РФ, когда объект преступного посягательства находится на ее территории. Это придает преступлениям международную окраску, что порождает необходимость сотрудничества с другими государствами — обмен оперативной информацией, запрос на проведение ОРМ, процессуальных действий и т.д. Успех такого сотрудничества зачастую зависит

от международной обстановки в целом, от характера отношений государств, вовлеченных в такие уголовно-правовые отношения.

Каковы же тенденции развития в оперативно-розыскном праве направления борьбы с компьютерной преступностью? Перспективным видится предложение МВД о дополнении одного из ОРМ. 28 мая 2021 г. МВД выступило с законопроектом о внесении изменений в п. 5 ч. 1 ст. 6 Закона об ОРД, ранее именовавшегося как «Исследование предметов и документов». Теперь МВД предлагает расширить данное ОРМ, назвав его «Исследование предметов, документов и компьютерной информации».

Чем вызваны попытки дополнить оперативно-розыскное законодательство такого рода нововведением?

Как объясняют свое предложение в МВД, одной из причин является отсутствие достаточных оперативных возможностей по документированию компьютерных преступлений. Например, сложности вызывает ситуация с использованием преступниками удаленных рабочих столов. Эта технология позволяет преступникам дистанционно уничтожить данные (например, экстремистские материалы) из облачного хранилища на удаленном сервере. На практике это приводит к утрате части доказательной базы даже в случае изъятия в рамках ОРМ средств коммуникации, используемых преступниками.

Смоделируем ситуацию, при проведении ОРМ «Обследование помещений…» в рамках расследования (или раскрытия) так называемого компьютерного преступления (состав в данном примере не важен) был изъят персональный компьютер как средство преступления. Казалось бы, с него были совершены преступные деяния. Только все преступные данные хранились в «облаке», т.е. на удаленном сервере. И эта же информация может быть удалена с абсолютно другого компьютера, телефона, планшета.

В этой связи законопроектом предлагается дополнить перечень оперативно-розыскных мероприятий новым ОРМ — «Исследование компьютерной информации». Сейчас, как мы уже упоминали, в этом перечне есть ОРМ «Получение компьютерной информации».

В МВД объясняют, что это даст возможность «оперативно исследовать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, в том числе с привлечением квалифицированных специалистов, на предмет установления следов преступления, совершенного с использованием информационных технологий, и их закрепления в качестве вещественных доказательств по уголовным делам» [9]. Пока что подробностей по данному законопроекту нет, а следовательно, познать его сущность можно будет несколько позднее. Можно лишь догадываться, что такого рода ОРМ позволит более эффективно бороться с компьютерными преступлениями. Полагаем, что введение подобного ОРМ будет целесообразным при возможности его проведения сотрудником не только оперативно-технического подразделения, как того требует уже существующее ОРМ «Получение компьютерной информации». Это позволит признать законным изучение оперативником содержания носителя информации, такого как смартфон или USB-накопитель, что, как отмечают некоторые авторы, сегодня вряд ли допустимо [3, с. 40].

Кроме всего прочего, как верно отмечают Г.Ю. Маклаков и Э.В. Рыжков, оперативно-розыскная деятельность в области высоких технологий в настоящее время должна базироваться на дополнительных специальных принципах:

- стратегия и тактика ОРД в области информационных технологий должны строится на основе самого широкого использования современных достижений в области данных технологий;
- на этапе разработки стратегии и тактики ОРД в области высоких технологий гласно и негласно должны привлекаться высококвалифицированные специалисты по информационным технологиям;
- необходимо существенно пересмотреть качественный состав субъектов при установлении конфиденциального сотрудничества (при осуществлении агентурной работы);
- арсенал оперативной техники необходимо пополнить современными техническими приборами и устройствами (в том числе компьютерными про-

граммами), разработанными и успешно применяемыми в информационно-технологической сфере народно-хозяйственного комплекса;

- личному составу специализированных оперативных подразделений необходимо пройти соответствующую подготовку (переподготовку) по применению такой техники [6].

Таким образом, организационно-правовая база отечественных оперативных подразделений на сегодняшний день в рамках борьбы с компьютерной преступностью не достигла совершенства. Имеется ряд вопросов, снятие которых позволит поставить под сомнение слабую эффективность оперативно-розыскных органов в передовой борьбе с компьютерными преступниками. Государством принимаются меры, которые в отдаленной перспективе позволят улучшить показатели противодействия преступлениям в области высоких технологий. Однако здесь и сейчас оперативно-розыскной инструментарий оставляет желать лучшего, поскольку не успевает за развитием преступного сектора.

**Список литературы**

1. Об оперативно-розыскной деятельности: Федеральный закон Российской Федерации от 12 авг. 1995 г. № 144-ФЗ: ред. от 02.08.2019 № 311-ФЗ // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.

2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства Российской Федерации. 2001. № 52. Ст. 4921.

3. Бакланов Л.А. Получение компьютерной информации в оперативно-розыскной деятельности // Научный вестник Омской академии МВД России. 2020. № 1 (76). С. 37-42.

4. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / А.В. Аносов и др. М.: Академия управления МВД России, 2019. Ч. 1.

2. Корнаухова Н.Г., Катков С.В. Получение компьютерной информации: проблемы теории и практики // Вестник Восточно-Сибирского института МВД России. 2020. № 1 (92). С. 182-191.

3. Маклаков Г.Ю., Рыжков Э.В. Особенности оперативно розыскной деятельности при расследовании преступлений в сфере высоких технологий. [Электронный ресурс]. URL: https://www.crime-research.ru/library/Rigkov0104.html

4. Каждое четвертое преступление в России происходит в сфере IT-технологий. [Электронный ресурс]. URL: https://pulse19.ru/74007-kazhdoe-chetvertoe-prestuplenie-v-rossii-proishodit-v-sfere-it-tehnologij/ (дата обращения: 29.05.2021).

5. Киберпреступность и киберконфликты: Россия. [Электронный ресурс]. URL: https://www.tadviser.ru/index.php (дата обращения: 29.05.2021).

6. МВД из-за киберпреступников правит закон об оперативно-разыскной деятельности. [Электронный ресурс]. URL: https://legal.report/mvd-iz-za-kiberprestupnikov-pravit-zakon-ob-operativno-razysknoj-deyatelnosti/ (дата обращения: 29.05.2021).

***В.А. Попов,*** *к.ю.н., старший преподаватель кафедры Рязанского филиала Московского университета МВД России имени В.Я. Кикотя, г. Рязань*
***Д.В. Бондарев,*** *преподаватель кафедры Рязанского филиала Московского университета МВД России имени В.Я. Кикотя, г. Рязань*

## ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В ДОКАЗЫВАНИИ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Современный период общественного развития характеризуется переходом к обществу нового типа, основанному на знаниях и информатизации. В связи с этим компьютерные технологии все активнее проникают в жизнь человека,

обеспечивая распространение информационных потоков в обществе и образуя глобальное информационное пространство.

В России, по данным Минкомсвязи РФ, по состоянию на август 2020 г. Интернетом регулярно пользуются около 100 миллионов человек из 145 миллионов жителей и граждан Российской Федерации [1].

В связи с процессом компьютеризации общества возник новый вид преступлений, ранее не известный отечественной юридической науке и практике. Он связан с использованием средств электронно-вычислительной техники в преступной деятельности.

Выделяют две большие группы компьютерных преступлений.

Во-первых, это общественно опасные деяния, предусмотренные гл. 28 УК РФ — преступления в сфере компьютерной информации.

Во-вторых, это иные преступления, совершенные при помощи компьютерных технологий, где использование подобного программного обеспечения выступает в качестве способа и отражает элемент субъективной стороны преступления. Поэтому самостоятельного состава преступления не выделяется.

В правоприменительной практике при расследовании уголовных дел в сфере информационных технологий следователь, как правило, тесно сотрудничает с органом дознания. В вопросах установления лиц, совершивших преступление в сфере информационных технологий, поиска скрывающихся от следствия преступников, обнаружения вещественных доказательств и т.д. нередко используется оперативно-розыскная деятельность, которую осуществляет орган дознания. А учитывая, что преступления, совершенные с применением цифровых технологий, часто совершаются в условиях неочевидности, то их раскрытие во многом зависит от грамотно простроенной оперативно-розыскной деятельности. Нередко именно в результате оперативно-розыскной деятельности удается установить причастных к преступлению лиц, свидетелей и очевидцев преступлений, а также разыскать орудия преступления.

Однако несмотря на объективную необходимость использования возможностей оперативно-розыскной деятельности в ходе расследования уголовных

дел, важно при этом помнить об обеспечении гарантии конституционных прав участников уголовного судопроизводства.

Доказывание при расследовании уголовных дел на основании полученных результатов оперативно-розыскной деятельности (далее — ОРД) на территории Российской Федерации осуществляется в соответствии с уголовно-процессуальным законодательством, устанавливающим запрет использования результатов указанной деятельности в процессе доказывания. Так, ст. 89 УПК РФ определяет, что «в процессе доказывания запрещается использование результатов оперативно-розыскной деятельности, если они не отвечают требованиям, предъявляемым к доказательствам настоящим Кодексом» [2].

Дискуссии относительно указанной нормы УПК РФ привели к тому, что статус таких результатов порождает еще большие споры. Так, О.В. Михайловская относит их к доказательствам по уголовным делам и предлагает закрепить их в перечне таковых, установленном ч. 2 ст. 74 УПК РФ, в виде самостоятельного объекта [3].

В свою очередь, Е.К. Антонович считает, что результаты ОРД в целях их использования в доказывании могут быть либо вещественными доказательствами (фонограмма), либо иными документами (справка) [4].

По мнению В.В. Хатуаевой и В.А. Заряева, понятие результатов ОРД, данное в ФЗ «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ, не тождественно понятию доказательства, данному в ст. 74 УПК РФ, поскольку доказательства, как совокупность формы и содержания, имеют процессуальную форму получения соответствующих сведений [5].

Из буквального толкования ст. 89 УПК РФ вытекает, что результаты оперативно-розыскной деятельности при расследовании уголовных дел могут быть «доказательством», однако только в тех случаях, когда они соответствуют требованиям, предъявляемым к доказательствам уголовно-процессуальным законодательством.

Вместе с тем в таком правотворческом подходе наблюдается ряд несоответствий.

Во-первых, в уголовно-процессуальном законе понятие результатов ОРД дается только в п. 36.1 ст. 5 УПК РФ и определяется как «сведения, полученные в соответствии с Федеральным законом об оперативно-розыскной деятельности, о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия или суда». И это несмотря на то, что правовой основой использования таких результатов является Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (ст. 11) [6].

В связи с чем понятие результатов оперативно-розыскной деятельности, указанное в уголовно-процессуальной норме, представляет собой данные, полученные в соответствии с указанным Федеральным законом, тогда как в соответствии с ч. 1 ст. 74 и ч. 1 ст. 75 УПК РФ, доказательствами являются сведения, полученные в соответствии с уголовно-процессуальным законодательством. Соответственно, требования к их получению и закреплению установлены разными законодательными актами.

Во-вторых, если результаты розыскной деятельности — это доказательства, то в соответствии с ч. 1 ст. 75 УПК РФ, они являются недопустимыми, как полученные в соответствии с нормами Федерального закона «Об оперативно-розыскной деятельности», а значит, не в соответствии с требованиями уголовно-процессуального законодательства. Таким образом, в соответствии со ст. 89 УПК РФ результаты оперативно-розыскной деятельности не могут быть использованы в доказывании.

Между тем на практике результаты ОРД повсеместно используются как доказательства по уголовным делам. А в отдельных случаях доказательственная база строится исключительно на результатах оперативно-розыскной деятельности.

Вместе с тем требования, установленные Федеральным законом «Об оперативно-розыскной деятельности» для розыскных мероприятий и уголовно-правового законодательства для следственных и судебных действий, различны.

В связи с чем проведение соответствующих оперативных мероприятий признаваться нарушением производства процессуальных действий не может.

В-третьих, согласно ч. 2 ст. 74 УПК РФ, в качестве доказательств допускаются «показания подозреваемого, обвиняемого; показания потерпевшего, свидетеля; заключение и показания эксперта; заключение и показание специалиста; вещественные доказательства; протоколы следственных и судебных действий; иные документы», а результаты ОРД в данном перечне отсутствуют.

Единственное, к чему можно отнести результаты ОРД, это к иным документам, так как в соответствии со ст. 12 и ст. 21 ФЗ «Об оперативно-розыскной деятельности» полученные результаты отражаются в оперативно-служебной документации. Любое проведенное оперативно-розыскное мероприятие в последующем фиксируется в справке, акте, отчете, рапорте и других документах. В противном случае оно вообще не будет иметь смысла.

Если законодатель в соответствии со ст. 89 УПК РФ относит результаты ОРД к доказательствам, то в п. 36.1 ст. 5 УПК РФ их следует именовать не сведениями, а документами, содержащими такие сведения. Тем более что указанные законодателем в ч. 2 ст. 74 УПК РФ допустимые доказательства имеют исключительно документальную форму, поскольку закрепляются в процессуальном порядке.

Только такое понимание результатов данной деятельности возможно для целей УПК РФ, то есть для применения в доказывании при расследовании уголовных дел, в том числе в сфере информационных технологий.

Проанализировав нормативные правовые акты, следственно-судебную практику и научные работы по рассматриваемому вопросу, можно сказать, что результаты оперативно-розыскной деятельности часто используются в доказывании при расследовании уголовных дел разной категории, однако их статус, закрепленный в уголовно-процессуальном законодательстве, неоднозначен. В связи с чем на практике доказательственной базой часто служат результаты ОРД, доказательства признаются недопустимыми, уголовные дела прекращаются, а у осужденных, ведущих антиобщественный и зачастую даже преступ-

ный образ жизни, возникает право на реабилитацию, и такие лица впоследствии продолжают заниматься противоправной преступной деятельностью.

Поэтому учитывая, что количество преступлений, совершенных с использованием цифровых технологий, с каждым годом возрастает, а в их раскрытии важное место занимают результаты оперативно-розыскной деятельности, важно все розыскные мероприятия проводить и документально оформлять в полном соответствии с законодательством, поскольку только в этом случае они могут служить доказательством по уголовному делу.

## Список литературы


1. Газета.ru: В Минкомсвязи назвали число пользователей интернета в России [Электронный ресурс]. URL: https://www.gazeta.ru/tech/news/2020/08/30/n_14866939.shtml (дата обращения: 12.05.2021).
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (с изм. с 07.03.2021) // Собрание законодательства РФ. 2001. № 52 (ч. I). Ст. 4921.
3. Михайловская О.В. Результаты оперативно-розыскной деятельности в доказывании по уголовным делам // Российская юстиция. 2019. № 1. С. 45-46.
4. Антонович Е.К. Использование в доказывании результатов прослушивания телефонных переговоров в условиях развития информационных технологий (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств) // Lex russica. 2019. № 7. С. 160-171.
5. Хатуаева В.В., Заряев В.А. Доктринальные проблемы использования результатов оперативно-розыскной деятельности в доказывании по уголовным делам // Современное право. 2017. № 9. С. 113-117.
6. Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 30.12.2020) «Об оперативно-розыскной деятельности» // Собрание законодательства РФ. 1995. № 33. Ст. 3349.

***П.С. Порываева,*** *эксперт-стажер отделения № 6 ЭКО УМВД России по г. Волгограду, г. Волгоград*
***Е.В. Прокофьева,*** *канд. физ.-мат. наук Волгоградской академии МВД России, доцент кафедры криминалистической техники УНК ЭКД, г. Волгоград*
***Р.А. Мерзликин,*** *начальник кафедры огневой подготовки Волгоградской академии МВД России, г. Волгоград*

# АНАЛИЗ МЕТОДОВ И СРЕДСТВ ВЫЯВЛЕНИЯ СЛЕДОВ ПАЛЬЦЕВ РУК НА РАЗЛИЧНЫХ ПОВЕРХНОСТЯХ ПРИ ОСМОТРЕ МЕСТА ПРОИСШЕСТВИЯ

Следы пальцев рук встречаются на месте происшествия чаще других следов. Эти следы имеют большое криминалистическое значение, так как информация, имеющаяся в следах, неотделима от человека и позволяет идентифицировать конкретное лицо [1].

Анализ традиционных и новых возможных методов и средств выявления следов пальцев рук открывает огромные перспективы в области криминалистики, именно на это направлено наше исследование [2].

На сегодняшний день выделяют следующие основные методы обнаружения и выявления следов рук: визуальный, физический, химический и физико-химический.

Наиболее часто при осмотре места происшествия при первичном осмотре применяется визуальный метод, а на следующей стадии осмотра — физический метод выявления следов пальцев рук. Причем качество выявляемых следов напрямую зависит как от свойств обрабатываемой дактилоскопическими порошками поверхности, так и от свойств самого порошка.

В процессе обработки поверхности дактилоскопическими порошками (физическим методом), частицы порошковидных материалов налипают на поверхность папиллярных валиков — это вызвано действием адгезионных сил. Интенсивность прилипания частиц, как непосредственно к потожировому веществу,

которым образован след, так и к твердым поверхностям, на которых следы оставлены, можно оценивать по силе прилипания, или по числу адгезии (отношению числа оставшихся на поверхности частиц к начальному их числу при данной силе отрыва). В этой связи целесообразно отметить уровни дисперсности порошков: мелкодисперсные (0,1-0,5 мкм); низкодисперсные (0,5-100 мкм); крупнодисперсные (от 100 мкм). Структура порошков напрямую влияет на возможность и качество выявления следов пальцев рук, что во многом зависит от характера и подготовки поверхности, на которой будет проводиться поиск возможных следов рук [3]. Прежде всего, определяется вид поверхности (бумага, металл, дерево, кожа, искусственная кожа и т.п.) и ее состояние (гладкая или шероховатая (грубая)), на которой будет осуществляться выявление следов физическим методом.

Для выявления «качественного» с криминалистической точки зрения следа необходимо соблюдать некоторые правила, важным из которых является наличие сухого, равномерно истолченного порошка, контрастирующего с поверхностью (где находится след), обладающего хорошей адгезией и не окрашивающего поверхности, на которой расположены следы. Для работы применяются дактилоскопические порошки, разные по магнетизму, магнитные и немагнитные, принципиально отличающиеся по дисперсности и, как следствие, по адгезионным свойствам и качеству выявляемого следа.

При работе с дактилоскопическими порошками на месте происшествия часто возникают вопросы выбора того или иного порошка. Затруднительно подобрать дактилоскопический порошок для обработки поверхности дерева, металла, изделий из кожи и его заменителей. На таких поверхностях довольно сложно выявить следы. У бумаги впитывающая способность и гигроскопичность довольно высокие, у металла, напротив, отсутствуют эти свойства, дерево изменяет свою гигроскопичность и способность впитывания он обработки материала древесины.

В рамках нашего исследования эксперимента были выявлены и изъяты следы пальцев рук на: полированном дереве, бумаге и гладком металле.

Для решения поставленной задачи были выбраны дактилоскопические немагнитные и магнитные порошки. Следы изымались на дактилоскопическую пленку на желатиновой основе и на липкую ленту-скотч. Результаты эксперимента представлены в сводной таблице (см. табл.) и на рисунках 1-3 [3, 4].

Оценка качества выявленных и изъятых следов

| Комбинация дакт. кисти и порошка | Полированное дерево | Бумага | Гладкий металл (неферромагнитный) |
|---|---|---|---|
| Магнитная кисть и магнитный порошок | + | + | + |
| Немагнитная кисть и магнитный порошок | – | + | + |
| Немагнитная кисть и немагнитный порошок | + | + | + |

Результаты эксперимента:

«+» — след хорошего/удовлетворительного качества и пригоден для идентификации личности;

«-» — след выявить не удалость, или выявленный след непригоден для идентификации личности.

Исходя из табличных данных, можно сделать вывод о том, что выбранные нами комбинации кисть/порошок почти на всех исследуемых поверхностях дали хороший результат, следы пальцев рук получились пригодными для идентификации личности. Однако для полированного дерева комбинация — немагнитная кисть и магнитный порошок не позволила выявить пригодные для идентификации следы.

а б в

Рис. 1. След пальца руки, выявленный на полированной деревянной поверхности: а — магнитная кисть и магнитный порошок; б — немагнитная кисть и магнитный порошок; в — немагнитная кисть и немагнитный порошок

а б в

Рис. 2. След пальца руки, выявленный на бумаге: а — магнитная кисть и магнитный порошок; б — немагнитная кисть и магнитный порошок; в — немагнитная кисть и немагнитный порошок

а б в

Рис. 3. След пальца руки, выявленный на гладком металле (неферромагнитном): а — магнитная кисть и магнитный порошок; б — немагнитная кисть и магнитный порошок; в — немагнитная кисть и немагнитный порошок

На основании проведенных исследований можно вывести ряд закономерностей:

1. В зависимости от пористости поверхности следует подбирать дисперсность порошка. Светлый дактилоскопический порошок следует выбирать при работе на гладких и темных поверхностях и, наоборот, темный дактилоскопический порошок следует выбирать при работе на светлых гладких поверхностях.

2. Для работы на неферромагнитных металлических поверхностях можно применять магнитную кисть и магнитный порошок и, наоборот, на ферромагнитных поверхностях — нельзя.

3. Дактилоскопический порошок должен быть надлежащего качества: непросроченный, не влажный, без комков и т.д.

4. При выборе пленки для изъятия следов стоит учитывать пористость и шероховатость поверхности, с которой изымается след, с гладких поверхностей следует изымать на желатиновую дактилоскопическую пленку. Если поверхность шероховатая, пористая, то следует применить липкую ленту-скотч.

**Список литературы**

1. Криминалистика для судебных экспертов: учебник / А.А. Курин и др.; под общ. ред. А.А. Курина. Волгоград: Волгоградская акад. МВД России, 2014. 550 с.

2. Возможности модернизации традиционных средств выявления следов пальцев рук // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXII междунар. науч.-практ. конф. (4-5 апреля 2019 г.) / отв. ред. Н.Н. Цуканов. Красноярск: СибЮИ МВД России, 2019. С. 121-122.

3. Адгезионные свойства порошков [Электронный ресурс]. URL: https://msd.com.ua/granulirovanie-materialov/adgezionnye-svojstva-poroshkov/ (дата обращения: 02.04.2021).

***А.В. Пуричи,*** *магистрант кафедры уголовного процесса и криминалистики Алтайского государственного университета, г. Барнаул*

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

## ОСОБЕННОСТИ ВЛИЯНИЯ АМОРАЛЬНОГО И ПРОВОЦИРУЮЩЕГО ПОВЕДЕНИЯ НА НАЗНАЧЕНИЕ НАКАЗАНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

В современный период времени обозначилась неизбежность цифровой трансформации правоприменительной практики в связи с начавшейся пандемией COVID-19. Так же как и для большинства государств, для России стал актуальным вопрос осуществления онлайн-правосудия и определения рамок его использования. Президиум Верховного Суда Российской Федерации и Президиум Совета Судей Российской Федерации совместными постановлениями определили временный порядок функционирования судов [1]. Суды стали более активно принимать документы через электронные интернет-приемные, рассмат-

ривать преимущественно безотлагательные дела, чаще использовать системы видеоконференц-связи [2].

По мнению Л.В. Головко, цифровизация в уголовном процессе — это лишь локальная и достаточно рутинная оптимизация некоторых процессуальных форм и институтов, не несущая в себе никаких рисков для традиционного правосудия по уголовным делам [3, с. 19].

В условиях цифровизации правосудия остается проблема определения единого подхода к решению вопроса о признании смягчающими обстоятельствами тех из них, которые прямо не предусмотрены ч. 1 ст. 61 УК РФ и тех, которые хотя прямо предусмотрены ч. 1 ст. 61 УК РФ, однако содержат в себе оценочные признаки.

К таким обстоятельствам относится, в частности, предусмотренное п. «з» ч. 1 ст. 61 УК РФ аморальность поведения потерпевшего, явившегося поводом для преступления. Относительно данного смягчающего обстоятельства Верховный Суд Российской Федерации не дает конкретных разъяснений, а Конституционный Суд Российской Федерации лишь указывает на отсутствие неопределенности в этой уголовно-правовой норме при ее, однако, соответствии Конституции Российской Федерации [4].

Аморальное поведение потерпевшего состоит в нарушении им моральных норм и правил поведения в обществе, что провоцирует совершение преступления [5, с. 336].

Аморальность поведения потерпевшего не требует какой-либо преюдиции и может быть признана смягчающим наказание обстоятельством в случае, если суд придет к выводу о несоответствии нормам морали действий потерпевшего и установит причинную связь между таким поведением потерпевшего и совершенным в отношении его преступным посягательством [6, с. 52].

Так, в п. 18 Постановления Пленума Верховного Суда «О судебном приговоре» указано: если суд установил обстоятельства преступления, которые не были отражены в предъявленном подсудимому обвинении, но признаны судом смягчающими наказание (например, аморальность поведения потерпевшего,

явившиеся поводом для преступления), эти обстоятельства также должны быть приведены при описании деяния подсудимого [7].

Установление аморальности поведения потерпевшего требует его оценки с позиции общепринятых в обществе моральных, нравственных и этических правил, представлений о таких категориях, как справедливость, честь, добро и зло и т.п. Мораль не является правовой категорией. Поэтому аморальность поведения означает нарушение правил поведения, принятых обществом, но не закрепленных нормативно. Аморальность поведения влечет за собой физические или нравственные страдания потерпевшего, причиняемые действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие потерпевшему другие нематериальные блага [8, с. 52].

В теории к проявлениям аморального поведения относят обман, предательство, растрату вверенных на сохранение денег, супружескую измену и другое. Однако степень выраженности такого аморального поведения должна обладать достаточным цинизмом и дерзостью, чтобы спровоцировать сильное душевное волнение виновного и вызвать у него решимость совершить преступление [9, с. 67].

Однако некоторые авторы, в том числе Сергей Владимирович Тасаков, считают, что аморальный проступок потерпевшего не может послужить основанием для совершения преступления и в связи с этим смягчения наказания. Другое дело, если аморальные действия потерпевшего вызвали у лица аффект, который и является смягчающим обстоятельством [10, с. 22].

Кроме того, нередко оценить действия людей как аморальные бывает достаточно сложно. Оценка действий людей и явлений с точки зрения добра и зла выражает ее нравственную оценку. Но практика показывает, что абсолютного добра для всех не существует. Границы между добром и злом являются подвижными, и то, что при одних условиях является добром, нередко в других случаях становится злом.

Так, по одному из уголовных дел суд не признал поведение потерпевшей аморальным и, соответственно, не учел его как обстоятельство, смягчающее наказание. Как установлено приговором Алтайского краевого суда, подсуди-

мый был ранее знаком с потерпевшей, общался с ней, самовольно проник к ней в дом и уже потом осуществил свои преступные действия. Его утверждения на предварительном следствии о том, что во время произошедшего потерпевшая ругалась на него, требовала, чтобы он ушел из ее дома, выталкивала его из своего дома, нельзя расценивать как аморальное поведение с ее стороны [11].

Судебная практика, в том числе Алтайского края, выработала понятие определения аморального поведения потерпевшего. Аморальность поведения, по мнению суда, — это несоответствие поведения потерпевшего нормам морали, правилам поведения в обществе [12].

Однако есть и иные подходы. Так, в Постановлении Алтайского краевого суда указано, что поводом для совершения осужденным преступления явилось аморальное поведение потерпевшего, выразившееся в том, что последний, находясь в гостях в доме осужденного, вступил в интимную близость с его гражданской женой Б., что и увидел Б.

Суд в приговоре признал показания Б. последовательными, согласующимися между собой и с другими доказательствами, использовал их в качестве доказательств. Напротив, к показаниям свидетеля Б., отрицавшей указанное осужденным обстоятельство, суд отнесся критически. Вместе с тем данное обстоятельство, предусмотренное п. «з» ч. 1 ст. 61 УК РФ, в качестве смягчающего судом не признано, и в приговоре отсутствуют какие-либо мотивы непризнания данного обстоятельства смягчающим.

При таких обстоятельствах президиум признал смягчающим наказание осужденного обстоятельством аморальность поведения потерпевшего, явившегося поводом для преступления, предусмотренное п. «з» ч.1 ст. 61 УК РФ, смягчил наказание [13].

Интересным представляется дело, рассмотренное Индустриальным судом г. Барнаула. Обстоятельствами, смягчающими наказание Н., суд признал и при назначении наказания учел аморальное поведение потерпевшего до произошедшего конфликта, выразившееся в его вызывающем поведении в общественном месте, приставании к людям, а также в оскорблении окружающих, среди

которых находился и подсудимый, грубой нецензурной бранью, что явилось поводом для совершения преступления [14].

Еще одним примером проявления аморального поведения потерпевшего Железнодорожный районный суд г. Барнаула признал и учел поведение Д., который некорректно вел себя в отношении гражданской супруги подсудимого, что вызвало негативные эмоции последнего и стало мотивом совершения преступления [15].

Итак, из вышеизложенных судебных решений можно сделать вывод, что в судебной практике Алтайского края, в частности г. Барнаула, в качестве аморального поведения, как обстоятельства, смягчающего наказание выступают вызывающее поведение в общественном месте, приставание к людям, оскорбление окружающих, некорректное поведение в отношении супругов, ревность [16], неоднократное оскорбление нецензурной бранью, угроза применения насилия [17].

Во многих случаях совершения преступлений значительная роль принадлежит потерпевшему, когда преступление представляется как результат взаимодействия преступника с потерпевшим от преступления.

Однако стоит отметить, что аморальное поведение на практике путают с провоцирующим поведением. Поэтому охарактеризуем провоцирующее поведение как повод для совершения преступления и сравним с аморальным поведением.

Виктимологические составляющие позволяют обратить внимание на провоцирующее поведение потерпевшего, когда в силу определенных его личных качеств он создает повод к совершению преступления. Именно из-за собственных личных качеств потерпевший становится жертвой преступления. Данное обстоятельство позволяет ученым выделять «провокацию преступления в уголовно-правовом смысле» и «провокацию преступления в криминологическом смысле». Однако это тема другого научного исследования.

Провоцирующее поведение в криминологическом аспекте рассматривается как обстоятельство, порождающее причины и условия совершения преступления, но не в качестве смягчающего наказание обстоятельства [18, с. 27]. Это подтверждается судебной практикой. Так, в Алтайском краевом суде осужден-

ный Т. указал, что потерпевший хранил свое имущество на видном месте (в кабине автомобиля), при этом дверь не была заперта, чем спровоцировал совершение преступления. Он просил признать указанное обстоятельство в качестве смягчающего [19]. Однако суд не нашел оснований для отнесения к обстоятельствам, смягчающим наказание, нахождение сумки потерпевшего в кабине автомобиля на видном месте, поэтому не расценил как провоцирующее поведение, способствовавшее совершению преступления.

Провоцирующее поведение потерпевших создает напряженную обстановку, подталкивающую виновного к совершению преступления в отношении потерпевшего. И в подобных случаях поведение потерпевших всегда находится в причинной связи с совершенным преступлением. Такое поведение характеризуется аморальными поступками потерпевшего, совершением им противоправных действий (например, применение насилия в отношении потерпевшего, нанесение ему тяжкого оскорбления, влекущего за собой совершение дисциплинарного проступка, гражданского правонарушения, самоуправные действия, вымогательство денег, иного имущества и других действий) [20, с. 381].

Стоит отметить, что при анализе судебной практики Алтайского края был найден только один случай, когда суд признал провоцирующее поведение потерпевшего в качестве смягчающего наказание.

Так, приговором Бийского районного суда установлено, что потерпевшая, разбив остекление в окне веранды дома, проникла в жилище и прошла в коридор, где ее встретил Ш. При этом потерпевшей было достоверно известно, что подсудимый в тот момент находился в состоянии алкогольного опьянения, и испытывал к ней личные неприязненные отношения из-за произошедшей накануне между ними ссоры, а также то, что способен применить к ней физическое насилие, так как ранее подобный факт уже имел место.

В этой связи суд признал, что в рассматриваемой ситуации потерпевшая допустила виктимное поведение.

Исходя из установленных по делу обстоятельств, свидетельствующих о совершении Ш. преступления в ответ на провоцирующее поведение потер-

певшей, суд учел дополнительно в качестве обстоятельства, смягчающего наказание подсудимого — провоцирующее поведение потерпевшей [21].

Таким образом, по нашему мнению, можно сделать вывод, что аморальность это и есть провоцирующее поведение, однако не всякое провоцирующее поведение может рассматриваться как аморальное. Аморальное поведение является общим по отношению к понятию «провоцирующее поведение». Влияние аморального и провоцирующего поведения на назначение наказания выражается в следующем.

Аморальное поведение, как смягчающее наказание обстоятельство, закрепленное легально в УК РФ, достаточно часто учитывается судами Алтайского края как такое обстоятельство. Если суд придет к выводу о том, что присутствовала аморальность поведения со стороны потерпевшего, соответственно, наказание будет смягчено.

Провоцирующее поведение потерпевшего в некоторых случаях влияет на квалификацию содеянного [22, с. 157]. Разнообразие провоцирующего поведения потерпевшего, выступающее в качестве повода совершения преступления, требует детального исследования, поскольку от этого напрямую зависит назначение справедливого наказания. Провоцирующее поведение может быть отнесено к смягчающим наказание обстоятельствам согласно ч. 2 ст. 61 УК РФ, как обстоятельства, не предусмотренные ч. 1 ст. 61 УК РФ. Но в судебной практике Алтайского края, в частности города Барнаула, встречается крайне редко, поскольку суды приходят к выводу о наличии именно аморального, нежели провоцирующего поведения потерпевшего.

## Список литературы

1. Постановление Президиума Верховного Суда Российской Федерации и Президиума Совета судей Российской Федерации от 18 марта 2020 г. [Электронный ресурс]. URL: http://supcourt.ru/files/28814/ (дата обращения 27.04.2021).

2. Постановление Президиума Верховного Суда Российской Федерации и Президиума Совета судей Российской Федерации от 8 апреля 2020 г. (с изм.

от 29 апреля 2020 г.) [Электронный ресурс]. URL: http://www.supcourt.ru/files/28873/ (дата обращения 28.04.2021).

3. Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15-25.

4. Определение Конституционного Суда РФ от 29 сентября 2015 г. № 1974-О «Об отказе в принятии к рассмотрению жалобы гражданина Ярушина Виктора Вениаминовича на нарушение его конституционных прав пунктом «з» части первой статьи 61 Уголовного кодекса Российской Федерации и частью первой статьи 401.15 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс» (дата обращения: 16.05.2021).

5. Уголовное право Российской Федерации: Общая часть: учебник для вузов / под ред. В.С. Комиссарова, Н.Е. Крыловой, И.М. Тяжковой. 2012. 466 с. // СПС «КонсультантПлюс» (дата обращения: 18.05.2021).

6. Жуков Г.К. Актуальные проблемы судебной практики назначения уголовного наказания // Уголовное право. 2017. № 5. С. 50-56.

7. Постановление Пленума Верховного Суда РФ от 29 ноября 2016 г. № 55 «О судебном приговоре» // СПС «КонсультантПлюс» (дата обращения: 17.05.2021).

8. Панова С.В., Байер С.С. Противоправное поведение потерпевшего — аффект для виновного или факт для суда? // Законность. 2015. № 11. С. 51-54.

9. Комментарий к Уголовному кодексу Российской Федерации (постатейный). 2-е изд. / под ред. А.В. Бриллиантова. М.: Проспект, 2015. 792 с.

10. Тасаков С.В., Тасаков В.С. Нравственные основы некоторых обстоятельств, смягчающих наказание по уголовному законодательству России // Российская юстиция. 2016. № 7. С. 22-23.

11. Приговор Алтайского краевого суда от 27 февраля 2019 г. по делу № 2-31/2018. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/fS6EaGIWdUJu/ (дата обращения: 08.05.2021).

12. Апелляционное постановление Завьяловского районного суда от 30 января 2019 г. по делу № 10-1/2019. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/gbfwnI8g5CUc/ (дата обращения: 09.05.2021).

13. Постановление Алтайского краевого суда от 22 января 2019 г. № 44У-1/2019. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/bqvqYowChcgW/ (дата обращения: 10.05.2021).

14. Приговор Индустриального районного суда г. Барнаула от 18 января 2019 г. по делу № 1-13/2019. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/mdrWhzbrrA6g/ (дата обращения: 10.05.2021).

15. Приговор Железнодорожного районного суда г. Барнаула от 19 октября 2018 г. по делу № 1-225/2018. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/5n65y78BKC5T/ (дата обращения: 11.10.2019).

16. Приговор Индустриального районного суда г. Барнаула от 25 мая 2018 г. по делу № 1-212/2018. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/T1GZUTJMeoY1/ (дата обращения: 09.05.2021).

17. Приговор Центрального районного суда г. Барнаула от 29 марта 2017 г. по делу № 1-65/2017. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/KOTc9GgnF4Nu/ (дата обращения: 10.05.2021).

18. Говорухина Е.В. Понятие и правовые последствия провокации в уголовном праве: дис. ... канд. юрид. наук: 12.00.08. Ростов-на-Дону, 2002. 176 с.

19. Апелляционное постановление Алтайского краевого суда от 9 февраля 2018 г. по делу № 22-527/2018. [Электронный ресурс]. URL: //sudact.ru/regular/doc/G8KhRkJdPEJQ/ (дата обращения: 27.04.2021).

20. Семенова Д.А. Провоцирующее поведение потерпевшего как повод совершения преступления // Молодой ученый. 2015. №18. С. 381-382. [Электронный ресурс]. URL: https://moluch.ru/archive/98/21973/ (дата обращения: 20.10.2021).

21. Приговор Бийского районного суда от 26 сентября 2016 г. по делу № 1-75/2016. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/NxGxloPeeOoL/ (дата обращения: 08.10.2021).

22. Уголовное право России. Общая и Особенная части: учебник / А.А. Арямов, Т.Б. Басова, Е.В. Благов и др.; отв. ред. Ю.В. Грачева, А.И. Чучаев. М.: КОНТРАКТ, 2017. 384 с.

***И.В. Рыжков,*** *преподаватель кафедры криминалистической техники учебно-научного комплекса экспертно-криминалистической деятельности Волгоградской академии МВД России, г. Волгоград*

## ТРАНСФОРМАЦИЯ ПОДХОДОВ К ОРГАНИЗАЦИИ И ВЕДЕНИЮ НАТУРНЫХ КОЛЛЕКЦИЙ В ОТЕЧЕСТВЕННЫХ ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКИХ ПОДРАЗДЕЛЕНИЯХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

От момента создания первых отечественных экспертно-криминалистических подразделений (далее — ЭКП) органов внутренних дел по настоящее время особое внимание уделяется учетно-регистрационной деятельности, направленной на информационное обеспечение правоохранительных органов в процессе предупреждения и расследования преступлений. При организации и функционировании фондов криминалистически значимых сведений одно из центральных мест занимают натурные коллекции, поскольку свойства входящих в них элементов позволяют сохранять в первоначальном виде ценную информацию об объекте или событии. Хранение в натурной форме данных о совершенном преступлении или предмете, представляющем криминалистический интерес, обусловливает возможность их применения как при расследовании преступлений, так при осуществлении научно-исследовательской деятельности в области судебной экспертизы и обучении новых сотрудников правоохранительных органов.

Функционирование и развитие коллекционной деятельности в отечественных криминалистических подразделениях характеризуется постоянной трансформацией подходов к способу организации коллекций, качественно-количес-

твенному составу и целям их ведения, обусловленной изменением криминогенной обстановки, уровнем развития судебной экспертизы и применяемых сотрудниками правоохранительных органов технических средств.

Анализ криминалистической литературы и исторических источников позволяет определить, что до начала XX в. коллекционная деятельность, направленная на организацию фондов натурных объектов, представляющих криминалистический интерес, носила несистемный, эпизодический и инициативный характер. Первые структурированные коллекции объектов в натурной форме, связанных с событием преступления, были организованы в 1907 г. на базе Центрального справочного аппарата Регистрационного отдела Департамента полиции [1, с. 14]. С целью установления причастности лица к совершенному преступлению формировались натурные фонды, предусматривающие систематизированные коллекции огнестрельного и холодного оружия, предметов и устройств, используемых при совершении противоправных деяний. Также стоит отметить факт существования в Регистрационном отделе коллекций образцов почерка преступников склонных к совершению мошенничеств.

Несмотря на цель ведения данных натурных фондов, заключающуюся в информационном обеспечении деятельности правоохранительных органов по установлению лица, совершившего противоправное деяние, указанные коллекции по причине отсутствия системного подхода при их формировании еще нельзя отождествить с современными коллекциями, сопровождающими экспертно-криминалистические учеты.

Дальнейшее развитие натурных фондов объектов, связанных с совершенными преступлениями, привело к организации при Департаменте полиции музея уголовного сыска и научной техники расследования преступлений. Однако в данном случае основная цель функционирования экспозиций заключалась в использовании экспонатов в процессе обучения полицейских чинов при подготовке к службе в сыскных подразделениях [2].

Отдельным направлением коллекционной деятельности в начале XX в. стоит выделить натурные фонды, сформированные с целью накопления эмпирического материла для развития основ судебной экспертизы. Так, отечествен-

ным ученым С.Н. Трегубовым была организована коллекция огнестрельного оружия, пуль и гильз со следами огнестрельного оружия, а также патронов, служившая необходимым элементом при написании им практического пособия для сотрудников правоохранительных органов, рассматривающего особенности исследования баллистических объектов [3, с. 40]. А профессором Е.Ф. Буринским при разработке научных основ почерковедческой экспертизы и технико-криминалистической экспертизы документов была сформирована фотографическая коллекция спорных рукописных текстов и технических подделок документов.

Необходимо указать, что деятельность по собиранию и ведению рассмотренных выше натурных фондов, организованных с целью развития научных и методических основ судебной экспертизы, осуществлялась в инициативном порядке и являлась новым направлением в отечественной криминалистике, предопределяя при этом дальнейшее развитие современных натурных коллекций справочно-информационных фондов.

Таким образом, рассматривая коллекционную деятельность в отечественных правоохранительных органах начала XX в., можно отметить, что формирование натурных фондов носило исключительно инициативный и эпизодический характер, при этом структурирование коллекций осуществлялось в основном по аналогии с системой организации музейных экспозиций. Несмотря на это дифференциация натурных фондов по целям их ведения и причинно-следственной связи их структурных элементов с событием преступления обусловила развитие криминалистической коллекционной деятельности в двух направлениях: натурные коллекции экспертно-криминалистических учетов и коллекции объектов, сопровождающих справочно-информационные фонды.

Дальнейшее осуществление деятельности по организации натурных коллекций, содержащих криминалистически значимые сведения, связано с развитием нормативного регулирования их функционирования. Причем основное внимание уделялось фондам натурных объектов, организованных с целью информационного обеспечения деятельности правоохранительных органов по

предупреждению и расследованию преступлений, а также обучению новых сотрудников.

Организация данных фондов по причине отсутствия методических рекомендаций их ведения осуществлялась по типу музейных экспозиций. В то же время дислоцирование рассматриваемых коллекций натурных объектов переместилось с музея уголовного сыска в специально созданные подразделения музейной кодификации при Научно-техническом отделе НКВД [4, с. 138]. Структурированные натурные фонды предусматривали систематически пополняемые коллекции поддельных денежных билетов, инструментов и предметов, используемых при совершении преступлений, огнестрельного оружия и наркотических веществ.

Отдельно стоит указать, что в соответствии с циркуляром Центрального административного управления НКВД РСФСР № 423 от 7 декабря 1923 г. сотрудникам подразделения музейной кодификации предписывалось в обязательном порядке направлять наиболее интересные в научном плане натурные объекты в центральный музей. Императивный характер данного предписания свидетельствует о значимости и необходимости для информационного обеспечения деятельности правоохранительных органов криминалистических коллекций объектов, изъятых с мест преступлений того времени.

Последующая трансформация коллекционной деятельности характеризуется более разветвленной и структурированной по сравнению с ранее существовавшими коллекциями системой натурных фондов, что в совокупности с развитием методических рекомендаций и научных основ судебной экспертизы способствовало значительному развитию криминалистической регистрации.

Наиболее ранними самостоятельными и систематически пополняемыми коллекциями можно считать баллистические натурные фонды. Так, вследствие значительного увеличения фактов применения при совершении преступлений огнестрельного оружия в середине 1940-х гг. в ряде субъектов СССР были организованы пулегильзотеки, а в 1949 г. была создана Центральная коллекция пуль, гильз и патронов, изъятых с мест преступлений [5, с. 24]. Необходимо отметить, что нормативными документами того времени уже предусматривался

уровневый подход к хранению натурных объектов, причем его эффективность подтверждалась ежегодным увеличением количества раскрытых преступлений на основании информации, полученной в результате проверок по Центральной пулегильзотеке. В то же время в отличие от современных пулегильзотек нормативными документами того времени регламентировалась постановка на учет гильз от патронов, стреляных из гладкоствольного огнестрельного оружия, что обусловливалось его широким распространением среди населения.

Учитывая опыт организации и ведения баллистических натурных коллекций, а также в связи со всплеском фальшивомонетничества в середине 1960-х гг. в ЭКП субъектов СССР начали активно формироваться натурные фонды, включающие поддельные денежные билеты, бланки ценных бумаг и бланки документов.

Необходимо указать, что предназначение баллистических коллекций и коллекций поддельных объектов технико-криминалистической экспертизы документов, помимо информационного обеспечения процесса предупреждения и расследования преступлений, заключалось в использовании объектов учета в качестве эмпирического материала при написании учеными-криминалистами научно-исследовательских работ теоретического и практического характера. Также стоит обратить внимание, что в начале 1970-х гг. активно начали формироваться коллекции следов орудий взлома и гипсовых слепков со следов обуви, обнаруженных на месте происшествия. Причем процесс функционирования фондов, сопровождающих учеты объектов, связанных с событием преступления, осуществлялся исключительно в соответствии с разработанными головным экспертным подразделением методическими рекомендациями.

В то же время параллельно и в дополнение к натурным коллекциям объектов, связанных причинно-следственной связью с совершенным преступлением, формировались фонды объектов, используемых в качестве информационно-справочного материала при производстве предварительных исследований, экспертиз и составлении ориентировок. Данные фонды были структурированы по видам судебных экспертиз и решаемых при их производстве задач и включали следующие виды объектов: полупары обуви, замки, фарные рассеиватели,

орудия взлома, огнестрельное оружие, патроны, мишени со следами выстрела, подлинные документы и т.д.

Вместе с тем в начале 1980-х гг. начали формироваться натурные фонды объектов специальных видов экспертиз. Данные фонды содержали наиболее встречаемые в экспертной практике объекты, которые использовались в качестве образцов для сравнения при проведении исследований. Отдельной группой данных фондов выступали эталонные образцы — вещества, соответствующие требованиям ГОСТов и ТУ.

Обратим внимание, что в рассматриваемый период пополнение натурных фондов, созданных с целью информационного обеспечения экспертов при производстве экспертиз и исследований, осуществлялось в основном силами сотрудников ЭКП при взаимодействии с предприятиями, осуществляющими производство и реализацию представляющих криминалистический интерес объектов. Причем в нормативных правовых документах того времени данный процесс регламентировался лишь отчасти.

Таким образом, подводя итог вышесказанному, отметим, что к концу 1980-х гг. в отечественных экспертно-криминалистических подразделениях сложилась полноценная система экспертно-криминалистических учетов и справочно-информационных фондов в их современном понимании. Однако несмотря на наличие действующих нормативных правовых актов, регламентирующих функционирование натурных коллекций, и методических рекомендаций по их ведению, единого ведомственного приказа, рассматривающего процессы организации и использования фондов натурных объектов, не существовало.

Современное состояние коллекционной деятельности в экспертно-криминалистических подразделениях характеризуется совершенствованием нормативных правовых основ ее осуществления. Начиная с 1990-х гг. Министерством внутренних дел Российской Федерации был издан ряд приказов, регламентирующих процесс функционирования натурных коллекций, сопровождающих экспертно-криминалистические учеты и справочно-вспомогательные фонды [6, 7, 8], что, безусловно, оказало позитивное влияние на деятельность по их организации, ведению и использованию.

Также в настоящее время наблюдается тенденция дополнения натурных фондов цифровыми информационными массивами, такими как «Металлы», «Оттиск», «Клеймо» и др. Данные базы данных существенно сокращают время поиска криминалистически значимой информации об объекте исследования. Однако полностью заменить натурные коллекции указанные информационно-поисковые системы не способны по причине невозможности использования содержащихся в них сведений об объектах в качестве материального объекта (эталонного образца) при проведении сравнительных исследований.

В целом деятельность отечественных экспертно-криминалистических подразделений по организации и ведению натурных коллекций криминалистически значимых объектов подвержена постоянной трансформации и развитию, что обусловлено изменением криминогенной обстановки, научным прогрессом, совершенствованием нормативной правовой базы и методических рекомендаций, а также задачами, стоящими перед оперативными, следственными и экспертными подразделениями органов внутренних дел.

## Список литературы

1. Корниенко Н.А. Российские и международные криминалистические учеты. СПб.: Юридический центр, 2004.

2. Во главе сыска в Москве и Империи. К 300-летию российской полиции, номер 47 (9599) от 12 декабря 2017г. // petrovka-38.com [Электронный ресурс]. URL: http://petrovka-38.com/arkhiv/item/vo-glave-syska-v-moskve-i-imperii (дата обращения: 18.05.2021).

3. Латышов И.В. Концептуальные основы судебно-баллистической диагностики: дис. ... д-ра юрид. наук. Волгоград, 2016.

4. История органов внутренних дел: учеб. пособ. / Д.В. Бойко, Е.В. Пантелеев, А.Г. Фастов. Волгоград: Волгоградская академия МВД России, 2016.

5. Морозов А.В. Использование экспертно-криминалистических учетов при расследовании преступлений прошлых лет: дисс. … канд. юрид. наук. М., 2016.

6. О формировании и ведении централизованных оперативно-справочных, розыскных, криминалистических учетов, экспертно-криминалистических коллекций и картотек ОВД РФ: приказ МВД России от 31.08.1993 года № 400.

7. Об организации использования экспертно-криминалистических учетов органов внутренних дел Российский Федерации: приказ МВД России от 10.02.2006 № 70 (ред. от 11.09.2018) // Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 18.05.2021).

8. О порядке функционирования криминалистических коллекций оружия и патронов в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: приказ МВД России от 04.02.2016 года № 53 // Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения 18.05.2021).

***В.И. Самарин,*** *к.ю.н., доцент, доцент кафедры уголовного процесса и прокурорского надзора Белорусского государственного университета, г. Минск*

## ИНСТИТУТ МЕЖДУНАРОДНОЙ ПРАВОВОЙ ПОМОЩИ ПО УГОЛОВНЫМ ДЕЛАМ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

В последние десятилетия контакты между государствами стали более тесными, упрощается процесс пересечения государственных границ, большее количество граждан посещает иностранные государства. Одновременно расширяется цифровизация общественных отношений, которая закономерно вовлекает лиц, склонных совершать преступления, породив и разнообразив преступления против компьютерной безопасности (киберпреступность), а также изменив местонахождение отдельных следов преступлений цифровой средой (например, сбыт наркотических средств). Способность совершать общественно опасные деяния из любой точки мира потребовала совершенствование инструментов международной правовой помощи по уголовным делам, так как органы уголов-

ного преследования сталкиваются с необходимостью собирать компьютерную информацию за границей либо у иностранного поставщика телекоммуникационных услуг. Кроме традиционных, стали появляться новые, обусловленные трансформацией следственной деятельности в уголовном процессе инструменты международной правовой помощи. В настоящей статье рассмотрим некоторые аспекты таких изменений.

Можно заметить, что институт международной правовой помощи по уголовным делам претерпевает изменения в последние десятилетия. Если абстрагироваться от политических аспектов, то государства принимают общую задачу по борьбе против общеуголовных преступлений. Влияние оказывает не только цифровизация, но и глобализация общественных отношений, а также проявление международно-правовой парадигмы современного уголовного процесса [1]. В результате смены парадигмы регулирование исследуемого института переместилось с преимущественно международного на уровень национальной правовой системы. В то же время такой переход происходил с сохранением архаичных форм, не всегда отвечающих требованиям времени. Так, ст. 469 Уголовно-процессуального кодекса Республики Беларусь (далее — УПК Беларуси) без каких-либо оговорок предусматривает возможность предоставления просьбы органа иностранного государства об оказании международной правовой помощи исключительно в письменной форме, заверенной подписью его должностного лица и скрепленной гербовой печатью. Аналогичная норма содержится в ст. 454 Уголовно-процессуального кодекса РФ (далее — УПК РФ). На практике в случаях, не терпящих отлагательства, документы направляются посредством электронных средств связи. Поэтому для ускорения процедуры видится целесообразным предоставить компетентным органам Республики Беларусь полномочие принимать решение на взаимной основе использовать указанные средства связи в ходе оказания международной правовой помощи. При переводе ведения уголовного дела в электронную форму отдельной задачей может быть обеспечение совместимости (аутентификации) электронных цифровых подписей для пересылки электронных документов в рамках оказания международной правовой помощи по защищенным каналам связи. Такую задачу необ-

ходимо ставить, по крайней мере, в рамках интеграционных образований (например, Евразийского экономического союза).

Еще одним аспектом является получение компьютерной информации, содержащейся на определенных носителях (жесткие диски компьютеров и серверов, USB-флеш-накопители, карты памяти и т.д.) Традиционно международными договорами и национальным законодательством (ст. 480 УПК Беларуси) допускается передача предметов, которые служили орудиями и средствами совершения преступления или сохранили на себе следы преступления, или добыты преступным путем, либо могут служить средствами по обнаружению преступления, установлению фактических обстоятельств уголовного дела, выявлению виновных либо опровержению обвинения (иными словами, впоследствии вещественных доказательств). Однако в сегодняшнем мире не только нецелесообразно, но иногда и невозможно передавать материальные носители электронной информации. Если следствие не интересует непосредственно сам носитель информации и следы на нем, то существует несколько вариантов передачи информации.

Прежде всего, допускается направление компетентному органу иностранного государства просьбы о производстве соответствующего следственного действия, связанного с осмотром информации на определенном носителе и ее копирование. Например, УПК Беларуси предусматривает возможность производства осмотра компьютерной информации по месту производства следственного действия (ст. $204^1$). В ходе осмотра компьютерной информации следователем, органом дознания могут производиться действия, предусмотренные функционалом информационных систем, информационных ресурсов, а также использоваться научно-технические средства, оборудование, аппаратура, приборы, компьютерные программы. При этом законодатель не указывает в качестве обязательного условия наличие по месту производства данного следственного действия носителя такой компьютерной информации. В необходимых случаях в просьбу об осуществлении осмотра компьютерной информации может включаться положение о разрешении присутствия представителей органа иностранного государства.

Носители компьютерной информации могут быть обнаружены при производстве иных следственных действий (осмотре места происшествия, помещения, жилища и иного законного владения, обыске, выемке, личном обыске). В этом случае при невозможности или нецелесообразности изъятия объекта, содержащего компьютерную информацию, имеющую значение для уголовного дела, может осуществляться ее копирование (фиксация) в отображаемой форме, в том числе создание образа носителя компьютерной информации (ч. $3^1$ ст. 204, ч. $13^1$ ст. 210 УПК Беларуси). В результате исполнения просьбы органа иностранного государства и производства таких следственных действий указанному органу должны быть переданы протокол, фиксирующий факт, ход и результат следственного действия, а также носитель с копией (образом) обнаруженной компьютерной информации. Данная доказательственная информация должна быть легализована в национальном уголовном процессе. Так, доказательства, полученные на территории иностранного государства по просьбе органа, ведущего уголовный процесс, на основе принципа взаимности или в соответствии с международными договорами Республики Беларусь, заверенные и переданные в установленном порядке этому органу, имеют такую же юридическую силу, как если бы они были получены на территории Республики Беларусь в соответствии с правилами УПК (ч. 3 ст. 88 УПК Беларуси — более узкий аналог нормы ст. 455 УПК РФ).

Интересные нормы для развития национального уголовно-процессуального законодательства в сфере собирания доказательственной цифровой информации содержатся в Конвенции Совета Европы о компьютерных преступлениях 2001 г. (Беларусь и РФ не являются участниками). Государства-участники должны предусмотреть в своем законодательстве возможность:

1) обеспечивать сохранность на основании постановления (приказа) *конкретных компьютерных данных*, включая данные о потоках информации, которые хранятся в компьютерной системе, в частности, когда имеются основания полагать, что эти компьютерные данные особенно подвержены риску утраты или изменения (ст. 16);

2) отдавать распоряжение (приказ) о предоставлении *конкретных компьютерных данных*, находящихся во владении или под контролем лица, которые хранятся в компьютерной системе или на том или ином носителе компьютерных данных (ст. 18);

3) отдавать распоряжение (приказ) поставщику услуг, предлагающему свои услуги на территории такого государства, — о предъявлении находящихся во владении или под контролем этого поставщика услуг *сведений о его абонентах* (ст. 18);

4) производить обыск или иной аналогичный доступ к компьютерным системам или их частям, а также хранящимся в них компьютерным данным, а также носителям компьютерных данных, на которых могут храниться искомые *компьютерные данные*, на ее территории (ч. 1 и 2 ст. 19);

5) производить выемку *компьютерных данных*, доступ к которым был получен в законном порядке, или иным аналогичным образом обеспечивать их сохранность (ч. 3 ст. 19);

6) осуществлять сбор в режиме реального времени *данных о потоках информации* (ст. 20);

7) перехватывать *данные* (ст. 21).

Как видим, часть из указанных действий носит характер следственных, а соответственно, должны предусматриваться в уголовно-процессуальном законодательстве. В то же время все эти действия могут стать предметом просьбы об оказании международной правовой помощи по уголовным делам, если они имплементированы в уголовно-процессуальное законодательство иностранного государства. Например, §100b Уголовно-процессуального кодекса ФРГ (далее — УПК ФРГ) с 2017 г. регулирует производство онлайн-обыска (*Online-Durchsuchung*), понимая под ним вмешательство технических средств в систему информационных технологий, используемую заинтересованным лицом, даже без ведома такого лица со сбором данных из нее (онлайн-поиск). §100j УПК ФРГ уполномочивает органы, ведущие уголовный процесс, запрашивать у поставщиков услуг данные, собранные в соответствии с законодательством.

Следует иметь в виду, что указанная конвенция содержит и инструменты, направленные на возможность производства указанных действий в рамках международной правовой помощи по уголовным делам:

1) просьба о неотложном обеспечении сохранности данных, которые хранятся в компьютерной системе, расположенной на территории другого государства, и в отношении которых запрашивающее государство намеревается в рамках взаимной помощи направить просьбу об обыске (аналогичных обеспечивающих доступ действиях), о выемке (аналогичном обеспечении сохранности) или разглашении этих данных (ст. 29);

2) просьба об обыске (аналогичном обеспечивающем доступ действии), выемке (аналогичное обеспечение сохранности) и раскрытии данных, хранящихся с помощью компьютерной системы, которая находится на территории запрашиваемого государства (ст. 31);

3) просьба о сборе данных о потоках информации в режиме реального времени, имеющих отношение к конкретным сообщениям на территории запрашиваемого государства с помощью компьютерной системы (ст. 33);

4) просьба о сборе или записи в режиме реального времени содержания данных конкретных сообщений, передаваемых с помощью компьютерной системы (ст. 34).

Последние нормы могут быть образцом для создания национального регулирования оказания международной правовой помощи по уголовным делам в сфере компьютерной безопасности. При этом следует учитывать также предписание ч. 1 ст. 15 Конвенции Совета Европы о компьютерных преступлениях 2001 г. и при имплементации указанных норм предусматривать процессуальные гарантии, обеспечивающие надлежащую защиту прав человека и свобод и обеспечивающие принцип соразмерности. Как вариант таких гарантий, называются судебный контроль, основания правомочности применения, ограничение сферы и сроков осуществления процедур.

В рамках Европейского союза с 2018 г. идут дискуссии о создании процедуры, упрощающей получение компьютерной информации в рамках уголовного расследования из другого государства. В определенном смысле представ-

ленные инструменты похожи на заложенные в Конвенции Совета Европы. Однако они должны вывести оказание международной правовой помощи в рамках ЕС на новый уровень. В 2018 г. со ссылкой на фундаментальную важность борьбы с терроризмом [2, p. 46] были представлены проекты регламента о Европейском приказе о предоставлении (*European Production Order*) и Европейском приказе о сохранении (*European Preservation Order*) в отношении электронных доказательств по уголовным делам и директивы, устанавливающей согласованные правила о назначении уполномоченных представителей с целью сбора доказательств в уголовном процессе в целях реализации указанного регламента. Европейский приказ на предоставление позволит судебному органу одного государства-члена запрашивать электронные доказательства непосредственно у поставщика услуг, предлагающего услуги в Европейском союзе, независимо от местонахождения данных. Европейский приказ о сохранении позволит обязать поставщика услуг сохранять конкретные данные, которые судебный орган может запросить позже. Такое законодательное предложение, основанное на дальнейшем расширении перечня взаимопризнаваемых процессуальных решений, вызывает озабоченность по поводу того, в какой степени такие приказы могут нанести ущерб свободе средств массовой информации, свободе выражения мнения и свободе информации. В литературе также отмечается, что новые приказы создадут дуальную систему с уже применяемым Европейским следственным приказом [3, p. 182]. Для новых приказов требуется больший уровень доверия, чем имеется во взаимоотношениях государств-членов Европейского союза на данном этапе (о чем свидетельствует практика Европейского Суда). Это обусловлено тем, что приказы будут обязательны для исполнения не органами, ведущими уголовный процесс, а непосредственными поставщиками услуг, то есть они без признания компетентным органом иностранного государства станут обязательными для частных лиц такого государства, не вовлеченных в уголовный процесс изначально. В связи со значительным вторжением в сферу фундаментальных прав справедливо предлагается ограничить применение Европейского ордера на предоставление определенными категориями преступлений (например, по размеру наказания) [2, p. 48].

Принимая во внимание дискуссию, ведущуюся в Европейском союзе, и допуская гармонизацию уголовно-процессуального права в рамках Евразийского экономического союза [4, с. 118], следует разработать аналогичные нормы в рамках данного интеграционного образования для обеспечения достижения целей создания общего рынка.

Таким образом, развитие информационных технологий и материального уголовного закона в сфере компьютерной безопасности закономерно требует изменения уголовно-процессуальных предписаний, направленных на регулирование международной правовой помощи по уголовным делам. На национальном уровне видится необходимым: 1) предоставление компетентным органам Республики Беларусь полномочий принимать решение на взаимной основе использовать электронные средства связи в ходе оказания международной правовой помощи; 2) создание соответствующих инструментов в рамках правовой помощи по уголовным делам (на основании просьбы органа иностранного государства предварительное сохранение компьютерной информации, осмотр и копирование компьютерной информации, собирание компьютерной информации). В рамках интеграционного образования, в котором участвуют Беларусь и Россия — Евразийского экономического союза, — следует предусмотреть возможность сохранения и запроса компьютерной информации у непосредственных поставщиков услуг в сфере информационных технологий, основываясь на опыте Европейского союза.

## Список литературы

1. Самарин В.И. Международно-правовая парадигма уголовного процесса: данность, которую не все принимают // Юридический вестник Самарского университета. 2019. Т. 5. № 4. С. 58-66.

2. Tinoco-Pastrana A. The Proposal on Electronic Evidence in the European Union // Eucrim — The European Criminal Law Associations' Forum. 2020. № 1. P. 46-50.

3. Tosza S. All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the Euro-

pean Production Order // New Journal of European Criminal Law. 2020. Vol. 11. Issue 2. P. 161-183.

4. Самарин В.И. Опыт гармонизации уголовно-процессуального законодательства в рамках наднационального права на европейском // Право.by. 2020. № 3. С. 114-120.

***В.Н. Сизова,*** *к.ю.н., ведущий научный сотрудник научно-исследовательского центра Академии управления МВД России, г. Москва*

## СОВЕРШЕНСТВОВАНИЕ ПРАВОВЫХ МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Положениями принятой в 2017 г. «Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» приоритетным направлением внутренней политики государства определено дальнейшее развитие и совершенствование информационных и коммуникационных технологий, а также формирование информационного пространства и соответствующей инфраструктуры [1].

При этом в современной юридической литературе авторами отмечается, что информационные технологии на сегодняшний день проникли практически во все сферы повседневной деятельности российского общества. Так, в частности, приводятся следующие данные: в 2020 г. в России на 100 человек приходилось 213,81 мобильных телефонов; при этом 89,32 из 100 активно пользовались услугами мобильного Интернета с учетом возросшего уровня средней скорости в сети на 42%. Это положение выводит нашу страну на равный уровень с такими странами, как Греция, Италия и др. [2, с. 5].

Нельзя не отметить, что электронные СМИ, информационно-телекоммуникационные системы, различного рода социальные сети, Интернет и мобиль-

ная связь уже стали неотъемлемой составляющей жизни практически каждого из нас. Более того, государством поддерживается и активно развивается созданная система оказания государственных и муниципальных услуг посредством электронной формы, предоставляя возможности для обращений в индивидуальном и коллективном порядке в те или иные государственные структуры.

Кроме того, на сегодняшний день продолжается интенсивная деятельность, направленная на цифровизацию многочисленных областей жизни общества при помощи использования широкого круга возможностей искусственного разума, идентификационной биометрии, организации процесса взаимодействия при работе с неограниченными объемами информации, развития облачных хранилищ информационной базы данных, организации работы банковского сектора в дистанционном формате и т.п. Дискуссионному обсуждению подвергаются и вопросы, связанные с применением блокчейн-технологий.

Вместе с тем не вызывает сомнений тот факт, что активно развивающиеся информационно-телекоммуникационные способы и методы предоставляют более широкие возможности лицам, совершающим преступные деяния, в первую очередь, в экономическом секторе, секторе общественной безопасности и т.д., что в совокупности вполне может рассматриваться в качестве определенного вызова системе правопорядка.

Характерной является следующая особенность вышеизложенных положений, заключающаяся в том, что современные возможности интернет-пространства вполне успешно позволяют реализовывать те преступные замыслы, которые прежде казались трудноосуществимыми. При этом использовать возможности информационно-телекоммуникационных технологий для совершения преступлений сегодня может и среднестатистический пользователь Сети, и высокоорганизованная профессиональная преступная группа [3, с. 37].

Следует учитывать и безграничные просторы Интернета, которые зачастую выступают своего рода цифровой платформой для совершения преступных деяний, создавая тем самым многочисленные сложности в процессе противодействия, выявления, раскрытия и расследования преступлений. В большинстве случаев уполномоченным органам и их должностным лицам приходится

прикладывать значительные усилия для установления сведений о потерпевших, данных о лицах, совершающих преступные деяния, выявления мест совершения преступлений.

Исследование экономической и социально-правовой обусловленности криминализации противоправных деяний в сфере информационно-телекоммуникационных технологий дает основание для формулирования вывода о том, что привлечение к уголовной ответственности за криминальную деятельность в данной сфере должно отвечать критериям криминализации деяний, в связи с чем важным является определение характера и степени общественной опасности совершаемых деяний, установление и анализ фактов преступных посягательств на права и законные интересы личности, общества, государства при обязательном учете целесообразности осуществляемой в этом диапазоне превентивной деятельности. Изложенное послужит эффективным средством при выработке результативных и действенных предложений, направленных на дальнейший процесс совершенствования уголовно-правовых средств противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий [4, с. 203].

Актуальность исследуемых в настоящей статье вопросов на сегодняшний день обусловливается не только и не столько стабильно высоким количеством преступлений в области использования информационно-телекоммуникационных технологий, но и активным ростом соответствующих уголовно наказуемых деяний в сферах незаконного оборота наркотиков, экономики и экстремизма.

Так, по данным ГИАЦ МВД России, за 2019 г. в Российской Федерации зарегистрировано 365 129 преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 73,2% больше по сравнению с 2018 г. В сети Интернет, согласно официальным статистическим данным, более половины преступлений совершается с использованием средств мобильной связи [5].

Согласно данным ФГКУ «ГИАЦ МВД России», в 2020 г. зарегистрировано 520,4 тыс. преступлений, совершенных с использованием ИТТ, что на 73,4%

больше, чем за аналогичный период прошлого года. Больше половины таких преступлений (52,4%) относится к категориям тяжких и особо тяжких.

Осуществляя общий анализ состояния преступности в Российской Федерации за более ранний период (с 2014 по 2017 год), можно констатировать, что число зарегистрированных преступлений данного вида увеличилось более чем в 25 раз (в 2014 г. было зарегистрировано 11 тыс. преступлений, в 2015 — 43,8 тыс., в 2016 — 65,9 тыс., в 2017 — 90,6 тыс., а с 2002 г. — почти в 50 раз (в 2002 г. — 6 тыс.) [6].

В юридической литературе отмечается, что в течение достаточно длительного периода времени осуществлялись предметные исследования данных преступлений, соответственно, увеличению подлежал и перечень уголовно-правовых норм, регламентирующих привлечение к ответственности за их совершение. Так, специалистами, занимающимися изучением исследуемой сферы, указывается, что на сегодняшний день в системе российского уголовного законодательства в девятнадцати статьях Особенной части УК РФ законодателем используется такой признак, как «с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)». Более того, в уголовно-правовой статистике учета преступлений экономической направленности отдельно классифицируются преступные деяния, которые совершены с использованием компьютерных и телекоммуникационных технологий.

Вместе с тем в процессе квалификации отдельных преступлений, совершение которых посягает на те или иные объекты уголовно-правовой охраны посредством использования информационно-телекоммуникационных технологий, возникают определенные сложности в выявлении признаков состава преступления. При этом важным обстоятельством является то, что на современном этапе развития цифровых технологий крайне важно изучать указанный вопрос более углубленно, поскольку расширение технических возможностей упрощает совершение неправомерных действий не только в сфере информации, но и в иных сферах человеческой жизнедеятельности [7, с. 22].

При этом изучение информации, полученной из территориальных органов МВД России на региональном уровне и подразделений центрального аппарата

МВД России, свидетельствует о том, что в настоящее время требуют разрешения вопросы, связанные с использованием электронной подписи и незаконно полученных персональных данных, в том числе сведений, составляющих коммерческую, налоговую или банковскую тайну.

Кроме того, правоприменители отмечают, что совершение преступлений, предусмотренных гл. 28 Уголовного кодекса Российской Федерации (далее — УК) «Преступления в сфере компьютерной информации», зачастую предопределяет достижение более масштабных общественно-опасных последствий (хищение имущества, нарушение конституционных прав граждан и др.).

Таким образом, по мнению автора, появление новых рисков и угроз при переходе на высокотехнологичный уровень взаимодействия между субъектами общественных отношений требует совершенствования правовых механизмов в сфере информационно-телекоммуникационных технологий, в том числе обеспечивающих безопасность в данной сфере.

Учитывая межотраслевой характер правоотношений в сфере использования информационно-телекоммуникационных технологий, при подготовке предложений по внесению изменений в законодательство Российской Федерации на сегодняшний день требуется научная проработка следующих вопросов.

- Какие деяния в сфере незаконного использования и оборота электронных подписей с учетом степени их общественной опасности могут быть криминализированы (в условиях наличия административной ответственности за нарушение обязанностей, предусмотренных законодательством Российской Федерации в области электронной подписи (ст. 13.33 Кодекса Российской Федерации об административных правонарушениях (далее — КоАП) и за нарушение установленных правил создания (замены) и выдачи ключа простой электронной подписи (статья 13.331 КоАП)?
- Что может выступать в качестве предмета предполагаемого уголовно наказуемого деяния (какие виды электронной подписи)?
- Какие неправомерные действия (бездействия) в области использования электронной подписи обладают более высокой общественной опасностью

и предполагают установление повышенной уголовной ответственности за их совершение?

- Оправдан ли перевод административно наказуемых деяний, связанных с нарушением законодательства в сфере электронной подписи, совершенных работниками удостоверяющих центров, в категорию преступлений?
- Какие общественные отношения выступают в качестве объекта таких предполагаемых противоправных деяний?
- Позволит ли усиление уголовной ответственности за преступления, предусмотренные гл. 28 УК, снизить уровень преступности в сфере использования информационно-телекоммуникационных технологий?
- Необходимо ли расширение уголовно-правовой превенции в сфере информационно-телекоммуникационных технологий?
- Целесообразно ли увеличение размера санкций части второй ст. 183 УК и, соответственно, отнесение закрепленных в ней преступлений к категории средней тяжести для обеспечения возможности проведения по ним оперативно-розыскных мероприятий в полном объеме?

Изложенное позволяет сделать вывод, что переход на высокотехнологичный уровень взаимодействия между субъектами общественных отношений требует совершенствования правовых механизмов противодействия преступлениям, совершенным с использованием информационно-телекоммуникационных технологий.

В этой связи с учетом сформулированных и требующих своего незамедлительного решения вопросов следует отметить:

1) необходимость криминализации уголовным законом различного рода действий в сфере незаконного использования и оборота электронных подписей, включая нарушения установленных правил создания (замены) и выдачи ключа простой электронной подписи;

2) целесообразность перевода в категорию преступлений части административно-правовых деяний, связанных с нарушением законодательства в сфере электронной подписи работниками удостоверяющих центров;

3) потребность в установлении уголовной ответственности должностных лиц за такие административные правонарушения как:

- невыполнение оператором выдачи ключа требования об установлении личности заявителя простой электронной подписи, а также выдачи ключа простой электронной подписи без получения от заявителя заявления об этом (ч. 2 ст. $13.33^1$ КоАП);

- создание (замена) или выдача ключа не уполномоченным на то лицом оператора выдачи ключа (ч. 5 ст. $13.33^1$ КоАП);

4) с целью предоставления правоприменителю возможности проведения оперативно-розыскных мероприятий в полном объеме по преступлениям, предусмотренным ч. 2 ст. 183 УК, представляется целесообразным увеличение размера санкции указанной уголовно-правовой нормы до 5 лет лишения свободы и отнесение тем самым данного преступного деяния к категории преступлений средней тяжести.

## Список литературы

1. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

2. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: в 2 ч. / А.В. Аносов и др. М.: Академия управления МВД России, 2019. Ч. 1. С. 5.

3. Майорова О.В. Доступ воспрещен: преступления против несовершеннолетних, совершаемые в цифровой среде // Сетевое издание «Академическая мысль». № 2 (11). 2020. С. 37.

4. Степанов М.В., Петрянин А.В. Социально-правовая обусловленность криминализации противоправной деятельности, сопряженной с использованием цифровых финансовых активов // Вестник Казанского юридического института МВД России. № 2 (40). 2020. С. 203.

5. Состояние преступности в России. [Электронный ресурс]. URL: https://мвд.рф/reports/item/19412450 (дата обращения 15.04.2021).

6. Краткая характеристика состояния преступности в Российской Федерации. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/23816756 (дата обращения 15.04.2021).

7. Ищук Я.Г., Пинкевич Т.В., Смольянинов Е.С. Цифровая криминология. М.: Академия управления МВД России, 2021. С. 22.

***М.А. Сильнов,*** *к.ю.н., доцент кафедры основ прокурорской деятельности Университета прокуратуры Российской Федерации, г. Москва*

## О КРИТЕРИЯХ ДОПУСТИМОСТИ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

*Информационные технологии* стремительно ворвались в нашу жизнь и активно меняют ее во всех сферах человеческой деятельности[33].

*Цифровые технологии* — частный случай информационных. Цифровыми они называются потому, что работа компьютеров основана на применении двоичного кода: есть сигнал — нет сигнала[34] [1, с. 5].

Эра цифровизации вторглась и в весьма закрытую, консервативную область государственной компетенции — сферу борьбы с преступностью. Новые способы получения криминалистической информации конкурируют с традиционными методами, насчитывающими порой более сотни лет [2, с. 5-10].

Новые технологии сегодня настолько плотно интегрированы в деятельность правоохранительных органов, что оперативно-розыскная или уголовно-

[33] Информационные технологии (ИТ, также информационно-коммуникационные технологии) — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. См.: Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

[34] *Цифровой формат* — тип сигналов и форматов данных в электронике, использующих дискретные состояния (в отличие от аналогового сигнала, использующего непрерывные изменения сигнала).

процессуальная деятельность немыслимы без персональных компьютеров, которые служат информационными банками данных, и средством аудио-, видео- и фотофиксации, помощником в изготовлении оперативно-розыскных или процессуальных документов, способом передачи-получения информации и т.д.

Поэтому в предлагаемой статье мы не будет выделять какие-то особые, основанные на оцифровке изображения и звука, способы получения доказательств, поскольку большинство из них по факту уже много лет таковыми и являются, а ограничимся характеристикой общих критериев допустимости использования при расследовании преступлений результатов оперативно-розыскных мероприятий.

В соответствии с ч. 2 ст. 11 Федерального закона «Об оперативно-розыскной деятельности в Российской Федерации» от 12.08.95г (далее — Закона об ОРД)[35] результаты оперативно-розыскной деятельности могут использоваться в доказывании в соответствии с положениями уголовно-процессуального законодательства, регламентирующими собирание, проверку и оценку доказательств.

Возможность использования таких данных в доказывании определяется прежде всего тем, не нарушены ли при их получении, при производстве розыскных мероприятий основополагающие нормы Конституции РФ о правах и свободах человека и гражданина, а также положения Закона об ОРД о задачах этой деятельности [3, с. 14].

Представляется, что условиями допустимости использования результатов оперативно-розыскных мероприятий являются:

- соответствие проведенных оперативно-розыскных мероприятий целям и задачам оперативно-розыскной деятельности (ст.1, 2 Закона об ОРД)[36];

---

[35] Об оперативно-розыскной деятельности в Российской Федерации: Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 30.12.2020).

[36] Так, Ширинский районный суд Республики Хакасия в приговоре от 28 мая 2014 года в отношении М., осужденного за совершение преступлений, предусмотренных п. «б» ч. 3 ст. 228.1 УК РФ, ч. 3 ст. 30, пп. «а», «б» ч. 3 ст. 228.1 УК РФ, оценив исследованные доказательства, пришел к выводу, что оперативно-розыскное мероприятие «проверочная закупка», проведенное 13 февраля 2013 года в отношении неустановленного лица по имени Александр в целях установления вида наркотика и проверки информации, соответствовало задачам оперативно-розыскной деятельности, указанным в ст. 2 Федерального закона «Об оперативно-розыскной деятельности». См.: Обзор судебной практики использования результатов опера-

- проведение ОРМ уполномоченным на то органом (ст. 13 Закона об ОРД);

- оперативно-розыскные мероприятия, в ходе которых была получена соответствующая информация предусмотрены Законом об ОРД. В соответствии со ст. 6 Закона об ОРД при осуществлении оперативно-розыскной деятельности проводятся следующие оперативно-розыскные мероприятия: опрос, наведение справок, сбор образцов для сравнительного исследования, проверочная закупка, исследование предметов и документов, наблюдение, отождествление личности, обследование помещений, зданий, сооружений, участков местности и транспортных средств, контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров, снятие информации с технических каналов связи, оперативное внедрение, контролируемая поставка, оперативный эксперимент, получение компьютерной информации. Приведенный перечень оперативно-розыскных мероприятий может быть изменен или дополнен только федеральным законом;

- наличие предусмотренных Законом оснований для производства ОРМ (ч. 1 ст. 7 Закона об ОРД);

- наличие дополнительных условий к производству ОРМ (ст. 8, 8.1 Закона об ОРД);

- соблюдение установленного законом порядка проведения оперативно-розыскных мероприятий[37]. В соответствии со ст. 9 Закона рассмотрение материалов об ограничении конституционных прав граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, на неприкосновенность жилища

---

тивно-розыскной деятельности, как средства доказывания в уголовном процессе Верховного Суда Республики Хакасия на второе полугодие 2015 года.

[37] Пленум Верховного Суда РФ обратил внимание судов на то, что результаты оперативно - розыскных мероприятий, связанных с ограничением конституционного права граждан на тайну переписки, телефонных переговоров, почтовых, телефонных и иных сообщений, а также с проникновением в жилище против воли проживающих в нем лиц (кроме случаев, установленных федеральным законом), могут быть использованы в качестве доказательств по делам, лишь когда они получены по разрешению суда на проведение таких мероприятий и проверены следственными органами в соответствии с уголовно-процессуальным законодательством. См.: Постановление Пленума Верховного Суда РФ от 31 октября 1995 г. № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия».

при проведении оперативно-розыскных мероприятий осуществляется судом, как правило, по месту проведения таких мероприятий или по месту нахождения органа, ходатайствующего об их проведении;

- соблюдение требований ст. 51 Конституции РФ;
- соблюдение требований Закона об ОРД о применении в ходе ОРМ надлежащих технических средств[38];
- наличие в материалах уголовного дела постановления начальника органа, осуществляющего оперативно-розыскную деятельность о представлении материалов следователю (ст. 11 Закона).

Как указал Верховный Суд РФ в постановлении от 29.11.2016 № 55 «О судебном приговоре», судам следует иметь в виду, «что использование в качестве доказательств по уголовному делу результатов оперативно-розыскных мероприятий возможно только в том случае, когда такие мероприятия проведены для решения задач, указанных в ст. 2 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», при наличии оснований и с соблюдением условий, предусмотренных ст. 7 и 8 указанного Федерального закона, а полученные сведения предоставлены органам предварительного расследования и суду в установленном порядке и закреплены путем производства соответствующих следственных или судебных действий. Например, произведенные аудио- и видеозаписи, изъятые предметы и документы должны быть осмотрены и приобщены к делу; обнаруженные вещества — подвергнуты экспертным исследованиям; лица, участвовавшие в проведении оперативно-розыскных мероприятий, — при необходимости допрошены в качестве свидетелей».

Как видим, легальных условий для оценки допустимости результатов оперативно-розыскных мероприятий на порядок больше, чем условий обеспечения законности следственных действий, что уже само по себе должно нацеливать соответствующих субъектов оперативно-розыскной и уголовно-процессуальной деятельности на тщательную проверку оснований, порядка проведения и оформления оперативно-розыскных мероприятий.

---

[38] В соответствии со ст.6 Закона об ОРД перечень видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, устанавливается правительством Российской Федерации. Подробнее см.: Постановление Правительства РФ от 01.07.1996 № 770.

Ранее мы писали о проблеме разграничения таких средств процессуального доказывания, как: «Контроль и запись переговоров» — ст. 186 УПК, «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» — ст. 186-1 УПК от схожих оперативно-розыскных мероприятий: «Просушивания телефонных переговоров» (ч. 1 п.10 ст.6 Закона об ОРД) и «снятия информации с технических каналов связи» (ч. 1 п. 11 ст. 6 Закона об ОРД) [4, с. 87-91].

Очевидно, что существует необходимость более детальной проработки в федеральном законодательстве и на уровне постановления Правительства РФ вопросов, касающихся круга должностных лиц, технических средств и порядка их использования при производстве указанных мероприятий.

Вместе с тем мы рекомендуем в рамках возбужденных уголовных дел использовать способы собирания доказательств, установленные ст. 186 и 186-1 УПК, поскольку производство соответствующим им оперативно-розыскных мероприятий хотя и не противоречит действующей редакции ст. 89 УПК РФ, но может повлечь жалобы со стороны защиты. Кроме того, добытой по делу оперативно-розыскной информации часто бывает недостаточно для установления всех обстоятельств, подлежащих доказыванию.

*Так, Аскизский районный суд Республики Хакасия, рассматривая уголовное дело в отношении Р. по ч. 3 ст. 30, п. «б» ч. 2 ст. 228.1, ч. 2 ст. 228, ч. 1 ст. 232 УК РФ, в отношении В. по ч. 2 ст. 228 УК РФ, исследовал протокол осмотра компакт-диска, содержащего материалы ОРМ «прослушивание телефонных переговоров», проведенных в отношении Р., а также прослушал в судебном заседании содержащиеся на ДВД-диске файлы, из которых усматривалось, что лица, ведущие телефонные переговоры, причастны к незаконному обороту наркотических средств. Оценив представленные доказательства с точки зрения относимости, допустимости и достоверности, путем сопоставления их с другими доказательствами, имеющимися в уголовном деле, суд пришел к правильному выводу о невозможности использования результатов оперативно-розыскного мероприятия для обоснования выводов о виновности подсудимых в инкриминируемых им деяниях. Суду не были представлены данные, на основа-*

*нии которых можно было сделать однозначный вывод о том, что телефонные переговоры велись именно Р., который, в свою очередь, не подтвердил данное обстоятельство в судебном заседании. Кроме того, в протоколе осмотра компакт-диска отсутствует указание на номера телефонов, которые прослушивались, в ходе предварительного расследования по делу лица, с которыми велись телефонные переговоры, достоверно установлены не были, а суждения свидетеля Б., высказанные им при проведении осмотра компакт-диска, о том, между кем велись переговоры, обоснованно отвергнуты судом, поскольку указанный свидетель не являлся участником данных телефонных переговоров, и его суждения носят чисто субъективный, предположительный характер*[39].

Указанными вопросами не исчерпывается круг непростых задач, связанных с оценкой допустимости результатов оперативно-розыскных мероприятий. Важно при этом понимать, что они неразрывно связаны с обеспечением законности расследования в целом.

**Список литературы**

1. Ярышев С.Н. Цифровые методы записи видеоинформации. СПб.: НИУ ИТМО, 2012. 86 с.

2. Торвальд Ю. Сто лет криминалистики. Пути развития криминалистики. М.: Прогресс, 1974. 439 с.

3. Кореневский Ю.В., Токарева М.Е. Использование результатов оперативно-розыскной деятельности в доказывании по уголовным делам. М., 1999. 144 с.

4. Сильнов М.А. Актуальные вопросы государственного регулирования применения технических средств в уголовном судопроизводстве // Проблемы правовой и технической защиты информации. 2020. Вып. № 8. С. 87-91.

[39] Обзор судебной практики использования результатов оперативно-розыскной деятельности, как средства доказывания в уголовном процессе Верховного Суда Республики Хакасия на второе полугодие 2015 года.

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

# СОБИРАНИЕ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, НАХОДЯЩЕЙСЯ НА ЦИФРОВЫХ НОСИТЕЛЯХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. I. ПРОБЛЕМЫ ЦЕЛЕПОЛАГАНИЯ

Компьютерные технологии проникли и применяются во многих сферах человеческой деятельности. Сегодня достаточно трудно представить общество, в котором не используются достижения современного технического и технологического прогрессов. Однако это повлекло за собой не только явно положительные результаты, но и негативные, к числу которых следует отнести совершение преступлений. Анализ состояния уровня преступности в России за последние годы указывает на значительный рост количества зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Так, за 2019 г. зарегистрировано 294 409 (+68,5%) таких преступлений, 2020 г. — 510 396 (+73,4%), за период с января по май 2021 г. — 226 962 (+25,7%)[40]. Приведенные данные свидетельствуют о востребованности рекомендаций относительно расследования исследуемой категории преступлений. Одним из важных аспектов такой деятельности является обнаружение, фиксация, изъятия и оформление информации, имеющей значение для уголовного дела.

Осуществление расследования преступлений предполагает деятельность по сбору доказательств путем производства следственных и иных процессуальных действий, предусмотренных Уголовно-процессуальным кодексом Российской Федерации (далее — УПК РФ). Порядок производства указанных действий урегулирован нормами УПК РФ и затруднений в их реализации, казалось бы, нет. Тем не менее остаются неразрешенными отдельные вопросы, связан-

[40] Статистика. Состояние преступности в России за январь-декабрь 2019, 2020, январь-май 2021 гг. [Электронный ресурс]. URL: https://мвд.рф/reports/1/ (дата обращения: 15.07.2021).

ные с целеполаганием[41] при производстве отдельных следственных действий, в том числе при расследовании обозначенной ранее категории преступлений.

Постановка проблем, связанных с определением целей и задач следственных действий в криминалистике не нова. Достаточно обстоятельными на сей счет выглядят результаты исследований А.С. Князькова, акцентирующего внимание на то, что «правильное понимание криминалистических целей и задач следственного действия позволяет системно представить поисково-познавательную деятельность субъектов предварительного расследования, структурировав ее посредством выделения логических и фактических действий» [1, с. 100].

Говоря о неоднозначности формулировок законодателя в вопросах целеполагания следственных действий, С.В. Пропастин обращает внимание, что «применительно к осмотру, следственному эксперименту, личному обыску, проверке показаний на месте и допросу эксперта в тексте соответствующих статей УПК РФ прямо указывается на цели следственного действия. Однако в случае с другими следственными действиями положения УПК РФ не детализируют их назначения до уровня целей, часто фиксируя лишь основания производства этих действий» [2, с. 21].

Справедливым представляется утверждение А.С. Князькова: «…для определения цели следственного действия необходимо оперировать не только нормой, непосредственно определяющей уголовно-процессуальный порядок его производства, но и нормой, закрепляющей основополагающие начала уголовного судопроизводства» [1, с. 100]. Полагаем, отсутствие единого подхода законодателя при определении целей и задач следственных действий способствует допущению ошибок в понимании соответствующих норм и сущности самих способов собирания доказательств.

В контексте предмета проводимого исследования, интересным представляется: основными задачами каких следственных действий является отыскание,

[41] Целеполагание представляет собой практическое осмысление своей деятельности человеком с точки зрения формирования (постановки) целей и их реализации (достижения) наиболее экономичными средствами. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/ Целеполагание (дата обращения: 18.07.2021).

обнаружение и фиксации информации, находящейся на цифровых носителях вычислительной техники[42]?

Анализ мнений ученых [3-12 и др.], сотрудников следственных и оперативных подразделений органов внутренних дел[43], осуществляющих деятельность по раскрытию и расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, а также судебной практики [13], показал, что наиболее эффективными с точки зрения отыскания, обнаружения и фиксации следов противоправной деятельности являются осмотр (места происшествия, предметов), обыск, назначение и производство судебно-компьютерной экспертизы.

Сегодня, несмотря на регулирующее воздействие уголовно-процессуального законодательства относительно исследуемых правоотношений, правоприменительная практика производства указанных следственных действий складывается не единообразно. Следует констатировать факт отсутствия в нормах уголовно-процессуального закона четкого ответа на поставленный нами ранее вопрос. Анализ мнений ученых позволяет сделать вывод о продолжающемся аккумулировании знаний относительно уголовно-процессуальных и криминалистических целей, задач следственных действий.

Определение целей и круга задач осмотра, обыска и судебно-компьютерной экспертизы являются предметом многих исследований. Обстоятельными в этой связи представляются мнение и аргументы С.В. Пропастина, согласно которым к целям осмотра, обыска и производства судебно-компьютерной экспертизы относятся: «1) получение и проверка доказательств (условно процессуальная цель); 2) получение сведений для выдвижения и проверки криминалистических версий (условно тактическая цель)» [2, с. 22]. К числу задач осмотра, обыска и судебной компьютерной экспертизы, ученый отнес, соответственно: 1) «обнаружение, фиксацию, изъятие, исследование и оценку материальных, в том числе электронно-цифровых, следов преступления (и получение тактической информации как результат отражения указанных следов в сознании следователя); фиксацию материальных признаков обследуемого объекта (и получе-

[42] К таковым относятся персональные компьютеры, ноутбуки, мобильные устройства и т.п.

[43] Опрошено 47 следователей территориальных подразделений Астраханской, Курганской, Омской и Томской областей.

ние тактической информации как результат отражения указанных признаков в сознании следователя)»; 2) «отыскание, обнаружении (в смысле выделения объекта, найденного в процессе обыска), фиксацию, изъятие, исследование и оценку материальных, в том числе электронно-цифровых, следов преступления (и получение тактической информации как результат отражения указанных следов в сознании следователя)»; 3) «установление тождества или его отсутствия между идентифицирующим и идентифицируемым объектом (и получение тактической информации как результат отражения итогов процесса установления данного тождества или его отсутствия в сознании следователя); диагностику представленного объекта (и получение тактической информации как результат отражения итогов процесса диагностики в сознании следователя)» [2, с. 22-23].

Таким образом, отыскание, обнаружение, фиксация, изъятие, исследование и оценка информации, находящейся на цифровых носителях вычислительной техники являются задачами, разрешаемыми в ходе осмотра (места происшествия, предметов), обыска и производства судебно-компьютерной экспертизы.

Точное понимание назначения следственных действий и задач, разрешаемых каждым из них, способствует минимизации допущения ошибок при определении способа собирания доказательств и тем самым повышению качества расследования преступления в целом.

**Список литературы**

1. Князьков А.С. Об уголовно-процессуальном и криминалистическом понимании целей и задач следственного действия // Вестн. Том. гос. ун-та. 2011. № 347. С. 100-105.

2. Пропастин С.В. Осмотр, обыск или судебная экспертиза: проблема выбора при расследовании преступлений, совершаемых с использованием интернет-технологий // Научный вестник Омской академии МВД России. 2015. № 2. С. 20-23.

3. Вехов В.Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь. 2004. № 7. С. 2-5.

4. Иванов А.Н. Удаленное исследование компьютерной информации: уголовно процессуальные и криминалистические проблемы // Изв. Сарат. ун-та Нов. сер. Сер. Экономика. Управление. Право. 2009. № 2. С. 74-77.

5. Никулина О.А. Особенности тактики производства осмотра места происшествия по делам о преступлениях в сфере компьютерной информации // Вестник Воронежского института ФСИН России. 2015. № 2. С. 65-69.

6. 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., 2017. 160 с.

7. Семикаленова А.И., Рядовский И.А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6. С. 178-185.

8. Поляков В.В. Особенности производства осмотра по компьютерным преступлениям // Российский следователь. 2017. № 21. С. 14-17.

9. Родивилина В.А., Цуканов Н.Н. Изъятие и осмотр мобильного телефона как электронного носителя информации // Вестник Восточно-Сибирского института МВД России. 2019. № 4. С. 107-114.

10. Смолин А.В., Зайцев А.А. Тактика производства отдельных следственных действий по преступлениям, совершённым с применением компьютерной техники // Криминалистика: вчера, сегодня, завтра. 2019. № 4. С. 52-57.

11. Гаврилин Ю.В., Балашова А.А. Совершенствование процессуального порядка собирания доказательственной информации, содержащейся в сетевых информационных системах // Криминалистика: вчера, сегодня, завтра. 2020. № 1. С. 129-137.

12. Соколов А.Б., Сысенко А.Р. Назначение и производство компьютерной экспертизы при расследовании преступлений, совершенных с использованием сети интернет: проблемы теории и практики // Криминалистика: вчера, сегодня, завтра. 2021. №1. С. 118-129.

13. Поляков В.В. Анализ судебной практики Алтайского края по преступлениям в сфере компьютерной информации // Вестник Новосибирского государственного университета. Серия: Право. 2014. Т. 10. № 1. С. 99-103.

***А.Б. Соколов,*** *к.ю.н., доцент, заместитель начальника кафедры криминалистики Омской академии МВД России, г. Омск*
***Р.П. Щербина,*** *преподаватель кафедры криминалистики Омской академии МВД России, г. Омск*

# СОБИРАНИЕ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, НАХОДЯЩЕЙСЯ НА ЦИФРОВЫХ НОСИТЕЛЯХ. II. ОСМОТР, ОБЫСК, СУДЕБНО-КОМПЬЮТЕРНАЯ ЭКСПЕРТИЗА

К числу наиболее эффективных с точки зрения отыскания, обнаружения и фиксации следов преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, являются осмотр (места происшествия, предметов), обыск, назначение и производство судебно-компьютерной экспертизы. Рассмотрим отдельные организационно-тактические особенности каждого из них.

Деятельность по производству осмотра места происшествия при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в криминалистической и уголовно-процессуальной науке исследована достаточно подробно [1-8 и др.]. Остановимся на проблеме, связанной с просмотром (обнаружением) содержимого цифровых носителей вычислительной техники при осмотре места происшествия. В соответствии с ч. 3 ст. 177 УПК РФ при производстве осмотра изъятию подлежат только те предметы, которые могут иметь отношение к уголовному делу. Установить это позволит просмотр содержащейся информации (файлов), например, в мобильном телефоне. В связи с этим нельзя не упомянуть наличие мнений о подмене обыска, исходя из возможной степени вторжения органов предварительного расследования в частную жизнь человека, осмотром места происшествия [9, с. 102].

На первый взгляд просмотр содержащейся в мобильном телефоне информации ошибочно ассоциируется с проведением обыска (деятельность по отысканию — носит активный поисковый характер), однако учитывая специфику электронной информации, полагаем, что это не совсем так. С технической точ-

ки зрения просмотр файлов (их наименования) является действием по обнаружению (в сравнении с отысканием носит пассивный характер). Обоснование данного тезиса предполагает обращение к изучению сущности файловой системы. Она на логическом уровне предоставляет возможность работать с данными, хранящимися в файлах. Именно файловая система определяет способ организации данных на каком-либо электронном носителе данных.

Одним из наиболее распространенных типов файловых систем являются файловые системы семейства FAT. В них дисковое пространство любого логического диска делится на две последовательно расположенных области: системную и область данных. Область данных содержит файлы и каталоги. Каталог FAT является обычным файлом, помеченным специальным атрибутом. При форматировании область данных разбивается на так называемые кластеры. Кластер — несколько смежных секторов области данных, а также минимальная адресуемая единица дискового пространства, выделяемого файлу. При создании нового файла операционная система отводит для него несколько свободных кластеров диска. Для каждого файла хранится список всех номеров кластеров, которые предоставлены данному файлу. В таблице FAT кластеры, принадлежащие одному файлу, связываются в цепочки. Обращаясь к файлу, операционная система считывает номер первого и последующих кластеров такого файла, согласно данным из таблицы FAT.

В другой, не менее распространенной файловой системе NTFS, используется общая таблица файлов или MFT (от англ. master file table). Каждая запись MFT соответствует какому-либо файлу. В соответствующей записи MFT хранится вся информация о файле, в том числе расположение на диске всех его фрагментов. Каталог в NTFS представляет собой специальный файл, хранящий ссылки на другие файлы и каталоги в нем.

Изучив техническую сторону размещения файлов, отметим, что кластер — это минимальная адресуемая единица дисковой памяти, выделяемая файлу; файлы состоят из цепочек необязательно последовательных кластеров; каталоги на самом деле являются особыми файлами. Исходя из сказанного, кластеры одного логического диска представляют собой одномерный массив адресованных ячеек. Все файлы, находящиеся на данном диске, можно представить как

последовательность бумажных листов документа, где один лист, это один кластер, но листы одного документа не обязательно следуют друг за другом.

Просматривая содержимое носителя информации, мы лишь перемещаемся от одной цепочки кластеров к другой, что не может относиться к действиям по отысканию (одна из задач обыска). При этом речь идет о получении информации относительно полного имени файла (его расположения), даты создания, редактирования (изменения) и последнего открытия, а также его размера.

Определенный интерес представляет осмотр предметов — цифровых носителей вычислительной техники. Преимуществом данного способа получения информации является его оперативность, заключающаяся в том, что данное следственное действие может быть произведено в кабинете с участием специалиста. Наиболее распространенными объектами осмотра являются мобильный телефон, планшет, ноутбук. Производство осмотра мобильного телефона обусловлено необходимостью получения сведений об истории переписки SMS/MMC, программ мгновенного обмена сообщениями (мессенджеры). При обнаружении в ходе визуального осмотра приложений для переписки, интересующей информации, следователь (специалист) производит фотографирование экрана устройства с последующим указанием соответствующих данных в протоколе осмотра предмета.

Отдельно обратим внимание на проблему, связанную с применением технико-криминалистических средств при осмотре цифровых носителей вычислительной техники. Анализ правоприменительной практики позволяет сказать о том, что встречаются случаи, когда при осмотре мобильного телефона применяются специализированные программно-аппаратные комплексы (UFED) с целью извлечения и последующего копирования информации на оптический диск однократной записи. При проведении опроса экспертов[44], производящих судебно-компьютерные экспертизы, на вопрос о возможности использования специализированных программно-аппаратных комплексов UFED, XRY, «Мобильный криминалист», ПО «Belkasoft evidence center x», а также средств восстановления удаленной информации, при осмотре цифровых носителей вычислительной

[44] Опрошено 3 эксперта ЭКЦ УМВД России по Омской области, имеющих право самостоятельного производства судебно-компьютерной экспертизы.

техники (вне производства экспертизы), были получены отрицательные ответы. Аргументом такой позиции выступало указание на использование при осмотре предметов, в том числе мобильных телефонов, только таких криминалистических средств, применение которых можно повторить в ходе судебного заседания. Таким образом, при осмотре мобильного телефона возможно получить информацию, которая в явном виде находится на устройстве и при условии отсутствия средств защиты или наличия у следователя (дознавателя) соответствующих данных (PIN, графический пароль и т.п.).

При производстве судебно-компьютерной экспертизы применение криминалистических средств, в том числе по обходу средств защиты устройства, содержащего искомую информацию, возможно. При этом в соответствующем постановлении лицо, назначившее судебную экспертизу, должно указать на возможность применения разрушающих методов исследования. Одновременно с этим появляется возможность чтения файлов баз данных, содержащих переписку, а также использования средств восстановления удаленной информации. Например, SMS-переписка хранится в файле базы данных, и при удалении SMS-сообщений стандартными средствами, по сути, сообщение не удаляется безвозвратно. В соответствующей строке таблицы базы данных сообщений устанавливается пометка «удалено» и сообщение перестает отображаться в списке сообщений приложении мобильного устройства.

Получение компьютерной информации с устройств при производстве обыска объединяет преимущества ранее названных способов: осмотра предметов (в части оперативности); производства судебно-компьютерной экспертизы (в части применения любых криминалистических средств). В ходе рассматриваемого следственного действия допускается применение разрушающих методов исследования, в том числе и специализированных программно-аппаратных комплексов.

Анализ правоприменительной деятельности позволяет обратить внимание и на то, что, осуществив в ходе обыска действия по отысканию, обнаружению, фиксации, изъятию, исследованию и оценке материальных, в том числе электронно-цифровых следов преступления, следователь, тем не менее, назначает судебно-компьютерную экспертизу.

Указанные в настоящей статье рекомендации направлены на совершенствование деятельности по собиранию доказательственной информации при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

**Список литературы**


1. Вехов В.Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь. 2004. № 7. С. 2-5.
2. Шаевич А.А. Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений: дисс. … канд. юрид. наук. Иркутск, 2007. 195 с.
3. 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.
4. Поляков В.В., Никитин А.С. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. I. Организационные основы // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами: сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул: Изд-во Алт. ун-та, 2017. Вып. XIV. С. 87-94.
5. Поляков В.В., Никитин А.С. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. II. Теоретические и практические проблемы // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействия киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами: сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул: Изд-во Алт. ун-та, 2017. Вып. XIV. С. 95-100.
6. Поляков В.В. Особенности производства осмотра по компьютерным преступлениям // Российский следователь. 2017. № 21. С. 14-17.

7. Коломинов В.В. Осмотр места происшествия по делам в сфере компьютерной информации // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3. С. 145-149.

8. 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., 2017. 160 с.

9. Черкасов В.С. Проблема разграничения следственных действий: осмотр и обыск при получении компьютерной информации // Правопорядок: история, теория, практика. 2018. № 1. С. 99-104.

***Л.Г. Суханова,*** *старший преподаватель кафедры уголовного процесса и криминалистики Юридического института Алтайского государственного университета, г. Барнаул*

## ОСОБЕННОСТИ УЧАСТИЯ АДВОКАТА-ЗАЩИТНИКА ПРИ ДОПРОСЕ СВИДЕТЕЛЯ С ИСПОЛЬЗОВАНИЕМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ

В 2011 г. в УПК РФ была введена ст. 278.1 и появилась законодательно закрепленная возможность использования видеоконференц-связи при проведении допроса свидетелей в судебном разбирательстве по уголовным делам. Согласно ч. 4 ст. 240 УПК РФ, потерпевший также может быть допрошен с использованием системы видеоконференц-связи.

В настоящее время система видеоконференц-связи активно используется в судебном производстве по уголовным делам и в науке уголовного процесса продолжает обсуждаться дальнейшее расширение границ ее применения и в досудебных стадиях уголовного судопроизводства. Вопросам использования видеоконференц-связи в уголовном судопроизводстве в своих работах уделили внимание Е.А. Архипова, А.Г. Волеводз, И.В. Казначей, В.А. Родивилина,

К.В. Авдонин, Д.В. Долгополов, О.В. Овчинникова, А.А. Хайдаров, Н.В. Осодоева и др.

В 2020 г. судами общей юрисдикции по уголовным делам было проведено 147 261 судебное заседание (количество дней) с использованием видеоконференц-связи и в 115 931 деле (в том числе материале) была применена система видеоконференц-связи [2]. Безусловно, отмеченные данные говорят об успешности и неотъемлемости применения видеоконференц-связи в судебном производстве по уголовным делам. Среди положительных свойств использования видеоконференц-связи, безусловно, можно назвать повышение качества и эффективности судопроизводства, процессуальную экономию времени и разрешения уголовных дел в разумные сроки, оптимизацию финансовых затрат.

В соответствии с п. 1.5 Регламента организации применения видеоконференц-связи при подготовке и проведении судебных заседаний, утвержденный Приказом Судебного департамента при Верховном Суде Российской Федерации № 401 от 28.12.2015 г видеоконференц-связь (ВКС) — способ осуществления процессуальных действий, предусмотренных законом, с использованием программно-технических средств передачи аудио- и видеоинформации по каналам связи с одним или несколькими абонентами [1].

В наименовании ст. 278.1 УПК РФ употреблено словосочетание «особенности допроса свидетеля путем использования систем видеоконференц-связи». Обращая внимание на содержание названной статьи, можно сделать вывод, что законодатель к особенностям допроса отнес выполнение организационных, подготовительных действий непосредственно связанных с использованием видеоконференц-связи в судебном следствии как судом, рассматривающим дело, так и судом, расположенным по месту нахождению свидетеля. Согласно ч. 3 ст. 278.1 УПК РФ допрос свидетеля проводится по общим правилам, установленным ст. 278 УПК РФ.

Значение участия адвоката-защитника в допросе свидетеля в судебном следствии нужно рассматривать с точки зрения участия защитника в доказывании и определяется целью проведения допроса свидетеля — получение доказа-

тельственной информации, подтверждающей занятую позицию защиты по конкретному уголовному делу.

Поскольку самим законодателем в ст. 278.1 УПК РФ обозначены особенности допроса свидетеля путем использования систем видеоконференц-связи, это не может не оказывать влияние на защитительную деятельность адвоката, ее форму, тактику и подачу, таким образом, необходимо говорить об особенностях участия адвоката-защитника при допросе свидетеля с использованием видеоконференц-связи. Для начала обратимся к научным взглядам, посвященным участию адвоката в допросе свидетеля в судебном разбирательстве, так скажем, в традиционной форме, когда участники находятся в одном месте — судебного заседания.

Так, В.Л. Кудрявцев отмечает важность тщательной, вдумчивой и кропотливой подготовки адвоката-защитника к участию в допросе подсудимого, потерпевшего и свидетеля, выделяет алгоритм действий защитника, включая в них следующие:

- анализ исходных данных и определение предмета участия в производстве допроса;
- изучение личности допрашиваемого;
- определение предполагаемого и уяснение фактического момента допроса лица со стороны обвинения и определение момента допроса лица со стороны защиты;
- составление плана допроса [3, с. 146];

Возьмем данный алгоритм за основу и попробуем определить особенности его реализации при проведении допроса свидетеля с использованием видеоконференц-связи.

Во-первых, как нам ответили 47% опрошенных респондентов (нами было проинтервьюировано 15 адвокатов Адвокатской палаты Алтайского края), проведение допроса в так называемом дистанционном формате требует немного другого подхода от адвоката, осуществляющего защиту по уголовному делу. Объясняя другой подход к участию в допросе с использованием видеоконференц-связи, респонденты отметили необходимость более кропотливой подго-

товки к созданию профессионального аудиовизуального образа адвоката, подготовки четкого динамичного плана допроса и готовности от адвоката маневрировать в случае каких-либо технических заминок при использовании видеоконференц-связи, иногда могут возникать сложности с установлением психологического контакта с допрашиваемым лицом, поскольку, как ответили 35% респондентов, несмотря на то, что взаимодействие хотя и происходит в режиме реального времени, все же имеется определенный барьер психологического плана. Также 32% опрошенных адвокатов пояснили, что по объемным многоэпизодным, сложным делам заявление адвокатом ходатайства о допросе свидетеля с использованием видеоконференц-связи не всегда может быть целесообразным, аргументируя это тем, что видеосвязь очень сильно искажает коммуникацию со свидетелями, а значит, важные фрагменты их показаний могут быть потеряны либо неверно восприняты.

Так, в апелляционной жалобе на постановление Верховного Суда Российской Федерации от 29 декабря 2020 г. адвокат С. выразила несогласие по поводу использования системы видеоконференц-связи при допросе свидетелей в суде первой инстанции, объясняя свою позицию тем, что с учетом обстоятельств предъявленного обвинения это не позволило стороне защиты в полной мере реализовать свои процессуальные права, учитывая необходимость в ходе допроса свидетелей непосредственного исследования письменных материалов уголовного дела [4].

Приведем еще один пример. В апелляционной жалобе адвоката М. на приговор суда первой инстанции приведен довод, что при допросе свидетеля А. в суде первой инстанции с использованием системы видеоконференц-связи подсудимый был лишен права на защиту, поскольку суд отказал в удовлетворении ходатайства о предоставлении на обозрение данному свидетелю А. схемы ДТП, хотя сам свидетель заявил, что для ответов на поставленные вопросы она ему необходима. При этом судом апелляционной инстанции доводы адвоката М. о нарушении права на защиту подсудимого, допущенного судом при допросе свидетеля А., признаны несостоятельными, как было отмечено в постановлении, обозрение имеющейся в материалах дела схемы ДТП свидетелем А.

во время его допроса в суде не представлялось возможным по техническим причинам — ввиду того, что допрос производился посредством видеоконференц-связи. Как было отмечено в решении суда, данное обстоятельство не свидетельствовало о неполноте допроса, об оставлении невыясненными существенно значимых обстоятельств дорожной ситуации и об отсутствии у подсудимого возможности реализовать свое право на защиту при допросе свидетеля обвинения [5].

По результатам проведенного опроса респондентов, изученных материалов судебной практики можно выделить особенности участия адвоката-защитника при допросе свидетеля с использованием видеоконференц-связи:

1. Особенности в установлении психологического контакта с допрашиваемым лицом — свидетелем, потерпевшим, что нередко выражается в сложности, трудности установлении психологического контакта. Это обусловливается тем, что, к сожалению, адвокат при использовании видеосвязи не всегда в полной мере может видеть мимику, жесты, реакцию допрашиваемого лица, а значит, правильно составить его психологический портрет. Также необходимо учитывать, что нередкими остаются случаи технических сбоев в работе видеоконференц-связи, что приводит к замене зала судебного заседания (при наличии) либо перерыву или переносу даты судебного заседания, дезорганизует выступление адвоката и свидетеля, при этом нельзя исключать влияние подобных случаев на желание, настрой свидетеля рассказать суду об обстоятельствах, имеющих значение для дела.

2. Особенности, связанные с представлением, обозрением допрашиваемому лицу и, соответственно, его восприятием письменных доказательств различных схем, рисунков, фотографий и т.д. Как было отмечено в вышеприведенном примере, обозрение имеющейся в материалах дела схемы ДТП свидетелем А. во время его допроса в суде не представлялось возможным по техническим причинам — ввиду того, что допрос производился посредством видеоконференц-связи. К сожалению, такие примеры встречаются в адвокатской практике, когда суды отказывают в удовлетворении ходатайства об обозрении свидетелю какого-либо документа, необходимого в целях проведения допроса ад-

вокатом. Гипотетически можно предположить, что суд в целях ознакомления свидетеля с таким документом может его направить по каналам связи (к примеру, телефаксу) в суд по месту нахождения свидетеля и после этого продолжить допрос, более того, УПК РФ это не запрещает, но и не регламентирует действия суда в таких случаях.

Обратимся к Регламенту организации применения видеоконференц-связи при подготовке и проведении судебных заседаний, утвержденного Приказом Судебного департамента при Верховном Суде Российской Федерации № 401 от 28.12.2015 г. Согласно п. 2.5 названного Регламента, участникам судебного заседания, проводимого в режиме ВКС, должна быть технически обеспечена возможность слышать и видеть ход судебного заседания, задавать вопросы и получать ответы в режиме реального времени, реализовывать другие процессуальные права и исполнять процессуальные обязанности, предусмотренные процессуальным законодательством Российской Федерации, в том числе передавать дополнительные документы и знакомиться с аудио- и видеодоказательствами, представленными в судебном заседании, изучать письменные доказательства (материалы дела). Передача дополнительных документов осуществляется с помощью ведомственной факсимильной связи (при наличии технической возможности), в ином случае посредством альтернативных средств связи (городской факс, электронная почта и т.п.) [1].

Таким образом, на уровне названного Регламента участникам судебного заседания гарантируется возможность передачи дополнительных документов, представленных в судебном заседании, изучения письменных доказательств (непосредственно касается приведенного нами примера), но, к сожалению, не всегда должным образом обеспечивается на практике.

Полагаем, в ст. 278.1 УПК РФ необходимо конкретизировать порядок проведения допроса с использованием системы видеоконференц-связи, а не только нормами о подготовке к допросу в таком формате, что будет способствовать обеспечению принципа состязательности сторон.

3. Особенности, связанные с подготовкой адвокатом-защитником плана допроса, который должен быть динамичным, рефлексивным, предусматривать

различные варианты постановки вопросов, выбор и применение различных тактических приемов с учетом складывающейся судебной ситуации, например, когда свидетель не явился в суд по месту его ожидания, суд отказал в удовлетворении ходатайства адвоката об обозрении свидетелю, допрашиваемому посредством видеоконференц-связи того или иного доказательства, об ознакомлении свидетеля с таким доказательством. Вопросы, сформулированные адвокатом и адресованные свидетелю, должны отличаться большей степенью емкости, но при этом краткости, понятности и однозначности. При этом пол, возраст, социальный статус и другие характеристики допрашиваемого лица необходимо учитывать по инициативе стороны защиты или обвинения.

4. Особенности, связанные подготовкой адвоката к представлению своего образа, внешнего вида (имиджа), мимики, жестов перед свидетелем, допрашиваемым посредством видеоконференц-связи. Иными словами, адвокату, помимо подготовки плана ведения допроса, необходимо подготовить, возможно, даже отрепетировать эмоциональную окраску вопросов, длительность допроса, продумать перспективное расположение участников в зале судебного заседания и экрана телевизора (монитора). В ходе очередного вебинара ФПА по повышению квалификации адвокатов с лекцией выступил управляющий партнер АБ «KALOY.RU» Калой Ахильгов, спикер, отметил, что вопрос, адресуемый свидетелю, должен быть достаточно простым. Для этого необходимо понимание существа обвинения, выдвинутого в отношении доверителя, и то, как оно доказывается, — в противном случае невозможно полноценно осуществлять защиту. Кроме того, отметил Ахильгов, не следует придавать излишнее значение эффектности (надменный тон, резкие движения) допроса — лучше спокойно и уверенно задавать вопросы, ссылаясь на те или иные доказательства [6].

Обратимся к судебной практике, складывающейся при применении системы видеоконференц-связи.

В обобщении материалов практики Ленинского районного суда г. Чебоксары применения в уголовном судопроизводстве систем видеоконференц-связи за период с 1 сентября 2019 г. до 1 сентября 2020 г. отмечается отсутствие в действующем УПК РФ регламентации обязательности и процедуры оглаше-

ния состава суда по месту нахождения свидетеля, потерпевшего и права сторон на заявление отводов данному составу суда, порядка участия адвоката и переводчика при допросе потерпевшего (подсудимого, свидетеля), их права на беседу и обеспечение ее конфиденциальности. Как отмечено в обобщении практики данного суда, указанные пробелы в законодательстве создают проблемы в применении видеоконференц-связи в судебной практике [7].

Так, суд апелляционной инстанции установил нарушения требований ст. 278.1 УПК РФ судом первой инстанции, а именно нарушение процедуры установления личности и отобрания подписки у свидетеля Ц., допрашиваемого посредством системы видеоконференц-связи, данные действия были осуществлены не судом по месту нахождения свидетеля, а сотрудником администрации исправительного учреждения. Апелляционный суд отметил, учитывая, что Ц. на момент допроса отбывал наказание в ФКУ ИК-2 УФСИН России по Тюменской области, а перевод его в следственный изолятор для доставления в судебное заседание для допроса занял бы длительное время, что повлекло бы за собой значительное затягивание рассмотрения уголовного дела по существу, суд первой инстанции принял решение о допросе Ц. путем использования систем видеоконференц-связи. Личность Ц. была установлена сотрудником администрации исправительного учреждения, права и обязанности были разъяснены ему председательствующим судьей, ею же он был предупрежден об уголовной ответственности, о чем дал расписку. Несмотря на допущенные нарушения, суд апелляционной инстанции отметил, что они не влияют на достоверность показаний, данных Ц. в ходе судебного заседания и, следовательно, однозначно не влекут их исключение из числа доказательств [8].

Приведем пример, в котором судом было принято абсолютно противоположное решение. Судом апелляционной инстанции установлено, что суд первой инстанции, постановив произвести допрос потерпевшего путем использования систем видеоконференц-связи, поручил организовать проведение допроса потерпевшего установить его личность, разъяснить ему права и обязанности, предусмотренные ст. 42 УПК РФ, ответственность, предусмотренную ст. 306-308 УПК РФ, администрации ФКУ ОИУ-26 ИК-42 ГУФСИН России. Апелля-

ционная инстанция расценила данные действия суда как нарушение требований ст. 278.1 УПК РФ, согласно которой установление личности потерпевшего, разъяснение ему прав и ответственности осуществляется только судом [9].

Еще один более ранний пример, однако также создающий диссонанс в понимании и применении ст. 278.1 УПК РФ. Суд апелляционной инстанции в своем решении указал, что не влечет отмену или изменение приговора в отношении К. те доводы защитника, что при допросе свидетеля М. путем видеоконференц-связи были нарушены требования ст. 278.1 УПК РФ, так как допрос был организован не судом по месту нахождения свидетеля, а неустановленным сотрудником исправительной колонии. Из материалов уголовного дела следует, что допрос свидетеля был организован и проведен самим судом, в производстве которого находилось уголовное дело, без существенных нарушений требований ст. 278.1 УПК РФ, допускающей использование для этих целей систем видеоконференц-связи [10].

По данному вопросу Н.В. Осодоева отмечает необходимость внесения дополнений в УПК РФ, предусматривающих удостоверение личности свидетеля, отобрание подписок свидетеля о предупреждении о наступлении уголовной ответственности не только судом, но и сотрудниками исправительных учреждений, поскольку имеются случаи, как отмечает автор, когда суды не признают нарушением удостоверение личности свидетелей (осужденных, отбывающих наказание в исправительных учреждениях) должностными лицами следственных изоляторов, исправительных колоний, кроме того, выполнение требований сотрудниками указанных учреждений ст. 278.1 УПК РФ никоим образом не нарушает законные права и интересы подсудимых, свидетелей (лиц, отбывающих наказание) [11, с. 224].

Таким образом, особенности участия адвоката-защитника в допросе свидетеля посредством видеоконференц-связи непосредственно связаны с дистанционным форматом его проведения, возможными техническими сбоями, а также с отсутствием на законодательном уровне положений, четко регламентирующих порядок проведения допроса свидетеля посредством видеоконференц-связи и участие в нем адвоката. Складывающаяся неоднозначная судебная

практика по подготовке и проведению допроса с использованием видеоконференц-связи требует активных мер по совершенствованию законодательства и обеспечению технической готовности абсолютного большинства судов к использованию системы видеоконференц-связи.

## Список литературы


1. Регламент организации применения видео-конференц-связи при подготовке и проведении судебных заседаний, утвержденный Приказом Судебного департамента при Верховном Суде Российской Федерации № 401 от 28.12.2015 г. [Электронный ресурс]. URL: http://www.consultant.ru/ (дата обращения: 28.05.2021).
2. Отчет о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции за 2020 год // Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. [Электронный ресурс]. URL: http://www.cdep.ru/index.php?id=79&item=5671 (дата обращения: 28.05.2021)
3. Кудрявцев В.Л. Актуальные вопросы участия адвоката-защитника в производстве допроса подсудимого, потерпевшего и свидетеля // Вестник Челябинского государственного университета. 2003. Т. 9. Вып. 2. С. 146-161.
4. Апелляционное определение Верховного Суда Российской Федерации по делу № АПЛ21-49 от 18.02.2021 г. [Электронный ресурс]. URL: https:// sudact.ru/ (дата обращения: 28.05.2021).
5. Апелляционное постановление Челябинского областного суда по делу № 10–2385/2020 от 02.07.2020 г. [Электронный ресурс]. URL: https:// sudact.ru/ (дата обращения: 28.05.2021).
6. Адвокатам рассказали о нюансах допроса свидетеля в ходе судебного разбирательства // Официальный сайт сетевого издания «Адвокатская газета» [ Электронный ресурс]. URL: https:// https://www.advgazeta.ru/novosti/advokatam-rasskazali-o-nyuansakh-doprosa-svidetelya-v-khode-sudebnogo-razbiratelstva/ (дата обращения: 28.05.2021).

7. Практика применения судом в уголовном судопроизводстве технических средств (ведения аудиозаписи (аудиопротоколирования), систем видеоконференц-связи и иных технических средств) за период с 1 сентября 2019 года до 1 сентября 2020 года // Официальный сайт Ленинского районного суда г. Чебоксары. [Электронный ресурс]. URL: https:// leninsky.chv.sudrf.ru/ modules.php?name=press_dep&op=3&did=37 (дата обращения: 28.05.2021).

8. Апелляционное постановление Тюменского областного суда по делу № 22-1561/19 от 30.07.2019 года [Электронный ресурс]. URL: https:// https://sudact.ru/ (дата обращения: 28.05.2021).

9. Апелляционное постановление Ордынского районного суда по делу № 10-5/2017 от 22.03.2017 г. [Электронный ресурс]. URL: https:// https://sudact.ru/ (дата обращения: 28.05.2021).

10. Апелляционное определение Судебной коллегии Челябинского областного суда по делу № 10-5107/2014 от 16.09.2014 г. [Электронный ресурс]. URL: https:// https://sudact.ru/ (дата обращения 28.05.2021).

11. Осодоева Н.В. К вопросу об установлении личности допрашиваемого лица при производстве допроса свидетелей посредством видео-конференц-связи в уголовном судопроизводстве // Криминалистика: вчера, сегодня, завтра. 2021. № 1 (17). С. 217-224.

***Ю.А. Телевицкая,*** *адъюнкт Нижегородской академии МВД России, г. Нижний Новгород*

## ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИЗЪЯТИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ В УГОЛОВНОМ ПРОЦЕССЕ ГОСУДАРСТВ-УЧАСТНИКОВ СНГ

На постсоветском пространстве СНГ является самым крупным по составу участников региональным интегральным объединением, способствующим углублению взаимодействия между государствами-участниками. Борьба с пре-

ступностью и противодействие новым угрозам является одним из основных направлений взаимодействия, закрепленным в базовом учредительном документе — Уставе СНГ.

Решением Совета глав государств СНГ 18 декабря 2020 г. были внесены изменения в Концепцию дальнейшего развития Содружества Независимых Государств и разработан план по ее реализации. Приоритетным направлением деятельности в плане мероприятий по концепции развития выделяются: сотрудничество стран СНГ в сфере международной безопасности, обеспечение стабильности, борьба с преступностью, противодействие новым вызовам и угрозам, а также обеспечение международной информационной безопасности. Для реализации международного сотрудничества по поддержанию и укреплению международной безопасности разработаны следующие мероприятия: совершенствование имеющихся механизмов по обмену информацией с целью противодействия трансграничной преступности, проведение межведомственных консультаций государств-участников СНГ, передача положительного опыта в области информационной безопасности и противодействию преступлений [1]. В настоящее время в условиях глобальной информатизации общества значительно увеличилось количество преступлений, имеющих международные связи. Всеобщая интегративная тенденция не обошла и преступные группировки, которые на данный момент распространяются и действуют в международном масштабе. Таким образом, наиболее актуальной среди правоохранительных органов является проблема международного сотрудничества в сфере борьбы с преступностью, в первую очередь значимым является взаимодействие Российской Федерации с государствами-участниками СНГ, как странами, находящиеся в непосредственной территориальной близости от границ государства и имеющих общую историю развития и становления.

А.С. Александров отмечает, что страны постсоветского пространства создают свое, новое, отличное от российского уголовно-процессуальное законодательство, которое далеко от модельного кодекса стран СНГ. Государства перестраиваются на новые стандарты, следуя современным реалиям, Россия же остается в интеллектуальной провинции [2, с. 27]. Мысль, лежащая в основе выска-

зывания автора, подтолкнула нас к изучению уголовно-процессуального законодательства ряда стран-участников СНГ с целью сравнительно-правового анализа норм права, затрагивающих вопросы уголовного судопроизводства, в частности, особенности выемки и изъятия электронных носителей информации.

*Республика Казахстан.* Особенностью уголовного процесса Республики Казахстан является переход к электронному судопроизводству, которое пронизывает все стадии производства по делу, начиная с подачи и регистрации заявления до исполнения вступившего в законную силу судебного акта. Судебные заседания проводятся в онлайн-формате, подробная инструкция к подключению и требования к IT-оборудованию подробно описаны на официальном сайте Верховного суда Республики Казахстан [3].

Действующий УПК Республики Казахстан [4] разработан на основе Концепции правовой политики государства на период с 2010 по 2020 г. [5], одним из основных направлений которой является упрощение и повышение эффективности уголовного процесса. В основе УПК РК 2014 г. лежит предыдущий опыт страны и разумные либеральные начала, которые сложились в мировой системе права [6, с. 12-18].

Электронные носители информации не выделяются в УПК РК в качестве отдельного вида доказательств. Условно информацию, хранящуюся на электронных носителях, можно отнести к документам как разновидности доказательств, предусмотренной УПК. Наряду с письменной формой процессуальное законодательство выделяет и иные формы фиксации информации, к которым относятся: материалы, содержащие компьютерную информацию, звуко- и видеозаписи, фото- и киносъемку.

Защитники и представители потерпевшего имеют право опросить лиц, которые предположительно владеют информацией по уголовному делу. Ход опроса и его результаты отражаются в письменной либо электронной форме. Информация, зафиксированная в электронном виде, предоставляется на электронном носителе, который в последующем приобщается к материалам уголовного дела и признается в качестве доказательств после прохождения необходимых процессуальных процедур (п. 5 ч. 3 ст. 122 УПК РК).

Следовательно, электронные носители информации признаются в качестве доказательств по расследуемому уголовному делу, однако определенного места в системе доказательств УПК РК они не занимают. Вопрос об отнесении электронных носителей информации к группе документов либо вещественных доказательств на данный момент является открытым.

Уголовное судопроизводство Республики Казахстан встало на путь правовой цифровизации, происходит постепенный переход от бумажного протоколирования как основного средства фиксации к электронному. Среди российских процессуалистов за цифровизацию уголовного судопроизводства РФ выступают следующие представители доктрины: А.С. Александров, О.И. Андреев, О.А. Зайцева [7], Л.В. Головко [8, с. 15-24], С.В. Власова [9, с. 9-18], С.В. Зуев [10, с. 587-595] и др. Право стороны защиты на самостоятельный сбор доказательственной информации, которая в том числе может быть предоставлена на электронных носителях, говорит о зарождении состязательности в уголовном процессе рассматриваемой страны. Однако следует отметить, что в УПК РК отсутствует понятие и процессуально закрепленное регулирование особенностей изъятия и копирования электронной информации, в кодексе лишь вскользь упоминается область применения данного вида доказательств.

*Азербайджанская Республика.* Одним из основных источников уголовно-процессуального законодательства Азербайджанской Республики является Уголовно-процессуальный кодекс, утвержденный в 2000 г. [11].

Особый интерес в уголовно-процессуальном законодательстве Республики Азербайджан представляет программа «Электронное уголовное дело», принятая с целью сокращения сроков расследования и повышения качества предварительного следствия. Программа реализуется с 2016 г. и направлена на повышение эффективности расследования налоговых преступлений [12, с. 67-73].

Однако несмотря на то, что законодательство Азербайджанской Республики сделало шаг в сторону электронного судопроизводства, на данном этапе говорить о готовности к полному переходу от протокольной формы к ведению электронного уголовного дела пока рано. Уголовно-процессуальное законодательство страны не содержит понятия, раскрывающего сущность и содержание

электронного носителя информации, не определено место электронных носителей в системе доказательств по уголовному делу, отсутствуют специальные нормы изъятия, копирования, оценки и хранения электронной информации.

*Кыргызская Республика.* УПК КР [13] регулирует отдельные положения хранения, изъятия и копирования электронных носителей информации (п. 8 ч. 2 ст. 89, ч. 16 ст. 205 УПК КР). Электронные носители информации изымаются с обязательным участием специалиста. Вопросы, затрагивающие копирование информации с электронных носителей и их хранение в качестве доказательств по делу, разрешаются аналогично схожим положениям российского процессуального законодательства.

В уголовный процесс Кыргызской Республики активно внедряется электронный документооборот. Электронный документ, подписанный электронной цифровой подписью, признается доказательством и имеет равную юридическую силу с информацией, закрепленной на бумажном носителе (ч. 3 ст. 91 УПК КР). Также еще одним шагом к цифровизации уголовного судопроизводства Кыргызской Республики является возможность проведения допроса (ст. 194 УПК КР), предъявления для опознания (ст. 202 КР) и производство допроса судом (ст. 280) с использованием видеоконференц-связи.

Таким образом, в результате анализа уголовно-процессуального законодательства Кыргызской Республики можно выделить следующие особенности. Разрешение на производство обыска и выемки выдает следственный судья, как лицо, осуществляющее оперативный судебный контроль над законностью и обоснованностью основных актов предварительного расследования, что само по себе является положительным направлением в развитии уголовного судопроизводства страны. За введение фигуры следственного судьи на территории Российской Федерации выступают многие отечественные процессуалисты [14-16], аргументируя это необходимостью проведения судебно-правовой реформы в стране с целью обеспечения независимого и качественного следствия и эффективного и справедливого суда. Кыргызская Республика встала на путь цифровизации уголовного судопроизводства, что может послужить положительным примером, в том числе и для Российской Федерации. К сожалению, в нашей

стране на данный момент переход к электронному документообороту, функционирующему в рамках производства по уголовному делу, находится лишь на дискуссионной стадии.

*Республика Молдова.* УПК Республики Молдова № 122-XV от 14 марта 2003 г. [17] относит привычные для российского процессуального законодательства следственные действия к средствам и методам доказывания, выделяя их в одноименную главу уголовно-процессуального кодекса. Выемка электронных носителей информации не имеет отдельного регулирования, однако основные положения изъятия устройств хранения данных и информационных систем описаны в ст. 128 УПК РМ, посвященной порядку производства обыска и выемки.

Следует отметить, что в соответствии с Молдавским уголовно-процессуальным законодательством ограничивается изъятие в оригинале не только электронных носителей информации, но и предметов и документов, если их отсутствие может привести к прекращению хозяйственной деятельности лица. Аналогичные положения приводятся в ст. 164.1 УПК РФ, однако в соответствии с российским уголовным процессом ограничение на изъятие относится только к электронным носителям информации по делам предпринимательской и иной экономической деятельности, указанные в ч. 4.1 ст. 164 УПК РФ. В настоящий момент считаем нецелесообразным перенятие опыта Республики Молдова в части ограничения изъятия предметов и документов, так как, по нашему мнению, данное регулирование представляется достаточным относительно электронных носителей информации, как представлено в российском Уголовно-процессуальном законодательстве.

В УПК РМ установлен срок возврата предметов, документов, информационных систем и устройств хранения данных, изъятие которых может привести к прекращению хозяйственной деятельности организаций и индивидуальных предпринимателей. В случае невозможности производства копирования информации с указанных выше предметов непосредственно на месте производства следственного действия, без ущерба их целостности и подлинности, либо если владелец препятствует проведению необходимых действий, орган предва-

рительного расследования изымает указанные предметы с целью выполнения копий, сохранения данных, либо фото- или видеозаписи (ч. $5^3$ ст. 128 УПК РМ). Изъятые предметы, документы и электронные носители информации должны бить возвращены владельцу в течение 3 дней с момента их изъятия. Исключением являются назначение судебной экспертизы или научно-технического исследования. Если по каким-либо причинам трехдневного срока оказалось недостаточно для изучения и копирования информации с изъятых предметов, то по мотивированному постановлению прокурора указанный срок может быть продлен до 20 дней (ч. $5^4$ ст. 128 УПК РМ).

Российское уголовно-процессуальное законодательство не предусматривает правовое регулирование случаев, при которых может произойти затруднения при копировании информации с электронных носителей, непосредственно на месте производства следственного действия. Однако как поступить лицу, производящему расследование в случае невозможности копирования информации на месте? В соответствии с ч. 1 ст. 164.1 изъять носители электронной информации не получится, за исключением ряда приведенных в законе случаев. В данной ситуации разрешить представленную проблему помогло бы регулирование временного изъятия электронной информации с целью ее копирования, при наличии ограниченного срока на возвращение носителей законному владельцу.

Таким образом, страны постсоветского пространства пытаются выйти на совершенно новый уровень развития уголовного судопроизводства, внедряя в уголовно-процессуальную деятельность современные технологии. Переход к электронному уголовному делу, внедрение электронного документооборота, проведение судебных заседаний в онлайн-формате — все это большой шаг к развитию уголовного процесса. Однако следует отметить, что вопросы, затрагивающие электронные носители информации, в полной мере не освещены ни в одной из рассматриваемых стран, что еще раз подтверждает необходимость разработки и совершенствования правового регулирования в рассматриваемой области.

## Список литературы

1. О Концепции дальнейшего развития Содружества Независимых Государств и План основных мероприятий по ее реализации: Решение Совета глав государств от 18.12.2020 г. // Официальный сайт ООН. [Электронный ресурс] URL: http://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=6363 (дата обращения: 29.03.2021 г.).

2. Александров А.С. Доктринальная модель уголовно-процессуального доказательственного права РФ и Комментарии к ней. М.: Юлитинформ, 2015. С. 27 // Международная организация содействия правосудию. [Электронный ресурс]. URL: https://www.iuaj.net/node/1844 (дата обращения: 30.03.2021 г.).

3. Как принять участие в судебном заседании посредством МВКС? // Верховный суд Республика Казахстан. [Электронный ресурс]. URL: https://sud.gov.kz/rus/content/kak-prinyat-uchastie-v-sudebnom-zasedanie-posredstvom-mvks/ (дата обращения: 03.30.2021 г.).

4. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 02.01.2021 г.) // СПС Параграф. [Электронный ресурс]. URL: https://online.zakon.kz/m/document?doc_id=31575852 (дата обращения: 30.03.2021 г.).

5. О концепции правовой политики Республики Казахстан на период с 2010 по 2020 года: Указ Президента Республики Казахстан от 24 августа 2009 г. № 858. [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/U090000858_ (дата обращения: 30.03.2021 г.).

6. Зайцев О.А. Об основах положения проекта уголовно-процессуального кодекса Республики Казахстан // Известия. 2014. № 5. С 12-18. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/ob-osnovnyh-polozheniyah-proekta-ugolovno-protsessualnogo-kodeksa-respubliki-kazahstan/viewer (дата обращения: 30.03.2021 г.).

7. Александров А.С., Андреева О.И., Зайцева О.А. О перспективах развития уголовного судопроизводства в условиях цифровизации // Международ-

ная Ассоциация Содействия Правосудию. [Электронный ресурс]. URL: https://www.iuaj.net/node/2782 (дата обращения: 30.03.2021 г.).

8. Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15-24.

9. Власова С.В. К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. 2018. № 1. С. 9-18.

10. Зуев С.В., Никитин Е.В. Информационные технологии в решении уголовно-процессуальных проблем // Всероссийский криминологический журнал. 2017. Т. 11. № 3. С. 587-595.

11. Уголовно-процессуальный кодекс Азербайджанской Республики (утвержден Законом Азербайджанской Республики от 14 июля 2000 года № 907-IQ) (с изм. и доп. по состоянию на 29.06.2020 г.) // СПС Параграф. [Электронный ресурс]. URL: https://online.zakon.kz/document/?doc_id=30420280&doc_id2=30420280#pos=5;-98&pos2=160;-90 (дата обращения: 05.04.2021 г).

12. Гридюшко П.В., Бушкевич Н.С. Об электронной форме ведения уголовного процесса // Вестник Академии МВД Республики Беларусь. 2017. № 2 (34). С. 67-73.

13. Уголовно-процессуальный кодекс Кыргызской Республики (с изм. И доп. по состоянию на 31.12.2020 г.) // СПС Параграф. [Электронный ресурс]. URL: https://online.zakon.kz/m/Document/?doc_id=36313326#sub_id=2040300 (дата обращения: 06.04.2021 г).

14. Ковтун Н.Н. О понятии и содержании термина «судебный следователь» (следственный судья) // Российский судья. 2010. № 5. С. 15-20.

15. Морозова О.С. Целесообразно ли ввести фигуру следственного судьи в уголовное судопроизводство // Сибирское юридическое обозрение. 2020. Т. 17. № 1. С. 83-87.

16. Пиюк А.В. «Следственный судья» или «судебный следователь»: какая реформа нам нужна? // Уголовная юстиция. 2014. № 2 (4). С. 24-28 и др.

17. Уголовно-процессуальный кодекс Республики Молдова № 122-XV от 14.03.2003 (с изменениями и дополнениями по состоянию на 16.12.2020 г.) // СПС. Континент. [Электронный ресурс]. URL: http://continent-online.com/Document/?doc_id=30397729 (дата обращения 11.05.2021 г.).

***Д.В. Теткин,*** *к.ю.н., доцент кафедры уголовного процесса Рязанского филиала Московского университета МВД России имени В.Я. Кикотя, подполковник полиции, г. Рязань*

***А.А. Пудовкин,*** *к.ю.н., начальник кафедры уголовного процесса Рязанского филиала Московского университета МВД России имени В.Я. Кикотя, полковник полиции, г. Рязань*

## ПРОБЛЕМНЫЕ АСПЕКТЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ СОВРЕМЕННОЙ ЦИФРОВИЗАЦИИ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ

В условиях современной цифровизации процесс развития современного мира не стоит на месте. Искусственный интеллект и новейшие технологии все прочнее внедряются в нашу повседневную жизнь и профессиональную деятельность. Несмотря на достаточно широкий спектр положительных последствий указанного явления, появление современных технологий открывает для преступника новые возможности для совершения противоправной деятельности.

Распространение интернет-ресурсов и технологических достижений способствовало глобальным изменениям в преступных сферах и разновидностях преступной деятельности. Данный факт подтверждается тем, что Интернет позволяет преступному миру получать доступ к большему числу жертв, скрывать свою противозаконную деятельность, а также совершать широкий круг преступных действий за короткий промежуток времени.

Криптовалюта, набравшая популярность за последнее десятилетие, является объектом для преступлений, причем как совершаемых виртуально, так

и осуществляемых преступными элементами без использования компьютерных технологий. Так называемая киберпреступность — это область, для расследования которой требуются как понимание особенностей работы IT-технологий, так и особые знания в области юриспруденции.

Рассматривая криптовалюту как предмет преступлений, стоит отметить, что в современной российской действительности статус криптовалюты остается неоднозначным. При этом говорить о запрещенности указанных цифровых валют не стоит. Их статус в современном российском законодательстве носит скорее ситуативный, нежели системный характер. Например, рассматривая дела о банкротстве, суд признает, включая биткоин как иное имущество в конкурсную массу для расчетов с кредиторами [1]. Обратной стороной указанного вопроса является отношение к криптовалюте со стороны правоохранительных органов (прокуратура, следственные органы) и Центробанка [2]. В начале развития отношений по поводу криптовалюты в Российской Федерации указанные органы рассматривали биткоин и иные альткоины как денежный суррогат, а соответственно, все операции по обращению с ними признавались уголовно наказуемыми деяниями.

Стоит отметить, что с 1 октября 2019 г. цифровые права официально отнесены к объектам гражданских прав [3].

Что касается ст. 128 ГК РФ, ввиду открытого перечня объектов гражданских прав криптовалюта отнесена к иному имуществу, то есть теперь цифровые активы являются законными в гражданском обороте, в том числе с целью уплаты налогов либо выплаты задолженностей кредиторам [4].

Существующие проблемные аспекты, вызванные расхождением правовых актов по своему содержанию, неопределенностью статуса криптовалюты, отсутствием выработанных стратегий и планов министерствами, ставят органы исполнительной власти в затруднительное положение. Рассматривая российские уголовные дела и зарубежные криминальные кейсы, связанные со сферой криптовалют, следует выделить некоторые составы преступлений, которые чаще всего фигурируют в подобных случаях.

Для более устойчивого понимания природы совершенных преступлений подразделим преступления со всей сферы на две наиболее значимые категории: преступления, совершенные в сетевом пространстве, и «классические» преступления, совершенные вне указанного поля. К последней категории относятся преступления, в которых правоотношения, связанные с правом владения и распоряжения криптовалютой, являются объектом преступления. Это дела о кражах, разбоях, мошенничествах, в рамках которых биткоин и иные альткоины являются предметом.

К первой категории относятся преступления, совершенные в интернет-пространстве с использованием соответствующих программ и оборудования. И здесь следует также провести дифференциацию составов преступлений. Прибегая к условности, установим два основных способа использования криптовалюты в преступной деятельности:

– к первой группе относим рассмотрение криптовалюты как предмета преступного посягательства в рамках сетевого пространства (хищение криптовалюты со счетов, интернет-мошенничество и др.). (Отметим, что самая большая категория киберпреступлений, связанных с криптовалютами в мире, в 2017 г. была связана с хакерскими атаками на обменники криптовалют при помощи вредоносных компьютерных программ, их создания, использования и распространения, и в дальнейшем непосредственно кражей криптовалют или фишингом);

– второй способ подразумевает использование криптовалюты в платежных целях при совершении операций незаконного характера. К подобным относят использование криптовалюты как средства оплаты услуг на просторах Даркнета как средство легализации доходов, полученных преступным путем, и т.д.

За 2015 г. количество преступлений в мире, отнесенных ко второй группе, в числовом соотношении превышало количество преступлений первой группы в 20 раз. Однако с 2017 г. наблюдается рост преступности, связанной с хищением криптовалюты, только за указанный 2017 г. количество указанных преступлений увеличилось на 300%.

Приведенная статистика является следствием возросшего статуса криптовалюты среди населения не только России, но и всего мира в целом. При этом

создание и распространение криптовалюты никак не было связано с преступным умыслом изначально. В связи с этим рассматривать криптовалюту как предмет, подлежащий законодательному запрету, является неверным, с нашей точки зрения. Криптовалюта открывает новые возможности для использования вычислительных ресурсов компьютерной аппаратуры с целью монетизации, дает способность биржевым трейдерам осуществлять свою деятельность независимо от режима работы крупнейших рынков, так как рынок криптовалют является интернациональным, а потому круглосуточно осуществляющим свою деятельность, и т.д.

Но при этом, несмотря на однозначные плюсы, криптовалюта является ликвидным инструментом не только в руках добропорядочного гражданина, но и в руках преступника. В аналитическом докладе Европола от 30 сентября 2015 г. было отражено, что в деятельности незаконных крипторынков (Silk Road, Evolution и др.) годовой доход каждого крипторынка превышал 20 млн долл. США. Однако в последние годы наблюдается тенденция снижения указанного преступного дохода примерно в 40-45 раз [5].

Опять же, в докладе Европола был отражено, что виртуальная валюта стала чаще использоваться и в сфере сексуальной эксплуатации детей в Интернете. Причина использования криптовалюты заключается в том, что оплата указанным способом почти гарантирует преступнику анонимность.

Как было отмечено в отчете ФАТФ, легализация преступных доходов является одной из наиболее востребованных сфер криминального использования криптовалюты [6].

В основном причиной популяризации криптовалюты на мировом рынке выступают ее техническое особенности: возможность множественного дробления без потери ценности, круглосуточным осуществлением транзакций, безвозвратностью транзакций, проверкой валидности, частичной анонимностью, децентрализованной эмиссией и др.

По ряду показателей криптовалюта является не просто отличительным финансовым инструментом, она уникальное явление современности. Причем именно ее технические особенности позволяют назвать ее надежной и безопасной.

История развития правоохранительных органов является длительной и динамично развивающейся [7, с. 14-31]. Однако нет оснований допускать, что преступления указанного характера будут оставаться слепым пятном для органов внутренних дел. В связи с тем, что технология блокчейна все еще находится на самой ранней стадии развития, имеется реальная возможность упростить работу правоохранительным органам. Блокчейн должен служить благим целям.

Одной из задач, стоящей перед правоохранителями при раскрытии и расследовании киберпреступлений, стоит определение MAC-адреса преступника. Это является достаточно сложно исполнимой задачей в случае, если кто-то использует несколько IP-адресов, TOR, прокси и т.д.

Вспомним о великолепной особенности блокчейна — способности отслеживать все транзакции определенного адреса, причем до самой первой транзакции, сделанной с него. Это позволяет отслеживать движения средств так, как это было невозможно никогда раньше. Выходит, что и Биткоин не так анонимен, как о нем говорят. Биткоин-адрес — это в теории номер счета. Если вы можете связать человека с адресом, то сможете узнать все транзакции, которые сделал человек.

Камнем преткновения при раскрытии и расследовании киберпреступлений выступают операторы интернет-соединения. Каждый из них имеет свои правила, а если он территориально расположен или документально оформлен за границей, вопрос о предоставлении персональных данных по транзакции может растянуться на годы. А в таком случае есть вероятность, что провайдер удалил данные. Блокчейн в свою очередь хранит данные вечно. Процедура их получения — намного легче. Для получения же истории транзакции при работе с блокчейном не требуются документы в силу его открытости.

Все вышесказанное не является теорией, не подтвержденной практикой. Например, дело «Silk Road» [8] продемонстрировало способность правоохранительных органов к использованию блокчейна для противодействия преступности. Так, по указанному криминальному кейсу среди представленных вещественных доказательств была диаграмма, показывающая, как правоохранительные органы отслеживали средства через блокчейн, несмотря на попытку Карла

Форса — обвиняемого, разделить с целью сокрытия личности транзакции по многочисленным адресам.

Подобным крупным примером международной организации противодействия киберпреступности в области криптовалют служит операция «Operation Shrouded Horizon». Участниками данного дела со стороны правоохранительных органов выступило 20 стран, в числе которых Австралия, Канада, Кипр, США и др. В результате данной операции было подвергнуто аресту около 300 злоумышленников, осуществлявших руководство форумом Darkode в Даркнете, созданном в целях покупки/продажи вредоносного программного обеспечения.

Итак, в основном учет криптовалюты децентрализован, она не подчиняется контролю ни одной стране, каждая операция проверяется майнерами (без них криптовалюта вообще не может существовать), его нельзя украсть, а также запретить или подделать. Как мы отметили выше, данные системы функционируют на таких технологиях, как блокчейн, и обычно информация о транзакциях не шифруется и доступна в открытом виде. Представляется, что именно доступность и открытость блокчейна позволяет правоохранительным органам без каких-либо проблем получать доступ к истории транзакций.

То есть успешное расследование данных преступлений возможно лишь при условии наличия квалифицированных специалистов в области IT-технологий (информационно-коммуникационных технологий). Для участия в следственных действиях, согласно УПК РФ [9], в обязательном порядке следует привлекать специалистов, в данном случае в области работы с компьютерной информацией и ее носителями, а также в сфере криптографии, электронных платежных средств и систем. Однако следует дополнить, что в настоящее время, несмотря на все принятые и принимаемые меры, уровень их подготовки в вузах остается довольно низким. Следовательно, в вузах следует создавать кафедры или факультеты по подготовке таких специалистов.

В настоящее время перед органами предварительного расследования стоит достаточно сложная задача, так как отсутствуют:

– правовые нормы, регулирующие функционирование криптовалюты;

– методические рекомендации по организации раскрытия и расследования данных преступлений;

– обобщенные материалы практики не только следственной, но и судебной;

– знания и опыт работы у следователей и работников органов дознания;

– источники доказательственной информации, так как преступления данной категории специфичны, они находятся в виде сайтов и страниц сети «Интернет», электронных документов и сообщений.

Резюмируя проведенное исследование, напрашивается вывод о том, что в скором времени указанные проблемные аспекты будут устранены. Несмотря на сложность структуры раскрытия и расследования преступлений указанных категорий, еще пять лет назад система правоохранительных органов не могла быстро отреагировать на возникшую проблему. Теперь, когда темпы нарастания преступности сбиты, стоит обратить внимание на устранение расхождений правового характера, а также на освоение системы блокчейна правоохранительными органами как России, так и других стран, с целью дальнейшего оказания взаимопомощи по раскрытию и расследованию преступлений в условиях современной цифровизации.

## Список литературы

1. [Электронный ресурс]. URL: https://sudact.ru/arbitral/doc/20EHFIeHovUP/ (дата обращения: 15.04.2021).

2. [Электронный ресурс]. URL: https://tass.ru/ekonomika/4546253 (дата обращения: 15.04.2021).

3. Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // Собрание законодательства РФ. 25.03.2019. № 12, ст. 1224.

4. [Электронный ресурс]. URL: https://www.audar-info.ru/na/article/view/type_id/15/doc_id/59252/ (дата обращения: 15.04.2021).

5. [Электронный ресурс]. URL: http://www.inhope.org/tns/resources/ statistics-and-infographics/statistics-and-infographics-2014.aspx. (дата обращения: 15.04.2021).

6. [Электронный ресурс]. URL: http://www.eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_9014.pdf (дата обращения: 15.04.2021).

7. Соборнов П.Е. История Органов внутренних дел // Директ-Медиа. М., 2020. 305 с.

8. [Электронный ресурс]. URL: https://web.archive.org/web/20131005061529/http://www1.icsi.berkeley.edu/~nweaver/UlbrichtCriminalComplaint.pdf (дата обращения: 15.04.2021).

9. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 15.04.2021).

***В.С. Черкасов,*** *преподаватель кафедры оперативно-разыскной и административной деятельности Владивостокского филиала Дальневосточного юридического института МВД России, г. Владивосток*

## ЭТАПЫ РАЗВИТИЯ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ ОТНОШЕНИЙ ПОД ВОЗДЕЙСТВИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Повсеместное внедрение информационных технологий привело к тому, что большой объем данных о деятельности человека сохраняется на централизованных информационных системах и электронных носителях. Для правоохранительных органов появились новые источники получения сведений, имеющих значение для уголовного дела. Адаптация уголовного досудебного производства к современным информационным технологиям представляет собой долгосрочный процесс, состоящий из трех основных этапов.

К первому этапу относится процесс ***утверждения внедрения информационных технологий как приоритетного направления науки уголовного процесса и законодательного регулирования***. Данный этап сопровождается нор-

мативным закреплением информационных технологий и смежных категорий в УПК РФ и других нормативных правовых актах, а также появлением многочисленных научных трудов в названной сфере.

Законодательное регулирование вопросов, связанных с внедрением в классическую модель уголовно-процессуальных средств доказывания информационных технологий, является достаточно молодым явлением для уголовного процесса. Данный процесс берет свое начало с введением в 2010 г. следственного действия «получение информации о соединениях между абонентами и (или) абонентскими устройствами», предусмотренного ст. 186.1 УПК РФ, а также с введением соответствующего понятия в ст. 5 п. 24.1. УПК РФ [1].

Последняя поправка была внесена в 2018 г. В УПК РФ была добавлена ст. 164.1 «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий» [2].

Научные исследования, полностью посвященные проблемам использования информационных технологий в уголовном судопроизводстве, начали появляться с 2010 г. В качестве примеров можно привести диссертационные исследования Н.А. Зигуры «Компьютерная информация как вид доказательств в уголовном процессе» (Челябинск, 2010) [6], В.Ю. Стельмах «Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие» (Екатеринбург, 2013) [9], П.С. Пастухова «Модернизация уголовно-процессуального доказывания в условиях информационного общества» (Москва, 2015) [8].

В настоящий момент исследования по внедрению информационных технологий в уголовное судопроизводство многочисленны и является одним из самых динамично-развивающимся направлением уголовно-процессуальной науки.

Так, С.В. Зуев отмечает, что научные исследования осуществляются по следующим направлениям [7]:

1. Разработка теоретических основ и научного обоснования системы информационного обеспечения уголовного процесса.

В данном направлении выделяются следующие подразделы:

– 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 удобной и надежной технологии удостоверения процессуального документа любым участником уголовного процесса вместо его обычной подписи;

– разработка пилотного проекта «Электронное уголовное дело» и апробация его в отдельных субъектах Российской Федерации;

– широкое применение дистанционных форм проведения процессуальных действий на любой стадии уголовного судопроизводства, 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.

2. Внедрение в классическую модель уголовно-процессуальных средств доказывания «электронных доказательств».

В данный раздел входят вопросы преобразования процесса собирания, проверки и оценки доказательств как структурных элементов доказывания. Определения природы, сущности и места «электронных доказательств» в модели уголовно-процессуальных доказательств. Совершенствование уголовно-процессуальных гарантий соблюдения прав человека и гражданина при осуществлении собирания «электронных доказательств».

3. Технико-криминалистическое обеспечение использования информационных технологий в уголовно-процессуальной деятельности.

Перечисленные направления являются примерными и их перечень может быть дополнен.

Следующим этапом интеграции информационных технологий в уголовное судопроизводство является ***широкое использование электронной информации и информационных технологий в производстве по уголовным делам.*** Представляется, что именно на данном этапе развития находится российское уголовное судопроизводство.

В качестве аргумента в пользу обозначенной позиции можно привести наличие многочисленных решений высших судебных инстанций по различным вопросам собирания «электронных доказательств»: Определение Конституционного Суда РФ от 26.01.2017 № 204-О [3], в котором рассматриваются практические вопросы изъятия электронных носителей и копировании с них информации; Определение Конституционного суда РФ от 25 января 2018 г. № 189-О [4], в котором рассматриваются вопросы соблюдения права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при производстве следственных действий в отношении электронных носителей информации; Постановление Пленума Верховного Суда РФ от 30.06.2015 № 29 «О практике применения судами законодательства, обеспечивающего право на защиту в уголовном судопроизводстве» [5], в котором говорится, что обвиняемый, находящийся под стражей или в местах лишения свободы, вправе лично участвовать в судебном заседании с использованием системы видеоконференц-связи, а также иные судебные решения.

По всей видимости, человечество находится на пороге очередной информационной революции, и поэтому следующим этапом развития уголовного судопроизводства станет ***появление и использование в уголовном процессе информации с учетом иных способов ее передачи, обработки и представления.***

Так, 16 июля 2019 г. Илон Маск презентовал технологию «Neuralink», позволяющую подключить мозг живого организма к компьютеру. В ходе проведенных экспериментов обезьяна смогла управлять компьютером, не прикасаясь к его органам управления (силой мысли). Илон Маск рассчитывает в ближайшее время получить разрешение на производство экспериментов с человеком и начать внедрение технологии [10].

Таким образом, процесс внедрения информационных технологий в уголовное судопроизводство позволяет выделить три основных этапа:

1. Утверждение внедрения информационных технологий как приоритетного направления науки уголовного процесса и законодательного регулирования.

2. Широкое использование информации в электронном виде, а также информационных технологий в производстве по уголовным делам.

3. Появление и использование в уголовном процессе информации с учетом иных способов ее передачи, обработки и представления.

Под воздействием информационных технологий законодатель продолжает реформировать уголовное досудебное производство. Активно ведутся научные исследования. Уголовно-процессуальные отношения находятся на этапе широкого использования информации в электронном виде, а также информационных технологий в производстве по уголовным делам.

**Список литературы**

1. Федеральный закон от 01.07.2010 № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2010. 07 июля.

2. Федеральный закон от 27.12.2018 г. № 533-ФЗ «О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуального кодекса Российской Федерации» // Российская газета. 2018. 31 декабря.

3. Определение Конституционного Суда РФ от 26.01.2017 № 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» // Доступ из СПС «КонсультантПлюс».

4. Определение Конституционного суда РФ от 25 января 2018 г. № 189-О «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 // Доступ из СПС «КонсультантПлюс».

5. Постановление Пленума Верховного Суда РФ от 30.06.2015 № 29 «О практике применения судами законодательства, обеспечивающего право на защиту в уголовном судопроизводстве» // Российская газета. 2015. 10 июля.

6. Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе: дисс. … канд. юрид. наук. Челябинск, 2010. 234 с.

7. Зуев С.В. Цифровая среда уголовного судопроизводства: проблемы и перспективы // Сибирский юридический вестник. 2018. № 4. С. 118-123.

8. Пастухов П.С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: автореф. дисс. … д-ра юрид. наук. М., 2015. 64 с.

9. Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: дисс. … канд. юрид. наук. Екатеринбург, 2013. 240 с.

10. Neuralink нейроинтерфейс для чтения мыслей и управления компьютерами. [Электронный ресурс]. URL: https://www.popmech.ru/science/493952-neuralink-neyrointerfeys-dlya-chteniya-mysley-i-upravleniya-kompyuterami/#part0 (дата обращения: 10.08.2019).

***Б.Б. Шавыркин,*** *старший преподаватель кафедры юридического менеджмента Донбасской юридической академии, г. Донецк, ДНР*

## ТЕХНОЛОГИЯ 3D-ПЕЧАТИ В КОНТЕКСТЕ ПРОБЛЕМЫ КОНТРОЛЯ ЗА ОБОРОТОМ И ПРИМЕНЕНИЕМ 3D-ОРУЖИЯ

**Актуальность проблемы.** Особая важность данного вопроса в условиях цифровизации обусловлена не только традиционными причинами роста преступлений с применением огнестрельного оружия, а также постоянно существующим интересом населения к оружию, как средству самообороны. Акту-

альность данной проблемы в условиях цифровизации обусловливается в первую очередь легкостью изготовления оружия путем новейшей технологии 3D-Printing.

**Анализ предшествующих исследований и публикаций.** Вопросам государственной политики в сфере оборота оружия посвящены работы российских правоведов-практиков и сотрудников МВД, таких как И.А. Кузнецовой [1], А.В. Кокина [2], А.Е. Шалагина, М.Ю. Гребенкина [3] и др. Однако новые условия оборота оружия выявили специфические и до конца неурегулированные проблемы, что обусловливает необходимость дальнейших исследований в указанном направлении.

**Целью исследования** является анализ и систематизация информации об обороте, контроле и применении 3D-оружия на основе уже существующих нормативно-правовых актов. Поиск решения о том, законно ли изготавливать и применять оружие технологии 3D-Printing в качестве самообороны. Показать опасный аспект технологии 3D-Printing в изготовлении оружия.

**Основное содержание.** XXI век справедливо считают веком глобализации и прогрессивных технологий, поскольку инновации в различных сферах жизнедеятельности общества появляются так часто, что невозможно за всем уследить. Многие из них сложны в изготовлении, однако весьма популярны.

Показательным примером является технология 3D-Printing, а именно огнестрельное оружие, изготовленное при помощи данной технологии. Первое в мире работающее огнестрельное оружие, напечатанное на 3D-принтере, было представлено в 2013 г. американцем Коди Уилсоном. Оружие, названное Liberator и представляющее собой аналог пистолета, не имело привычного всем вида, однако уже спустя полтора года был выпущен полноценный трехмерный пистолет Colt M 1911. С тех пор технология печати оружия только совершенствуется,и вполне обоснованно начала представлять угрозу для общества. Ведь понятно, что распространение столь сложных, а потому дорогих принтеров вопрос не самого ближайшего будущего. Но стоит отметить тот факт, что изготовление оружия на 3D-принтере заинтересовало не только простых интернет-

пользователей, но и профессиональные корпорации, которые специализируются на создании оружия и техники для оборонных нужд [4]. Этот факт предполагает, что продажа подобных изделий вскоре тоже станет возможна.

Таким образом, когда технология будет отработана, оружие, изготовленное с помощью 3D-принтера, будет гораздо дешевле оружия, изготовленного классическим способом. Появится возможность приобретения отличного, эффективного и доступного средства самообороны. То есть оно де-факто станет так называемым «гражданским оружием» — оружием, предназначенным для использования гражданами в целях самообороны, для занятий спортом и охоты. Гражданское огнестрельное оружие должно исключать ведение огня очередями и иметь емкость магазина (барабана) не более 10 патронов.

Одновременно с этим законодательство стран, за исключением США, не предполагает узаконивание оружия, напечатанного на 3D-принтере. Кроме того, во многих странах изготовление любого оружия самостоятельно — преступление, регламентированное Уголовным кодексом. Иными словами, во многих странах правовой статус 3D-оружия такой же, как и у самодельного оружия. Производить, хранить, продавать и передвигаться с ним нельзя [5]. В США же легализация 3D-оружия стала возможна, потому что в этой стране легализовано изготовление самодельного оружия.

Однако, с другой стороны, касательно 3D-оружия, Нижняя палата Конгресса Соединенных Штатов Америки проголосовала за продление действия Акта об оружии, которое нельзя выявить с помощью металлодетектора (Undetectable Firearms Act) на 10 лет. Конгрессмены поспешили утвердить продление срока действия, чтобы преступники не получили шанс проносить пластиковое оружие в государственные здания [6].

Как показывают события, происходящие в Соединенных Штатах Америки, меры большинства стран обоснованные, поскольку напечатанное оружие не имеет идентификационного номера и идентификационной карты, следовательно, невозможно установить его владельца и отследить подобное оружие. К вопросам идентификации добавляется то, что, например, после выстрела

из пистолета Liberator ствол и другие части которого (за исключением гвоздя-ударника) изготовлены из пластика, на пулях следы ствола оружия не отобразятся по причине того, что материал оболочки пули более твердый, чем материал ствола. Исключением может быть статический след металлического гвоздя-ударника на капсюле гильзы, да и то только если он не пробьет металл капсюля насквозь [2].

Кроме того, в 3D-оружии содержится большое количество пластика и лишь немного металла для соединения элементов и изготовления бойка, значит, его не смогут обнаружить металлоискатели. Данному факту также способствует и внешний вид оружия, внешне оно может быть похоже на безобидную детскую игрушку, но несет в себе скрытую опасность. Ввиду особенностей внешнего вида данного оружия возможно использование злоумышленниками детей при транспортировке такого оружия, чтобы вызвать как можно меньше подозрений со стороны правоохранительных органов [5].

В данном контексте интересно и то, что сама технология 3D-Printing, используемая в подобных целях, является опасной. Тому существуют недавние печальные подтверждения.

1 октября 2017 г. совершено массовое убийство в Лас-Вегасе на 32 этаже гостинично-развлекательного комплекса. Преступник использовал полуавтоматическую винтовку, переоборудованную в автомат с помощью обычных деталей, купленных в магазине. Спустя почти год в интервью «USA Today» владелец компании по 3D-печати рассказал о клиенте, который хотел при помощи пластиковой детали превратить полуавтоматическую винтовку в автомат, то есть применить такую же технологию, но с использованием обычного 3D-принтера [5].

Таким образом, с криминалистической точки зрения интерес представляет применение технологии 3D-печати для изготовления «гибридного» огнестрельного оружия, в котором комбинируются детали от стандартных образцов стрелкового оружия и напечатанные на аддитивном принтере. Наиболее известным примером подобного оружия является самозарядный пистолет Shuty-9 MP1 ка-

либра 9x19, созданный американским плотником Дервудом. Автоматика пистолета основана на использовании энергии отдачи свободного затвора. Данный пистолет состоит из следующих пластиковых элементов: рамки, затворной коробки, затвора, магазина емкостью 9 патронов и приемника магазина. Металлическими являются несколько деталей от винтовки AR15, ствол пистолета Glock, передняя часть затвора, курок, ударник, пружины и несколько винтов. Гибридизация позволила существенно повысить прочностные и боевые характеристики изначально ненадежного пластикового оружия. По информации его создателя, из пистолета уже отстреляно более 800 патронов, а пластиковая конструкция позволяет выстреливать два магазина подряд, после чего для продолжения стрельбы требуется незначительное время для снижения температуры разогретого пластика [2].

Естественно, главной задачей со стороны криминалистического исследования оружия, созданного с применением 3D-печати, будет решение вопроса о его отнесении к огнестрельному оружию. При решении этого вопроса обязательно должны быть выявлены критерии (признаки), присущие огнестрельному оружию: оружейность, огнестрельность, надежность [2]. «Гибридное» огнестрельное оружие отвечает всем этим требованиям, а, следовательно, может быть отнесено к огнестрельному.

**Выводы.** На основе проведенного исследования можно заключить:

1. В последние несколько лет рассматриваемые технологии достигли достаточно высокого уровня. Оборудование, то есть 3D-принтеры (аддитивные принтеры), которое изначально позиционировалось как промышленное, постепенно стало доступно для домашнего применения. Сегодня бытовой настольный принтер с легкостью справляется с печатью сложных механизмов. Помимо простых вещей, современные аддитивные принтеры позволяют в домашних условиях изготавливать дизайнерскую обувь, инженерные инструменты и даже квадрокоптеры. 3D-печать огнестрельного оружия оставалась лишь вопросом времени, и сегодня она стала реальностью [2].

2. Технология 3D-печати уже активно используется во всех отраслях жизни общества.

3. Сейчас 3D-оружие — слабая угроза нашему обществу. Однако технологии не стоят на месте. Распространяется гибридный способ: часть оружия печатается на принтере, часть его — металлическая. В США это довольно популярная схема, потому что запчасти винтовок не отслеживаются; можно безнаказанно делать почти боевое огнестрельное оружие.

4. Кроме того, принтер позволяет модифицировать оружие. В связи с чем в законе следует определить и постоянно дополнять понятие оружия и перечислить его конкретные виды и части, на которые распространяется либо не распространяется действие соответствующих правовых норм [1, 7].

5. Для уменьшения динамики изменения законодательства, улучшения его стабильности и устранения пробелов в нем нужно рассмотреть опыт зарубежных стран. В частности, США, где действует Акт об оружии, которое нельзя выявить с помощью металлодетектора. При рассмотрении этого вопроса важно и необходимо адаптировать данное законодательство под условия нашей Республики.

## Список литературы

1. Кузнецова И.А. Проблемы понятия «оружие». Гражданско-правовой аспект // Вестник Челябинского государственного университета. 2010. Т. 9. № 2. С. 79-91. [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/ problemy-ponyatiya-oruzhie-grazhdansko-pravovoy-aspekt (дата обращения: 16.03.2019).

2. Кокин А.В. 3D-оружие и перспективы его криминалистического исследования // Теория и практика судебной экспертизы. 2017. Т. 12. № 2. С. 34-41. [Электронный ресурс]. URL: https://www.tipse.ru/jour/article/view/307/ 309# (дата обращения: 16.03.2019).

3. Шалагин А.Е., Гребенкин А.Ю. Незаконный оборот оружия и его предупреждение. [Электронный ресурс]. URL: https://cyberleninka.ru/

article/v/nezakonnyy-oborot-oruzhiya-i-ego-preduprezhdenie (дата обращения: 16.03.2019).

4. Бяширов Н.Д., Салаватов А.Т. Актуальные вопросы применения и исследования 3Д оружия // Общественные и экономические науки. Студенческий научный форум: электр. сб. ст. по мат. V междунар. студ. науч.-практ. конф. № 5 (5). [Электронный ресурс]. URL: https://nauchforum.ru/archive/SNF_social/5(5).pdf (дата обращения: 16.03.2019).

5. Огилец Д.В. Скачал, распечатал, застрелил. Так ли опасно 3D-оружие? [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/nezakonnyy-oborot-oruzhiya-i-ego-preduprezhdenie (дата обращения: 16.03.2019).

6. Сириенко О.С. Конгресс США продлил запрет на 3D-печать оружия на 10 лет. [Электронный ресурс]. URL: http://3dwiki.ru/kongress-ssha-prodlil-zapret-na-3d-pechat-oruzhiya-na-10-let/ (дата обращения: 16.03.2019).

7. Временное положение о порядке регистрации, хранения и ношения нарезного боевого огнестрельного оружия и боеприпасов к нему: Закон Донецкой Народной Республики от 09.04.2015 № 5-6. [Электронный ресурс]. URL: http://smdnr.ru/wp-content/uploads/2016/06/5-6.pdf (дата обращения: 16.03.2019).

***Н.В. Шепель**, к.ю.н., доцент кафедры уголовного процесса Калининградского филиала Санкт-Петербургского университета МВД России, г. Калининград*

## ПРОБЛЕМЫ ПРАКТИКИ ПРИВЛЕЧЕНИЯ СОТРУДНИКОВ ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКИХ ПОДРАЗДЕЛЕНИЙ В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

На сегодняшний день одним из приоритетных направлений деятельности правоохранительных органов Российской Федерации является борьба с преступлениями, совершаемыми с применением информационных технологий.

В связи с резко возросшим количеством в 2020 г. указанных видов преступлений органы внутренних дел Российской Федерации последовательно наращивают усилия в данной области. Так, по статистическим данным МВД РФ, в 2020 г. зарегистрировано более 510 тысяч преступлений, совершенных с использованием информационных технологий, что на 73,4% больше, чем в 2019 г., 98,6% такого рода преступлений выявляются органами внутренних дел [5].

Учитывая актуальность проблемы и практику расследования преступлений, совершаемых с применением информационных технологий, нередко возникают объективные сложности в расследовании, в том числе в использовании специальных знаний, помощи специалистов при проведении следственных действий, назначении и проведении компьютерных экспертиз. В итоге остаются неустановленными либо не подтвержденными проводимыми впоследствии экспертными исследованиями ключевые обстоятельства по уголовным делам данной категории. Еще раз подчеркнем, что для проведения исследования средств компьютерной техники и информации необходимо привлекать грамотных специалистов, которые имеют определенные знания и умения в данной области [2, с. 882].

Следует отметить, что обязательное участие специалиста при производстве следственных действий, сопровождающихся изъятием электронных носителей информации, закреплено в ч. 2 ст. 164.1 Уголовно-процессуального кодекса Российской Федерации.

Реализация такого подхода на практике неизбежно привела к тому, что в большинстве случаев при производстве следственных действий с изъятием электронных носителей информации, таких как осмотр, выемка, обыск, в качестве специалистов привлекаются эксперты отделов компьютерных экспертиз Экспертно-криминалистических центров МВД России по субъектам РФ. Безусловно, указанное обстоятельство имеет ряд положительных аспектов, а именно, качество проведенных следственных действий, осведомленность о специфике преступного поведения по данной категории дел, о преступных целях, какие возможны способы оказания противодействия в ходе проведения след-

ственных действий, повышение практического опыта самого эксперта в роли специалиста и т.д.

Однако, как уже было отмечено, с резким ростом за последнее время преступлений, совершаемых с применением информационных технологий, закономерно возросло и количество компьютерных экспертиз, проводимых в экспертно-криминалистических подразделениях органов внутренних дел. Данное обстоятельство в свою очередь отразилось на увеличении нагрузки на экспертов и сроках проведения экспертиз. Численность штата экспертов отдела компьютерных экспертиз ЭКЦ МВД России по субъектам РФ, как правило, достаточно мала, в среднем 5-7 экспертов, в зависимости от регионов. По статистическим данным экспертно-криминалистических подразделений МВД России на одного эксперта в 2020 г. пришлось в среднем 60-70 заключений[45] (при норме 30 экспертиз и исследований в год) [3]. Обозначенная нагрузка сказывается и на очередности проведения исследований, от поступления материалов до его исполнения в среднем приходится три месяца.

Возникновение данных проблем, по нашему мнению, представляется вполне закономерным. Нецелесообразно с такой нагрузкой проведения компьютерных экспертных исследований привлекать для каждого следственного действия, связанного с изъятием электронных носителей информации экспертов отдела компьютерных экспертиз Экспертно-криминалистических центров МВД России по субъектам РФ в качестве специалистов.

В свою очередь, судами была выработана позиция, в соответствии с которой изъятие электронного носителя информации в ходе обыска или выемки может правомерно осуществляться без участия специалиста, если изъятие не представляет сложности и не требует специальных знаний и навыков.

Так, Первомайским районным судом города Новосибирска по делу о нарушении правил дорожного движения повлекшее по неосторожности причинение тяжкого вреда здоровью человека (ч. 1 ст. 264 УК РФ) был признан

[45] В качестве приведенных сведений указаны данные ЭКЦ УМВД России по Калининградской области и Алтайскому краю за 2020 год.

несостоятельным довод подсудимого и его защитника о недопустимости доказательства — протокола осмотра места происшествия по изъятию видеозаписи. Аргумент защиты был в получении доказательства в нарушение требований уголовно-процессуального закона, а именно в отсутствии специалиста, так как ст. 164.1 УПК РФ предусматривает обязательное его участие при изъятии электронных носителей информации. При этом суд, ссылаясь на нормы ч. 5 ст. 164 УПК и ст. 168 УПК РФ, указал, что следователь вправе привлечь к участию в следственном действии специалиста, но не обязан. Не соглашаясь с мнением защитника, суд исходил из того, что следователь не произвел никаких действий, требующих специальных знаний в какой-либо отрасли [4].

Новые требования, методы и подходы в практике борьбы с преступлениями, совершаемыми с применением информационных технологий, требуют решения проблем привлечения и выбора специалиста [1, с. 149]. Следователю необходимо предоставить право, а не обязанность привлечения специалиста для изъятия электронных носителей информации. Кроме того, в качестве специалиста возможно привлекать не только экспертов экспертно-криминалистических центров органов внутренних дел, но и сотрудников организаций, в профессиональные обязанности которых входит работа с компьютерной техникой и информационными технологиями, наличие у них диплома о завершении соответствующего вуза по профилю и наличия практического опыта работы с электронными носителями информации.

## Список литературы

1. Лазарева Л.В. О доказывании преступлений в сфере информационных технологий с использованием специальных знаний // 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 / отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул: Изд-во Алт. ун-та, 2020. 276 с.

2. Лантух Э.В., Ишигеев В.С., Грибунов О.П. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации // Всероссийский криминологический журнал. Иркутск. 2020. Т. 14. № 6. С. 882-890.

3. О вопросах организации деятельности экспертно-криминалистических центров органов внутренних дел: приказ МВД России от 30 мая 2003 г. № 366 // Доступ из справ.-правовой системы «КонсультантПлюс».

4. Приговор Первомайского районного суда города Новосибирска № 1-443/2019 1-93/2020 от 25 мая 2020 г. по делу № 1-153/2019. [Электронный ресурс]. URL: http://www.sudact.ru (дата обращения: 30.03.2021).

5. Состояние преступности в Российской Федерации за январь-декабрь 2020 г.: краткий анализ состояния преступности. [Электронный ресурс]. URL: <http://www.mvdinform.ru/МВД — Статистика> (дата обращения 23.03.2021).

***В.А. Шурухнов,*** *к.ю.н., доцент, старший преподаватель кафедры предварительного расследования Московской академии Следственного комитета Российской Федерации, г. Москва*

## СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Развитие научно-технического прогресса во всем мире на сегодняшний день коснулось практически всех сфер жизни общества. Было бы наивным предполагать, что изменения, происходящие в данной области, остались незамеченными криминальными структурами. Отсутствие бюрократических препятствий, наблюдаемых при внедрении современных информационных технологий в практическую деятельность правоохранительных органов и других систем государства, позволяет криминальным структурам в кратчайшие сроки

приспосабливать для своих нужд самые передовые технологии для достижения преступного результата и извлечения сверхприбыли при реализации преступной деятельности, не считаясь с территориальными ограничениями ее реализации.

На сегодняшний день проблемы информационных технологий, применяемых и используемых в качестве орудий и средств преступной деятельности, обозначаются на самом высоком уровне. Президент РФ отметил, что «за последние шесть лет число преступлений в ИТ-сфере выросло в десять раз. Понятно, сами технологии быстро развиваются, мы за ними не успеваем». По словам президента, «важно своевременно информировать людей о способах защиты от мошенников, наладить более четкое взаимодействие правоохранительных органов с банковским сообществом, интернет-провайдерами и операторами сотовой связи» [1].

Серьезные опасения в области применения информационных технологий при совершении преступлений вызывают у руководителей практически всех правоохранительных структур государства, которые задействованы в процессе борьбы, с рассматриваемыми видами преступлений.

Так, по данным представителей Следственного комитета, в России за последние семь лет уровень киберпреступности поднялся в 20 раз, действия злоумышленников в этой сфере становятся все агрессивнее. Сегодня каждое седьмое преступление в России совершается с помощью информационных технологий или в киберпространстве, и число таких преступлений продолжает расти [2].

Генеральный прокурор Российской Федерации заявил, что за последние 5 лет число преступлений, связанных с киберпреступностью, возросло в 25 раз (в 2019 г. — 294 тыс.), особенно с учетом низкой их раскрываемости (25%). В первом полугодии текущего года негативная тенденция лишь усилилась. Зафиксирован рост на 92% (225 тыс.). Причем это касается деятельности всех правоохранительных органов, поскольку новые технологии все чаще выступают средством совершения самого широкого круга преступлений, от хищений

денежных средств с расчетных пластиковых карт до угроз критической инфраструктуре страны и обеспечению ее безопасности [3].

Анализ судебно-следственной практики позволяет сделать выводы, что только за последние два года темпы роста преступлений с применением и использованием информационно-телекоммуникационных технологий увеличились и стали носить угрожающий характер. Так, по данным МВД России, в январе-декабре 2019 г. было зарегистрировано более 294 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что почти на 70% больше, чем за аналогичный период прошлого года. Половина таких преступлений совершается с использованием сети «Интернет», а более трети — средств мобильной связи. В 2020 г. число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети «Интернет» — на 91,3%, при помощи средств мобильной связи — на 88,3% [4].

Такое положение вполне объяснимо. В процесс реализации преступлений с использованием информационно-телекоммуникационных технологий активно включились организованные преступные формирования, сущность деятельности которых носит высокоорганизованный характер, в том числе террористической и экстремистской направленности, а их уровень определяется транснациональным характером реализации преступной деятельности. Это обусловлено тем, что для повышения эффективности уровня своей преступной деятельности активно используются компьютерно-технические средства и телекоммуникационные сети и, самое главное, их скрытые возможности («темный Интернет» (DarkNet), криптовалюта и т.п.). Вся совокупность современных средств и технологий позволяют не только осуществлять процесс координации деятельностью формирований и их структурных подразделений, функционирующих по всему миру, активно вербовать их членов, но и достаточно быстро и без серьезных проблем и потерь осуществлять финансовые операции в любой точке мира.

Кроме этого, технические средства и информационные технологии используются в качестве орудий и средств совершения не только корыстных преступлений, но и более тяжких, таких как терроризм и экстремизм.

Приходится констатировать, что такая ситуация в области роста преступлений, связанных с применением современных информационных и телекоммуникационных технологий, в свою очередь, обусловливает рост организованной преступной деятельности, которая активно и повсеместно использует возможности современных информационных и телекоммуникационных технологий. Например, в 2019 г. организованными группами или преступными сообществами в России совершено 15,6 тыс. тяжких и особо тяжких преступлений (+3,1%), а их удельный вес в общем числе расследованных преступлений этих категорий увеличился с 7,1% в январе-декабре 2018 г. — до 7,4%. В 2020 г. организованными группами или преступными сообществами совершено 17,0 тыс. тяжких и особо тяжких преступлений (+8,6%), причем их удельный вес в общем числе расследованных преступлений этих категорий вырос еще с 7,4% в январе-декабре 2019 г. — до 7,8% [4].

Характер принимаемых мер и их результатов в рассматриваемой сфере указывает на необходимость реализации комплексного подхода, направленного на противодействие преступлениям, совершаемым с применением современных информационных технологий. Представляется, что в системе реализации мер такого комплексного подхода должны быть задействованы все правоохранительные органы, на уровне активного взаимодействия с учеными и специалистами, активно ведущими исследования в рассматриваемых сферах, а его результаты должны активно внедряться в практическую деятельность правоохранительных органов.

Учитывая создавшееся положение, Министр внутренних дел Российской Федерации уже по итогам заседания коллегии, которая прошла в ноябре 2019 г., принял решение о создании в структуре Министерства подразделений, которые будут специализироваться на противодействии преступлениям, совершаемым с использованием IT-технологий. Глава МВД России подчеркнул, что эти но-

вые подразделения будут сформированы по отраслевому принципу в пределах имеющейся штатной численности как в центральном аппарате Министерства, так и в территориальных органах внутренних дел [5].

Активную работу в разработке и внедрении данного решения и других аналогичных мер должны принять ученые и специалисты в рассматриваемой сфере. В рамках реализации комплексного подхода ими должен осуществляться постоянный мониторинг появления новых и совершенствования уже существующих способов, орудий и средств совершения преступлений, с применением информационных технологий, выявление проблем и недостатков в области правого, научного и практического обеспечения деятельности по раскрытию и расследованию рассматриваемых видов преступлений.

Следует отметить, что такая деятельность уже ведется достаточно успешно на протяжении длительного времени и, учитывая указанные обстоятельства, учеными и специалистами разрабатываются [6], совершенствуются и внедряются методические и практические рекомендации [7, 8] выявления, раскрытия и расследования преступлений, совершаемых с применением информационных технологий, учитывая характер изменений и активного использования высоких технологий в повседневной жизни общества и преступной среде.

В современных условиях развития научно-технического прогресса наиболее приемлемой и необходимой в области противодействия преступлениям, совершаемым с применением информационных телекоммуникационных технологий, особенно организованными преступными формированиями, сегодня была бы активная прогностическая деятельность ученых и специалистов, реализуемая в целях разработки научных положений и создании на их основе практических рекомендаций, по борьбе с преступлениями рассматриваемого характера правоохранительными органами. Такая деятельность в условиях активной разработки и внедрения новых информационных и телекоммуникационных систем и технологий их применения позволила бы сформировать систему активного взаимодействия всех государственных структур, в том числе и с зарубежными заинтересованными учреждениями, на уровне взаимовыгодного сотрудниче-

ства. Результаты такой деятельности способствовали бы снижению уровня преступности в сфере IT-технологий и явилось бы существенным фактором не только выявления и пресечения, но и предупреждения и профилактики рассматриваемых видов преступлений. Особенно необходимой в этой сфере видится такая деятельность в области противодействия преступлений, совершаемых организованными преступными формированиями, в том числе на транснациональном уровне.

## Список литературы


1. Путин словами «мы не успеваем» объяснил рост числа преступлений в ИТ. [Электронный ресурс]. URL: https://www.rbc.ru/politics/03/03/2021/603f6ae59a7947b29b0e9b18 (дата обращения: 19.04.2021).
2. В СК заявили о росте киберпреступности в России за семь лет в 20 раз. [Электронный ресурс]. URL: https://www.rbc.ru/rbcfreenews/6000f7b39a7947863c0244d2 (дата обращения: 19.04.2021).
3. Генпрокурор России Игорь Краснов провел совещание по теме борьбы с преступлениями, связанными с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий. [Электронный ресурс]. URL: https://genproc.gov.ru/smi/news/genproc/news-1880616/ (дата обращения: 19.04.2021).
4. Состояние преступности в Российской Федерации. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 19.04.2021).
5. В МВД России будут созданы новые подразделения по борьбе с преступностью в сфере высоких технологий. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/news/item/18809813 (дата обращения: 19.04.2021).
6. Милованова М.М., Петранцова Т.С. Современные технико-криминалистические средства и возможности при расследовании преступлений // Legal Bulletin. 2020. Т. 5. № 1. С. 57-62.

7. Багмет А.М., Бычков В.В., Скобелин С.Ю., Ильин Н.Н. Цифровые следы преступлений / Следственный комитет Российской Федерации; Московская академия Следственного комитета Российской Федерации. М., 2021.

8. Скобелин С.Ю. Цифровая криминалистика: объект и направление развития // Российский следователь. 2020. № 4. С. 42-44.

***В.Л. Юань,*** *старший преподаватель кафедры уголовного процесса Российского государственного университета правосудия, г. Томск*

## АНАЛИЗ БИОГРАФИЧЕСКИХ СВЕДЕНИЙ ЛИЦ, СКЛОННЫХ К ГРУППОВОЙ МОРАЛИ, В РАМКАХ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ЗЛОУПОТРЕБЛЕНИЙ ДОЛЖНОСТНЫМИ ПОЛНОМОЧИЯМИ

Какие криминалистически значимые закономерности характерны для биографии лиц, злоупотребляющих своими должностными полномочиями (ст. 285 УК РФ)? Лишь на первый взгляд кажущийся умозрительным вопрос на деле позволяет обеспечить следствие научным знанием о характерных (типичных) психологических свойствах таких лиц, об их привычных образах действий, поведенческих шаблонах, что даст преимущество на этапе производства следственных действий, а также об их образе жизни, что поможет спланировать расследование в целом и предупредить стратегию противодействия расследованию со стороны такого обвиняемого [1, с. 237; 2, с. 55-56; 3, с. 167; 4, с. 167].

Ранее проведенные исследования (анализ судебной практики через ГАС «Правосудие» по Томской области за период с 2010-2020 гг.) показали, что чаще всего данное преступление совершают лица, наделенные полномочиями и чья профессиональная деятельность так или иначе связана со службой: служба в правоохранительных органах, военная служба, государственная и муниципальная служба, однако работа в государственном или муниципальном учре-

ждении в силу своей специфики также связана со служением, поскольку корпоративная этика внутри трудовых коллективов там в полной мере эквивалентна корпоративной этике, доминирующей в государственных и муниципальных органах. Необходимо подчеркнуть, что в случае с работниками бюджетных образовательных учреждений речь идет также о просвещении. Все выделенные группы профессий имеют в качестве основного источника денежных средств бюджетный доход.

Для понимания личности контрагента необходимо, в частности, понимание, что в обычной жизни часть граждан руководствуется нормами не общей, а корпоративной этики, что нередко может предопределить неожиданное для человека, незнакомого с этим фактом, поведение контрагента. Так, в рамках правил одной групповой этики написание доносов — это этически спорное поведение, в другой — этически неоднозначное, в третьей — морально-нравственно состоятельное. Следовательно, даже при установлении психологического контакта с участником расследования можно сформировать у последнего негативную установку ввиду чуждости для него норм корпоративной этики, которой руководствуется следователь.

Что касается морально-этических взглядов, то очевидно, что первые три группы (сотрудники правоохранительных органов, сотрудники государственных и муниципальных органов [5, с. 112], военнослужащие) — это ярко выраженные носители групповой этики в силу специфики работы на соответствующих должностях. Если же проанализировать особенности работы такой группы работников в государственных и муниципальных учреждениях (предприятиях), как школьные учителя [6, с. 217, 239], то становится видно, что и они также являются представителями тех, кто следует нормам корпоративной этики, т.е. являются носителями групповой этики. Поскольку из 7 случаев почти половина — это работники сферы просвещения, то это в определенной степени позволяет экстраполировать выводы на всю остальную совокупность.

Если обратиться к анализу профессиональных привычек, то видно, что они не обнаруживают четко выраженной взаимосвязи, поскольку в выборке встре-

чаются лица, имеющие любые из основных профессиональных привычек: работники сферы образования (познавательные профессиональные привычки), военнослужащие (рефлекторные профессиональные привычки), государственные и муниципальные служащие (в выборке встречались участковые лесничие).

Если провести ранжирование биографических фактов в аспекте выраженности связи со склонностью к злоупотреблению должностными полномочиями, то получаются следующие выводы (табл.).

Взаимосвязь биографических фактов с тенденцией к предрасположенности к совершению преступления, предусмотренного ст. 285 УК РФ

| | Выраженная взаимосвязь | Невыраженная взаимосвязь |
|---|---|---|
| Профессиональная деятельность | Служение, просвещение | Сервис, производство, торговля |
| Разновидность источников доходов | Бюджетный | Предпринимательский, договорный |
| Морально-этические взгляды | Групповая мораль и этика | Индивидуальная и коллективистская мораль и этика |
| Профессиональные привычки | Познавательные, рефлекторные, навыковые | - |

Из вышеприведенной таблицы следует, что типичный портрет лица, злоупотребляющего должностными полномочиями, — это сотрудник, занятый в сфере служения обществу, имеющий бюджетный доход, являющийся носителем групповой морали. Стоит отметить, что профессиональные привычки могут быть самыми разными: все они показали выраженную взаимосвязь, следовательно, эту группу биографических фактов надлежит исключить из анализа, поскольку они не дают знания о каких-либо закономерностях.

Относительно корреляции ярко выраженных черт личности с теми или иными биографическими фактами, показавших высоковыраженную или слабовыраженную взаимосвязь, следует отметить следующее:

1. Относительно профессиональной деятельности.

Лица, занятые в сфере просвещения, чаще всего обладают высокими навыками аналитического, абстрактного мышления и работы с информацией [6, с. 83-85, 99]; лица, состоящие на военной или правоохранительной службе, имеют склонность к иерархии и подчинению, и, как правило, имеют сравнительно неплохой уровень физической подготовки [7, с. 24].

2. Относительно разновидности источника доходов.

Лица, имеющие преимущественно доходы из средств государственного или местного бюджета, характеризуются стремлением к стабильности, слабой адаптацией и неуверенностью в себе [8, с. 120-121]. В последнем случае имеется в виду, скорее, заработная плата, а не премиальные выплаты. То есть сказанное характерно для рассматриваемых лиц, у которых заработная плата сопоставимо выше премиальных выплат, и нехарактерно для лиц, у которых ситуация обстоит наоборот.

3. Относительно морально-этических взглядов.

Носители групповой морали (носители норм корпоративной этики, а также члены малых социальных групп) предрасположены к конформизму, следованию принятым в группе нормам, имеют высокий уровень отражения особенностей, характерной для группы в целом, предрасположенность к агрессии по отношению к окружающим, не входящим в группу [9, с. 21, 46, 63-64, 111].

Несмотря на то, что в основе представленного исследования лежит микровыборка, это позволяет выявить определенные тенденции, которые можно выразить следующим образом: психологический портрет личности лица, злоупотребляющего должностными полномочиями, т.е. использующего свои служебные полномочия вопреки интересам службы из корыстной или иной личной заинтересованности, — это лицо, обладающее высокими навыками аналитического, абстрактного мышления и работы с информацией или склонное к иерархии и подчинению, и, как правило, имеющее неплохой уровень физической подготовки, стремящееся к стабильности, обладающее слабой адаптацией и неуверенное в себе. При этом лицо, предрасположенное к конформизму, следованию принятым нормам корпоративной этики, имеющее высокий уровень отра-

жения особенностей, характерной для его малой социальной группы в целом, предрасположенное к агрессии по отношению к окружающим, не входящим в его малую социальную группу.

Вышесказанное позволяет сделать вывод о необходимости разработки как тактики проведения следственных действий, так и планирования расследования преступления, связанного со злоупотреблениями должностными полномочиями, на основе знания о том, что фактически перед следователем будет лицо, тяготеющее к нормам групповой морали и знакомое с корпоративной этикой в той же степени, как и сам следователь.

**Список литературы**

1. Ведерников Н.Т. Избранные труды. Т. 1. Томск: Изд-во Томского ун-та, 2009. 250 с.

2. Ахмедшин Р.Л. Криминалистическая характеристика личности преступника: природа и содержание // Вестник Томского гос. ун-та. 2004. № 283. С. 55-62.

3. Алексеева Т.А. Криминалистическая структура устной речи // Вестник Томского гос. университета. 2014. № 381. С. 167-170.

4. Юань В.Л. Механизм гомеостаза в системе биографического метода криминалистического исследования личности // Вестник Томского гос. ун-та. 2015. № 399. С. 167-169.

5. Бояркин М.Ю., Долгополова О.А., Зиновьева Д.М. и др. Психологическое и профессиональное благополучие государственных служащих: монография. Волгоград: Изд-во ФГОУ ВПО ВАГС, 2007. 216 с.

6. Ефремова О.И. Психология профессиональной деятельности и личности учителя: учеб. пособие для студентов педагогических институтов. Таганрог: Изд-во Таганрог. гос. пед. ин-та имени А.П. Чехова, 2012. 300 с.

7. Брыкова Е.Ю. Психологическая и личностная готовность к овладению воинскими специальностями: дисс. … канд. психол. наук. 19.00.01 - Общая

психология, психология личности, история психологии (психологические науки). М., 2015. 171 с.

8. Токарева Д.В. Особенности мотивации работников бюджетной сферы (на примере ФГУ «Консультационно-методический центр лицензирования») // Вестник РУДН. Серия Государственное и муниципальное управление. 2015. № 1. С. 119-123; 120-121.

9. Эксакусто Т.В. Основы психологии малых групп и управления коллективом: учебное пособие. Таганрог: Изд-во Южного федерального ун-та, 2016. С. 21, 46, 63-64, 111.

***Т.В. Якушева,*** *к.ю.н., доцент кафедры уголовного процесса и криминалистики АлтГУ, г. Барнаул*

***Л.А. Темиржанова****, к.ю.н., доцент кафедры теории и истории государства и права, конституционного права ЕНУ им. Л.Н. Гумилева, адвокат Коллегии адвокатов города Нур-Султан, советник юстиции в отставке, г. Нур-Султан, Республика Казахстан*

***Ж.А. Жадауова,*** *к.ю.н., доцент кафедры теории и истории государства и права, конституционного права ЕНУ им. Л.Н. Гумилева, г. Нур-Султан, Республика Казахстан*

## АКТУАЛЬНЫЕ ПРОБЛЕМЫ ВОЗМЕЩЕНИЯ УЩЕРБА И ОБЕСПЕЧЕНИЯ ПРАВ ГРАЖДАН В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ РЕСПУБЛИКИ КАЗАХСТАН В СВЕТЕ ПРЕДСТОЯЩЕГО СУДЕБНОГО РЕФОРМИРОВАНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

В настоящее время обозначилась неизбежность цифровой трансформации правоприменительной практики в связи с начавшейся пандемией COVID-19. Так же как и для большинства государств, для Казахстана стал актуальным вопрос осуществления онлайн-правосудия и определения рамок его использования.

По мнению Л.В. Головко, цифровизация в уголовном процессе — это лишь локальная и достаточно рутинная оптимизация некоторых процессуальных форм и институтов, не несущая в себе никаких рисков для традиционного правосудия по уголовным делам [1, с. 19].

В Послании Главы государства Касым-Жомарта Токаева народу Казахстана от 1 сентября 2020 г. «Казахстан в новой реальности: время действий» указано: «В рамках Концепции правовой политики, путем изменения законодательства следует обеспечить баланс между уровнями правовой регламентации. Нынешняя ситуация в стране предъявляет новые требования к правоохранительным органам, которые должны идти навстречу запросам граждан. Критически важно принять новые меры по защите прав человека. Укрепление доверия общества к судам должно стать приоритетной целью» [2].

Также, по мнению Президента страны, «Слышащее государство» — это, по сути, концепция строительства «Справедливого государства». Недостаточно просто слышать и видеть проблемы граждан, главное — правильно и объективно реагировать на них [3].

Полиция должна выявлять преступления, устанавливать причастных лиц, собирать и закреплять улики; прокурор обязан давать независимую оценку собранным доказательствам, пресекать нарушения прав граждан, не допускать вовлечения добросовестных граждан в уголовный процесс, поддерживать обвинение в суде; суд — рассматривать жалобы на действия органов и выносить окончательный вердикт по делу [4]. Соответственно, это сущность предстоящего судебного реформирования и зерно трехзвенной системы.

Абсолютно прав в этом отношении д.ю.н. С. Молдабаев, поясняющий, что «в период рыночных отношений всех нас должно интересовать, сколько «стоят» преступления? Сколько средств тратит правительство на борьбу с преступностью? Насколько реально возмещается вред от преступления потерпевшим, обществу, государству?» [5].

Основными правовыми актами в анализируемой сфере являются Закон Республики Казахстан «О Фонде компенсации потерпевшим» от 10.01.2018 г.

№ 131-VI ЗРК *(с изм. по сост. на 03.07.2020 г.)*, Нормативные постановления Верховного суда РК: «О применении судами законодательства о возмещении морального вреда» № 7 от 27.11.2015 г.; «О практике применения законодательства, регламентирующего права и обязанности лиц, потерпевших от преступлений» № 2 от 24.04.1992 г. с изм. от 22.12.2008 г. № 3 и т.д.

Безусловно, информационные технологии намного облегчили само уголовное судопроизводство как сотрудникам правоохранительной и судебной системы, так и обычным гражданам, пользователям информационных систем, электронные платформы являются удобным инструментом для населения, в том числе и при направлении гражданских исков в порядке уголовного судопроизводства через портал «Судебный кабинет». В судебной системе хорошо зарекомендовала себя информационная база «Төрелік». В 2011-2012 гг. в Казахстане внедрена электронная регистрация всех заявлений и сообщений о преступлениях (КУЗ). С 2015-го внедрен Единый реестр досудебных расследований (ЕРДР). Интеграция аналитической информационной системы суда («Төрелік») и органов прокуратуры (ЕРДР) позволила Верховному суду и Генеральной прокуратуре заработать проекту «Заңдылық».

Проведенный анализ позволил нам обозначить имеющиеся в правоприменительной практике проблемы:

- Несмотря на то, что возмещение вреда потерпевшим с точки зрения современной уголовной политики является одним из важных аспектов восстановления социальной справедливости на практике потерпевшие хоть и взыскали формально причиненный вред с осужденного, ничего не могут у него получить, так как у последнего отсутствуют денежные средства, имущество, соответственно — тупик, замкнутый круг, имущественные права потерпевшего фактически не восстанавливаются.

- Зачастую в правоприменительной практике дознаватель, следователь при производстве досудебного расследования не всегда себя утруждает разъяснениями потерпевшему его прав на предъявление гражданского иска по уголовному делу, что по каждому делу об уголовном правонарушении, причинив-

шем ему материальный ущерб или моральный вред, он может предъявить такой иск. Конечно, при самостоятельном предъявлении такого иска с подачи адвоката или представителя потерпевшего досудебный орган признает его гражданским истцом, подозреваемого гражданским ответчиком и приобщит к делу поданный иск.

- Имеется какое-то предубеждение и страх возможных жалоб от потерпевших у следователей, дознавателей, что в случае детального им разъяснения возможной истребуемой суммы материального ущерба или морального вреда, исходя из среднего показателя правоприменительной практики, или каких-либо предполагаемых перспектив, либо стоимостной разумности требований и т.д., что у потерпевшего возникнут сомнения, якобы в какой-либо «заинтересованности» органа преследования, в том числе и в якобы намеренном снижении запрашиваемых сумм (что тоже небезосновательно и в практике имеются различные жалобы в адрес следователей по указанным основаниям), как потерпевший ведет себя в досудебном и судебном процессе, насколько он адекватен в запрашиваемых суммах. К примеру, имел место в практике следующий случай, когда за причинение средней тяжести вреда здоровью (ст. 107 ч. 1 УК РК — умышленное причинение средней тяжести вреда здоровью) потерпевший в возмещение вреда просил 40 миллионов тенге. Это фактически решение не столько проблем здоровья потерпевшего, но также решение жилищных проблем и т.д. В то же время за две смерти в результате ДТП, учитывая то, что оно совершено по неосторожности, — суды Казахстана в среднем взыскивают в счет компенсации морального вреда от 1 до 5 миллионов тенге и т.д. Но здесь имеется смерть, а там человек жив и требует такую сумму. Да, бесспорно, взыскатель также исходит и из материальной обеспеченности виновного лица, в том числе возможной помощи ответчику его родственниками, родителями и т.д., но не всегда объективно оценивают свои завышенные предъявляемые суммы в счет возмещения морального вреда.

- По составам мошенничества сейчас растет социальная напряженность, поскольку изменилась уголовная политика государства, сам состав мо-

шенничества всегда был граничащим с гражданско-правовыми отношениями, тем более сейчас, учитывая большое количество оправданных судом по данному признаку. Соответственно, при любом имеющемся договоре досудебные органы и прокуратура неумолимо снижают количество предания суду таких уголовных дел, даже если лицо ранее судимо за мошенничество и явно нацелено на дальнейшее развитие своих преступных навыков, сейчас эти мошенники остаются на свободе. И именно в данном формате остались без внимания и защиты правоохранительных органов и судов потерпевшие граждане, им не возмещается фактически ущерб. Если мошеннику не грозит лишение свободы, в любом случае угроза изоляции психологически давит на сознание и заставляет его быстрее найти средства и погасить ущерб, при гражданском же разбирательстве, должник, ответчик расслабляется и взыскание суммы затягивается на долгие годы и в конечном итоге так и они умышленно и не возмещаются. При этом никак мошенник не работает, не имеет якобы средств, имущества, если было, к примеру, решение суда о взыскании задолженности с ИП (индивидуального предпринимателя), то чтобы уйти от выплат, мошенник специально регистрирует ТОО и работает, но при этом не возвращает долг, мотивируя тем, что взыскание было с ИП, а не с ТОО и т.д.

Имея прямой умысел на совершение мошенничества и совершение 7-10 эпизодов, прикрываясь гражданско-правовыми договорами, фактически мошенники уходят от ответственности, разъясняя всем, что у них не было умысла на совершение мошенничества, что у них с потерпевшим были гражданско-правовые отношения, соответственно отсутствует принцип восстановления нарушенных имущественных, гражданских, конституционных прав потерпевших.

Например, многострадальное дело: так, потерпевшая К. в 2013 г. открыла Центр в г. Нур-Султане, который занимается детьми с различными отклонениями в развитии, заболеваниями. В марте 2016 г. К. подала объявление в ОЛХ о том, что ищет дизайнера и планирует ремонт мебели Центра. В октябре 2017 г. А., ранее привлекавшаяся к ответственности за мошенничество, но су-

димость погашена, продолжает фактически свое преступное ремесло, выходя на новый уровень, зарегистрировав ИП с целью материального обогащения путем обмана и злоупотребления доверием, разместила рекламу на сайте ОЛХ о якобы предлагаемых ею дизайнерских услугах и осуществляемом ремонте мебели, при этом не имея офиса, ни материальной базы и т.д. А. созвонилась с К. и предложила ей услуги по дизайну и изготовлению мебели, войдя в доверие, К. уверила последнюю, что изготовит мебель на заказ в короткие сроки. К., находясь в состоянии заблуждения от преступных действий А., осознавая, что своим отказом может лишиться возможности за короткий срок оборудовать Центр развития для детей, не подозревая о корыстных целях А., передала А. денежные средства в сумме 4 000 000 тенге, согласно типовому договору, составленному и разработанному А. В дальнейшем было подано заявление в органы полиции о мошенничестве, досудебное производство проведено, но дело в суд не было предано ввиду отсутствия состава преступления. Необходимо учесть, что по аналогичной схеме развода на удочку А. попалось еще 6 потерпевших, всего семь эпизодов, но везде был договор. Обжалованное действие прокурора следственный суд оставил без изменения.

В дальнейшем гражданка К. взыскала через суд у ИП А. в порядке гражданского судопроизводства понесенную сумму ущерба и морального вреда, но прошло уже 4 года, а К. так и не получила ни копейки, так как ИП не работает, дохода нет. Замкнутый круг. Теперь узнает К., что А. открыла два ТОО и спокойно поживает, но ей не возвращает долг, так как решение суда было в отношении ИП, а не ТОО и т.д.

Таким образом, изменением правоприменительной практики, излишней гуманизацией в отношении некоторых составов преступлений складывается порочная практика ухода от уголовной ответственности явных мошенников и, естественно, абсолютно нарушается социальная справедливость, возникает тупиковая ситуация, ущерб не возмещается, потерпевшие остаются сами по себе со своими проблемами, государство их не защищает и неумолимо растет социальное напряжение.

- Нет установленного принципа достаточности размера компенсации.

- С учетом того, что «при определении размера компенсации судам надлежит исходить из принципов справедливости и достаточности» — жизненная важность блага, бывшего объектом посягательства (жизнь, здоровье, честь, достоинство, свобода, неприкосновенность жилища и т.д.); тяжесть последствий правонарушения (убийство близких родственников, причинение телесных повреждений, повлекших инвалидность, лишение свободы, лишение работы или жилища и т.п.); характер и сфера распространения ложных позорящих сведений в том числе и по соцсетям; жизненные условия потерпевшего (служебные, семейные, бытовые, материальные, состояние здоровья, возраст и др. — субъективной оценки истца о тяжести причиненных ему нравственных, физических страданий и, конечно же, объективной оценки суда о сложившейся ситуации, нет установленной условной градации по запрашиваемым потерпевшим суммам, «разумности» сумм (в совокупности с экспертизами по вреду здоровью, предполагаемых дополнительных операций и т.д.).

Таким образом, очень актуально, чтобы в правовой политике государства уголовная политика совершенствовалась путем объективной, правильной, комплексной, взаимосвязанной коррекции уголовного, уголовно-процессуального, уголовно-исполнительного права, а также само правоприменение должно быть ориентировано на социальную справедливость. Для объективности всегда необходимо мысленно себя ставить на место потерпевшего, либо ассоциировать, а вдруг с близкими родственниками произойдет нечто подобное, вот тогда и отношение сразу меняется, и человек душой болеет за то, чтобы предлагаемая к принятию норма обеспечивала действительно полное восстановление нарушенных прав и интересов.

На основании вышеизложенного полагаем целесообразным рекомендовать следующее, памятуя о том, что каждое дело индивидуально:

- установить для судов и для правоохранительных органов так называемый принцип достаточности размера компенсации (ориентируясь не только

на пожелание истца в уголовном судопроизводстве, но и руководствуясь объективными данными);

- разработать условную градацию по запрашиваемым суммам, «разумности» запрашиваемых потерпевшим сумм исходя из судебной практики (к примеру, по телесным повреждениям, по делам об изнасиловании и т.д.);

- разработать новое Нормативное постановление Верховного Суда РК «О судебной практике средней стоимости возмещения материального ущерба и морального вреда»;

- ввести публичный реестр кибермошенников, публичный реестр злостно уклоняющихся от возмещения ущерба и вреда. Данный реестр создать на базе МВД и КПСиСУ ГП РК, с их фотопортретами, адресами проживания и иной информацией. В базу вносить сведения по всем мошенникам, в отношении которых состоялся судебный акт, вступивший в законную силу, с кратким описанием способа мошенничества *(в США 26 июня 2006 г. начал работу Национальный публичный реестр сексуальных преступников — общеамериканская онлайновая база данных лиц, совершивших сексуальные преступления, к которой присоединились 50 штатов).* В РК подобный реестр следует ввести не только в отношении половых насильников, но и в отношении мошенников и лиц, злостно уклоняющихся от возмещения ущерба и вреда). Данный список лиц с их фото постоянно транслировать на билбордах всей страны и во всех общественных местах: учебных заведениях, государственных органах, частных структурах, чтобы население РК знало мошенников в лицо;

- выпускать социальные ролики, повышать правовую грамотность населения (внедрить учебные занятия по возмещению ущерба, в программу школьного и вузовского обучения);

- создать отдельную отрасль права, к примеру, под названием «Возмещение ущерба и вреда», в которой систематизировать в данной сфере все правовые акты — национальные и международные;

- правоохранительным органам необходимо активизировать праворазъяснительную работу о формах и видах мошенничеств, о возмещении ущерба и вреда о тесном взаимодействии:

- с операторами сотовой связи *(направление голосовых, письменных сообщений);*

- активизировать работу инспекторов полиции по делам несовершеннолетних в организациях образования по профилактике мошенничества среди несовершеннолетних *(лекции, собрания)*;

- проводить наглядную агитацию *(билборды, информация в торговых точках, общественном транспорте)*;

- систематически освещать результаты работы правоохранительных органов по противодействию мошенничеству, по результатам возмещения ущерба и вреда в средствах массовой информации *(создать блок передач на указанную тематику, видеоролики)*.

**Список литературы**

1. Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15-25.

2. Послание Главы государства Касым-Жомарта Токаева народу Казахстана от 1 сентября 2020. Казахстан в новой реальности: время действий. [Электронный ресурс]. URL: http://adilet.zan.kz/rus/docs/K2000002020.

3. Послание Главы государства Касым-Жомарта Токаева народу Казахстана от 1 сентября 2020. Казахстан в новой реальности: время действий. [Электронный ресурс]. URL: https://gkb4-almaty.kz/poslanie-prezidenta-respubliki-kazahstan/

4. Полномочия между полицией, прокуратурой и судом планируют разграничить в Казахстане. [Электронный ресурс]. URL: https://www.zakon.kz/5069801-polnomochiya-mezhdu-politsiey.html

5. Молдабаев С. К вопросу об обновлении уголовного законодательства на основе возмездного принципа // Зангер. 2012. № 3. С. 36.

*Научное издание*

**ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ**
**В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

*Сборник статей XIX Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае», посвященной памяти советского и российского ученого-криминалиста Вениамина Константиновича Гавло, доктора юридических наук, профессора, заслуженного деятеля науки РФ, заслуженного юриста РФ*

Выпуск XVII

Редактирование и подготовка оригинал-макета — *С.И. Тесленко*

Оформление обложки — *Ю.В. Луценко*

ЛР 020261 от 14.01.1997.
Подписано в печать 06.12.2021. Формат 60x84 / 16.
Бумага офсетная. Усл.-печ. л. 29,08.
Тираж 200 экз. Заказ № 476

Издательство Алтайского государственного университета

Типография Алтайского государственного университета:
656049 Барнаул, ул. Димитрова, 66