УДК 347.963
ББК 67.72
П80

Электронные версии книг
на сайте www.prospekt.org

Рецензенты:
Брусницын Л. В., доктор юридических наук, профессор кафедры уголовного процесса, правосудия и прокурорского надзора Московского государственного университета им. М. В. Ломоносова;
Винокуров А. Ю., доктор юридических наук, профессор, ведущий научный сотрудник отдела научного обеспечения прокурорского надзора и укрепления законности в социально-экономической сфере Научно-исследовательского института Университета прокуратуры Российской Федерации;
Качалова О. В., доктор юридических наук, доцент, профессор кафедры уголовно-процессуального права им. Н. В. Радутной Российского государственного университета правосудия;
Быкова Е. В., кандидат юридических наук, ведущий научный сотрудник отдела научного обеспечения проблем прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Научно-исследовательского института Университета прокуратуры Российской Федерации.

П80 Прокурорский надзор за исполнением законов при выявлении, расследовании и предупреждении преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации : монография. — Москва : Проспект, 2022. – 280 с.

ISBN 978-5-392-36095-6

В работе исследованы состояние компьютерной преступности, проблемы ее предупреждения, пресечения, выявления и расследования. Отдельное внимание уделено вопросам квалификации преступлений в компьютерной сфере, основам зарубежного опыта борьбы с киберпреступлениями и международного сотрудничества государств по противодействию компьютерной преступности.

В монографии тщательно изучены деятельность прокурора, обеспечивающая соответствие требованиям законов при организации и осуществлении правоохранительной деятельности, и его участие в международном сотрудничестве в связи с совершением рассматриваемых преступных посягательств.

Законодательство приведено по состоянию на ноябрь 2020 г.

Работа предназначена для широкого круга исследователей, практиков и учащихся организаций высшего образования, интересующихся проблемами противодействия преступлениям в сфере информационно-коммуникационных технологий на современном этапе развития правовой науки.

УДК 347.963
ББК 67.72

Научное издание

Камчатов Кирилл Викторович и др.

ПРОКУРОРСКИЙ НАДЗОР ЗА ИСПОЛНЕНИЕМ ЗАКОНОВ ПРИ ВЫЯВЛЕНИИ, РАССЛЕДОВАНИИ И ПРЕДУПРЕЖДЕНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Монография

Подписано в печать 02.12.2021. Формат 60×90 $^{1}/_{16}$.
Печать цифровая. Печ. л. 17,5. Тираж 1000 (1-й завод 150) экз. Заказ №

ООО «Проспект»
111020, г. Москва, ул. Боровая, д. 7, стр. 4.

ISBN 978-5-392-36095-6

АВТОРСКИЙ КОЛЛЕКТИВ

К. В. Камчатов (руководитель авторского коллектива), заведующий отделом научного обеспечения проблем прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Научно-исследовательского института Университета прокуратуры Российской Федерации (далее — НИИ Университета), кандидат юридических наук — список принятых сокращений, введение, параграф 1.2 (в соавторстве с М. А. Соколовым, авторство не разделено), параграфы 2.2, 3.1–3.5, заключение, список литературы.

Е. А. Архипова, старший научный сотрудник отдела научного обеспечения международного сотрудничества прокуратуры и сравнительного правоведения НИИ Университета, кандидат юридических наук — параграфы 4.1–4.2 (в соавторстве с В. Н. Додоновым, авторство не разделено).

Е. В. Великая, старший научный сотрудник отдела научного обеспечения проблем прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве НИИ Университета — параграф 3.6 (в соавторстве с Решетовой Н. Ю., авторство не разделено).

В. Н. Додонов, ведущий научный сотрудник отдела научного обеспечения международного сотрудничества прокуратуры и сравнительного правоведения НИИ Университета, кандидат юридических наук — параграфы 4.1–4.2 (в соавторстве с Е. А. Архиповой, авторство не разделено).

Н. Ю. Решетова, старший научный сотрудник отдела научного обеспечения проблем прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве НИИ Университета — параграф 3.6 (в соавторстве с Е. В. Великой, авторство не разделено).

М. А. Соколов, заместитель заведующего лабораторией криминологического обеспечения прокурорской деятельности НИИ Универ-

ситета, кандидат юридических наук — параграф 1.2 (в соавторстве с К. В. Камчатовым, авторство не разделено).

М. В. Ульянов, старший научный сотрудник отдела научного обеспечения прокурорского надзора и укрепления законности в сфере федеральной безопасности, межнациональных отношений и противодействия экстремизму НИИ Университета, кандидат юридических наук — параграф 1.1 (в соавторстве с Э. Т. Халиуллиной), параграф 2.1.

Э. Т. Халиуллина, старший научный сотрудник отдела научного обеспечения предупреждения преступности НИИ Университета — параграф 1.1 (в соавторстве с М. В. Ульяновым).

А. И. Халиуллин, научный сотрудник отдела научного обеспечения проблем прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве НИИ Университа — приложение.

СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ

CardToCard — это технология (сервис) перевода денежных средств с карты на карту любого банка по ее номеру, доступная круглосуточно и без выходных. Перевод не идет напрямую между банками, он в обязательном порядке осуществляется через международную платежную систему, к примеру, Visa, MasterCard, отечественная МИР и т.д.

CD-диск (Compact Disc) — оптический носитель информации, процесс записи и считывания информации которого осуществляется при помощи лазера.

CVV (англ. card verification value) — трехзначный код проверки подлинности карты платежной системы Visa.

DDoS-атака (Distributed Denial of Service) — распределенная атака типа «отказ в обслуживании»; хакерская атака на вычислительную систему с целью довести ее до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам) либо этот доступ затруднен.

Flash-карта — запоминающее устройство, использующее в качестве носителя флеш-память и подключаемое к компьютеру или иному считывающему устройству по интерфейсу USB.

IMEI (International Mobile Equipment Identity) — международный идентификатор мобильного оборудования, номер для идентификации телефонов GSM, WCDMA и IDEN, а также некоторых спутниковых телефонов.

IMSI (International Mobile Subscriber Identity) — международный идентификатор мобильного абонента (индивидуальный номер абонента), ассоциированный с каждым пользователем мобильной связи стандарта GSM, UMTS или CDMA.

IP-адрес (Internet Protocol Address — адрес интернет-протокола) — уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP.

MAC-адрес (Media Access Control — управление доступом к среде, также Hardware Address, также физический адрес) — уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.

MAIL (электронная почта, англ. *email, e-mail,* от англ. *electronic mail*) — технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределенной (в том числе глобальной) компьютерной сети. Основным отличием от прочих систем передачи сообщений (например, служб мгновенных сообщений) является возможность отложенной доставки и развитая (и запутанная из-за длительного времени развития) система взаимодействия между независимыми почтовыми серверами.

PayPass (MasterCard Contactless, прежнее название MasterCard PayPass) — это совместимая с EMV бесконтактная технология проведения платежа, основанная на стандарте ISO/IEC 14443, предоставляющая держателям карт MasterCard и Maestro способ совершения оплаты путем близкого поднесения платежной карты или прикосновения ею либо иным платежным инструментом, таким как телефон или брелок для ключей, к считывающему платежному терминалу вместо проведения ею для считывания или вставки ее в терминал.

PIN-код (Personal Identification Number) — персональный идентификационный номер, являющийся секретным кодом карты.

QIWI Кошелек — российский платежный сервис.

СИМ-карта (Subscriber Identification Module) — идентификационный модуль абонента, применяемый в мобильной связи.

СМС-сообщения (Short Message Service — служба коротких сообщений) — технология, позволяющая осуществлять прием и передачу коротких текстовых сообщений с помощью мобильного телефона.

TOR (сокр. от англ. The Onion Router) — свободное и открытое программное обеспечение для реализации второго поколения так называемой луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

URL (Uniform Resource Locator — унифицированный указатель ресурса) — система унифицированных адресов электронных ресурсов, или единообразный определитель местонахождения ресурса (файла).

VoIP (Voice over IP) — телефонная связь по протоколу IP посредством набора коммуникационных протоколов, технологий и методов, обеспечивающих набор номера, дозвон и двустороннее голосо-

вое общение, а также общение по сети Интернет или любым другим IP-сетям.

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

Web-сайт (web — паутина, сеть, site — место, сегмент, часть в сети) — одна или несколько логически связанных между собой веб-страниц, также место расположения контента.

Wi-Fi-роутер — точка доступа, с помощью которой можно создать домашнюю беспроводную сеть с использованием технологии беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11.

ВВЕДЕНИЕ

Расширение сфер применения цифровых коммуникационных технических решений в сфере государственного управления и экономики актуализирует вопросы осуществления противодействия преступлениям, связанным с использованием информационно-телекоммуникационных технологий и компьютерных сетей[1]. Наша страна, как и многие развитые страны, принимает на себя все неизбежные сложности стремительной повсеместной информатизации общественной жизни.

Современные вызовы киберпреступности неоднократно акцентировались в выступлениях руководства Генеральной прокуратуры Российской Федерации. Прежде всего это относится к чрезмерной и наибольшей (по сравнению с другими категориями преступных деяний) динамике данных преступлений.

Так, число преступлений, совершаемых в сфере ИКТ, с 2013 по 2016 г. увеличилось в 6 раз (с 11 тыс. до 66 тыс.). Значительный их рост наблюдался и в 2017 г. (26%, 40 тыс.). По данным статистики, в России за первое полугодие 2017 г. ущерб составил более 18 млн долл. США[2]. Согласно сведениям, представленным на официальном сайте Генеральной прокуратуры Российской Федерации, в 2017 г. почти каждое 20-е преступление совершалось в сфере информационных и телекоммуникационных технологий[3].

За последние 5 лет число таких преступлений возросло в 25 раз (в 2019 г. — 294 тыс.), особенно с учетом низкой их раскрываемости (25%). В первом полугодии 2020 года негативная тенденция лишь

---

[1] Далее «в сфере ИКТ», «в сфере компьютерной информации», «компьютерные преступления», «киберпреступления».

[2] Выступление Генерального прокурора Российской Федерации Ю. Я. Чайки на III Встрече руководителей прокурорских служб государств БРИКС, посвященной вопросам противодействия киберпреступности // Сайт Генеральной прокуратуры Российской Федерации. URL: https://goo.gl/WUsihT (дата обращения: 01.10.2017).

[3] См.: О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий // Сайт Генеральной прокуратуры Российской Федерации. URL: https://genproc.gov.ru/smi/news/genproc/news-1431104 (дата обращения: 15.01.2019).

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[1].

Жертвами мошенников, совершающих преступления с применением современных информационно-телекоммуникационных технологий, нередко становятся пользователи социальных сетей и различных электронных ресурсов, в которых задействованы электронные финансовые средства. Используя низкую компьютерную грамотность и доверчивость людей, преступники придумывают новые способы совершения подобных преступлений.

Повышенная общественная опасность компьютерной преступности выражается в ее умышленном и организованном характере, в том, что компьютерные преступления обладают высокой латентностью и с технической точки зрения являются транснациональными, что осложняет ведение успешной борьбы с ними в отдельном государстве. Дополнительные трудности в борьбе с этим криминальным явлением обусловлены достаточно непростым механизмом международно-правового сотрудничества и взаимодействия правоохранительных органов зарубежных стран в уголовно-правовой сфере.

Качественные и количественные показатели состояния компьютерной преступности, особенно уровень и прогнозы ее латентной части, свидетельствуют о необходимости повышения требований как к эффективности выявления и предупреждения рассматриваемого вида преступных посягательств, так и к качеству предварительного расследования преступлений данной категории, организации и осуществлению межведомственного взаимодействия.

Особую роль в противодействии данным преступлениям играет деятельность надзирающих прокуроров и государственных обвинителей, которые посредством своевременного выявления и предупреждения нарушений требований федерального законодательства и применения соответствующих мер реагирования позволяют повысить эффективность уголовных процедур и достижения назначения уголовного судопроизводства.

Вопросы противодействия преступлениям в сфере компьютерной информации, а также применения компьютерных технологий (информации) при расследовании преступлений затрагивались в научных

[1] Генпрокурор России Игорь Краснов провел совещание по теме борьбы с преступлениями, связанными с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий // URL: https://genproc.gov.ru/smi/news/genproc/news-1880616/ (дата обращения: 08.10.2020).

исследованиях следующих авторов: Т. В. Аверьяновой, Р. С. Белкина, Н. В. Булановой, В. Б. Вехова, Б. Я. Гаврилова, Ю. В. Гаврилина, Р. В. Жубрина, А. Ю. Комиссарова, Н. Г. Шурухнова, А. Г. Халиулина и других.

В научных исследованиях неоднократно отмечалось, что в условиях опережающего развития способов совершения преступлений в сфере компьютерной информации по отношению к механизмам обеспечения информационной безопасности деятельность правоохранительных органов по выявлению, пресечению, предупреждению и расследованию преступлений на данном направлении не в полной мере соответствует существующим угрозам, что предопределяет необходимость анализа сложившейся ситуации и безотлагательной реализации мер, направленных на совершенствование организационных подходов и федерального законодательства Российской Федерации.

При анализе правоприменительной практики и результатов исследований, проводимых в Университете прокуратуры Российской Федерации в рамках плановых тем, а также в других научных учреждениях, выявлен комплекс причин, условий и факторов, влияющих на состояние законности в рассматриваемой сфере, что осложняет выявление, пресечение, расследование и предупреждение преступлений в сфере компьютерной информации, организации эффективного ведомственного контроля и прокурорского надзора. Все это требует более глубокого разноплановой научного исследования.

Объектом исследования являются современное состояние, структура и динамика данных видов преступлений, а также комплекс социальных процессов и правоотношений, возникающих при реализации прокурором полномочий по осуществлению надзора за процессуальной деятельностью органов дознания и органов предварительного следствия при выявлении, предупреждении и расследовании преступлений в сфере компьютерной информации.

Предметом исследования определены общие закономерности и специфика уголовно-процессуальной деятельности; доктринальные, концептуальные и иные разработки ученых по вопросам противодействия преступности в сфере компьютерной информации; процессуальная деятельность участников правоотношений, входящих в объект исследования; положения федерального и иного законодательства, регламентирующего полномочия прокурора и иных участников рассматриваемых правоотношений при осуществлении надзора за исполнением законов при выявлении, предупреждении и расследовании преступлений в сфере компьютерной информации, а также правовая база международного сотрудничества и зарубежный опыт законодательного регулирования отношений по борьбе с вышеуказанными преступлениями.

Цель исследования — на основе проведенного анализа положений законов и иных нормативных правовых актов, регулирующих вопросы информационной безопасности, состояния преступности в сфере информационно-телекоммуникационных сетей и компьютерной информации, а также практики осуществления прокурорского надзора за исполнением законов при выявлении, предупреждении и расследовании преступлений в данной сфере выработать научно обоснованные предложения по совершенствованию законодательства и данного вида деятельности, а также повышению ее эффективности.

В задачи исследования входят:

— анализ состояния преступности в сфере компьютерной информации, действующего законодательства, прокурорской, следственной и судебной практики (с учетом внесенных за последнее время изменений и дополнений в положения федерального законодательства) в части реализации прокурором полномочий по осуществлению надзора за исполнением законов при выявлении, предупреждении и расследовании преступлений в данной сфере;
— выявление проблемных ситуаций, возникающих в процессе осуществления прокурором полномочий по надзору за исполнением законов при выявлении, предупреждении и расследовании преступлений в данной сфере;
— анализ деятельности органов прокуратуры по пресечению распространения информационных материалов экстремистского характера в информационно-телекоммуникационных сетях;
— выявление и разрешение актуальных проблем, возникающих при уголовно-правовой оценке преступлений, совершаемых с использованием компьютерной информации, возможных путей их решения;
— выявление актуальных проблем, возникающих при осуществлении международного сотрудничества в противодействии вышеуказанным преступлениям, в том числе связанных с гармонизацией уголовного законодательства Российской Федерации и других стран;
— выработка предложений по повышению эффективности деятельности участников рассматриваемых правоотношений.

Научные гипотезы исследования:

— не все причины и факторы, влияющие на состояние законности в сфере информационной безопасности, выявлены и научно обоснованы, а те, которые установлены, не всегда адекватно принимаются практиками во внимание;
— законодательное обеспечение рассматриваемой сферы правоотношений существенно отстает от тенденций развития инфор-

мационной цифровой сферы и тем самым не в состоянии выступать эффективным универсальным регулятором отношений;
- на законодательном уровне целесообразно усилить полномочия органов прокуратуры в сфере координации деятельности правоохранительных органов по информационному противоборству терроризму и экстремизму, оказанию комплексного воздействия на террористическую и экстремистскую информационную среду;
- виртуальная среда совершения преступлений в сфере компьютерной информации предъявляет качественно новые требования к оперативным и уголовным процедурам;
- в деятельности прокурора по реализации полномочий при осуществлении надзора за исполнением законов при выявлении, предупреждении и расследовании преступлений в сфере информационно-телекоммуникационных сетей и компьютерной информации отмечаются проблемные ситуации, требующие преимущественно научного разрешения посредством выработки предложений по их устранению.

Эмпирическую базу исследования составили результаты анкетирования прокурорских работников прокуратур субъектов Российской Федерации, проходивших в 2017–2019 гг. обучение на факультете профессиональной переподготовки и повышения квалификации Университета прокуратуры Российской Федерации, статистические данные различных форм учета, результаты правоприменительной деятельности прокуратур субъектов Российской Федерации за 2003–2020 гг.

Глава 1

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1. Состояние преступности в сфере информационно-телекоммуникационных сетей и в сфере компьютерной информации

На современном этапе развития ИКТ информационная безопасность общества стала глобальной социальной проблемой, от решения которой зависит степень защищенности государства и личности в сфере использования компьютерных технологий.

В Российской Федерации особое внимание уделяется вопросам развития цифровых технологий и защиты информации. В 2020 году на встречах рабочей группы по подготовке изменений в Конституцию Российской Федерации Президент страны В. В. Путин поддержал предложение сделать информационные технологии и оборот данных граждан предметом ведения деятельности Российской Федерации как государства. «То, что вы предлагаете в Конституции отметить, что при развитии технологий нужно обеспечить безопасность личности, общества и государства, — это чрезвычайно важно и, конечно, востребовано. Поэтому, безусловно, все это будет поддержано», — заверил В. В. Путин. Он добавил, что надо найти баланс, как обеспечить безопасность личности с развитием интернет-технологий. «В связи с развитием информационных технологий встает ряд проблемных вопросов, которые мы, безусловно, должны решать... Обеспечение безопасности личности... приобретает достаточно острый характер в связи с развитием этих технологий»[1].

---

[1] URL: https://vz-ru.turbopages.org/s/vz.ru/news/2020/2/26/1025860.html (дата обращения: 21.04.2020).

4 июля 2020 г. соответствующие поправки были внесены в Конституцию нашей страны. Они относятся к статье 71, устанавливающей сферы деятельности, которые находятся в ведении Российской Федерации, и включают в сферу ведения государства информационные технологии и связь, а также обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных.

В настоящее время в России активно проводится цифровая трансформация, представляющая собой внедрение и использование современных цифровых технологий в сфере материального и нематериального производства с целью повышения производительности и конкурентоспособности предприятий и организаций.

Среди основополагающих документов, посвященных развитию цифровой экономики в нашей стране, следует назвать: Федеральную целевую программу «Электронная Россия» (постановление от 28 января 2002 г. № 65), действовавшую в период 2002–2010 гг. и направленную на формирование электронного государства и электронного правительства; Стратегию развития информационного общества в Российской Федерации на 2017–2030 гг. (Указ Президента РФ от 9 мая 2017 г. № 203); Правительственную программу «Цифровая экономика Российской Федерации» (распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р); «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 г.» (Указ Президента РФ от 7 мая 2018 г., известный также как второй майский Указ Президента страны).

В июле текущего года Президент Российской Федерации В. В. Путин определил национальные цели развития до 2030 г., подписав Указ «О национальных целях развития Российской Федерации на период до 2030 года»[1]. В качестве национальных целей в документе наряду с сохранением населения, здоровьем и благополучием людей; возможностями для самореализации и развития талантов; комфортной и безопасной средой для жизни; достойным, эффективным трудом и успешным предпринимательством названа цифровая трансформация. Указ также устанавливает конкретные показатели, характеризующие достижение национальных целей к 2030 г.

В рамках национальной цели «Цифровая трансформация»: достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления; увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95%; рост доли домохозяйств, которым обеспечена возможность широкополосного

[1] URL: http://kremlin.ru/events/president/news/63728 (дата обращения: 29.07.2020).

доступа к сети Интернет, до 97%; увеличение вложений в отечественные решения в сфере информационных технологий в четыре раза по сравнению с показателем 2019 г.

Вместе с тем, как справедливо замечают ученые[1], обеспечение информационной и экономической безопасности цифровой экономики нуждается в защите от хакерских атак, взломов и вирусов. Оцифровывание всей системы жизнедеятельности человека и общества порождает одновременно с прогрессом следующие угрозы: рост безработицы; дальнейшая поляризация общества и усиление неравенства; риски и проблемы кибербезопасности; интернет-мошенничество, внедрение вирусов, усиление хакерства; новый виток киберпреступности, терроризма и организованной преступности. Цифровая экономика кардинально меняет характер преступности и терроризма, порождает новые угрозы глобального масштаба, позволяя атаковать объекты дистанционно из любой точки земли. Значительно вырастают масштабы компьютерной преступности в банковско-финансовой сфере и в области нарушения конституционных прав и свобод человека и гражданина, включая неприкосновенность частной жизни, личной и семейной тайны. Кроме того, происходит взлом частной информации (несанкционированное проникновение в нее), растут масштабы и количество скоординированных компьютерных атак на финансово-экономические и военно-стратегические объекты.

Таким образом, повсеместное внедрение ИКТ во все сферы жизнедеятельности с неизбежностью породило новые угрозы государственной и общественной безопасности. Экспертами Всемирного экономического форума к основным мировым угрозам, как в краткосрочной, так и в долгосрочной перспективе, отнесены киберпреступность и кибератаки на информационную инфраструктуру. Последние стали обычным явлением для таких секторов, как энергетика, здравоохранение и транспорт[2].

По разным оценкам, общие потери мировой экономики от преступлений в сфере ИКТ составляют ежегодно порядка 2 трлн долл., а в перспективе могут увеличиться в два и более раза. Наметившиеся в предыдущие годы тенденции компьютерной преступности стали более выражены в период 2019 г. — начало 2020 г. с усилением цифровизации общества ввиду развития ситуации, связанной с распространением коронавирусной инфекции и применением ограничительных мер. Ярким свидетельством является значительное, почти в 2 раза (в 1,77 раза), увеличение преступлений рассматриваемой категории за

---

[1] *Петров А. А.* Цифровизация экономики: проблемы, вызовы, риски // Торговая политика. 2018. № 3 (15). С. 9–30. URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-ekonomiki-problemy-vyzovy-riski (дата обращения: 10.10.2020).

[2] The Global Risks Report 2020. 15th Edition. World Economic Forum.

9 месяцев 2020 г. в сравнении с 2019 г. — с 205 116 до 363 034. Среди преступлений рассматриваемой категории следует особо выделить преступления, совершенные с использованием пластиковых карт; их количество возросло на 500,2%, или в 6 раз, — с 23 259 за 9 месяцев 2019 г. до 139 597 за 9 месяцев 2020 г.

На состоявшейся в июле текущего года коллегии Генеральной прокуратуры Российской Федерации по итогам работы за первое полугодие и задачам по повышению эффективности надзора на второе полугодие первый заместитель Генерального прокурора Российской Федерации А. Э. Буксман пристальное внимание обратил на существенный рост количества «фейков»[1] в сети Интернет в связи с пандемией. «В органы прокуратуры поступило свыше 340 уведомлений о распространении недостоверной информации. В целях ее блокировки в Роскомнадзор направлено 153 требования (в аналогичном периоде 2019 г. — 6). По итогам рассмотрения 219 требований заблокировано свыше 4 тыс. сайтов, с более чем 25 тыс. ресурсов противоправные сообщения удалены. В первом полугодии 2020 г. число зарегистрированных преступлений по сравнению с аналогичным периодом прошлого года незначительно снизилось. При этом число преступлений, совершенных с использованием ИКТ, увеличилось на 91,7%»[2].

Кроме того, 17 июля 2020 года под председательством Генерального прокурора Российской Федерации И. В. Краснова состоялось заседание Координационного совещания руководителей правоохранительных органов Российской Федерации по вопросу «О состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации».

В своем вступительном слове И. В. Краснов подчеркнул, что вынесенные на обсуждение вопросы крайне актуальны. «За последние 5 лет число таких преступлений возросло в 25 раз (в 2019 году — 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 преступле-

---

[1] Буквально «фальшивка», «подделка» (англ. — fake). В сфере ИКТ означает создание медиаконтента, содержание которого, как правило, заведомо для автора не соответствует действительности. Активно используется для создания информационного шума и дезинформации в киберпространстве.

[2] URL: http://www.genproc.gov.ru/smi/news/genproc/news-1884166/ (дата обращения: 31.07.2020).

ний, от хищений денежных средств с расчетных пластиковых карт, до угроз критической инфраструктуре страны и обеспечению ее безопасности», — отметил Генеральный прокурор Российской Федерации.

С каждым днем появляются новые способы шифрования данных, максимально повышающие анонимность совершаемых действий. Наблюдается широкое распространение криминального использования криптовалют в сфере незаконного оборота наркотиков, коррупции, финансирования организованной преступности, экстремизма и терроризма.

Генеральный прокурор Российской Федерации обратил внимание участников совещания на ежегодный рост компьютерных атак, организаторы которых нередко используют инфраструктуру иностранных государств для попыток взлома информационных систем российских государственных органов, корпораций, крупных банков. Бесконтактный и быстрый способ совершения таких преступлений делает общество все более уязвимым перед новыми вызовами. При этом правоохранительные органы зачастую оказываются к ним неготовыми. Низкая выявляемость и раскрываемость киберпреступлений порождает безнаказанность и чувство вседозволенности, хотя возможности противостоять новым угрозам у правоохранителей имеются.

В этой связи И. В. Краснов указал на необходимость эффективно отвечать на вызовы в киберпространстве, использовать те же технологии для раскрытия преступлений, предупреждать и прогнозировать их, своевременно устранять правовые пробелы.

Подводя итоги обсуждения, И. В. Краснов указал, что выявленные проблемы требуют реагирования со стороны всей правоохранительной системы, подчеркнул важность единообразного понимания вызовов и четкой координации работы по их нейтрализации. Он потребовал принять меры по совершенствованию системы профилактики и раннего выявления преступлений, совершенных с использованием ИТ-технологий и компьютерной информации, поставив ряд конкретных задач:

1. Проанализировать эффективность взаимодействия оперативных служб с центрами реагирования на инциденты в сфере информационной безопасности. Проработать вопрос о возможности создания автоматизированных поисковых систем, в том числе на базе уже существующих путем расширения функционала по предупреждению и пресечению киберпреступности, а также их интеграции с другими базами данных.

2. Кардинально изменить подходы к организации оперативно-разыскной деятельности и предварительного расследования таких фактов. Учитывая специфику их выявления, стремительное распространение криминального использования виртуальных активов, компьютерных атак на критическую информационную инфраструк-

туру государства, необходимо внедрять специализацию сотрудников, осуществлять их профессиональный отбор, добиваться устойчивого повышения раскрываемости преступлений.

3. Обеспечивать максимально тесное взаимодействие прокуроров, сотрудников оперативных, в том числе технических, служб и органов следствия на всех стадиях выявления данных посягательств и осуществления уголовного преследования виновных лиц, комплексно развивать систему экспертного сопровождения.

4. Учитывая трансграничный характер киберпреступлений, необходимо более эффективно использовать возможности специализированных сетей правоохранительных органов, международного полицейского взаимодействия и сотрудничества в порядке уголовного судопроизводства.

Также Генеральный прокурор Российской Федерации обратил внимание на необходимость совершенствования действующего законодательства в части расширения признаков преступлений в сфере IT-технологий, введения в процессуальные нормы понятия «электронное доказательство», процедур внесудебной блокировки «зеркал» ранее заблокированных сайтов, а также по ряду других вопросов. Он указал на необходимость активного участия в этой работе всех ведомств.

«Усилия органов прокуратуры, в свою очередь, будут сосредоточены на повышении эффективности и качества прокурорского надзора за законностью в сфере безопасного использования информационно-коммуникационных технологий в целях оперативного решения всех стоящих перед нами задач», — подчеркнул И. В. Краснов.

По результатам состоявшего обсуждения было также отмечено, что одновременно с ростом количества телекоммуникационных устройств и пользователей информационных сетей увеличивается число потенциальных жертв, а также возрастают возможности эксплуатации сети Интернет для совершения противоправных деяний.

Говоря о национальном уголовном законодательстве, регламентирующем ответственность за преступления в сфере компьютерной информации, нельзя не отметить следующее.

Хищения из банков и нарушения работы предприятий обусловили включение норм, устанавливающих ответственность за совершение преступлений в сфере компьютерной информации, уже в первую редакцию Уголовного кодекса Российской Федерации[1] 1996 г. Были криминализированы неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ).

[1] Далее — УК РФ.

Среди преступлений, совершенных с помощью компьютеров в те годы, можно назвать хищение 125,5 тыс. долларов из Внешэкономбанка (1991 г.), попытки хищений из Центробанка России на сумму 68 млрд руб. (1993 г.) и хищение 2,8 млн долларов из Сити-банка (1995 г.)[1]. Учеными прогнозировалась вероятность того, что в будущем придется столкнуться с противозаконным «использованием конфиденциальной информации и компьютера» не только при нападениях на информационные системы финансовых учреждений, но и при совершении преступлений против собственности, экономической деятельности и иных объектов[2].

Подтверждая данные прогнозы, законодателем последовательно расширялся перечень преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации. В УК РФ были включены ст. 159^3 «Мошенничество с использованием платежных карт», ст. 159^6 «Мошенничество в сфере компьютерной информации», ст. 274^1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»; ряд статей был дополнен квалифицирующим признаком «совершенные с использованием информационно-телекоммуникационных сетей».

С учетом того, что легальное определение «компьютерной преступности» отсутствует, в настоящее время около 40 составов можно отнести к таким преступлениям. В частности, статистическая форма 1-ВТ «Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации» включает в себя сведения о преступлениях, предусмотренных ч. 1 ст. 138, ст. 138^1, 146, 158, 159, 159^3, 159^6, 165, 171^2, 183, 242, 242^1, 242^2, 272, 273, 274 УК РФ. Это далеко не полный список исследуемых преступлений.

Более полный перечень содержится в разделе 11 «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выявленных и предварительно расследованных субъектами регистрации», введенном в статистическую форму 4-ЕГС 1 января 2018 г., которая включает в себя 36 составов.

Необходимо обратить внимание на то, что в действующем на сегодняшний день Перечне статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности, ежегодно утверждаемом совместным указанием Генеральной прокуратуры Российской Федерации и МВД России, раздел

---

[1] *Ляпунов Ю. В.*, *Максимов В. Ю.* Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 8.

[2] *Крылов В. В.* Информационные преступления — новый криминалистический объект // Российская юстиция. 1997. № 4. С. 22.

«Преступления, совершенные с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации» до сих пор отсутствует. На наш взгляд, в целях проведения качественного анализа целесообразно рассмотреть вопрос о включении такого раздела в следующий перечень.

Исходя из имеющихся данных за последние годы количественные показатели зарегистрированных преступлений, совершенных с использованием в сфере ИКТ), постоянно возрастали (таблица 1.1).

Таблица 1.1

Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации[1]

Год	Количество преступлений, зарегистрированных в отчетном периоде	
	Всего	Темп прироста, %
2003	10 920	–
2004	13 261	21,4
2005	14 910	12,4
2006	14 042	–5,8
2007	11 821	–15,8
2008	14 189	20,0
2009	17 535	23,6
2010	12 698	–27,6
2011	7974	–37,2
2012	10 227	28,3
2013	11 104	8,6
2014	10 968	–1,2
2015	43 816	+299,5
2016	65 949	+50,5
2017	90 587	+37,4
2018	174 674	+92,8
2019	294 409	+68,5

[1] Здесь и далее сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации до 2017 г. включительно, приведены по форме статистической отчетности 1-ВТ; сведения о преступлениях после 2018 г. приведены по форме статистической отчетности № 4-ЕГС (494).

В период 2003–2017 гг. количество зарегистрированных преступлений анализируемой категории возросло более чем в 8 раз (с 10 920 в 2003 г. до 90 587 в 2017 г.). По данным формы № 4-ЕГС, в 2018 г. их количество составило 174 674, в 2019 г. — уже 294 409[1]. Тенденцию роста компьютерной преступности отметили и более 60% опрошенных в ходе исследования экспертов[2].

В то же время обеспечению полноты и объективности статистических данных во многом способствовали прокурорские проверки достоверности документов первичного учета и баз данных информационных центров территориальных органов МВД России[3]. Применение комплексного подхода к обеспечению достоверности статистики в отдельных регионах заметно отразилось на росте показателей анализируемой преступности. Например, в Курской области количество преступлений, совершенных с использованием ИКТ, в 2016–2018 гг. возросло в 3 раза[4].

Очевидно, что увеличение количественных показателей обусловлено не только совершенствованием регистрации и учетно-регистрационной дисциплины, но и объективным ростом совершенных с использованием ИКТ мошенничеств (ст. 159 УК РФ), которые в 2019 г. составили 40,7% (119 903) всех преступлений, и краж (ст. 158 УК РФ) — 33,6% (98 798). Существенный сегмент (24 677, 8,4%) составили преступления, предусмотренные ст. 228[1] УК РФ (таблица 1.2).

В настоящее время практически каждое седьмое преступление совершается в сфере ИКТ, в том числе с применением расчетных пластиковых карт (34,3 тыс., +109,3%), компьютерной техники (18,6 тыс., +21,5%), сети Интернет (157 тыс., +45,4%) и средств мобильной связи (116,1 тыс., +89,5%).

Изучение региональных особенностей преступности с использованием ИКТ показывает, что в 2019 г. наибольшее количество преступлений зарегистрировано в Приволжском (69 765) и Центральном (63 946) федеральных округах. Среди субъектов Российской Федерации выделяются Москва (23 580), Республика Татарстан (10 095), Краснодарский край (11 331) и Тюменская (12 410) области (см. таблицу 1.3).

---

[1] Форма статистической отчетности № 4-ЕГС (494).

[2] См.: Приложение.

[3] Обзор Генеральной прокуратуры Российской Федерации «Нарушения при формировании показателей о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий» от 28 сентября 2018 г. № 110-7-2018/Ип11412.

[4] *Гурин А. Д.* Обеспечение достоверности официальных статистических данных о преступлениях в сфере информационных технологий // Законность. 2020. № 2 (1024). С. 8–9.

Таблица 1.2

Сведения о зарегистрированных преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации в период 2014–2019 гг.

Статьи УК РФ	2014	2015	2016	2017	2018	2019
Ст. 110 «Доведение до самоубийства»	Сведения отсутствуют				13	4
Ст. 110[1] «Склонение к совершению самоубийства или содействие совершению самоубийства»					18	11
Ст. 137 «Нарушение неприкосновенности частной жизни»					432	508
Ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан»	43	42	30	42	143	180
Ст. 138[1] «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации»	352	369	320	434	289	125
Ст. 146 «Нарушение авторских и смежных прав»	697	689	553	524	406	332
Ст. 151 «Вовлечение несовершеннолетнего в совершение антиобщественных действий»	Сведения отсутствуют				1	0
Ст. 151[2] «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего»					1	0
Ст. 158 «Кража»	2334	8449	9762	6945	32 668	98 798
Ст. 159 «Мошенничество»	2187	13 483	32 875	51 513	90 664	119 903
Ст. 159[3] «Мошенничество с использованием платежных карт»	Сведения отсутствуют		77	11	4242	16 119
Ст. 159[6] «Мошенничество в сфере компьютерной информации»	995	5443	4329	2195	970	687

Ст. 163 «Вымогательство»	Сведения отсутствуют				1621	2090
Ст. 165 «Причинение имущественного ущерба путем обмана или злоупотребления доверием»	7	11	15	14	11	21
Ст. 171^2 «Незаконные организация и проведение азартных игр»	37	475	720	825	875	842
Ст. 172^2 «Организация деятельности по привлечению денежных средств и (или) иного имущества»	Сведения отсутствуют				0	0
Ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну»	171	132	150	115	90	185
Ст. 185^3 «Манипулирование рынком»	Сведения отсутствуют				0	2
Ст. 187 «Неправомерный оборот средств платежей»					203	433
Ст. 205^2 «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма»					169	212
Ст. 222, 222^1 «Незаконные приобретение, передача, сбыт, хранение, перевозка или ношение оружия...»					68	56
Ст. 228^1 «Незаконные производство, сбыт или пересылка наркотических средств...»					18 805	24 677
Ст. 228^2 «Нарушение правил оборота наркотических средств или психотропных веществ»					0	0
Ст. 228^4 «Незаконные производство, сбыт или пересылка прекурсоров наркотических средств...»					2	10
Ст. 230 «Склонение к потреблению наркотических средств, психотропных веществ или их аналогов УК РФ»					5	1
Ст. 234 «Незаконный оборот сильнодействующих или ядовитых веществ в целях сбыта»					106	129

Окончание табл. 1.2

Статьи УК РФ	2014	2015	2016	2017	2018	2019
Ст. 242 «Незаконное изготовление и оборот порнографических материалов или предметов»	650	435	434	558	725	972
Ст. 242[1] «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних»	758	529	408	508	548	704
Ст. 242[2] «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов»	9	28	105	101	195	240
Ст. 272 «Неправомерный доступ к компьютерной информации»	1151	1396	994	1079	1761	2420
Ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»	585	974	751	802	733	455
Ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации...»	3	12	3	2	5	4
Ст. 274[1] «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»	Введена в 2018 г.				1	–
Ст. 280 «Публичные призывы к осуществлению экстремистской деятельности»	Сведения отсутствуют				253	257
Ст. 280[1] «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации»					10	6
Ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства»					733	12

Таблица 1.3

Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий и компьютерной информации, в 2019 г. по федеральным округам[1]

Округ	Количество преступлений, зарегистрированных в отчетном периоде
	Всего
ЦАО	63 946
СЗФО	26 148
СКФО	8616
ЮФО	29 659
ПФО	69 765
УФО	33 357
СФО	41 277
ДФО	17 481

В 2019 г. в Российской Федерации было зарегистрировано 294 409 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. В 1,7 раза, или на 68,5%, больше, чем в 2018 г. (174 674).

Почти каждое третье (32,1%) такое преступление совершается в девяти субъектах Российской Федерации. В Москве — 23 580, в Краснодарском крае — 11 331 в Республике Татарстан — 10 095, в Челябинской области — 9601, в Свердловской области — 8509, в Пермском крае — 8164, в Кемеровской области — 7866, в Красноярском крае — 7811 и в Республике Башкортостан — 7571.

Коэффициент преступлений, совершенных с использованием ИКТ, в 2019 г. — 200,6 преступлений на 100 тыс. населения. В 1,7 раза (или на 68,7%) больше, чем в 2018 г. (119,0). Размах значений показателя в субъектах Российской Федерации — 485 преступлений. Максимальное значение показателя в Республике Коми (489,1), минимальное — в Чеченской республике (15,5).

Десять процентов населения проживает в регионах с наибольшими значениями показателя: от 489,1 в Республике Коми до 267,6 в Томской области (табл. 1.4).

Десять процентов населения проживает в регионах с наименьшими значениями показателя: от 489,1 в Республике Коми до 267,6 в Томской области (табл. 1.5).

[1] Сведения по форме статистической отчетности № 4-ЕГС (494).

Таблица 1.4

Субъекты Российской Федерации, в которых проживает 10% населения страны и где наибольшие значения коэффициента преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в 2019 г.

Субъект Российской Федерации	Коэффициент
Республика Коми	489,1
Ямало-Ненецкий автономный округ	397,4
Магаданская область	394,4
Республика Карелия	363,7
Архангельская область	363,4
Курганская область	339,9
Ханты-Мансийский автономный округ	338,8
Республика Удмуртия	327,6
Кировская область	326,7
Мурманская область	324,7
Пермский край	312,7
Тюменская область	304,3
Вологодская область	297,7
Кемеровская область	294,1
Ненецкий автономный округ	289,8
Камчатский край	286,3
Челябинская область	276,2
Чувашская республика	271,9
Красноярский край	271,8
Амурская область	267,8
Томская область	267,6
Среднее значение	**338,2**

Децильный коэффициент[1] (соотношение средних значений исследуемого показателя в этих группах) достаточно высок (9,7), но далек от критического значения.

[1] Оценка дифференциации субъектов Российской Федерации по исследуемому показателю.

Таблица 1.5

Субъекты Российской Федерации, в которых проживает 10% населения страны и где наименьшие значения коэффициента преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в 2019 г.

Субъект Российской Федерации	Коэффициент
Московская область	54,15
Санкт-Петербург	41,10
Республика Ингушетия	16,08
Республика Дагестан	15,46
Чеченская республика	4,39
Среднее значение	**35,0**

Коэффициент преступности в Республике Коми значительно отличается от среднего значения по стране (он в 2,4 раза больше). По исследуемому показателю Республика Коми нарушает статистическую однородность всех субъектов Российской Федерации. Исследовать преступления, совершенные с использованием ИКТ, в республике следует отдельно.

Остальные 84 субъекта Российской Федерации подразделяются на 5 типологических групп.

В группу I (с низким значением коэффициента преступности) входят три республики Северного Кавказа: Республика Ингушетия — 16,1 преступления на 100 тыс. жителей, Республика Дагестан — 15,5 и Чеченская республика — 4,4. Среднее значение коэффициента преступлений, совершенных с использованием ИКТ, в группе I — 12,3.

В группу II (со значением коэффициента преступности ниже среднего) входят семь субъектов Российской Федерации: Республика Крым — 115,0 преступления на 100 тыс. жителей, Тульская область — 114,6, Республика Северная Осетия Алания — 113,3, Республика Калмыкия — 103,8, Кабардино-Балкарская Республика — 101,1, Московская область — 54,1 и Санкт-Петербург — 41,1. Среднее значение коэффициента преступлений, совершенных с использованием ИКТ, в группе II — 66,8.

В группу III (со средним значением коэффициента преступности) входят 55 субъектов Российской Федерации (см. таблицу 1.6). От 131,1 преступления на 100 тыс. жителей в Рязанской области до 271,9 — в Чувашской Республике. Среднее значение коэффициента преступлений, совершенных с использованием ИКТ, в группе III — 204,6.

Таблица 1.6

Субъекты Российской Федерации, которые относятся к группе (со средним значением коэффициента преступности)

Чувашская республика	271,9
Красноярский край	271,8
Амурская область	267,8
Томская область	267,8
Республика Хакасия	263,4
Алтайский край	261,8
Еврейская автономная область	260,8
Оренбургская область	260,0
Республика Татарстан	258,9
Хабаровский край	255,5
Костромская область	253,9
Сахалинская область	249,6
Смоленская область	242,5
Новгородская область	240,2
Нижегородская область	233,8
Республика Алтай	233,5
Курская область	232,9
Республика Марий Эл	232,2
Ивановская область	231,8
Тверская область	230,8
Волгоградская область	228,1
Пензенская область	226,4
Иркутская область	219,6
Калужская область	211,0
Республика Мордовия	209,8
Псковская область	205,7
Владимирская область	204,5
Ярославская область	201,6
Воронежская область	200,8
Краснодарский край	200,6

Окончание табл. 1.6

Свердловская область	197,2
Ставропольский край	196,0
Омская область	195,0
Тамбовская область	192,1
Чукотский автономный округ	189,3
Саратовская область	189,0
Орловская область	187,7
Ульяновская область	187,3
Москва	186,9
Республика Башкортостан	186,9
Забайкальский край	186,1
Белгородская область	184,9
Карачаево-Черкесская республика	182,1
Новосибирская область	181,9
Калининградская область	180,7
Самарская область	180,0
Республика Бурятия	179,8
Приморский край	178,2
Ростовская область	173,6
Республика Саха (Якутия)	170,4
Республика Тыва	168,3
Астраханская область	167,9
Ленинградская область	164,9
Брянская область	134,3
Рязанская область	131,1
Республика Адыгея	130,4
Липецкая область	122,9
Севастополь	120,5

В группу IV (со значением коэффициента преступности выше среднего) входят 12 субъектов Российской Федерации (см. таблицу 1.7). От 276,2 преступления на 100 тыс. жителей в Челябинской области до 339,9 — в Курганской области. Среднее значение коэффициента преступлений, совершенных с использованием ИКТ, в группе IV — 307,1.

Таблица 1.7

Субъекты Российской Федерации, которые относятся к группе (со средним значением коэффициента преступности)

Курганская область	339,9
Ханты-Мансийский автономный округ	338,8
Республика Удмуртия	327,6
Кировская область	326,7
Мурманская область	324,7
Пермский край	312,7
Тюменская область	304,3
Вологодская область	297,7
Кемеровская область	294,1
Ненецкий автономный округ	289,8
Камчатский край	286,3
Челябинская область	276,2

В группу V (с высоким значением коэффициента преступности) входят четыре субъекта Российской Федерации: Ямало-Ненецкий автономный округ — 397,4 преступления на 100 тыс. жителей, Магаданская область — 394,4, Республика Карелия — 363,7 и Архангельская область — 363,4. Среднее значение коэффициента преступлений, совершенных с использованием ИКТ, в группе IV — 373,0.

Наиболее часто ИКТ используются при совершении хищений. Причем доступность технологий широким слоям населения, с одной стороны, и развитие систем электронной защиты — с другой, привели к увеличению числа тех преступников, которые отказываются от сложных способов совершения преступлений в пользу проверенных временем методов, основанных на социальной инженерии.

Так, например, в 2014–2015 гг. получили распространение хищения денежных средств с помощью считывающих переносных устройств (скиммеров), которые устанавливались злоумышленниками в банкоматы под видом конструктивных деталей. Устройства записывали информацию с магнитной полосы карты потерпевшего, в то время как видеорегистратор фиксировал набираемый им PIN-код. Однако после внедрения финансовыми организациями банковских карт с чипом, количество таких преступлений резко сократилось.

Данные компаний, специализирующихся на информационной безопасности, также подтверждают, что не менее 80% хищений с использованием ИКТ совершаются посредством социальной инжене-

рии, например путем отправки сообщений потенциальным жертвам или звонков с номеров СИМ-карт, приобретенных без регистрации или оформленных на третье лицо. Выведение похищенных денег осуществляется через подставные банковские карты, счета в интернет-магазинах, лицевые счета мобильного телефона[1].

В качестве примера использования приемов социальной инженерии можно привести действия И., осужденного по ч. 3 ст. 30, ч. 1 ст. 158 (14 эпизодов), ч. 1 ст. 158 (2 эпизода), п. «в» ч. 2 ст. 158 (7 эпизодов) и ч. 2 ст. 159 УК РФ. И., имея в распоряжении сим-карту и банковскую карту, оформленные на третьих лиц, осуществлял рассылку СМС-сообщений на абонентские номера телефонов широкого круга лиц с текстом о том, что их банковские карты заблокированы, а информацию о разблокировке можно получить, позвонив на его абонентский номер. После чего И. сообщал потерпевшим, что он является сотрудником технического отдела ПАО «Сбербанк России», а также о произошедшем сбое в банковской системе и блокировке банковских карт. Для разблокировки необходимо провести ряд банковских операций, чтобы сохранить на ней денежные средства. В некоторых случаях потерпевшие сообщали И. номера своих банковских карт, идентификационные данные, необходимые для получения доступа к лицевому счету, а затем и коды для доступа в мобильный банк; в иных случаях потерпевшие самостоятельно осуществляли через банкомат переводы денежных средств на счета И.[2]

Зачастую для совершения хищений злоумышленникам не требуются специальные познания в области информационных технологий, что особенно относится к преступлениям с использованием платежных карт.

Так, в 2018 г. была осуждена Ж. по ч. 2 ст. 159[3] УК РФ. После совместного распития спиртных напитков со своим знакомым Т. она похитила у него из сумки дебетовую карту, заведомо зная, что с помощью нее можно осуществлять покупки без введения карты в терминал и набора PIN-кода на сумму до 1000 руб. После чего приобрела в разных магазинах необходимый ей товар на общую сумму 7761 руб.[3]

Такого рода преступления в современных условиях стали типичными. С учетом этого очевидно, что одним из наиболее важных направлений противодействия их совершению является принятие широкого комплекса мер по повышению уровня грамотности населения в сфере информационных технологий.

Технологии социальной инженерии, фишинг электронной почты, перехват деловой переписки, кибератаки на организации и отдель-

---

[1] См.: ThreatZone'19. Иллюзия безопасности. 2019 // URL: https://ict.moscow/research/threat-zone19-illiuziia-bezopasnosti/ (дата обращения: 10.10.2020).

[2] Приговор Ленинского районного суда г. Самары № 1-137/2018 от 20 ноября 2018 г. по делу № 1-137/2018

[3] Приговор Кировского районного суда г. Самары № 1-581/2018 от 28 ноября 2018 г. по делу № 1-581/2018.

ных лиц получили заметно большее распространение во время применения карантинных мер, вызванных глобальным распространением пандемии COVID-19. Ограничения перемещений, изоляция отразились на психологическом состоянии граждан, увеличении спроса на определенные товары, расширении использования онлайн-сервисов для решения повседневных вопросов, а также значительных объемах электронной торговли.

Мировые тренды киберпреступности[1] коснулись и нашей страны. Преступники быстро воспользовались распространением инфекционных заболеваний и возросшим спросом на информацию и товары. С начала марта 2020 г. рядом компаний и финансовых организаций сообщалось о нарушениях[2]. Компания «Лаборатория Касперского» подтвердила факты использования пандемии для придания вредоносным письмам убедительности[3]. Рост обращений по поводу мошеннических действий на фоне пандемии также отметили и в ГУ МВД России по г. Москве[4].

Еще одним негативным последствием самоизоляции и увеличения интернет-активности явилось увеличение фактов распространения в Интернете материалов, связанных с сексуальной эксплуатацией несовершеннолетних. Согласно данным Европола, ситуация вокруг пандемии предоставила преступникам доступ к широкой группе потенциальных жертв. Несовершеннолетние стали чаще пользоваться сетью при отсутствии контроля родителей как в свободное время, которого стало значительно больше, так и во время получения образования в рамках дистанционных учебных программ. Переместились в Интернет и сами злоумышленники[5].

Актуальность данного мирового тренда для Российской Федерации в настоящий момент требует дополнительной проверки. В то же время имеющиеся данные позволяют говорить о достаточно большом сегменте подобных преступлений в истекший период. Количе-

---

[1] Pandemic profiteering: how criminals exploit the Covid-19 crisis. European Union Agency for Law Enforcement Cooperation, 2020; Catching the virus — cybercrime, disinformation and the COVID-19 pandemic. European Union Agency for Law Enforcement Cooperation, 2020.

[2] Мошенники начали звонить клиентам «Аэрофлота» по поводу отмены рейсов из-за COVID-19 // URL: https://www.interfax.ru/russia/699139 (дата обращения: 15.04.2020); ЦБ обнаружил более 2 тыс. мошеннических сайтов о коронавирусе // URL: https://www.rbc.ru/finances/10/04/2020/5e9093519a7947dc566339d5/ (дата обращения: 15.04.2020).

[3] Коронавирус как приманка // URL: https://www.kaspersky.ru/blog/coronavirus-corporate-phishing/27706/ (дата обращения: 15.04.2020).

[4] См.: URL: https://tass.ru/obschestvo/8017343 (дата обращения: 05.07.2020).

[5] Exploiting isolation: offenders and victims of online child sexual abuse during the Covid-19 pandemic. European Union Agency for Law Enforcement Cooperation, 2020.

ство выявленных преступлений, предусмотренных ст. 242[1] УК РФ, в 2014–2019 гг. варьировалось от 408 до 758. Одновременно с этим преступления по ст. 242[2] УК РФвозросли с 9 в 2014 г. до 240 в 2019 г.

Например, в 2019 г. в отношении М. было возбуждено уголовное дело о преступлении, предусмотренном п. «г» ч. 2 ст. 242[1] УК РФ, по факту распространения в сети Интернет информации с порнографическим изображением несовершеннолетних посредством программ «Шариаза» и сервиса пиринговой сети «Гнутелла2» интернет-провайдера ПАО «Ростелеком». В апреле 2019 г. приговором Калининского районного суда г. Тюмени М. был осужден по пункту «г» ч. 2 ст. 242[1] УК РФ к наказанию в виде 3 лет лишения свободы условно[1].

Расширение возможностей наркоторговли онлайн отражается на существенной доле и тенденциях роста преступлений в сфере незаконного оборота наркотических средств, совершаемых с использованием ИКС[2]. Правоохранительными органами пресекается деятельность региональных и межрегиональных нелегальных интернет-магазинов. Как правило, механизм преступной деятельности предполагает наличие функционально обособленных структурных подразделений, большого количества участников с установленными обязанностями (закладчики, курьеры, операторы и др.), использование широкого набора программных продуктов в целях обеспечения конспирации, включая мессенджеры (Brosix, Vipole и др.) и сервисы обмена фотографиями (Imgur, Postimge и др.), не имеющие широкого распространения, VPN-сервисы, плагины, обеспечивающие шифрование переписки, электронные платежные системы[3].

В 2018–2019 гг. на территории города Великого Новгорода и Новгородской области была пресечена деятельность преступного сообщества, осуществлявшего сбыт наркотических средств через места скрытого хранения (тайники или «закладки») бесконтактным способом с использованием Telegram, ViPole, Signal, электронной платежной системы Visa QIWI Wallet, цифровой криптовалюты Bitcoin через сайт «www.ibizza7.biz», доступный через технологию VPN и программное обеспечение TOR. Работникам данного интернет-магазина поступали инструкции, как установить приложение, чтобы они могли создать электронные кошельки, для поступления криптовалюты. Возбуждены уголов-

---

[1] Докладная записка прокуратуры Тюменской области «О состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации в 2019 г.».

[2] Далее — ИТС.

[3] *Земцова С. И.* Интернет-магазины, осуществляющие незаконный сбыт синтетических наркотических средств: дифференциация и характерные признаки // Вестник Сибирского юридического института МВД России. 2019. № 1 (34). С. 36–40. URL: https://cyberleninka.ru/article/n/internet-magaziny-osuschestvlyayuschie-nezakonnyy-sbyt-sinteticheskih-narkoticheskih-sredstv-differentsiatsiya-i-harakternye (дата обращения: 11.10.2020).

ные дела по ст. 210 УК РФ в отношении неустановленного лица, создавшего преступное сообщество, и в отношении 11 участников организованного преступного сообщества[1].

Необходимо отметить, что посредством интернет-магазинов распространяются преимущественно синтетические наркотики. Неслучайно в 2019 г.п. 2 ст. 7 Федерального закона от 13 марта 2006 г. № 38-ФЗ «О рекламе» был дополнен указанием на запрет рекламы потенциально опасных психоактивных веществ[2].

С применением новых способов осуществляются преступления в сфере компьютерной информации, а именно предусмотренные ст. 272, 273, 274 и 274[1] УК РФ и включенные в главу 28 («Преступления в сфере компьютерной информации») УК РФ. В этом отношении нельзя не согласиться с мнением о том, что современная компьютерная преступность в последние годы вышла на новый технический и качественный уровень, что связано с научно-техническим прогрессом, эволюцией IT-технологий и формированием технотронного общества[3].

Совершение таких преступлений зачастую требует от злоумышленников наличия специальной технической подготовки.

Так, приговором Центрального районного суда г. Читы от 23 октября 2018 г. был осужден К. по ч. 2 ст. 273, ч. 3 ст. 272, ч. 3 ст. 183 и ч. 4 ст. 159[6] УК РФ. С 2015 г. участники организованной группы подбирали в сети Интернет лиц, которые рассылали неопределенному кругу СМС-сообщения со ссылками на интернет-сайты с вредоносными компьютерными программами. При переходе по ним члены организованной группы получали доступ к сервису, позволяющему совершать банковские переводы со счетов владельцев мобильных устройств. Затем денежные средства выводились на счета банковских карт и электронных кошельков, оформленных на неустановленных лиц, проживающих в различных регионах Российской Федерации. В результате деятельности организованной группы денежные средства были похищены у 21 лица[4].

---

[1] Докладная записка прокуратуры Новгородской области о результатах проверки состояния работы правоохранительных органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации в 2019 г.

[2] Федеральный закон от 1 мая 2019 г. № 89-ФЗ «О внесении изменений в статью 4 Закона Российской Федерации «О средствах массовой информации» и статью 7 Федерального закона «О рекламе».

[3] *Евдокимов К. Н.* Новые угрозы информационной безопасности России: от компьютерной преступности к анекселенктотичной технотронной преступности (частная научная теория) // Основные направления государственной политики России в сфере обеспечения национальной безопасности: материалы международной научно-практической конференции / отв. ред. Е. М. Якимова. Иркутск: Байкальский государственный университет, 2018. С. 57–65.

[4] Приговор Центрального районного суда г. Читы № 1-949/2018 от 23 октября 2018 г. по делу № 1-949/2018.

Обратим внимание на то, что на практике зачастую выявляются лица, использующие вредоносные компьютерные программы в преступных целях, но вовсе не создатели таковых продуктов. На фоне значительного увеличения почти всех преступлений с использованием ИКТ количественные характеристики преступлений, предусмотренных ст. 273 УК РФ, показывают отрицательную динамику. Проблемы их выявления правоохранительными органами традиционно увязывают с недостатками профессиональной подготовки сотрудников соответствующих ведомств, призванных бороться с киберпреступностью.

Все чаще ИТС стали использоваться для распространения сведений о частной жизни, составляющих личную или семейную тайну.

Например, в производстве СО по ЮАО г. Оренбурга находилось уголовное дело о преступлении, предусмотренном ч. 1 ст. 137 УК РФ по факту распространения О. в июле 2019 г. полученных из личной переписки с Р. в социальной сети «ВКонтакте» изображений личного характера. О. с предъявленным обвинением в совершении преступления согласился и заявил ходатайство о прекращении уголовного дела по ст. 25[1] УПК РФ и назначении судебного штрафа[1].

Получили распространение атаки на пользователей iOS, когда злоумышленники получают данные для входа в облачный сервер, на котором клиенты Apple часто хранят логины и пароли для других сервисов и полные копии устройств. Нередко с пользователем выходят на связь и шантажируют компрометирующими материалами. Зачастую жертвы в таких случаях стремятся выплатить требуемую сумму[2].

Неудивительно, что количество преступлений, предусмотренных ст. 138 УК РФ, более чем в 4 раза увеличилось за последние пять лет (с 42 в 2015 г. до 180 в 2019 г.). Растет число так называемых взломов электронных почтовых ящиков, аккаунтов в социальных сетях, в результате которых появляется возможность незаконно знакомиться с перепиской потерпевшего.

Трудно судить о перспективах состояния защищенности личности с учетом последних событий. Однако сохранность персональных данных декларируется в качестве одной из ценностей на международном уровне. В 2018 г. в Европейском союзе вступил в силу Общий регламент по защите данных, который обязывает соблюдать единые стандарты при сборе и обработке сведений о пользователях. Ужесточены требования к прозрачности действий организаций, которые должны сообщать об утечке данных не позднее 3 суток после обнаружения.

---

[1] Докладная записка прокуратуры Оренбургской области «О результатах проверки состояния работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации в 2019 г.».

[2] См.: ThreatZone'19. Иллюзия безопасности. 2019.

В соответствии с регламентом уже оштрафованы ряд компаний, в том числе корпорация Google в мае 2019 г.[1]

Отдельно хотелось бы выделить преступления, предусмотренные ст. 146 УК РФ («Нарушение авторских и смежных прав»). На протяжении последних 15 лет самым распространенным предметом данного посягательства становились программные продукты корпорации Microsoft. Именно с деятельностью данной компании, в том числе тесным взаимодействием с правоохранительными органами, в нашей стране связано резкое ужесточение практики привлечения к уголовной ответственности по данной статье в середине прошлого десятилетия. В последние годы снизилось не только количество зарегистрированных преступлений, предусмотренных ст. 146 УК РФ, но и количество осужденных по данной статье. Так, если в 2014 г. по данной статье было осуждено 808 лиц, то в 2019 г. — 224 лица. В том числе это связано и с изменениями способов реализации программных продуктов.

Распространение экстремистской идеологии в сфере ИКТ оказывает влияние на динамику как террористической, так и экстремистской преступности[2]. В 2019 г. с использованием сети Интернет было совершено 346 преступлений террористической направленности, что составило 19% всех зарегистрированных террористических преступлений (1806). Для сравнения, в 2015 г.[3] удельный вес таких преступлений был равен 8,6% (133 от 1538).

С использованием сети Интернет совершается большинство преступлений экстремистской направленности. В 2019 г. они составили более половины от общего числа зарегистрированных преступлений этого вида (309 от 585).

В то же время в уголовном законодательстве Российской Федерации, как и в большинстве государств, специальный состав, посвященный кибертерроризму, отсутствует. Это представляется вполне оправданным. На наш взгляд, справедливо мнение исследователей, утверждающих, что угроза кибертерроризма в виде прямых атак на объекты критической инфраструктуры для достижения политических, религиозных или иных целей в определенной степени преувеличивается. Значительно больший ущерб экономике государства и гражданам наносит общеуголовная преступность с использованием

---

[1] См.: URL: https://habr.com/ru/post/437026/ (дата обращения: 05.07.2019).

[2] Организация экстремистского сообщества: проблемы квалификации и доказывания: пособие / П. В. Агапов и др.; под. ред. В. В. Меркурьева; Акад. Ген. Прокуратуры Рос. Федерации. М., 2013. 248 с.

[3] В 2015 г. в статистическую форму отчетности Антитеррор (282) была введена позиция «с использованием сети «Интернет».

ИКТ[1]. Информационные технологии используются террористическими организациями прежде всего с точки зрения возможностей обмена информацией и вербовки.

Стоит также отметить, что преступления, предусмотренные ст. 207 (заведомо ложное сообщение об акте терроризма) УК РФ, не включаются в статистику по преступлениям с использованием ИКТ. Вместе с тем в последние годы значительный сегмент сообщений о минировании перестал носить спонтанный характер, в целях сохранения анонимности злоумышленниками используется IP-телефония. На факты совершения преступлений с использованием современных технологий, в частности, указал советник председателя Национального антитеррористического комитета А. С. Пржездомский[2].

Очередная волна анонимных сообщений о минировании объектов инфраструктуры прокатилась осенью 2019 г. Это повлияло на динамику зарегистрированных преступлений, предусмотренных ст. 207 УК РФ, которые в том же году увеличились на 60,5% и составили 2465 преступлений (2018 г. — 1530).

Большинство преступлений совершались целенаправленно для дестабилизации работы правоохранительных органов, транспорта, образовательных учреждений, дезорганизации служб спасения, в том числе медицинских учреждений. Это обусловливает необходимость принятия мер по повышению качества и эффективности оперативно-разыскной деятельности, направленной на выявление, пресечение и раскрытие данных преступлений, совершенных с использованием ИКТ.

Ущерб, причиненный ложным сообщением об акте терроризма, подлежит возмещению путем предъявления к виновным лицам требований о возмещении ущерба, причиненного государству, предприятиям и организациям, и упущенной выгоды, а также требований о компенсации морального вреда. Для установления размера ущерба выясняются реальные затраты на устранение последствий сообщения (расходы на горюче-смазочные материалы автомобилей; амортизация транспорта, расходы, связанные с обеспечением безопасности в районе предполагаемого места происшествия, дополнительные расходы на оплату труда, сверхурочной работы, ущерб от возможного повреждения имущества, простоя и т.п.). Ряд проблемных вопросов, связанных с организацией работы по возмещению ущерба, причиненного совершением преступления, предусмотренного ст. 207 УК РФ, разъяснен

---

[1] *Кулешова Г. П.*, *Капитонова Е. А.*, *Романовский Г. Б.* Правовые основы противодействия кибертерроризму в России и за рубежом с позиции общественно-политического измерения // Всероссийский криминологический журнал. 2020. Т. 14. № 1. С. 156–165.

[2] См.: URL: https://rg.ru/2018/02/28/v-nak-obiasnili-zvonki-o-lzheminirovanii-huliganskim-povedeniem.html.

в информационном письме Генеральной прокуратуры Российской Федерации от 3 апреля 2019 г. № 8–12–2019.

Количество осужденных лиц, совершивших преступления, предусмотренные гл. 28 УК РФ, снизилось. Если в 2014 г. по ст. 272–274 УК РФ было осуждено 218 лиц, то в 2019 г. — уже 165 лиц. Обращает на себя внимание возрастной и образовательный состав осужденных. В 2019 г. треть (55) всех осужденных составляли лица в возрасте 18–24 лет, 22,4% (37) — лица 25–29 лет, 40,6% (67) — лица 30–49 лет. Высшее образование имели 37,6% (62) осужденных, среднее профессиональное — 29,1% (48), среднее общее — 24,8% (41), и лишь 8,5% осужденных имели основное общее или начальное образование (см. таблицу 1.8).

Таблица 1.8

Сведения о составе лиц, осужденных за совершение преступлений в сфере компьютерной информации (ст. 272–274[1] УК РФ) в период 2014–2019 гг.[1]

		2014	2015	2016	2017	2018	2019	Среднее
Всего		218	235	185	202	129	165	189
Из них осуждено	Женщин	9	9	10	11	16	24	13,2
	Лиц в возрасте:							
	14–17 лет	1	0	3	6	3	2	2,5
	18–24 лет	79	93	65	60	42	55	65,7
	25–29 лет	56	72	45	60	31	37	50,2
	30–49 лет	77	63	66	71	47	67	65,2
	50 лет и старше	5	7	6	5	6	4	5,5
	Иностранных граждан	6	5	6	6	1	0	4
	Имеющих образование:							
	высшее проф.	73	70	72	78	42	62	66,2
	среднее проф.	76	88	54	56	42	48	60,7
	среднее общее	57	62	49	50	35	41	49
	неполное среднее, начальное или нет образования	12	15	10	18	10	14	13,2

[1] Отчет Судебного департамента при Верховном Суде Российской Федерации «О составе осужденных, месте совершения преступления» по форме № 11 за период 2014–2019 гг.

Несмотря на то, что составить портрет компьютерного преступника, как и установить единый критерий, позволяющий выделить компьютерного преступника, достаточно сложно, так как виды и характер совершаемых преступлений достаточно широки, по результатам исследования личности преступника в сфере компьютерной информации на определенном этапе (более 20 лет назад) все же удалось сконструировать некий тип правонарушителя. Так, в 1998 г. в Экспертно-криминалистическом центре МВД России проведен классификационный анализ лиц, замеченных в применении компьютеров для совершения противоправных деяний. Обобщенный портрет отечественного хакера, созданный на основе этого анализа, выглядел следующим образом:

- мужчина в возрасте от 15 до 45 лет, имеющий многолетний опыт работы на компьютере либо почти не обладающий таким опытом;
- в прошлом к уголовной ответственности не привлекался;
- яркая мыслящая личность;
- способен принимать ответственные решения;
- хороший, добросовестный работник, по характеру нетерпимый к насмешкам и потере своего социального статуса среди окружающих его людей;
- любит уединенную работу;
- приходит на службу первым и уходит последним, часто задерживается на работе после окончания рабочего дня и очень редко использует отпуск и отгулы[1].

Типичным компьютерным преступником может быть как немолодой хакер, использующий телефон и домашний компьютер для получения доступа к большим компьютерам, так и служащий, которому разрешен доступ к системе[2]. Нельзя не согласиться с мнением экспертов о том, что обобщенный криминологический портрет преступника сильно изменился за это время и в основном не совпадает с реально существующим. Это обусловлено рядом объективных факторов. Например, за последние годы значительно возросла доступность разнообразной компьютерной техники (включая коммуникаторы, планшетные компьютеры и смартфоны) и появилась возможность беспроводного доступа к сети Интернет с высокими скоростями передачи данных[3].

Принимая во внимание, что в современных условиях социально-экономического развития России компьютерная преступность стала

---

[1] URL: http://www.lghost.ru/lib/security/kurs5/theme08_chapter01.htm#02 (дата обращения: 05.06.2020).

[2] URL: https://www.securitylab.ru/contest/382194.php (дата обращения: 05.06.2020).

[3] *Ефремов К. А.* Личность преступника, совершающего преступления в сфере компьютерной информации // Общество: политика, экономика, право. 2016. № 6. С. 92–95.

реальностью общественной жизни, выяснение причин ее возникновения и развития требует анализа сложившихся кризисных ситуаций, влияющих на социальное, экономическое и правовое развитие российского общества.

В Университете прокуратуры Российской Федерации в последние годы пристальное внимание уделяется вопросам прокурорского надзора за исполнением законов при выявлении, расследовании и предупреждении преступлений, совершаемых с использованием ИКТ (в 2018 г. подготовлен информационный обзор, в 2019 г. — научный доклад по указанной теме). В текущем году, наряду с настоящим исследованием, подготовлено соответствующее пособие. Основываясь на результатах анализа статистических данных, судебной практики, а также специализированной литературы, можно выделить основные **детерминанты** данной преступности:

— информационно-технологическое оборудование предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных;
— реальная возможность получения значительной экономической выгоды за противоправные деяния с использованием компьютерной техники;
— низкая эффективность работы правоохранительных органов, создающая ощущение безнаказанности;
— ненадлежащее отношение к вопросу обеспечения информационной безопасности;
— низкий уровень программно-технических средств защиты информации;
— небрежность в обеспечении конфиденциальности информации[1].

Среди основных причин компьютерной преступности заслуживает внимания классификация по сферам общественной жизни, предложенная К. Н. Евдокимовым.

Социальные причины компьютерной преступности следующие:

— всеобщая компьютеризация российского общества (активное развитие компьютерных технологий, информационно-телекоммуникационных сетей, информационных услуг, электронного документооборота и т.п.), что создает необходимую среду для деятельности компьютерных преступников[2];
— противоречия между реальными потребностями населения в информационных услугах, программной продукции и воз-

---

[1] *Богданова Т. Н.* Причины и условия совершения преступлений в сфере компьютерной информации // Вестник Челябинского государственного университета. 2013. № 11 (302). Серия «Право». Вып. 36. С. 64–67.

[2] См: *Вехов В. Б.* Компьютерные преступления: способы совершения и раскрытия / под ред. Б. П. Смагоринского. М.: Право и Закон, 1996. 182 с.

можностью их удовлетворения легальными способами в силу низкого уровня жизни;

— легкомысленное отношение российского общества к компьютерной преступности[1];

— доверчивость граждан при онлайн-покупке различных товаров и услуг (оплата товаров и услуг до их получения, особенно через интернет-кошельки, а не через расчетные счета банков). Изобретение новых способов отъема денег — появление в Интернете объявлений от благотворительных организаций с просьбой о помощи (при этом мошенники создают сайты-дублеры, меняя реквизиты для перечисления денег)[2].

В качестве ***правовых причин*** выступают:

— несовершенство российского уголовного законодательства в сфере борьбы с компьютерной преступностью[3]. По результатам анкетирования эффективность действующего законодательства в сфере компьютерной информации оценена прокурорами следующим образом: на среднем уровне — 54,3%; на низком — 41,3%; на высоком — 4,4%;

— отсутствие единообразной судебной практики по уголовным делам о компьютерных преступлениях. До сих пор отсутствуют разъяснения пленума Верховного Суда РФ по вопросам квалификации и определению наказаний за компьютерные преступления, что негативно сказывается на следственно-судебной практике и единообразии понимания и применения уголовно-правовых норм правоохранительными органами. Кроме того, недостаточная жесткость наказания компьютерных преступников, по нашему мнению, способствует рецидиву совершения преступлений данной категории и дальнейшему развитию компьютерной преступности в нашей стране;

— недостатки в деятельности органов предварительного следствия, дознания и органов, осуществляющих оперативно-разыскную деятельность.

В последние годы отмечается появление причин и условий, носящих ***политический характер***, затрагивающих сферу национальной безопасности и обороны, международных отношений, функциони-

---

[1] Теоретические основы предупреждения преступности на современном этапе развития российского общества: монография / под общ. ред. Р. В. Жубрина; Академия Генеральной прокуратуры Российской Федерации. М.: Проспект, 2016. 655 с.

[2] РГ. Федеральный выпуск. № 6707 (136).

[3] *Евдокимов Е. Н.* Проблемы квалификации и предупреждения компьютерных преступлений: монография. Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2009. 142 с.

рования государственной власти и местного самоуправления[1]. Среди них, в частности, выделяют: отсутствие эффективного государственного контроля над киберпространством и средствами массовой информации; существование и развитие «хактивистского» движения; использование кибероружия между враждующими (соперничающими) государствами в геополитическом аспекте (кибершпионаж).

С методологической точки зрения причины, определяющие развитие компьютерной преступности в современной России, представляется возможным классифицировать по сферам общественной жизни и на основании этого критерия выделить следующие их виды: экономические, кадровые, технические, организационные, корпоративные.

Экономические причины компьютерной преступности в России:

— использование вредоносных компьютерных программ производителями программного обеспечения в целях недобросовестной конкуренции между ними и для получения сверхприбылей[2];
— компьютерное преступление рассматривается преступниками как способ быстрого и относительного безопасного незаконного обогащения;
— возможность использования преступниками информационных ресурсов персональных компьютеров и корпоративных компьютерных сетей в корыстных целях путем создания ботнетов (сетей «зомби-компьютеров»)[3], в том числе проведение кибератак с целью вымогательства. Злоумышленники все чаще используют взломанные серверы для майнинга (добычи) криптовалют;
— резкие изменения (падение) курсов всех криптовалют. В результате DDoS-атаки остаются одним из простейших методов монетизации вредоносного программного обеспечения, будь то зараженные серверы или ботнеты, основанные на персональных компьютерах и телефонах[4].

Говоря о социально-экономических факторах, влияющих на преступность в сфере компьютерной информации, первое место респонденты отдают низкой компьютерной грамотности населения — 63%. Далее следуют: особенности этого вида преступлений как быстрого

---

[1] Теоретические основы предупреждения преступности на современном этапе развития российского общества: монография / под общ. ред. Р. В. Жубрина; Академия Генеральной прокуратуры Российской Федерации. М.: Проспект, 2016. 665 с.

[2] *Евдокимов Е. Н.* Проблемы квалификации и предупреждения компьютерных преступлений: монография. Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2009. 142 с.

[3] Теоретические основы предупреждения преступности на современном этапе развития российского общества: монография / под общ. ред. Р. В. Жубрина; Академия Генеральной прокуратуры Российской Федерации. М.: Проспект, 2016. 665 с.

[4] URL: https://rg.ru/2019/03/05/chislo-kiberatak-na-kreditnye-organizacii-vyroslo-v-dva-raza.html (дата обращения: 13.09.2018).

и относительно безопасного способа незаконного обогащения — 45,7%; переход на безналичные расчеты — 39,6%; компьютеризация российского общества — 38,7%; низкий уровень жизни населения — 8,8%; недобросовестная конкуренция между производителями программного обеспечения и антивирусной защиты — 7,3%; безработица — 3,2%; высокая налоговая нагрузка — 1,2%.

Кадровые причины компьютерной преступности в России:

недостатки в деятельности органов предварительного следствия при расследовании уголовных дел по компьютерным преступлениям (неправильная оценка деяний как не содержащих состава преступления или как «малозначительных»; неумение органов предварительного расследования должным образом доказывать виновность по данным видам преступлений; нежелание должностных лиц расследовать сложные посягательства подобного рода; недостатки в системе учета преступлений и т.п.)[1].

Официальная статистика показывает, что в 2018 г. по 74,9% преступлений, предусмотренных гл. 28 УК РФ, уголовные дела были приостановлены на стадии предварительного следствия[2]. Причем в последние годы прослеживается тенденция к росту количества приостановленных уголовных дел. Так, их доля в 2015 г. составила 30,9%, в 2016 г. — 46,7%, в 2017 г. — 58,7%. В 2019 г. количество преступлений, уголовные дела по которым приостановлены на основании п. 1 ч. 1 ст. 208 УПК РФ, составило свыше 206 тыс. (+72,5%). Во многих случаях такие решения принимались при явной неполноте следствия и дознания, в связи с чем четверть из них отменены прокурорами как незаконные.

Следует отметить, что по всем преступлениям, совершенным в сфере ИКТ, качество предварительного следствия заметно не отличается. Это подтверждает тезис о недостатках проводимого расследования преступлений данного вида и качества подготовки следователей;

недостатки в деятельности органов и должностных лиц, осуществляющих оперативно-разыскную деятельность по компьютерным преступлениям. С учетом транснационального и трансграничного характера рассматриваемых преступлений сложность в раскрытии указанных преступлений очевидна. Раскрываемость[3] таких преступлений остается невысокой (26,6% в 2018 г., 24,3% в 2017 г., 23,8% в 2016 г.,

---

[1] См.: Противодействие киберпреступности в аспекте обеспечения национальной безопасности: монография / П. В. Агапов и др.; Акад. Ген. прокуратуры Рос. Федерации. М., 2014. 135 с.

[2] См: Сводные отчеты по формам 1-ЕГС и 4-ЕГС по РФ.

[3] Под раскрываемостью понимается удельный вес количества преступлений, уголовные дела по которым окончены расследованием либо разрешены, в структуре преступлений, уголовные дела по которым окончены расследованием либо разрешены, и преступлений, уголовные дела по которым впервые приостановлены.

34,5% в 2015 г.), что значительно ниже раскрываемости по всем видам преступлений, которая на протяжении указанного периода сохраняется на уровне 55–56%. Общая раскрываемость преступлений в сфере использования информационно-коммуникационных технологий в 2019 г. составила всего 24%. Следовательно, работа оперативных подразделений не в полной мере соответствуют существующим угрозам.

Значительная часть опрошенных респондентов (72,7%) признает, что эффективность деятельности правоохранительных органов по борьбе с преступностью в сфере компьютерной информации крайне низкая. Только четверть респондентов оценивают ее на среднем уровне. Среди недостатков в деятельности правоохранительных органов отмечены следующие: несовершенство технологий выявления и борьбы с этими преступлениями (67,9%); недостатки при осуществлении оперативно-разыскной деятельности по компьютерным преступлениям (61,6%) и при расследовании уголовных дел данной категории (27,1%); несовершенство судебной практики по уголовным делам о преступлениях в сфере компьютерной информации (19,6%).

Организационно-технические причины компьютерной преступности в России:

1. Высокая латентность компьютерных преступлений, обусловленная их высокотехнологичностью, инновационностью в сфере компьютерной информации и IT-технологий. По информации Национального координационного центра по компьютерным инцидентам (НКЦКИ), только в 2018 г. на Россию было совершено более 4,3 млрд кибератак на критическую информационную инфраструктуру, 17 тысяч из них — наиболее опасные. Только на информационную инфраструктуру ЧМ-2018 совершено более 25 млн вредоносных воздействий[1].

Неслучайно большая часть (более 40%) опрошенных в ходе исследования прокуроров считает, что уровень латентности компьютерной преступности занижен почти в 2 раза. К основным причинам респонденты отнесли сложность выявления преступлений в сфере компьютерной информации (53%), скрытость для большинства населения (примерно 51%), создание новых IT-технологий, увеличение пользователей сети Интернет, мобильных компьютерных устройств, переход к электронному документообороту (43%); отсутствие эффективного государственного контроля над киберпространством и средствами массовой информации (33%).

2. Наличие у большинства веб-сайтов уязвимостей, которые могут приводить к утечке персональных и иных данных пользователей. Наиболее распространенной уязвимостью аналитики называют «межсайтовое выполнение сценариев». Этот недостаток систем поз-

[1] См.: URL: https://rg.ru/2018/12/12/za-god-na-rossiiu-bylo-sovershenno-bolee-chetyreh-milliardov-kiberatak.html/ (дата обращения: 04.07.2019).

воляет злоумышленникам создавать копии страниц для сбора данных пользователей. Такая уязвимость базируется на недостаточной проверке источника, отправляющего на сайт запрос на авторизацию. В итоге пользователь, отправив запрос, получает поддельную страницу, вводит данные, которые попадают к злоумышленнику. Поддельный сервис при этом вводит данные в настоящую форму без ведома пользователя. В большинстве веб-приложений экспертами обнаружены «ошибки конфигурации», когда система самого сайта раскрывает в своих стандартных параметрах информацию о пользовательском персональном оборудовании и путях его установки, что дает возможность собрать информацию для дальнейшей атаки. В основном уязвимости ищут в тех приложениях, которые представляют финансовый интерес. Наиболее очевидной мишенью становятся форумы и интернет-магазины, которые используют единые системы управления контентом, а также социальные сети и порталы крупных компаний и интернет-гигантов.

Утечка учетных записей грозит пользователям потерей их аккаунтов и кражей всей информации, которая в них хранится, которая в дальнейшем используется злоумышленниками для выполнения действий от имени законных владельцев взломанных аккаунтов. Такого рода данные могут быть использованы злоумышленниками впоследствии для социальной инженерии, когда, к примеру, представляясь сотрудниками различных компаний, злоумышленники оперируют реальными данными клиентов и вводят последних в заблуждение, подталкивая их к совершению тех или иных ошибочных действий. Злоумышленник может запустить определенный скрипт (программа или программный файл, автоматически исполняющий тот или иной сценарий без ручного использования интерфейса программы) внутри веб-приложения, который может дать ему права администратора, а в дальнейшем позволит проникнуть на сервер и в базы данных компании, получить контроль над операционной системой всего сервера.

Корпоративные причины компьютерной преступности предполагают организованный и профессиональный характер компьютерной преступности, позволяющий преступникам считать себя «хакерским» сообществом, научно-техническим андеграундом. В свою очередь, для поддержания такого неординарного статуса и подтверждения принадлежности к криминальному миру предполагается дальнейшее совершение компьютерных преступлений.

Самодетерминации такой преступности способствует также свободное размещение в сети Интернет информации самого разного свойства, в том числе и криминального, и доступ к ней неограниченного круга лиц как фактор, стимулирующий совершение пре-

ступления молодыми лицами с низкой нравственной и правовой культурой[1].

Безусловно, быстрый количественный рост преступности и ее качественные изменения, обусловленные обострением противоречий в различных областях общественной жизни, несовершенство и серьезные упущения в правоприменительной практике, на наш взгляд, способствуют ускорению процессов развития компьютерной преступности как социального явления.

В свою очередь, устранение рассмотренных причин компьютерной преступности, безусловно, должно носить комплексный характер.

В ходе настоящего исследования выявлена прямая умеренная корреляционная зависимость[2] между коэффициентом преступлений, совершенных с использованием ИКТ, и следующими коэффициентами социально-экономических показателей (зависимость указывает на то, что на эти показатели действуют одни и те же факторы).

1. Потребность работодателей (человек на 100 тыс. жителей). Коэффициент корреляции — 0,46. В тех субъектах Российской Федерации, где больше потребность работодателей, там и больше коэффициент преступности. На рис. 1 представлено распределение социального показателя в типологических группах[3] (по значению коэффициента преступности).

В тех группах, где больше коэффициент преступности, там и больше потребность работодателей. Исключение: в группе III со средним коэффициентом преступности потребность работодателей — 1128 чел. на 100 тыс. жителей, в группе IV с коэффициентом преступности выше среднего потребность работодателей — только 1004.

Дисперсионный анализ выявил, что разнообразие значений коэффициента преступности на 20,3% обусловлено разнообразием коэффициента потребности работодателей.

2. Профицит (дефицит) бюджета (тыс. рублей на 100 тыс. жителей). Коэффициент корреляции — 0,44. В тех субъектах Российской Федерации, где больше профицит (дефицит) бюджета, там и больше коэффициент преступности. На рис. 2 представлено распределение социального показателя в типологических группах (по значению коэффициента преступности).

---

[1] *Кесареева Т. П.* Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: автореф. дис. ... канд. юрид. наук. Специальность 12.00.08 / Генеральная прокуратура РФ. Научно-исследовательский институт проблем укрепления законности и правопорядка. М., 2002. 25 с.

[2] *Коимшиди Г. Ф.*, *Черникова И. А.*, *Камаев Б. Г.* Анализ рядов динамики (методы математической статистики в криминологии и социологии): учебно-методическое пособие. М.: ВНИИ МВД России, 2007. 47 с.

[3] Здесь и далее использованы данные Росстата // URL: https://gks.ru/bgd/free/B02_83/Main.htm (дата обращения: 05.06.2020).

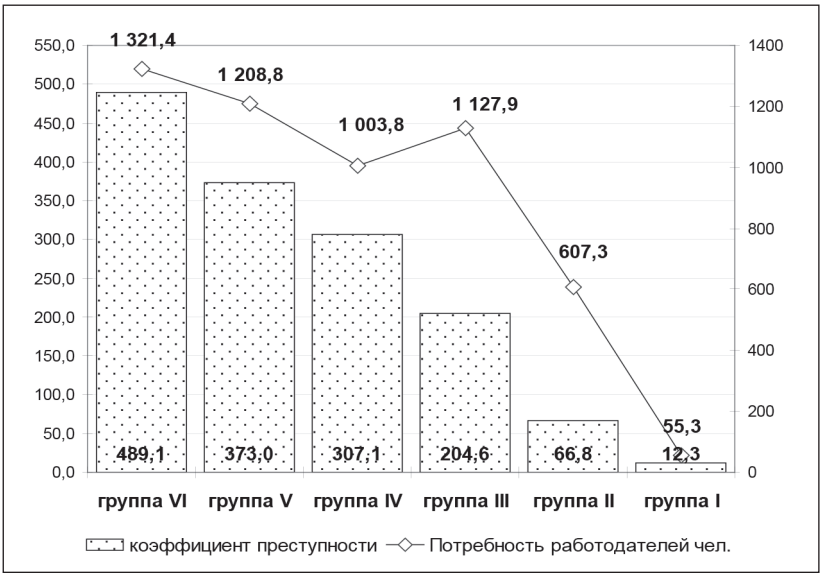

Рис. 1. *Распределение социального показателя (потребность работодателей) в типологических группах (по значению коэффициента преступности)*

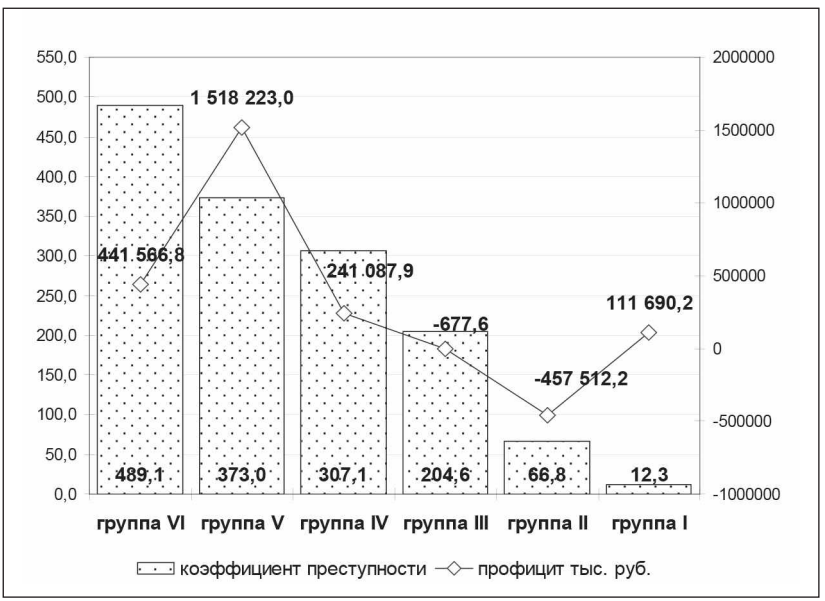

Рис. 2. *Распределение социального показателя (профицит бюджета) в типологических группах (по значению коэффициента преступности)*

В тех группах, где больше коэффициент преступности, там и больше профицит (дефицит). Исключение: в группе I с низким коэффициентом преступности профицит бюджета — 111,7 млн руб. на 100 тыс. жителей, а в группе III со средним коэффициентом преступности дефицит бюджета — 677,6 тыс. руб.

Дисперсионный анализ выявил, что разнообразие значений коэффициента преступности на 23,8% обусловлено разнообразием коэффициента профицита (дефицита) бюджета.

3. Удельный вес безработных в структуре всей рабочей силы (%). Коэффициент корреляции составляет 0,42. В тех субъектах Российской Федерации, где больше удельный вес безработных в структуре всей рабочей силы, там и больше коэффициент преступности. На рис. 3 представлено распределение социального показателя в типологических группах (по значению коэффициента преступности).

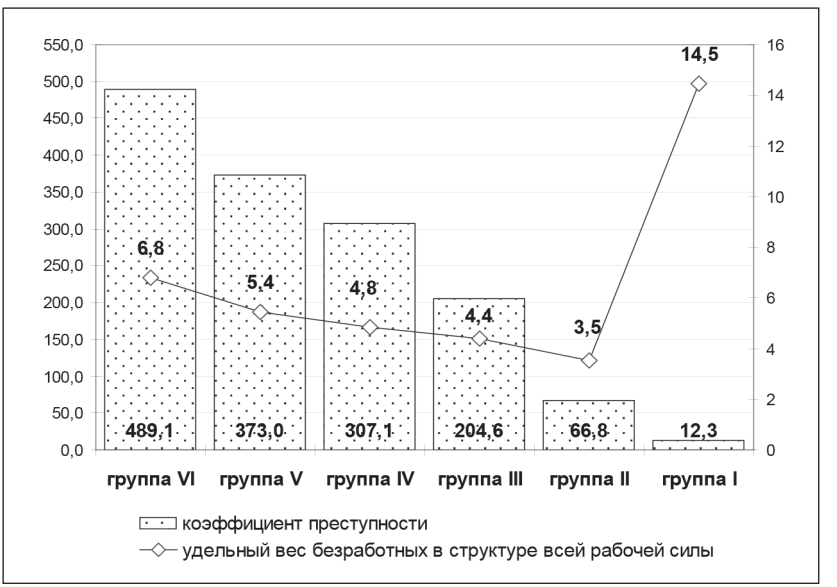

Рис. 3. *Распределение социального показателя (удельный вес безработных) в типологических группах (по значению коэффициента преступности)*

В тех группах, где больше коэффициент преступности, там и больше удельный вес безработных в структуре всей рабочей силы. Исключение: в группе I с низким коэффициентом преступности удельный вес безработных в структуре всей рабочей силы 14,5%, а в группе V с высоким коэффициентом преступности удельный вес безработных в структуре всей рабочей силы 5,4%.

Дисперсионный анализ выявил, что разнообразие значений коэффициента преступности на 48,6% обусловлено разнообразием удельного веса безработных в структуре всей рабочей силы.

4. Индекс потребности работодателей (рост в%). Коэффициент корреляции составляет 0,41. В тех субъектах Российской Федерации, где больше рост потребности работодателей, там и больше коэффициент преступности. На рис. 4 представлено распределение социального показателя в типологических группах (по значению коэффициента преступности).

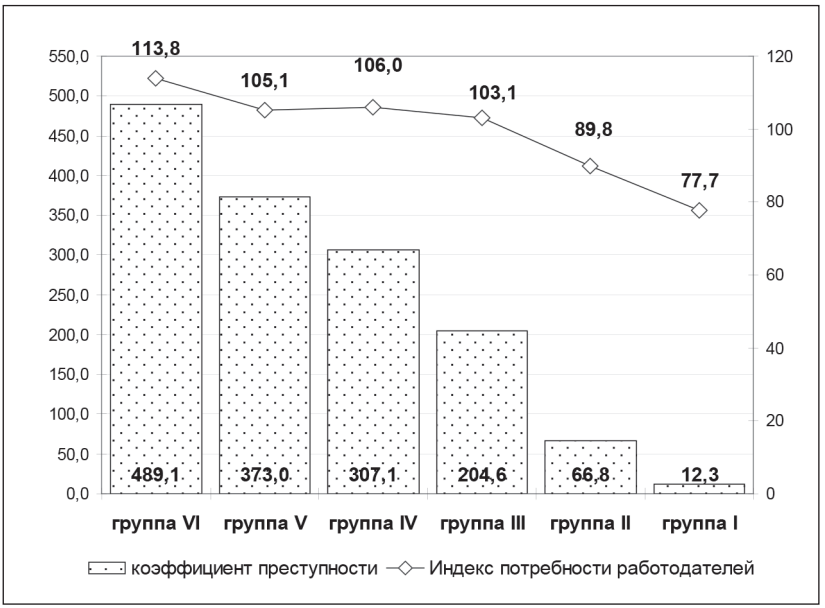

Рис. 4. *Распределение социального показателя (индекс потребностей работодателя) в типологических группах (по значению коэффициента преступности)*

В тех группах, где больше коэффициент преступности, там и больше рост потребности работодателей. Исключение: в группе IV с коэффициентом преступности выше среднего рост потребности работодателей — 106%, а в группе V с высоким коэффициентом преступности рост потребности работодателей немного меньше — 105,1%.

Дисперсионный анализ выявил, что разнообразие значений коэффициента преступности на 19,1% обусловлено разнообразием индекса потребности работодателей.

5. Уровень безработных (количество безработных на 100 тыс. населения). Коэффициент корреляции составляет 0,38. В тех субъектах

Российской Федерации, где больше уровень безработных, там и больше коэффициент преступности. На рис. 5 представлено распределение социального показателя в типологических группах (по значению коэффициента преступности).

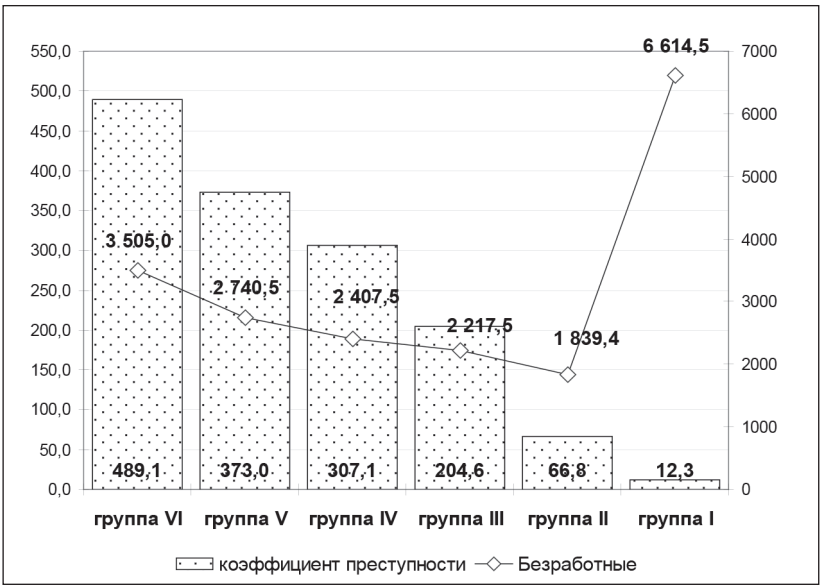

Рис. 5. *Распределение социального показателя (уровень безработных) в типологических группах (по значению коэффициента преступности)*

В тех группах, где больше коэффициент преступности, там и больше уровень безработных. Исключение: в группе I с низким коэффициентом преступности уровень безработных самый высокий — 6614,5 безработных на 100 тыс. населения.

Дисперсионный анализ выявил, что разнообразие значений коэффициента преступности на 44,2% обусловлено разнообразием уровня безработных.

Кроме того, выявлена обратная умеренная корреляционная зависимость между коэффициентом преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, и следующими коэффициентами социально-экономических показателей.

1. Индекс безработных (рост в процентах). Коэффициент корреляции составляет –0,43. В тех субъектах Российской Федерации, где больше индекс безработных, там меньше коэффициент преступности. На рис. 6 представлено распределение социального показателя в типологических группах (по значению коэффициента преступности).

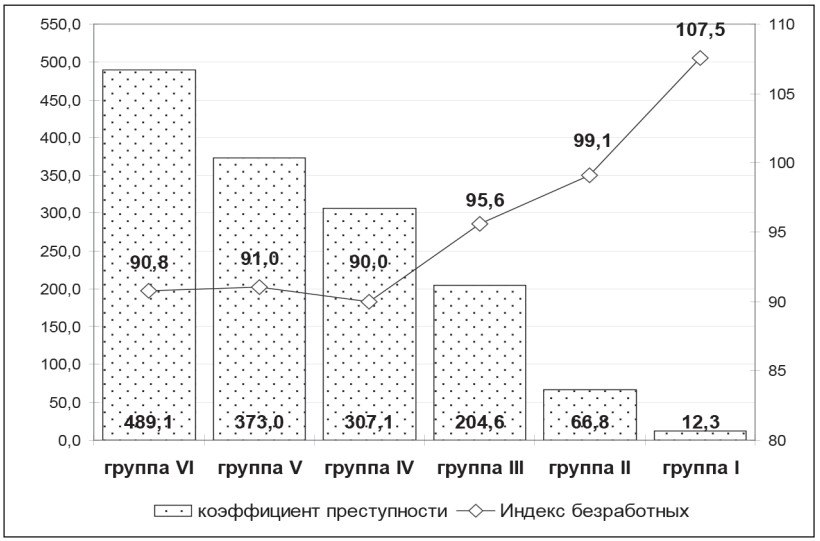

Рис. 6. *Распределение социального показателя (индекс безработных) в типологических группах (по значению коэффициента преступности)*

В тех группах, где больше коэффициент преступности, там меньше индекс безработных. Исключение: в группе V с высоким коэффициентом преступности индекс безработных — 91,0, а в группе IV с коэффициентом преступности выше среднего индекс безработных немного меньше — 90,0%.

Дисперсионный анализ выявил, что разнообразие значений коэффициента преступности на 20,3% обусловлено разнообразием индекса безработных.

2. Уровень миграционного прироста (чел на 100 тыс. населения). Коэффициент корреляции составляет –0,41. В тех субъектах Российской Федерации, где больше уровень миграционного прироста, там меньше коэффициент преступности. На рис. 7 представлено распределение социального показателя в типологических группах (по значению коэффициента преступности).

В тех группах, где больше коэффициент преступности, там меньше уровень миграционного прироста. Исключение — в группе I с низким коэффициентом преступности. В 2019 г. уровень мигрантов снизился на 100,3 человек на 100 тыс. населения. А в группе IV с коэффициентом преступности выше среднего уровень мигрантов снизился только на 30,7.

Дисперсионный анализ выявил, что разнообразие значений коэффициента преступности на 19,4% обусловлено разнообразием уровня миграционного прироста.

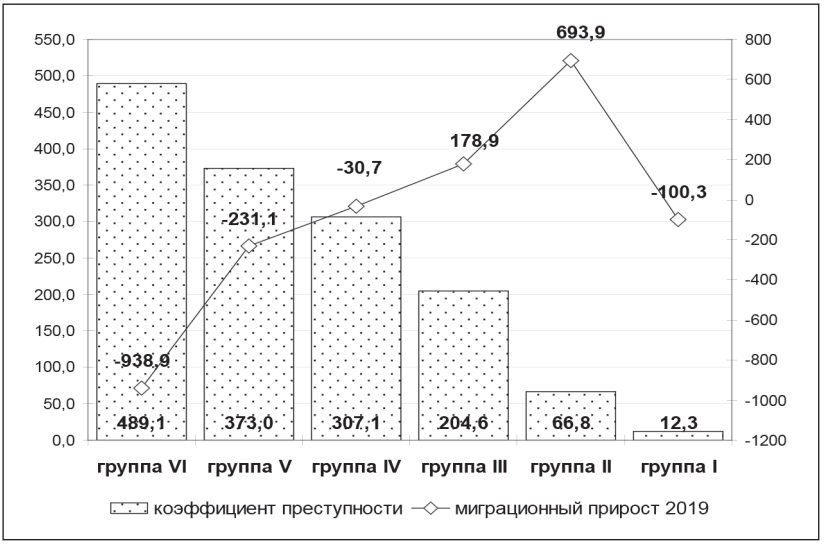

Рис. 7. *Распределение социального показателя (уровень миграционного прироста) в типологических группах (по значению коэффициента преступности)*

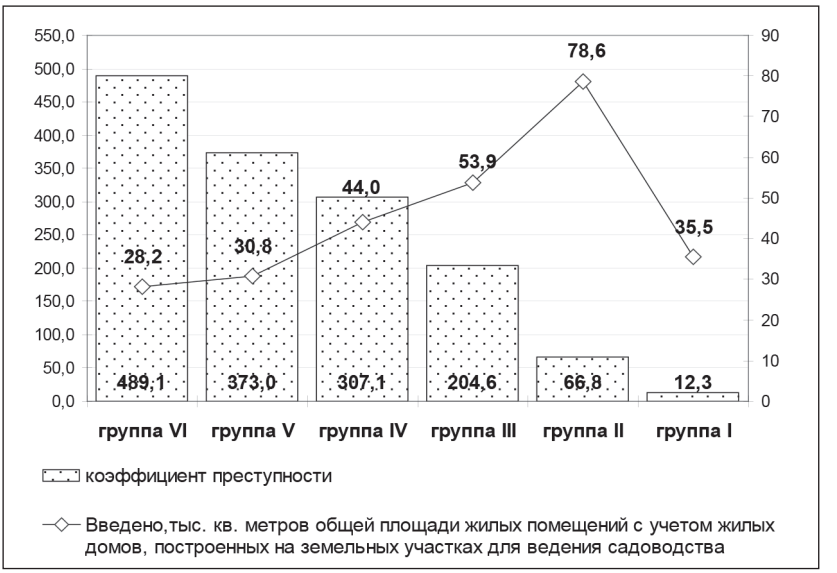

Рис. 8. *Распределение социального показателя (уровень ввода жилых домов) в типологических группах (по значению коэффициента преступности)*

3. Уровень ввода жилых домов как с учетом жилых домов, построенных для ведения садоводства (тыс. кв. метров на 100 тыс. населения), так и без них. Коэффициент корреляции составляет –0,37. В тех субъектах Российской Федерации, где больше уровень ввода жилых домов, там меньше коэффициент преступности. На рис. 8 представлено распределение социального показателя в типологических группах (по значению коэффициента преступности).

В тех группах, где больше коэффициент преступности, там ниже уровень ввода жилых домов с учетом жилых домов, построенных для ведения садоводства. Исключение: в группе I с низким коэффициентом преступности, где уровень ввода жилых домов с учетом жилых домов, построенных для ведения садоводства (35,5 тыс. кв. метров на 100 тыс. населения), меньше, чем в группе IV с коэффициентом преступности выше среднего (44,0).

Дисперсионный анализ выявил, что разнообразие значений коэффициента преступности на 18,3% обусловлено разнообразием уровня ввода жилых домов с учетом жилых домов, построенных для ведения садоводства.

Бесспорно, что заметное влияние на уровень преступности оказывают социально-экономические факторы. Таким образом, с помощью факторного и корреляционного анализа из всей совокупности факторов были выделены наиболее существенные, которые достаточно точно характеризуют состояние преступности в компьютерной сфере в нашей стране. Проведенный корреляционный анализ показал связь отдельных социально-экономических факторов (потребность работодателей; профицит (дефицит) бюджета; удельный вес безработных в структуре всей рабочей силы; индекс потребности работодателей; уровень безработных) с коэффициентом преступлений, совершенных с использованием ИКТ. После построения корреляционной матрицы также проведен анализ, в ходе которого определены те факторы (индекс безработных; уровень миграционного прироста; уровень ввода жилых домов), которые совершенно не коррелируют с рассматриваемыми преступлениями.

Прикладная актуальность проведенного анализа социально-экономических детерминант преступности позволяет проводить перспективное планирование деятельности правоохранительных органов, также устанавливать тенденции изменения уровня преступности данного вида. В дальнейшем можно использовать полученные модели для построения прогноза количества преступлений и факторов, влияющих на преступность указанной категории.

В качестве мер, необходимых для повышения эффективности противодействия преступлениям в сфере компьютерной информации, значительная часть опрошенных респондентов (41%) указала на не-

обходимость привлечения на стадиях выявления преступлений и расследования уголовных дел специалистов в области IT-технологий; налаживание международного сотрудничества правоохранительных органов в борьбе с преступлениями в указанной сфере. На совершенствование координации деятельности правоохранительных органов в борьбе с преступлениями в сфере компьютерной информации указывают 38%, повышение компьютерной компетенции работников правоохранительных органов — 35%, формирование единообразной судебной практики по уголовным делам о компьютерных преступлениях — 33%, своевременное выявление жертв преступлений — 25%, улучшение материально-технического обеспечения государственных органов, осуществляющих противодействие компьютерным преступлениям, — 21%.

Во взаимодействии с заинтересованными правоохранительными органами и Банком России Генеральной прокуратурой Российской Федерации разработан комплекс практических мер по повышению эффективности деятельности по борьбе с компьютерными преступлениями. Среди практических мер по организации борьбы с компьютерными преступлениями можно выделить следующие:

- подготовка единых критериев отнесения преступлений к совершенным с использованием (применением) информационно-телекоммуникационных технологий;
- принятие дополнительных мер, направленных на усиление эффективности профилактической работы с населением, повышение уровня правовой и финансовой грамотности граждан;
- изучение практики выявления нарушений, предусмотренных ст. 13.29–13.30 КоАП РФ, и привлечение к ответственности за их совершение, с принятием дополнительных мер, направленных на пресечение фактов незаконной реализации идентификационных модулей абонентов (СИМ-карт); с этой целью организация проверок мест розничной и оптовой торговли, транспортных узлов и иных общественных мест;
- разработка дополнительных средств и способов обеспечения постоянного мониторинга средств информационной коммуникации в целях предупреждения распространения в сети Интернет запрещенной информации и нарушения прав граждан в потребительском секторе;
- выработка механизма внесудебной блокировки «зеркал» сайтов, ранее заблокированных;
- проработка вопроса о внедрении автоматизированных информационно-поисковых систем «Дистанционные преступления» в единую систему правоохранительных и контролирующих ор-

ганов в целях предупреждения совершения преступлений, выявления их на стадии приготовления и привлечения лиц, их совершающих, к уголовной ответственности и другие.

В заключение отметим следующие негативные тенденции преступности с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации:

— высокая латентность преступлений, предусмотренных гл. 28 УК РФ, обусловленная сложностью их выявления, а также внедрением новых информационных технологий;
— отсутствие необходимости в наличии специальных знаний и навыков для совершения большинства преступлений с использованием информационно-телекоммуникационных сетей;
— возрастание угрозы сохранности персональных данных граждан;
— новые риски кибербезопасности, возникшие вследствие распространения новых инфекционных заболеваний в 2019–2020 гг. и изоляции граждан, в том числе увеличение мошенничеств с помощью ИКТ.

С учетом этого, на наш взгляд, важно уделять особое внимание выявлению и расследованию преступлений в сфере компьютерной информации (гл. 28 УК РФ), в том числе установлению лиц, создающих и реализующих вредоносные компьютерные программы, используемые для совершения преступлений. Кроме того, важно принять меры по повышению уровня грамотности населения в сфере информационных технологий.

Также целесообразно рассмотреть вопрос о введении в ст. 207 УК РФ ответственности за заведомо ложное сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, совершенное с использованием ИКТ.

Прямая корреляционная зависимость между коэффициентом преступлений, совершенных с использованием ИКТ, и коэффициентами отдельных социально-экономических показателей (профицит (дефицит) бюджета, уровень безработных, уровень миграционного прироста и др.) свидетельствует, что компьютерная преступность обусловлена рядом взаимозависимых социально-экономических факторов. Исходя из этого эффективный прокурорский надзор на направлениях, не касающихся напрямую противодействия компьютерной преступности, будет способствовать как профилактике преступности в целом, так и компьютерной преступности в частности. В этом отношении особое внимание необходимо уделять совершенствованию координации деятельности субъектов профилактической деятельности.

1.2. Квалификация прокурором преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации

Удешевление высокотехнологичного производства, совершенствование компьютерной техники и научно-технический прогресс в целом обусловили проникновение ИКТ во все сферы жизни общества. Не явилась исключением и сфера преступности. С одной стороны, блага тотальной информатизации используются в целях совершения «общеуголовных» преступлений, объективная сторона которых может быть выполнена посредством использования ИКТ и ИКС, с другой стороны, появилась самостоятельная группа компьютерных преступлений, посягающих на охраняемую законом информацию и безопасность информационно-коммуникационной инфраструктуры.

Сообразно развитию новейших технологий, эволюции регулятивных и охранительных правоотношений в этой сфере актуализируются проблемы уголовно-правовой оценки посягательств, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации.

Статья 272 УК РФ устанавливает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. Под компьютерной информацией в соответствии с п. 1 примечания к указанной статье следует понимать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Несмотря на существование легального определения компьютерной информации, в теории уголовного права нет единого мнения относительно содержания отдельных признаков предмета преступления. Так, различным образом сегодня трактуется признак «охраняемая законом информация».

Наиболее распространена позиция, согласно которой под охраняемой законом информацией следует понимать лишь закрытую информацию, то есть составляющую государственную, служебную, коммерческую, банковскую, врачебную, нотариальную, адвокатскую тайну, персональные данные и т.д.[1] В методических рекомендациях Генеральной прокуратуры Российской Федерации, в частности, указано, что по смыслу ст. 272 УК РФ охраняемой законом информацией являются лишь сведения, в отношении которых установлен специаль-

[1] *Гузеева О. С.* Квалификация преступлений в сфере компьютерной информации. М., 2016. С. 30.

ный режим правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные)[1]. Поддерживается такой подход и в судебной практике.

Апелляционным приговором Судебной коллегии по уголовным делам Верховного Суда Чувашской Республики был отменен обвинительный приговор нижестоящего суда по следующим основаниям. По смыслу закона под охраняемой законом понимается информация, для которой установлен специальный режим ее правовой защиты. Судом первой инстанции сделаны выводы, что информация (новости, советы логопеда, психолога и т.п.) охраняется законом. Однако информация, содержащаяся на сайте, в редактировании и удалении которой признана виновной К., является общедоступной информацией, к ней относятся общеизвестные сведения, и в отношении нее отсутствует необходимость установления специального режима ее правовой защиты[2].

Существо противоположного подхода к уголовно-правовой оценке охраняемой законом информации сводится к тому, что общедоступная информация, в том числе та, что размещена в свободном доступе в сети Интернет, также является защищаемой[3]. На этом основании ученые заключают, что доступ к компьютерной информации является неправомерным при любом обращении к информации вопреки воле ее владельца[4]. Следует заметить, что у такой позиции есть весьма убедительное нормативное обоснование. Согласно ст. 6 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» любой обладатель информации сам вправе устанавливать режим доступа к своей информации, если иное не предусмотрено федеральными законами. Кроме того, в соответствии с Приказом Минкомсвязи России от 27 июня 2013 г. № 149 «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети Интернет в форме открытых данных, а также для обеспечения ее использования» общедоступная информация, размещаемая на сайте

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс» (дата обращения: 10.08.2020).

[2] Апелляционный приговор от 3 июня 2015 г. по делу № 22-1054/2015 / Судебная коллегия по уголовным делам Верховного суда Чувашской Республики // ГАС «Правосудие». URL: https://www.bsr.sudrf.ru/ (дата обращения: 01.01.2019).

[3] См., например: *Русскевич Е. А.* Неправомерный доступ к компьютерной информации: теория и судебная практика // Судья. 2018. № 10. С. 46–49.

[4] См.: *Доронин А. М.* Уголовная ответственность за неправомерный доступ к компьютерной информации: автореф. дис. ... канд. юрид. наук. М., 2003. С. 6; *Малышенко Д. Г.* Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук. М., 2002. С. 58; *Дремлюга Р. И.* Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // Уголовное право. 2018. № 4. С. 52–57.

в форме открытых данных, должна быть защищена от уничтожения, модификации, блокирования, а также от иных неправомерных действий в отношении такой информации.

Указанная позиция находит широкое отражение в судебной практике. Так, по одному из уголовных дел суд указал, что если владелец информации предпринял меры по ее защите, то информация признается охраняемой по закону в контексте ст. 272 УК РФ, также как и информация, которая явно указана законом или другим нормативным актом как таковая[1].

Полагаем, что проиллюстрированный подход в большей мере соответствует законодательной формулировке предмета преступления и обеспечивает должный уровень защиты общества, граждан и организаций от посягательств на охраняемую законом компьютерную информацию. Вместе с тем в тех случаях, когда компьютерная информация, подвергшаяся форматированию, находилась в свободном доступе, содеянное в силу малозначительности может не представлять общественной опасности, что должно влечь применение положений ч. 2 ст. 14 УК РФ.

Особенностью компьютерных преступлений в целом и неправомерного доступа к компьютерной информации в частности является их «инструментальный» характер. Сами по себе компьютерные преступления не представляют интереса для злоумышленников, они выступают, как правило, способом достижения иных преступных целей. В связи с этим наиболее распространенными вопросами, возникающими при применении соответствующих статей, является возможность квалификации компьютерных преступлений по совокупности с иными преступными деяниями (ст. 128[1], 137, 138, 165, 183, 283, 283[1] УК РФ и др.).

Сложности возникают при уголовно-правовой оценке посягательств на информацию, находящуюся в электронной форме и ограниченную в доступе. К таковой относятся личная, семейная, банковская и другие тайны. Подобные деяния необходимо квалифицировать по совокупности со ст. 272 УК РФ, если они совершены путем незаконного доступа именно к компьютерной информации[2].

Так, А. с помощью персонального компьютера, используя полученные путем обмана у Л. ее логин и пароль от персональной страницы в социальной сети «ВКонтакте», осуществил доступ к хранящейся на ней компьютерной информации, а именно личной переписке Л. с другими пользователями, и с помощью компьютерной программы сделал скриншоты ее личной переписки, тем самым скопировал

---

[1] Определение Курганского областного суда от 25 июня 2013 г. по делу № 22-1475/2013 // ГАС «Правосудие». URL: https://www.bsr.sudrf.ru/ (дата обращения: 01.01.2019).

[2] См.: *Шарков А. Е.* Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук. Ставрополь, 2004. С. 8.

компьютерную информацию к себе на персональный компьютер[1]*. Деяние А. было верно квалифицировало по ч. 1 ст. 272 и ч. 1 ст. 138 УК РФ как неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло копирование информации, а также как нарушение тайны переписки и иных сообщений граждан.*

Между тем нередко аналогичные посягательства получают неполную уголовно-правовую оценку и квалифицируются лишь по ст. 272 УК РФ.

К примеру, гражданин А. с помощью персонального компьютера получил неправомерный доступ к охраняемой законом компьютерной информации — СМС-сообщениям, поступающим на мобильный телефон П., скопировав их содержание на используемый им в сети интернет-сервер. Приговором суда А. был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 272 УК РФ (совершение неправомерного доступа к охраняемой законом компьютерной информации)[2]*.*

Очевидно, что в результате противоправных действий А. вред был причинен самостоятельному объекту уголовно-правовой охраны — общественным отношениям, обеспечивающим реализацию права на тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан. Таким образом, действия А. должны быть квалифицированы не только по ч. 1 ст. 272 УК РФ, но и по ч. 1 ст. 138 УК РФ.

Аналогичным образом следует подходить к оценке действия лица, когда оно путем неправомерного доступа осуществляет копирование, модификацию, уничтожение или блокирование компьютерной информации, составляющей коммерческую или государственную тайны. Подобные действия должны квалифицироваться по совокупности ст. 272 и 183 УК РФ или ст. 272 и 283[1] УК РФ соответственно.

Так, Г., являясь работником ООО «М», не имел доступа к коммерческой тайне. Вместе с тем, используя логин и пароль А., действуя со своего персонального компьютера, получил доступ к сведениям, составляющим коммерческую тайну, после чего совершил копирование указанной информации на внешний накопитель. Приговором суда Г. признан виновным в совершении преступлений, предусмотренных ст. 272 и 183 УК РФ[3]*.*

За неправомерным доступом к компьютерной информации личного характера может следовать распространение в сети Интернет заведомо ложных сведений, порочащих честь и достоинство потерпевшего или

---

[1] Приговор Тайшетского городского суда Иркутской области от 10 июня 2014 г. по делу № 1-211/2014 // ГАС «Правосудие». URL: https://www.bsr.sudrf.ru/ (дата обращения: 01.01.2019).

[2] Приговор Яйского районного суда Кемеровской области от 21 мая 2018 г. по делу № 1-46/2018 // ГАС «Правосудие». URL: https://www.bsr.sudrf.ru/ (дата обращения: 01.01.2019).

[3] Приговор Канавинского районного суда г. Нижний Новгород от 6 июня 2018 г. по делу № 1-283/2018 // ГАС «Правосудие». URL: https://www.bsr.sudrf.ru/ (дата обращения: 01.01.2019).

подрывающих его репутацию (например, о нетрадиционной сексуальной ориентации либо оказании услуг сексуального характера и т.д.). В таких случаях действия виновных следует квалифицировать по совокупности преступлений, предусмотренных ст. 272 и 128[1] УК РФ (клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию).

Например, Е. совершила неправомерный доступ к принадлежащему К. электронному почтовому ящику «В», изменив фоновое изображение на странице К. Кроме того, внесла заведомо ложные сведения, связанные с оказанием К. услуг сексуального характера за денежное вознаграждение, а также распространила на ее странице фотографии, доступные для неограниченного числа пользователей. При этом Е. достоверно знала, что они носят заведомо ложный характер и порочат честь и достоинство К., а также будут доступны для неограниченного круга лиц в сети Интернет. Действия виновной были квалифицированы по ч. 1 ст. 128[1] и ч. 2 ст. 272 УК РФ[1].

Другое проявление «инструментальности» компьютерных преступлений заключается в возможности одномоментного совершения нескольких компьютерных преступлений, образующих идеальную совокупность, где одно компьютерное преступление является способом совершения второго. Так, вредоносные компьютерные программы, ответственность за создание, использование и распространение которых предусмотрена ст. 273 УК РФ, чаще всего используются именно для получения несанкционированного доступа к компьютерной информации с ее последующим копированием, блокированием, модификацией либо удалением.

Например, Я., будучи осведомленным о необходимой комплектации оборудования и схеме его работы при законном подключении и просмотре платных закодированных телевизионных спутниковых каналов «НТВ-ПЛЮС», используя подключение к сети Интернет, установил на купленный им заранее ТВ-тюнер измененное программное обеспечение, содержащее вредоносную программу «XcamClient2», с использованием которого возможен просмотр платных зашифрованных телевизионных спутниковых каналов по технологии, позволяющей осуществлять копирование данной компьютерной информации и передачу ее через сеть Интернет к специализированному серверу, без ведома законного владельца «НТВ-ПЛЮС», и осуществил просмотр указанных каналов. Приговором суда Я. признан виновным в совершении преступлений, предусмотренных ч. 2 ст. 272, ч. 2 ст. 273 УК РФ[2].

---

[1] Постановление Завьяловского районного суда Удмуртской Республики от 1 августа 2011 г. (см.: *Евдокимов К. Н.* Некоторые особенности уголовно-правовой квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела // Российский следователь. 2017. № 4. С. 39–44).

[2] Приговор Ленинского районного суда г. Махачкала от 23 октября 2017 г. по делу № 1-423/2017 // ГАС «Правосудие». URL: https://www.bsr.sudrf.ru/ (дата обращения: 01.01.2019).

Между тем в правоприменительной практике встречаются случаи, когда подобные деяния не получают должной правовой оценки.

Так, А., используя принадлежащий ему ноутбук, имеющий доступ к сети Интернет, осуществил поиск и копирование вредоносной компьютерной программы «Private Keeper», заведомо предназначенной для перебора учетных данных пользователей торговой площадки «ebay.com» и получения полного доступа к аккаунтам третьих лиц. После чего осуществил запуск указанной вредоносной программы и в результате ее использования получил аутентификационные данные (логин, пароль), а также иные персональные данные 69 граждан Венгрии, Великобритании, США, Франции, Индии, Бельгии, Италии, Бразилии, Швейцарии, Австралии, Швеции, Гваделупы, Китая, являющихся пользователям интернет-ресурса ebay.com. Органами предварительного расследования и судом действия А. были квалифицированы по ч. 1 ст. 273 УК РФ[1].

Данная квалификация представляется неполной, поскольку А., используя вредоносную компьютерную программу, осуществил неправомерный доступ к компьютерной информации, повлекшей ее копирование (скопированы логины и пароли, а также иные персональные данные 69 лиц). Следовательно, действия виновного необходимо квалифицировать по совокупности преступлений, предусмотренных ст. 272 и 273 УК РФ.

Таким образом, «инструментальный» характер компьютерных преступлений проявляется в их свойстве выступать способом достижения иных преступных целей, в том числе клеветы, нарушения тайны переписки, получения и разглашения сведений, составляющих государственную, коммерческую, налоговую, банковскую тайны, что обусловливает необходимость квалификации компьютерных преступлений по совокупности между собой и с иными составами преступлений.

Статья 274 УК РФ устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо ИКС и оконечного оборудования, а также правил доступа к ИКС, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Из толкования диспозиции следует вывод, что субъект данного состава преступления является специальным. Аналогичного мнения придерживается большинство исследователей[2]. Таким образом, исполнителем рассматриваемого преступления может быть признано лишь лицо, имеющее в силу должностных обязанностей доступ к средствам хранения, обработки или передачи охраняемой компьютерной

---

[1] Приговор Северского городского суда Тамбовской области от 17 мая 2018 г. по делу № 1-135/2018 // ГАС «Правосудие». URL: https://www.bsr.sudrf.ru/ (дата обращения: 01.01.2019).

[2] См.: *Русскевич Е. А.* Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий. М., 2019. С. 87.

информации либо информационно-телекоммуникационным сетям и оконечному оборудованию, а также к ИКС, и обязанное соблюдать установленные для них правила эксплуатации[1].

Неправильное понимание правоприменителем признаков субъекта нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИКС ведет к квалификационным ошибкам.

К примеру, Ш., обладая техническими познаниями в области использования вредоносных компьютерных программ в операционных системах терминалов самообслуживания кредитно-финансовых учреждений, подобрав электронные носители информации с вредоносной компьютерной программой, обеспечивающей тайное хищение денежных средств, посредством неправомерного доступа к компьютерной информации и несанкционированного подключения к устройству самообслуживания, принадлежащего ООО банк «Аверс», путем копирования перенес в операционную систему указанного устройства самообслуживания вредоносную компьютерную программу, с помощью которой путем уничтожения, блокирования и модификации компьютерной информации вывел его из рабочего состояния, что позволило в дальнейшем осуществить хищение денежных средств в размере 516 тыс. руб. Указанные действия Ш. квалифицированы органами предварительного расследования и судом по ст. 272, 273, 274, 159[6] УК РФ[2].

Полагаем, что уголовная-правовая оценка действий виновного по ст. 274 УК РФ является необоснованной, поскольку Ш. не был работником, который в силу служебного положения имел доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию, а также к информационно-телекоммуникационным сетям, и не был обязан соблюдать установленные для них правила эксплуатации.

В ряде территориальных субъектов на досудебной стадии уголовного судопроизводства имелись проблемные вопросы квалификации преступлений при разграничении деяний, предусмотренных п. «г» ч. 3 ст. 158 и ст. 159[3] УК РФ.

В 2019 г Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» корректировке подверглись ст. 158 УК РФ (часть 3 дополнена квалифицирующим признаком п. «г» — с банковского счета, а равно в отношении электронных денежных средств, при отсутствии признаков преступления, предусмотренного статьей 159[3] УК РФ); 159[3] УК РФ (изложена в новой редакции — «мошенничество с использованием

---

[1] Комментарий к Уголовному кодексу Российской Федерации: в 4 т. (постатейный) / А. В. Бриллиантов, А. В. Галахова, В. А. Давыдов и др.; отв. ред. В. М. Лебедев. М.: Юрайт, 2017. Т. 3: Особенная часть. Раздел IX // СПС «КонсультантПлюс».

[2] Приговор Кировоградского районного суда от 5 августа 2016 г. по делу № 1-105/2016 // ГАС «Правосудие». URL: https://www.bsr.sudrf.ru/ (дата обращения: 01.01.2019).

электронных средств платежа», изменена диспозиция и санкции); 159^6 УК РФ (часть 3 дополнена квалифицирующим признаком п. «в» — с банковского счета, а равно в отношении электронных денежных средств).

Исходя из позиции законодателя, изложенной в пояснительной записке к проекту этого закона, внесенные изменения были обусловлены высокой степенью общественной опасности указанных противоправных деяний и направлены на законодательное закрепление возможности использования в целях профилактики и предотвращения данных преступлений, совершаемых, как правило, лицами, обладающими специальными знаниями, использующими для совершения преступлений технические средства, всего арсенала оперативно-разыскных мероприятий.

В этой связи квалифицирующий признак кражи с банковского счета, а равно в отношении электронных денежных средств, на наш взгляд, мог иметь место лишь при хищении безналичных и электронных денежных средств путем их перевода в рамках применяемых форм безналичных расчетов, в том числе с использованием виновными специальных познаний либо современных технических средств, тогда как хищение, совершенное путем снятия наличных денежных средств с банковского счета через банкомат, должно рассматриваться как обычное хищение вещей, наделенных физическим признаком.

В совокупности названные изменения направлены на усиление ответственности за хищение денежных средств клиентов кредитных организаций.

При рассмотрении вопросов о юридической оценке обстоятельств совершенных деяний ключевыми остаются положения постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», где содержится правовая регламентация вопросов квалификации преступлений. Между тем практика применения новелл уголовного закона только нарабатывается.

Разграничение смежных составов: п. «г» ч. 3 ст. 158 УК РФ (кража с банковского счета, а равно в отношении электронных денежных средств), ст. 159 (мошенничество) и ст. 159^3 УК РФ (мошенничество с использованием электронных средств платежа), вызывает затруднения у прокуроров и следователей.

Так, в ходе проведенной прокуратурой Волгоградской области в октябре проверки вскрыты неединичные факты необоснованной квалификации преступлений по ст. 159 УК РФ при хищении безналичных денежных средств с использованием необходимой для получения доступа к ним конфиденциальной информации держателя платежной карты (например, персональных данных владельца, контрольной информации, паролей), переданной злоумышленнику самим держателем под воз-

действием обмана или злоупотребления доверием. Юридическую оценку подобному необходимо было давать по ст. 158 УК РФ.

На отсутствие единства судебной практики обращают внимание ученые-правоведы[1] и надзирающие прокуроры. Сложности правоприменения рассматриваемой материальной нормы отмечаются при обжаловании следственными органами постановления нижестоящего прокурора о возвращении дела для дополнительного расследования.

Так, постановлением прокурора Индустриального района г. Барнаула возвращено для производства дополнительного следствия уголовное дело по обвинению Н. в совершении преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ. По мнению прокурора района, обвиняемая переводила денежные средства в сумме 1100 руб. с одного счета на другой, используя доступный для широкого круга лиц банковский сервис, что исключает привлечение ее к уголовной ответственности по указанной статье уголовного закона.

Изучение материалов уголовного дела в прокуратуре Алтайского края в порядке, установленном ч. 4 ст. 221 УПК РФ, показало, что указанное процессуальное решение прокурора является необоснованным. Вопреки выводам прокурора района, в действиях Н., совершившей кражу денежных средств с банковского счета М., усматривался состав преступления, предусмотренный п. «г» ч. 3 ст. 158 УК РФ. В ходе предварительного расследования получено достаточно доказательств виновности Н. в совершении инкриминируемого ей преступления, которые добыты с соблюдением требований уголовно-процессуального законодательства. С учетом изложенного заместителем прокурора края утверждено обвинительное заключение по уголовному делу, которое направлено в суд, где рассмотрено по существу с вынесением обвинительного приговора без изменения квалификации содеянного.

Такая позиция надзирающего прокурора была связана с отсутствием устоявшейся прокурорско-следственной и судебной практики при квалификации действий обвиняемого п. «г» ч. 3 ст. 158 УК РФ. В целях единообразного применения уголовного закона в мае 2019 г. надзирающим прокурорам направлено информационное письмо о практике применения норм УК РФ, предусматривающих ответственность за совершение преступлений, связанных с хищением денежных средств с банковских счетов и с использованием электронных средств платежа[2].

Практика рассмотрения судами уголовных дел рассматриваемой категории складывается по-разному даже в рамках одного территориального субъекта.

Приговором Ленинского районного суда г. Кирова от 11 сентября 2018 г. за совершение кражи по п. «г» ч. 3 ст. 158 УК РФ осужден Т. Судом установлено, что 27 мая 2018 г. он, тайно похитив у С. банковскую карту, находясь в помещении

---

[1] См., например: *Яни П. С.* Мошенничество с использованием электронных средств платежа // Законность. 2019. № 5 (1015). С. 25–28.

[2] По материалам деятельности прокуратуры Алтайского края.

отделения ПАО «Сбербанк России» установил карту в банкомат, ввел известный ему PIN-код банковской карты С. и провел операцию по снятию и хищению денежных средств в размере 25 тыс. руб. Апелляционное представление государственного обвинителя, в котором был поставлен вопрос несогласия с квалификацией вышеуказанных действий Т. по п. «г» ч. 3 ст. 158 УК РФ, 23 октября 2018 г. судебной коллегией по уголовным делам Кировского областного суда оставлено без удовлетворения, а приговор — без изменения.

Приговором мирового судьи судебного участка № 17 Кирово-Чепецкого судебного района Кировской области от 12 сентября 2018 г. Б. осуждена по ч. 1 ст. 158 УК РФ. Согласно обвинительному заключению и приговору мирового судьи она совершила в том числе тайное хищение принадлежащих С. денежных средств в сумме 29,9 тыс. руб. путем проведения операций по их снятию с расчетного счета, открытого на имя потерпевшей в ПАО «Сбербанк России», с использованием ее банковской карты и известного ей PIN-кода карты потерпевшей. Апелляционным постановлением Кирово-Чепецкого районного суда Кировской области от 22 ноября 2018 г. указанный приговор был отменен, уголовное дело в порядке ст. 237 УПК РФ возвращено прокурору. По мнению суда апелляционной инстанции, действия Б. должны быть квалифицированы не по ч. 1 ст. 158 УК РФ, а с учетом внесенных ФЗ от 23 апреля 2018 г. № 111-ФЗ изменений по п. «г» ч. 3 ст. 158 УК РФ.

Такая квалификация подобных действий хищения наличных средств в размере, например, 1 тыс. руб. к преступлению не относит. А хищение наличных денежных средств сумму от 5 тыс. до 250 тыс. руб. квалифицируется по п. «в» ч. 2 ст. 158 УК РФ как кража с причинением значительного ущерба и является преступлением средней тяжести с наказанием в виде лишения свободы сроком до 5 лет, а также с возможностью прекращения уголовного дела за примирением сторон и освобождением от уголовной ответственности с назначением судебного штрафа. В то же время хищение 1 тыс. руб. путем их снятия через банкомат с использованием похищенной банковской карты и известного виновному лицу PIN-кода подлежит квалификации по п. «г» ч. 3 ст. 158 УК РФ, что относится к категории тяжких преступлений и предусматривает наказание до 6 лет лишения свободы.

Помимо этого, у следственных органов и суда нет единого подхода при квалификации действий виновного в случае хищения денежных средств с банковского счета путем перевода их через мобильный банк, мобильное приложение (например, «Сбербанк Онлайн»).

К примеру, приговором Яранского районного суда Кировской области от 12 октября 2018 г. С. признан виновным в совершении преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ. Судом установлено, что С., находясь вместе со своим знакомым в офисе одного из банков п. Тужа, узнал логин и пароль для доступа к личному кабинету банковского счета последнего. После чего воспользовавшись телефоном потерпевшего, осуществил перевод денежных средств в сумме 155 тыс. руб. с его банковской карты на банковские карты своих знакомых, которые ранее одолжил, таким образом совершил хищение денежных средств в указанной сумме с банковского счета потерпевшего.

В то же время аналогичные действия Б. в Верхнекамском районе были квалифицированы по п. «в» ч. 2 ст. 158 УК РФ (в июле 2018 г., имея доступ к сотовому телефону Г., через приложение «мобильный банк» перевел с банковского счета потерпевшего на свой счет 8 тыс. руб., чем причинил значительный ущерб), в результате уголовное дело прекращено судом за примирением сторон на основании ст. 25 УПК РФ.

Серьезные затруднения вызывает квалификация действий лица, оплатившего покупки в торговой организации, похищенной либо найденной банковской картой.

Так, органами предварительного следствия Б. обвинялся по п. «г» ч. 3 ст. 158 УК РФ в том, что он тайно вытащил банковскую карту из кармана брюк потерпевшего и в течение вечера неоднократно приобретал спиртное и продукты питания, оплачивая их его картой, прикладывая ее к терминалу оплаты (функция «pay-pass»), тем самым похитил денежные средства на общую сумму 1004 руб. Из показаний свидетеля — продавца кафе следует, что Б. расплачивался банковской картой путем прижатия ее к терминалу для оплаты, не вводя PIN-код и не передавая ей карту. Кому принадлежала эта карта, свидетель не выясняла и не осознавала незаконность изъятия имущества, так как не знала истинного владельца банковской карты.

15 ноября 2018 г. в ходе рассмотрения дела Яранский районный суд усмотрел в действиях Б. признаки преступления, предусмотренного ч. 1 ст. 159[3] УК РФ, однако ввиду недостаточности суммы ущерба для его привлечения к уголовной ответственности подсудимого оправдал. Мотивируя свое решение, суд сослался на п. 17 постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», согласно которому действия лица следует квалифицировать по ст. 159[3] УК РФ в случаях, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой. Апелляционная инстанция признала указанное решение районного суда законным и обоснованным, оставив представление государственного обвинителя без удовлетворения.

Между тем с таким решением сложно согласиться, поскольку в подобной ситуации работник торговой организации не осознает незаконности изъятия имущества и обмана, как и не знает истинного владельца банковской карты. В соответствии с п. 4 постановления Пленума Верховного Суда РФ «О судебной практике по делам о краже, грабеже, разбое» хищение является тайным и в случаях, когда присутствующее при незаконном изъятии чужого имущества лицо не осознает противоправность этих действий.

Кроме того, обязанность владельца банковской карты предъявлять документ, удостоверяющий личность, при проведении расчетов нормативными правовыми актами не установлена. Следовательно, при

предъявлении похищенной банковской карты сотруднику торговой организации без документа, удостоверяющего личность, и, более того, при оплате товара без передачи карты кассиру и без участия сотрудника торговой организации (путем прикладывая к терминалу без введения PIN-кода) владелец карты никого не обманывает и не вводит в заблуждение, хотя умалчивает о своей личности.

Несмотря на это, судебная практика стала придерживаться именно такой позиции, и в случае, если лицо во время хищения денежных средств с использованием электронных средств платежа выдает себя за собственника карты, обманывая сотрудника торговой организации (прикладывая карту к терминалу оплаты с использованием функции «pay-pass»), преступное деяние квалифицируется по ст. 159^3 УК РФ. При этом в случае, когда размер похищенного составляет менее 2500 руб., состав преступления в действиях виновного фактически отсутствует.

Приговором Ленинского районного суда от 31 января 2019 г. Т., действия которого органами предварительного следствия были квалифицированы по ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ, осужден по ч. 3 ст. 30, ч. 2 ст. 159^3 УК РФ.

Фактически Т., найдя банковскую карту Ч., позволяющую производить оплату товара без введения PIN-кода, совершил в магазинах города 14 покупок и пытался совершить еще одну, на общую сумму 11 248, 69 руб. В случае доведения преступных действий Т. до конца потерпевшей был бы причинен значительный ущерб. Суд, рассматривая дело в особом порядке, счел юридическую оценку действий подсудимого, данную органом расследования, необоснованной.

В то же время при аналогичных обстоятельствах, но по ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ Ленинским районным судом г. Кирова 10 декабря 2018 г. осуждена Р., которая, обнаружив в банкомате ПАО «Сбербанк» банковскую карту с функцией «pay-pass» (бесконтактной оплаты при сумме покупки до 1000 руб.) на имя Ш., путем совершения покупок в магазинах города через терминалы безналичной оплаты пыталась тайно похитить денежные средства потерпевшей на общую сумму 7199,37 руб.

Так, по уголовному делу в отношении К., М., П. и выделенного из него уголовного дела в отношении С. государственный обвинитель, верно оценив обстоятельства совершенного преступления, в ходе судебного следствия обоснованно изменил предъявленное указанным лицам обвинение, переквалифицировав деяния подсудимых с п. «г» ч. 3 ст. 158 УК РФ на ч. 2 ст. 159^3 УК РФ.

Подсудимые обвинялись в том, что, найдя банковскую карту на имя Ч., поддерживающую бесконтактную оплату товаров, П. и М., действуя группой лиц по предварительному сговору, осуществили с нее 3 расходные операции по оплате товаров на общую сумму 1310 руб., не сообщив продавцу магазина о принадлежности банковской карты потерпевшему. После чего М., вступив в предварительный преступный сговор с К. и С., находясь в баре «Платинум» в г. Магадане, осуществил 26 расходных операций по оплате приобретенных товаров на общую сумму 13 550 руб., не сообщив работнику бара о незаконном владении банковской

картой, а С. также ввел последнего в заблуждение, убедив, что банковская карта принадлежит его брату.

При этом в тех случаях, когда сумма похищенных денежных средств не превышала 2500 руб. судами принимались решения об оправдании подсудимых (например, в Костромской области по данному основанию в 2019 г. оправдано 3 лица) или о прекращении уголовного дела по реабилитирующим основаниям.

Проведенный анализ актуальных вопросов квалификации преступлений, совершаемых с использованием ИКТ, позволяет сформулировать направления совершенствования правообеспечительной и правоприменительной практики:

— для целей применения ст. 272 УК РФ под охраняемой законом информацией следует понимать информацию, которая явно указана законом или другим нормативным актом в качестве таковой (информация ограниченного доступа), а равно ту, в отношении которой ее обладателем приняты меры по защите;
— в тех случаях, когда компьютерная информация, подвергшаяся форматированию, находилась в свободном доступе, содеянное в силу малозначительности может не представлять общественной опасности, что должно влечь применение положений ч. 2 ст. 14 УК РФ;
— «инструментальный» характер компьютерных преступлений проявляется в их свойстве выступать способом достижения иных преступных целей, в том числе клеветы, нарушения тайны переписки, получения и разглашения сведений, составляющих государственную, коммерческую, налоговую, банковскую тайны, что обусловливает необходимость квалификации компьютерных преступлений по совокупности между собой и с иными составами преступлений (ст. 128^1, 137, 138, 165, 183, 283, 283^1 и др.);
— исполнителем преступления, предусмотренного ст. 274 УК РФ, может быть признано лишь лицо, имеющее в силу должностных обязанностей доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо ИКС и оконечному оборудованию, а также к ИКС и обязанное соблюдать установленные для них правила эксплуатации;
— для правильной квалификации преступлений, связанных с хищением электронных денежных средств, остро необходимы разъяснения Верховного Суда Российской Федерации относительно применения новелл, введенных в гл. 21 УК РФ, для четкого понимания понятия «кража, совершенная с банковского счета, а равно в отношении электронных денежных средств»;

— требуют разъяснения и вопросы квалификации преступных действий лица в случае хищения части денежных средств с использованием банковской карты потерпевшего путем их обналичивания через терминал и с последующей оплатой этой картой различных покупок путем прикладывания карты к терминалу с использованием функции «pay-pass» (например, снял наличные в размере 1000 руб. и оплатил картой товар на сумму менее 2500 руб.).

Глава 2

ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1. Деятельность прокуратуры по предупреждению и пресечению преступлений экстремистской и террористической направленности, совершенных с использованием информационно-телекоммуникационных сетей

Как и в большинстве государств, в Российской Федерации принимается комплекс мер, направленный на противодействие использованию ИКТ в преступных целях. Среди субъектов обеспечения информационной безопасности выделяются органы прокуратуры, которые осуществляют надзор за исполнением законов другими субъектами и проводят работу по ограничению доступа к запрещенной информации. Особая роль органов прокуратуры заключается в координации деятельности правоохранительных органов по борьбе с преступностью, представляющей собой одну из серьезных угроз информационной безопасности[1].

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации) объектами надзорных мероприятий выступают обладатели информации, операторы информационных систем, владельцы сайтов, провайдеры[2].

Помимо перечисленных прокуратурой проводятся проверки уполномоченных органов исполнительной власти. В деятельности регио-

---

[1] *Ефремова М. А.* Прокуратура в системе обеспечения информационной безопасности: монография / М. А. Ефремова, Э. Б. Хатов; Ун-т прокуратуры Рос. Федерации. М., 2019. 128 с.

[2] *Паламарчук А. В.* Прокурорский надзор за исполнением законодательства в сфере противодействия правонарушениям в сети Интернет // Законность. 2016. № 12. С. 3–9.

нальных управлений Роскомнадзора, например, устанавливаются такие типичные нарушения, как несвоевременное направление протоколов о возбуждении дел об административных правонарушениях в отношении средств массовой информации и их руководителей, возбуждение дел по истечении сроков привлечения к административной ответственности, нарушения при контроле операторов связи, несвоевременно осуществляющих блокирование доступа к запрещенной информации. В адрес руководителей управлений Роскомнадзора вносятся соответствующие представления.

Кроме того, Генеральной прокуратурой Российской Федерации осуществляется взаимодействие с ФСБ России, в ведении которой находятся вопросы выявления и пресечения компьютерных атак на объекты критической информационной инфраструктуры. Прокурорами вскрываются нарушения, связанные с неисполнением субъектами критической информационной инфраструктуры обязанностей, возложенных на них Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Вносятся меры прокурорского реагирования на нарушения правил категорирования[1].

В целях предупреждения использования информационных технологий в преступных целях правоохранительными и контролирующими органами в последние годы модифицированы механизмы мониторинга, блокировки и удаления противоправного контента из сети Интернет. Органы прокуратуры принимают участие как в выявлении и блокировке запрещенной информации во взаимодействии с уполномоченными органами исполнительной власти, так и в выявлении нарушений федерального законодательства, связанных с неисполнением операторами связи и иными обладателями информации законодательства о защите информации.

Полномочия по обращению в суд с административным исковым заявлением о признании информации, размещенной в ИТС, информацией, распространение которой в Российской Федерации запрещено, в полной мере отражают предупредительный потенциал прокурорской деятельности.

Основаниями для обращения прокуроров в суды с исковыми заявлениями являются факты размещения в Интернете:

— информации о способах изготовления взрывчатых веществ или взрывных устройств, огнестрельного оружия;
— объявлений о продаже огнестрельного оружия без получения соответствующих разрешений;

---

[1] См.: постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

— информации, содержащей рекламу услуг по легализации денежных средств без наличия соответствующей лицензии;
— информации, способной причинить вред здоровью и развитию несовершеннолетних, в том числе побуждающую к агрессии и другим асоциальным проявлениям;
— информации, пропагандирующей алкоголизацию, наркоманию, проституцию, самоубийства;
— информации порнографического характера;
— объявлений о незаконной реализации посредством ИТС лекарственных средств и медицинских изделий;
— информации о незаконных способах уклонения от воинской обязанности и военной службы;
— объявлений о продаже поддельных документов (дипломов о высшем образовании, медицинских справок, больничных листов, водительских удостоверений, полисов ОСАГО, трудовых и медицинских книжек, паспортов граждан Российской Федерации, лицензий и др.);
— информации о продаже, изготовлении и способах незаконных ловли и охоты, содержащей жестокое обращение с животными;
— информации, связанной с незаконными азартными играми;
— информации о способах обналичивания денежных средств и материнского капитала и др.

Заявления о признании информации запрещенной рассматриваются с учетом положений, предусмотренных гл. 27[1] Кодекса административного судопроизводства РФ[1]. Несоблюдение особенностей производства по данной категории административных дел служит основанием для возвращения искового заявления.

Исходя из ч. 2 ст. 2652 КАС РФ помимо общих сведений, предусмотренных пп. 1, 2, 9 ч. 2 ст. 125 КАС РФ, в заявлении о признании информации запрещенной должны быть указаны:
— сведения, предусмотренные п. 3 ч. 2 ст. 125 КАС РФ, в случае установления административного ответчика;
— доменные имена и (или) указатели страниц сайтов в ИТС, содержащих запрещенную информацию;
— обоснование доводов об отнесении информации, размещенной в ИТС, к информации, распространение которой в Российской Федерации запрещено, с указанием соответствующих норм права;
— в случае, если доступ к информации, размещенной в ИТС, ограничен, сведения, необходимые для получения доступа суда к такой информации;
— сведения о соблюдении досудебного порядка признания информации, размещенной в ИТС, информацией, распространение

[1] Далее — КАС.

которой в Российской Федерации запрещено в случае, если такой порядок установлен законом.

Когда установить владельца сайта или домена не представляется возможным, исковые заявления прокурора рассматриваются с участием представителя Роскомнадзора. В иных случаях к участию в деле привлекаются администраторы соответствующих информационных ресурсов.

Так, Московским районным судом г. Санкт-Петербурга было рассмотрено административное исковое заявление прокурора к Роскомнадзору о признании информации о том, как приготовить в домашних условиях жидкостную зажигательную гранату («коктейль Молотова»), по адресу http://readfree.ru/book/C998/ запрещенной к распространению в Российской Федерации. Определением суда от 13 мая 2020 г. ненадлежащий ответчик Роскомнадзор заменен надлежащим Ц., являющимся администратором доменного имени «readfree.ru», дело передано в г. Нижний Новгород по месту жительства ответчика10.

Исходя из положений ст. 2653 КАС РФ, судья прекращает производство по административному делу, если указанные в нем доменное имя, указатель страницы сайта уже включены в реестр запрещенной информации, который расположен по электронному адресу https://eais.rkn.gov.ru/. Так, например, в 2019 г. из 21 искового заявления, направленного прокуратурами Приморского края в суды, производство по 5 делам было прекращено в связи с блокировкой сайтов на момент рассмотрения дела.

В случае несоблюдения предусмотренного законом досудебного порядка признания информации, размещенной в ИТС, информацией, распространение которой в Российской Федерации запрещено, в соответствии с п. 5 ст. 2653 КАС РФ судья оставляет заявление без рассмотрения. В то же время, как отмечают некоторые исследователи, в настоящее время законодательно порядок досудебного рассмотрения не предусмотрен, что может приводить к отказам со стороны судей в принятии заявлений прокурора.

По решению суда адреса ресурсов, содержащих запрещенную информацию, включаются в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (далее — реестр запрещенной информации)[1].

---

[1] См.: постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 (ред. от 16 мая 2020 г.) «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено».

Ведение реестра запрещенной информации осуществляется Роскомнадзором, который также в соответствии с п. 2 ст. 265^3 КАС РФ участвует в рассмотрении административного дела о признании информации, размещенной в Интернете, информацией, распространение которой в Российской Федерации запрещено, в качестве заинтересованного лица.

Обновленная Стратегия противодействия экстремизму в Российской Федерации до 2025 года, утвержденная Указом Президента Российской Федерации от 29 мая 2020 г. № 344, выделяет ИТС в качестве основного средства связи экстремистских организаций, используемого для привлечения новых членов, а также организации и координации совершения экстремистских посягательств и распространения соответствующей идеологии (п. 14).

С учетом этого своевременное предупреждение экстремистских проявлений, выявление и устранение причин и условий, способствующих экстремизму и терроризму, является одной из важнейших задач, стоящих перед органами прокуратуры. В настоящее время имеется соответствующая правовая база для ее решения.

В аспекте предупреждения экстремистских проявлений полномочия прокурора по признанию информации запрещенной имеют особое значение. Для недопущения использования средств массовой информации и ИТС в террористических целях прокурорами на постоянной основе проводится мониторинг с учетом рекомендаций, содержащихся в обзорах Генеральной прокуратуры Российской Федерации «Реализации прокурорами полномочий по противодействию распространению запрещенной информации в сети Интернет» от 13 февраля 2018 г. № 74/1-12-2018 и от 18 марта 2019 г. № 74/1-12-2019, информационном письме «О мерах по противодействию распространению запрещенной информации в сети Интернет» от 25 декабря 2018 г. № 74/1-12-2018 и др.

Целью мониторинга выступает выявление материалов, призывающих к осуществлению террористической деятельности либо обосновывающих (оправдывающих) необходимость ее осуществления. При выявлении нарушений принимаются меры к ограничению доступа к противоправной информации.

Так, прокуратурой г. Североуральска Свердловской области по результатам мониторинга в ИТС выявлены материалы (книга «Бомба из хозмага», статья «Яды из хозмага и ближайшего пустыря»), содержащие описание способов изготовления из подручных и легкодоступных материалов в домашних условиях взрывчатых веществ и устройств, а также различных ядов. По иску прокурора решениями суда от 23 июля 2019 г. и 12 августа 2019 г. информация признана запрещенной к распространению5.

Основаниями для обращения прокуроров в суды с исковыми заявлениями, помимо фактов размещения в ИТС информации о спо-

собах изготовления взрывчатых веществ или взрывных устройств, огнестрельного оружия, выступают:

факты размещения объявлений о продаже огнестрельного оружия без получения соответствующих разрешений, которое может быть использовано для совершения преступлений, в том числе террористических актов;

факты размещения в ИТС информации, содержащей рекламу услуг по легализации денежных средств без наличия соответствующей лицензии, что может способствовать финансированию террористической деятельности и др.

Правовыми основаниями признания информации о способах изготовления и применения взрывчатых веществ и взрывных устройств, огнестрельного оружия запрещенной наравне с Законом об информации является также Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму», а в ряде случаев — законодательство, регулирующее деятельность по профилактике правонарушений несовершеннолетних[1].

Предоставление доступа к информации о способе изготовления взрывных устройств фактически является распространением запрещенной информации, что противоречит целям действующего законодательства в сфере противодействия терроризму. Она адресована неограниченному кругу лиц и склоняет к совершению преступных действий.

Так, Советским районным судом Республики Марий Эл было удовлетворено административное исковое заявление прокурора к Управлению Роскомнадзора по Республике Марий Эл о признании запрещенной информации о том, как в домашних условиях можно приготовить взрывное устройство. Вход на соответствующую интернет-страницу свободный, ознакомиться с ее содержание может любой пользователь, ограничения на передачу и копирование отсутствуют[2].

По сведениям Минкомсвязи России, количество внесенных в реестр запрещенной информации электронных адресов возрастает, что свидетельствует об увеличении рынка криминальных услуг в ИТС и о вовлеченности исполнительных органов в процесс регулирования сети. В 2019 г. в реестр внесено 2942 адреса, содер-

---

[1] См.: федеральные законы от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» и от 24 июня 1999 г. № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних».

[2] *Реуцкий Д. В.* Информационные материалы в проект сборника тезисов касательно вопроса противодействия распространению идеологии терроризма в информационно-телекоммуникационной сети «Интернет» (материалы Департамента информационной безопасности Минкомсвязи России) // Борьба с криминальными рынками в России: законодательные и правоприменительные проблемы: реализация положений Конвенции ООН против транснациональной организованной преступности: сб. материалов межведомственной науч.-практ. конф. (Москва, 28 апреля 2020 г.) / под общ. ред. О. С. Капинус. Ун-т. прокуратуры Рос. Федерации. М., 2020. С. 285–289.

жащих сведения о способах изготовления взрывчатых веществ или взрывных устройств (2015 г. — 618, 2016 г. — 1458, 2017 г. — 1638, 2018 г. — 2225), огнестрельного оружия — 1315 (2015 г. — 1, 2016 г. — 89, 2017 г. — 739, 2018 г. — 731). Материалы в отношении взрывчатых веществ и оружия могут быть ориентированы на «теневой» Интернет и распространяться в сетях, не поддающихся контролю в настоящее время («Тог»). Кроме того, подобные сайты в основном регистрируются и размещаются в иностранной юрисдикции, что затрудняет идентификацию их владельцев. Исходя из этого блокировка противоправной информации не всегда эффективна. Более результативными могут быть меры экономического воздействия к провайдерам, в том числе в рамках положений Федерального закона от 2 декабря 2019 г. № 405-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», увеличившего размеры административных штрафов для субъектов, не исполняющих установленные законом обязанности[1].

По имеющимся статистическим сведениям, только в 2019 г. прокурорами в суды общей юрисдикции направлен 22 701 иск (заявление) в сфере противодействия экстремистской и террористической деятельности, более 40% (9108) из которых касаются нарушений с использованием сети Интернет[2].

Несмотря на рост показателей в целом, в отдельных субъектах Российской Федерации Генеральной прокуратурой Российской Федерации отмечается недостаточный уровень выявления нарушений в сфере пресечения распространения противоправной информации о способах изготовления и применения взрывчатых веществ, а также огнестрельного оружия в террористических целях[3].

В качестве еще одного инструмента противодействия распространению экстремистской идеологии и вербовке в международные террористические организации выступает порядок признания информа-

---

[1] *Реуцкий Д. В.* Информационные материалы в проект сборника тезисов касательно вопроса противодействия распространению идеологии терроризма в информа-ционно-телекоммуникационной сети «Интернет» (материалы Департамента информационной безопасности Минкомсвязи России) // Борьба с криминальными рынками в России: законодательные и правоприменительные проблемы: реализация положений Конвенции ООН против транснациональной организованной преступности: сб. материалов межведомственной науч.-практ. конф. (Москва, 28 апреля 2020 г.) / под общ. ред. О. С. Капинус. Ун-т. прокуратуры Рос. Федерации. М., 2020. С. 285–289.

[2] Форма статистической отчетности ФБ «Надзор за исполнением законов о федеральной безопасности» за 2019 г.

[3] Обзор Генеральной прокуратуры Российской Федерации «Состояние законности и практики прокурорского надзора в сфере противодействия экстремизму и терроризму» от 30 марта 2020 г. № 32-17-2020.

ционных материалов экстремистскими[1]. Большинством государств предусмотрен судебный порядок признания материалов экстремистскими. Соответствующие нормы находят свое отражение в законах о противодействии экстремистской деятельности не только Российской Федерации, но и республик Беларусь, Казахстан, Молдова, Таджикистан, Узбекистан и Кыргызской Республики.

Понятие экстремистских материалов закреплено в п. 3 ст. 1 Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (далее — Закон № 114-ФЗ); к ним, в частности, относится информация, призывающая к осуществлению экстремистской деятельности либо обосновывающая или оправдывающая необходимость осуществления такой деятельности.

Приказом Генерального прокурора Российской Федерации от 21 марта 2018 г. № 156 «Об организации прокурорского надзора за исполнением законов о противодействии экстремистской деятельности» прокурорам предписано организовать мониторинг сети Интернет в целях недопущения использования средств массовой информации для осуществления экстремистской деятельности (п. 2.3).

Количество исков (заявлений) прокуроров о признании материалов экстремистскими существенно снизилось за последние пять лет. Если в 2015 г. было направлено 712 исков, то в 2019 г. — уже 81 (2016 г. — 286, 2017 г. — 122, 2018 г. — 103)[2]. Это положительная тенденция, свидетельствующая о формировании единообразной практики и внимательном подходе к подготовке заявлений.

Исключению из практики прокурорского надзора типичных нарушений, таких как дублирование заявлений, способствовало издание приказа Генерального прокурора Российской Федерации от 16 марта 2016 г. № 159 «О порядке реализации прокурорами полномочий по направлению в суд заявлений о признании информационных материалов экстремистскими», исходя из положений которого соответствующие заявления не могут быть направлены в суд прокурорами городов и районов. Реализация полномочий осуществляется прокурорами субъектов Российской Федерации и приравненными к ним прокурорами специализированных прокуратур после предварительного согласования с управлением по надзору за исполнением законов о федеральной без-

---

[1] *Агапов П. В., Борисов С. В.*, *Меркурьев В. В.* и др. Противодействие киберпреступности в аспекте обеспечения национальной безопасности. М.: Акад. Ген. прокуратуры Рос. Федерации, 2014; *Меркурьев В. В.* Задачи прокуратуры Российской Федерации по противодействию экстремизму и терроризму в контексте обеспечения национальной безопасности // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. № 3. С. 44–53.

[2] Статистический отчет «Надзор за исполнением законов о федеральной безопасности» по форме ФБ (утв. приказом Генерального прокурора Российской Федерации № 35 от 26 января 2017 г.) за период 2015–2019 гг.

опасности, межнациональных отношениях, противодействии экстремизму и терроризму Генеральной прокуратуры Российской Федерации.

Кроме того, приказом предписано не допускать действий, провоцирующих неблагоприятные социальные последствия. В данном случае имеется в виду риск возрастания общественного недовольства.

В 2019 г. в следственные органы прокурорами направлено 55 постановлений в порядке, установленном п. 2 ч. 2 ст. 37 УПК РФ, о фактах распространения в ИТС призывов к экстремистской и террористической деятельности (2017 г. — 89, 2018 г. — 73), по которым возбуждено 26 уголовных дел (2017 г. — 63, 2018 г. — 42)[1].

На середину 2020 г. Федеральный список экстремистских материалов (URL: https://minjust.ru/ru/extremist-materials) включает в себя уже более 5000 пунктов. Реализация полномочий по ведению федерального списка возложена на Министерство юстиции Российской Федерации, деятельность которого в данной части проверяется Генеральной прокуратурой Российской Федерации.

Особенности производства по административным делам о признании информационных материалов экстремистскими регламентированы гл. 27[2]. КАС РФ.

В то время как исковое заявление о признании информации запрещенной подается в районный суд по адресу административного истца или ответчика, заявление о признании материалов экстремистскими направляется в районный суд по месту их обнаружения или по адресу организации, осуществляющей их производство.

Если распространитель материалов не установлен, к участию в административном деле привлекается Уполномоченный по правам человека в Российской Федерации или субъекте Российской Федерации для дачи заключения по административному делу.

Помимо перечисленных полномочий Генеральный прокурор Российской Федерации и его заместители во внесудебном порядке направляют в Роскомнадзор требования о принятии мер по ограничению доступа к информационным ресурсам. Перечень распространяемой с нарушением закона информации определен ст. 15[3] Закона об информации и включает:

— информацию, содержащую призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка;
— недостоверную общественно значимую информацию, распространяемую под видом достоверных сообщений, которая соз-

[1] Статистический отчет «Надзор за исполнением законов о федеральной безопасности» по форме ФБ (утв. приказом Генерального прокурора Российской Федерации от 26 января 2017 г. № 35) за 2015–2019 гг.

дает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи;

— информационные материалы иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации в соответствии с Федеральным законом от 28 декабря 2012 г. № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации»;

— сведения, позволяющие получить доступ к указанным информации или материалам.

По 134 требованиям Генеральной прокуратуры Российской Федерации об ограничении доступа к распространяемой с нарушением закона информации, направленным в Роскомнадзор в 2019 г. (2018 г. — 140, 2017 г. — 157, 2016 г. — 165), было заблокировано порядка 81,5 тыс. интернет-ресурсов и с 45,4 тыс. информация была удалена (2017 г. — 2 тыс. и 20 тыс., 2018 г. — 13,7 тыс. и 57,4 тыс. соответственно)[1].

Дополнительными полномочиями по ограничению доступа к недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, Генеральный прокурор Российской Федерации и его заместители были наделены в 2019 г., по итогам года которого в Роскомнадзор направлены 12 требований об ограничении доступа к данным информационным материалам[2].

На основании этого на сайте Роскомнадзора публикуется список ресурсов, распространяющих недостоверную информацию[3], который может быть учтен прокурорами при осуществлении деятельности в указанном направлении.

В первом полугодии 2020 г. прокурорами активно вносились требования об ограничении доступа к ресурсам, распространяющим недо-

---

[1] Справка управления по надзору за исполнением законов о федеральной безопасности, межнациональных отношениях, противодействии экстремизму и терроризму Генеральной прокуратуры РФ о состоянии законности в сфере межнациональных отношений и противодействия экстремистской деятельности в 2018 г. и 2019 г.

[2] Информационно-аналитическая справка Генеральной прокуратуры Российской Федерации об итогах работы и состоянии законности в сфере федеральной безопасности, межнациональных отношений, противодействия экстремизму и терроризму в 2019 г.

[3] См.: URL: https://rkn.gov.ru/mass-communications/p1104/.

стоверную информацию о масштабах заболеваемости коронавирусной инфекцией, методах лечения и др.

Так, например, в марте 2020 г. прокуратурой Пензенской области в ходе мониторинга социальной сети «ВКонтакте» прокуратурой был выявлен материал, содержащий, согласно исследованию специалиста, высказывания, призывающие к враждебным действиям по отношению к группе лиц, заболевших коронавирусной инфекцией. На основании ч. 1 ст. 15[3] Закона об информации по требованию прокурора Роскомнадзором были приняты меры по ограничению доступа к ней[1].

Представляется, что обобщение практики применения полномочий, предусмотренных ст. 15[3] Закона об информации в части ограничения доступа к недостоверной информации, распространяемой под видом достоверных сообщений, могло бы способствовать повышению эффективности данного направления деятельности прокуратуры.

Статьей 15.1-1 Закона об информации Генеральный прокурор Российской Федерации и его заместители также наделены полномочиями по обращению в Роскомнадзор с требованием об ограничении доступа к информации, выражающей явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации. Ответственность за размещение указанных сведений установлена ч. 3–5 ст. 201 и ч. 9–11 ст. 13.15 КоАП РФ. Обо всех случаях возбуждения дел об этих административных правонарушениях органы внутренних дел и подразделения Роскомнадзора обязаны уведомлять органы прокуратуры.

Полномочия, предусмотренные ст. 15.1-1 Закона об информации, стали применяться органами прокуратуры непосредственно после наделения ими. Так, по требованию первого заместителя Генерального прокурора Российской Федерации от 30 мая 2019 г. на основании материалов прокуратуры Чеченской Республики Роскомнадзором с канала YouTube удалены видеозаписи с выступлениями Басаева, оскорбляющими государственные символы Российской Федерации[2].

Расширение перечня информации, распространяемой с нарушением закона, потребовало изменения подходов к организации работы по рассмотрению Генеральной прокуратурой Российской Федерации уведомлений о распространении информации с нарушением закона. В частности, в целях реализации полномочий, предусмотренных ст. 15.1-1 и ст. 15.3 Закона об информации, издан приказ Генерального прокурора Российской Федерации от 26 августа 2019 г. № 596 «Об ут-

---

[1] См.: URL: https://genproc.gov.ru/smi/news/archive/news-1818170/ (дата обращения: 02.07.2020).

[2] *Паламарчук А. В.* О реализации новых полномочий прокурора по вопросам ограничения доступа к информации, распространяемой в сети Интернет с нарушением закона // Законность. 2019. № 10 (1020). С. 3–6.

верждении Инструкции о порядке рассмотрения уведомлений о распространяемой с нарушением закона информации в информационно-телекоммуникационных сетях, в том числе в сети «Интернет».

Данной инструкцией разграничена компетенция по рассмотрению тех или иных видов уведомлений о распространяемой с нарушением закона информации между Главным управлением по надзору за исполнением федерального законодательства и управлением по надзору за исполнением законов о федеральной безопасности, межнациональных отношениях, противодействии экстремизму и терроризму Генеральной прокуратуры Российской Федерации, а также управлениями Генеральной прокуратуры Российской Федерации в федеральных округах.

По результатам рассмотрения уведомлений, которые могут поступать от органов государственной власти и местного самоуправления, организаций или граждан, указанные подразделения готовят требования о принятии мер по удалению информации или ограничению доступа к ней, которые подписываются Генеральным прокурором Российской Федерации или его заместителями. В Роскомнадзор требования направляются через личный кабинет либо посредством факсимильной связи.

Особенности рассмотрения уведомлений о распространении информации, содержащей призывы к массовым беспорядкам и участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, обусловлены необходимостью оперативного пресечения такой информации. При поступлении данных уведомлений в органы прокуратуры незамедлительно истребуются сведения об организаторах, времени, месте проведения мероприятия и количестве участников. Подготовка требования осуществляется в срок до 5 дней или незамедлительно соответствующим управлением Генеральной прокуратуры Российской Федерации в федеральном округе.

Следует отметить, что прокурорами уделяется внимание нарушениям, связанным с беспрепятственным доступом к запрещенной информации посредством анонимайзеров и VPN-сервисов. Порядок действий уполномоченных органов при выявлении таких фактов определен в ст. 158 Закона об информации.

В целях формирования у граждан позитивного отношения к принимаемым мерам по противодействию терроризму и экстремизму прокурорами в местных СМИ на сайтах управ, информационных стендах размещаются материалы по вопросам противодействия террористическим проявлениям. В некоторых регионах среди населения распространяются памятки по мерам противодействия терроризму и действиям в особый период. Органами исполнительной власти и местного самоуправления на постоянной основе публикуются статьи, в СМИ размещается информация по вопросам антитеррористической защищенности. Информация о выявленных прокурорами нарушениях за-

конодательства о противодействии терроризму, а также о нарушениях, снижающих уровень антитеррористической защищенности объектов и принятых в этой связи мерах реагирования публикуется как в местных средствах массовой информации, так и на официальных сайтах органов государственной власти и местного самоуправления.

В целях профилактики и предупреждения преступлений рассматриваемой категории особое внимание уделено вопросам организации действенного взаимодействия правоохранительных и контролирующих органов: изучению эффективности и качества межведомственного взаимодействия и выработке совместных предложений, направленных на повышение результативности этой деятельности; проработке вопроса о создании межведомственных автоматизированных поисковых систем, направленных на выявление, предупреждение и пресечения отдельных категорий преступлений; разработке межведомственных практических рекомендаций по выявлению преступлений в сфере информационно-коммуникационных технологий, организации их расследования и документированию деятельности лиц, их совершивших, сбору, фиксации доказательств и использованию экспертных познаний; проведению межведомственных семинаров-совещаний с привлечением специалистов в сфере защиты информационной безопасности и многому другому.

Активное использование ИТС для распространения экстремистской идеологии подтверждает необходимость укрепления и международного сотрудничества в области противодействия использованию информационно-коммуникационных технологий в террористических и криминальных целях.

Российская Федерация участвует в процессах, связанных с обеспечением глобальной информационной безопасности. В 2018 г. по инициативе Российской Федерации Генеральной Ассамблеей ООН приняты резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/RES/73/27 от 5 декабря 2018 г.) и «Противодействие использованию информационно-коммуникационных технологий в преступных целях» (A/RES/73/187 от 17 декабря 2018 г.).

В частности, Генеральной Ассамблеей ООН обращено внимание на необходимость поиска наилучших путей сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании информационно-коммуникационных технологий.

В сфере противодействия распространению экстремистской идеологии также было инициировано принятие резолюции «Борьба с героизацией нацизма, неонацизмом и другими видами практики, которые способствуют эскалации современных форм расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости» (A/RES/73/157 от 17 декабря 2018 г.).

В указанном документе констатируется, что в силу различия национальных стандартов, запрещающих человеконенавистническую риторику, некоторые страны могут служить убежищем для распространителей неонацистских, агрессивных националистических, ксенофобских или расистских идей, поскольку многие неонацистские и близкие к ним экстремистские группы расистского и ксенофобского толка действуют на транснациональном уровне, опираясь на поставщиков интернет-услуг или социальные медиаплатформы.

В декабре 2019 г. Генеральной Ассамблеей ООН одобрено предложение Российской Федерации разработать международную конвенцию о противодействии использованию информационно-коммуникационных технологий в преступных целях, учрежден специальный межправительственный комитет экспертов[1]. Предполагается, что выработка универсальных международных правил будет способствовать скоординированной деятельности государств в данной сфере.

Изложенное позволяет выделить следующие направления совершенствования мер по предупреждению использованию ИТС в преступных целях:

— профилактическая деятельность, направленная на формирование у граждан неприятия террористической и экстремистской идеологии;
— повышение качества и эффективности оперативно-разыскной деятельности, направленной на выявление, пресечение и раскрытие преступлений, предусмотренных ст. 207 («Заведомо ложное сообщение об акте терроризма») УК РФ, совершенных с ИТС;
— мониторинг сети Интернет совместно с Роскомнадзором на предмет выявления запрещенной информации и принятие мер, направленных на исключение распространения указанных сведений;
— разработка рекомендаций, направленных на повышение эффективности, по результатам обобщения практики применения полномочий, предусмотренных ст. 15.3, 15.1-1 Закона об информации.

2.2. Деятельность прокурора по установлению причин и условий, способствующих совершению преступлений в сфере информационно-телекоммуникационных сетей и компьютерной информации

Представляется необходимым отдельно рассмотреть практику установления причин и условий, способствующих совершению преступлений в сфере ИКТ.

---

[1] Резолюция Генеральной Ассамблеей ООН от 27 декабря 2019 г. № 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях».

Очевидно, что способ совершения дистанционных мошенничеств заключается в психологическом, моральном воздействии на потенциальную жертву. Противодействие посредством предупреждения таким преступлениям может быть эффективным только при наличии активной пропагандистской работы ввиду массово развивающихся электронных и платежных систем.

С учетом требований УПК РФ (ст. 71, ч. 2 ст. 158) следователями практически повсеместно принимались меры по установлению причин и условий, способствующих совершению преступлений, случаев их отклонения представлений практически не имелось.

Например, по всем оконченным производством уголовным делам следователями направлены представления о принятии мер по устранению обстоятельств, способствовавших совершению преступления, в том числе в исправительные учреждения, где находились обвиняемые на момент совершения преступлений. Однако в 2020 г. указанная проблема остается актуальной. В целях усиления контроля за организацией профилактической деятельности следователей органов внутренних дел по уголовным делам, находящимся в производстве, обеспечением применения ст. 17.7 КоАП РФ в случаях невыполнения требований следователя по исполнению представления, вынесенного в порядке ч. 2 ст. 158 УПК РФ, ГСУ ГУ МВД России по Пермскому краю издано распоряжение № 5/2503 от 14 марта 2019 г. и разработаны методические рекомендации.

Основной их массив касается требований усиления службами органов внутренних дел по месту совершения преступления профилактической работы среди соответствующих категорий населения, усиления мониторинга информационно-телекоммуникационных сетей. Также представления направлялись в администрацию социальных сетей.

По уголовным делам, предварительное следствие по которым приостановлено, в адрес начальников территориальных подразделений внутренних дел направляются также информационные письма о необходимости усиления профилактической работы с населением.

Ответы о результатах рассмотрения поступают практически по всем направленным представлениям.

Как правило, в ответах содержится информация о заслушивании на служебных (оперативных) совещаниях должностных лиц, допустивших нарушения закона, в ходе которых им, как правило, строго указывается на ненадлежащее исполнение служебных обязанностей; также проводятся дополнительные занятия с личным составом с целью недопущения подобных нарушений впредь.

Использовались меры профилактического воздействия, в том числе с доведением до общественности форм и методов дистанционного мошенничества, необходимый алгоритм действий потенциальных потерпевших с привлечением сотрудников службы участковых уполномоченных полиции, данных о появлении новых видов совершения

хищения имущества и денежных средств у законопослушных граждан, меры к обеспечению сохранности имущества.

Например, в целях профилактики мошенничества общеуголовной направленности с использованием мобильных средств связи и сети Интернет МВД по Республике Башкортостан разработана памятка для распространения среди населения.

Анализ принятых органами предварительного расследования мер по устранению обстоятельств, способствовавших совершению преступлений, свидетельствует, что соответствующие представления вносятся своевременно, однако качество принятых органами предварительного расследования мер остается на неудовлетворительном уровне и зачастую носит формальный характер: не отражают суть выявленных нарушений, причин и условий, способствовавших совершению преступлений; описательная (мотивационная) часть представления излагается общими фразами, в этой связи ответы на них не содержат сведений о принятии каких-либо конкретных мер, направленных на устранение причин и условий, способствующих совершению преступления. Как следствие, принимаемые меры в своем большинстве не оказывают должного влияния на количество совершенных преступлений анализируемой категории. Примеров реального влияния внесенных представлений на состояние законности в рассматриваемой сфере практически не имеется.

Важно отметить, что следователями и дознавателями не всегда используются полномочия, предоставленные ч. 2 ст. 158 УПК РФ по внесению представления о принятии мер по устранению причин и условий, способствовавших совершению преступления. Зачастую это обусловлено спецификой совершения таких преступлений, а также действиями самого потерпевшего, способствовавшими совершению преступления (например, при совместном распитии спиртного потерпевший сам передает банковскую карту малознакомому лицу и сообщает ее PIN-код).

Как представляется, заложенный предупредительный потенциал рассматриваемых норм УПК РФ практически не реализуется ввиду крайне недостаточного процессуального регулирования. Тем не менее это единственное полномочие для недопущения повторной и новой виктимизации в рамках уголовных процедур. УПК РФ не содержит конкретной формы самих требований, порядок (кроме срока) их рассмотрения. Научные категории «причины и условия совершения преступления» носят междисциплинарный характер и имеют ярко выраженную криминологическую природу, которая среднестатистическому следователю и дознавателю просто подчас непонятна.

Не менее важное значение имеет понимание практическими работниками сути и правовой природы данного полномочия. Так, неясно, к какому роду полномочий закон относит данные требования. Какие подходы и методики применяются на практике для определения того, что именно стало причиной и условием совершения преступления?

Какими процессуальными и следственными действиями это устанавливается в процессе предварительного расследования?

Представляется, что в контексте определения процессуальной природы данного полномочия не до конца определена роль надзирающего прокурора. По форме, основанию и механизму внесения представление может быть логично и обоснованно соотнесено с актами прокурорского реагирования при реализации им надзорной функции. С учетом ранее проведенных исследований полагаем, что перспективной моделью развития рассматриваемого полномочия будет передача его прокурору, реализацию которого правильнее всего перенести на момент утверждения им обвинительного заключения (акта, постановления).

Таким образом, одним из основных факторов, способствующих совершению рассматриваемого вида преступлений, является низкая информированность населения при использовании электронных средств платежей об уровне и степени необходимой информационной безопасности и цифровой гигиены.

В целом среди причин и условий, способствующих совершению анализируемых преступлений, стоит отметить низкий уровень правовой грамотности среди граждан, которые своим виктимным поведением приводят к совершению в отношении них преступлений указанной категории. В этой связи особую роль играет профилактика, направленная на дополнительное информирование и проведение разъяснительной работы с населением. Однако принимаемыми мерами положительный результат не достигнут, число регистрируемых преступлений растет. Как представляется, несмотря на обязательность требований закона, оценить эффективность принимаемых мер можно только с формальной стороны.

Зачастую потерпевшие не понимают необходимости сокрытия конфиденциальной информации и сами в конкретных ситуациях, будучи введенными в заблуждение под различными предлогами, называют и сообщают достоверные исходные данные и сведения по своим счетам и суммам вкладов, позволяющие злоумышленникам беспрепятственно осуществлять незаконные и мошеннические операции с их счетами и вкладами в банковских учреждениях; при этом разъяснительная и иная профилактическая работа среди населения органами правопорядка практически на данном направлении не ведется.

Изучение практики внесения и рассмотрения представлений об устранении причин и условий, способствующих совершению преступления, направленных на предупреждение повторной и новой виктимизации, свидетельствует о формальном подходе в отдельных случаях ответственных должностных лиц органов предварительного расследования к выполнению требований данной нормы закона и, как следствие, к неоказанию какого-либо профилактического воздействия на уровень и состояние преступности.

Глава 3

ДЕЯТЕЛЬНОСТЬ ПРОКУРОРА ПО ОБЕСПЕЧЕНИЮ ИСПОЛНЕНИЯ ЗАКОНОВ ПРИ ВЫЯВЛЕНИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

3.1. Теоретико-правовые основы прокурорского надзора за исполнением законов при выявлении и расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации

Практика организации и осуществления прокурорского надзора в рассматриваемой сфере формируется с учетом требований федерального законодательства, ведомственных организационно-распорядительных актов, а также подходов, основанных на специфике механизма совершения противоправных деяний в сфере ИКТ. В подобной ситуации нельзя недооценивать роль прокурорского надзора, поскольку своевременное выявление нарушений норм федерального законодательства и использование мер прокурорского реагирования позволяют избежать признания собранных по уголовному делу доказательств недопустимыми и необоснованного привлечения лица к уголовной ответственности, обеспечить потерпевшим от преступлений доступ к правосудию, включая возмещения ущерба от преступления.

Сущностная характеристика прокурорского надзора за исполнением законов при выявлении и расследовании преступлений, совершаемых с использованием ИКТ, определяется исключительной компетенцией (полномочиями) органов прокуратуры по обеспечению соблюдения прав и законных интересов, исполнению законов, выявлению, пресечению и предупреждению правонарушений, привлечению лиц к предусмотренной законом ответственности.

Рассматриваемая деятельность осуществляется в соответствии с общегосударственными приоритетами и концентрируется на таких базисных направлениях, как положения о защите участников уголовного процесса, закрепленные в ст. 6 УПК РФ, которые, в свою очередь, конкретизированы в его отдельных нормах. Неуклонное выполнение требований закона, определяющих задачи прокурорской деятельности в уголовном судопроизводстве, является непременным условием достижения назначения уголовного судопроизводства.

Любое направление прокурорской деятельности характеризуется специальным *Объектом, предметом, задачами и полномочиями* прокурора[1]. В целях всесторонней характеристики видится возможным также указать на *пределы его осуществления и специализированное нормативное правовое регулирование*.

Объект прокурорского надзора представляет собой совокупность юридических и физических лиц, государственных и муниципальных должностных лиц, на которые распространяется надзорная деятельность прокуратуры[2]. Применительно к рассматриваемому направлению объект прокурорской деятельности можно определить, как совокупность субъектов правоотношений, осуществляющих в пределах своей компетенции процессуальную и оперативно-разыскную деятельность в целях выполнения определенных в законе[3] задач и достижения назначения уголовного судопроизводства. Прокурор осуществляет надзор за исполнением законов названными *субъектами правоотношений* — объектами надзора (нижестоящий прокурор, следователь, следователь-криминалист, руководитель следственного органа, орган дознания, начальник подразделения дознания, дознаватель)[4].

Как справедливо отмечает А. Х. Казарина, в наибольшей степени выбор оптимальной модели прокурорского надзора зависит от правильного понимания его предмета, так как через эту правовую категорию раскрывается содержание деятельности органов прокуратуры[5]. В *предмет прокурорского надзора* в соответствии со ст. 29 Закона о прокуратуре входит соблюдение прав и законных интересов заинтересованных лиц, установленного порядка разрешения заявлений и сообще-

---

[1] См.: *Березовская С. Г.* Нормы прокурорского надзора и их место в системе советского права // Вопросы прокурорского надзора. М., 1972. С. 38; *Спиридонов Б. М.* Понятие отрасли прокурорского надзора // Совершенствование прокурорского надзора в СССР. М., 1973. С. 86.

[2] См.: Прокурорский надзор: учебник для вузов / под ред. засл. юриста РФ, д.ю.н., профессора А. Я. Сухарева. М.: Норма, 2005. С. 16.

[3] См.: ст. 2 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».

[4] См.: *Рябцев В. П.* Прокурорский надзор: курс лекций. М.: Норма, 2006. С. 23–24.

[5] См.: *Казарина А. Х.* Эволюция взглядов на предмет прокурорского надзора // Вестник Академии Генеральной прокуратуры Российской Федерации. 2013. № 2. С. 36.

ний о совершенных и подготавливаемых преступлениях; проведение предварительного расследования; законность решений, принимаемых органами, осуществляющими дознание и предварительное следствие[1], а в целом — законность и обоснованность процессуальной деятельности органов дознания и органов предварительного следствия (ч. 1 ст. 37 УПК РФ)[2]. Приказы и инструкции Генерального прокурора Российской Федерации, совместные организационно-распорядительные акты нацеливают прокуроров на максимальное использование всех возможностей, предусмотренных законом.

Следует обратить внимание читателей, что в качестве участников уголовного судопроизводства (потерпевших, гражданских истцов и др.) могут выступать не только физические, но и юридические лица; следовало бы расширить предмет прокурорского надзора в этой части, указав в ст. 29 Закона о прокуратуре вместо соблюдения прав и свобод «человека и гражданина» соблюдение прав и свобод «участников уголовного судопроизводства, а также иных лиц, чьи права и законные интересы затрагиваются в ходе производства по уголовному делу»[3].

Задачи прокурорской деятельности вытекают из профессиональных функций прокурора: это прокурорский надзор и уголовное преследование от имени государства. Применительно к рассматриваемой сфере задачи этой деятельности сводятся к обеспечению законности как на досудебных, так и на судебных стадиях уголовного судопроизводства, а именно:

- — надзор за исполнением требований закона об осуществлении оперативно-разыскной деятельности;
- — надзор за законностью приема, регистрации и разрешении сообщений о преступлениях, постановлений о возбуждении и отказе в возбуждении уголовных дел, исполнением требований закона о соблюдении прав и законных интересов участников уголовного процесса и иных заинтересованных лиц;
- — своевременность и полнота принятия мер для всестороннего, полного и объективного расследования преступлений;
- — исполнение объектами надзора требований закона об установлении всех обстоятельств, подлежащих доказыванию по уголовным делам; установление характера и размера вреда, причиненного преступлением; своевременное принятие мер обеспечения исполнения приговора в части гражданского иска,

---

[1] См.: *Рябцев В. П.* Прокурорский надзор: курс лекций. М.: Норма, 2006. С. 26–27.

[2] См.: Прокурорский надзор: учебник для вузов / под ред. засл. юриста РФ, д.ю.н., профессора А. Я. Сухарева. М.: Норма, 2005. С. 290.

[3] *Жубрин Р. В.* Проблемы теории и практики прокурорского надзора за исполнением законов при расследовании незаконного предпринимательства: автореф. дис. ... канд. юрид. наук. М., 2004. С. 9.

других имущественных взысканий или возможной конфискации имущества;
- соблюдение установленных сроков при расследовании уголовных дел и проведении оперативно-разыскных мероприятий;
- соблюдение процессуального порядка производства следственных и иных процессуальных действий;
- обеспечение соответствия требованиям закона действий и решений, принимаемых в процессе производства по уголовным делам;
- обжалование судебных решений, нарушающих права и законные интересы участников уголовного судопроизводства, и др.

Функции прокурора[1] как разновидность уголовно-процессуальной функции в рассматриваемом аспекте, представляют собой направления его деятельности как участника уголовного процесса, обусловленные его ролью, назначением или целью участия в уголовном деле[2] и осуществляемые с использованием специфических форм и методов, в рамках четко очерченных компетенций этого органа[3]. Более развернутое и разделяемое нами понятие уголовно-процессуальной функции дала Н. А. Якубович, которая рассматривает их как «осуществляемую участниками уголовного процесса деятельность, характер и содержание которой определяются законом в зависимости от процессуального положения участников (их роли и назначения) в процессе, направленном на решение стоящих перед ними задач уголовного судопроизводства, отстаивание процессуальных интересов или выполнение процессуальных обязанностей»[4].

В настоящее время сложно сказать, какая из представленных функций является главенствующей, существует ли между ними конкуренция, поэтому с практической точки зрения мы будет рассматривать их как равноценные. В то же время мы полностью разделяем позицию, согласно которой нужно крайне осмотрительно перераспределять основные функции между существующими правоохранительными

---

[1] В силу положений ст. 1 Закона о прокуратуре и сложившихся в теории прокурорской деятельности догматов функция прокуратуры — это деятельность, возложенная на нее законом. В данном случае термин «прокурор» используется для характеристики его деятельности как участника уголовного процесса.

[2] См.: Уголовный процесс: учебник для вузов / под ред. проф. П. А. Лупинской. М., 1995. С. 47.

[3] См.: *Соловьев А. Б.* О функциях прокуратуры в досудебных стадиях уголовного судопроизводства // Проблемы совершенствования прокурорского надзора (к 275-летию российской прокуратуры). Материалы научно-практической конференции. М., 1997. С. 120; Прокуратура Российской Федерации (Концепция развития на переходный период). М., 1994. С. 27.

[4] См.: *Якубович Н. А.* Процессуальные функции следователя // Проблемы предварительного следствия в уголовном судопроизводстве. М., 1980. С. 15.

органами. Это может обусловить наделение государственного органа несколькими основными функциями, вызовет их конкуренцию и в конечном счете обусловит подчиненное положение перераспределяемой функции, превратит ее из основной в дополнительную, которая не должна противоречить основной функции, осуществляемой этим органом[1]. Речь идет о таких специфичных полномочиях прокурора, как дача дознавателю письменных указаний о направлении расследования, производстве процессуальных действий (п. 4 ч. 2 ст. 37 УПК РФ); возвращение уголовного дела дознавателю, следователю со своими письменными указаниями о производстве дополнительного расследования (п. 15 ч. 2 ст. 37 УПК РФ). В этой связи можно говорить, что анализ сущности уголовного преследования порождает вопрос о характере этой деятельности применительно к прокурору и ее соотношении с другими сферами деятельности органов предварительного расследования. Именно через призму обеспечения законности должна рассматриваться деятельность прокуратуры по обеспечению уголовного преследования. Представляется, что прокурор же должен вмешиваться в процесс расследования для осуществления уголовного преследования лишь с целью предупреждения, выявления и устранения нарушений закона. Выполнение же функций по организации расследования, присущей органам дознания и предварительного следствия, с учетом современного процессуального положения прокурора представляется излишним с концептуальной точки зрения.

Важное теоретическое и практическое значение имеет определение *пределов прокурорской деятельности,* под которыми понимают правовую категорию, определяющую границы должного, возможного и запрещенного при выборе прокурором объектов проверки, применении полномочий по ее проведению и средств прокурорского реагирования. Традиционно понятие пределов прокурорского надзора раскрывается через круг нормативных правовых актов, надзор за исполнением которых должен осуществлять прокурор, перечень поднадзорных объектов, а также через объем полномочий прокурора. В числе нетрадиционных сущностных критериев указывают «характер прокурорского надзора и характер мероприятий, рекомендованных прокурорами в целях устранения нарушений закона»[2].

Прокурор не вправе участвовать в правоотношениях, если для этого нет законного основания, например дать руководителю следственного

---

[1] См.: *Соловьев А. Б.* О функциях прокуратуры в досудебных стадиях уголовного судопроизводства // Проблемы совершенствования прокурорского надзора (к 275-летию российской прокуратуры). Материалы научно-практической конференции. М., 1997. С. 122.

[2] См.: *Казарина А. Х.* Теоретические и прикладные проблемы прокурорского надзора за исполнением законов экономической направленности: автореф. дис. ... д-ра юрид. наук. М., 2009. С. 40.

органа указание (контексте меры реагирования) о незамедлительном возбуждении уголовного дела. Особую значимость это приобретает в судебном разбирательстве, где надзорные полномочия государственный обвинитель не реализует, а действует в целях законного и обоснованного поддержания государственного обвинения, реализуя посредством уголовного преследования защиту публичных и частных интересов.

Пределы надзорной деятельности прокурора за исполнением закона при совершении следственных действий, по мнению В. Ф. Крюкова, определяются границами предмета надзора: процессуальной деятельностью органов дознания и органов предварительного следствия. Тактическая, методическая, управленческая и иная организационная деятельность руководителя следственного органа, следователя, органа дознания и дознавателя при производстве предварительного расследования, не входящая в сферу процессуальной деятельности производства по уголовному делу, в предмет прокурорского надзора не входит. В противном случае это ограничивает процессуальную самостоятельностью следователя и руководителя следственного органа[1]. Таким образом, пределы деятельности прокурора в рассматриваемой сфере определяются такими вышеуказанными элементами, как объект, предмет, его полномочия, полномочия субъектов правоотношений, основания для любого действия, средства (формы) прокурорской деятельности[2], применение актов прокурорского реагирования[3].

В то же время анализ полномочий прокурора, в частности право давать дознавателю письменные указания о направлении расследования, производстве процессуальных действий (п. 4 ч. 2 ст. 37 УПК РФ), позволяет говорить о том, что прокурор уполномочен вмешиваться в организацию, тактику и методику предварительного расследования, осуществляемого органами дознания и дознавателями[4].

Система нормативных правовых актов, регулирующих деятельность прокурора в рассматриваемой сфере, включает положения Конституции Российской Федерации, Закона о прокуратуре, кодексов (УПК РФ, УК РФ, ГК РФ и др.). Также следует учитывать поло-

---

[1] *Крюков В. Ф.* Уголовное преследование в досудебном производстве. М., 2010. С. 304, 327.

[2] *Химичева О. В.* Концептуальные основы процессуального контроля и надзора на досудебных стадиях уголовного судопроизводства. М.: Юнити-Дана, 2005. С. 165.

[3] Теоретико-правовые и организационные основы участия прокурора в уголовном судопроизводстве: монография / под общ. ред. А. Г. Халиулина; Акад. Ген. прокуратуры Рос. Федерации. М., 2016. С. 250.

[4] *Буланова Н. В.*, *Ережипалиев Д. И.*, *Яловой О. А.* Деятельность прокурора на досудебных стадиях уголовного судопроизводства: организационный, процессуальный и криминалистический аспекты: пособие / Акад. Ген. прокуратуры Рос. Федерации. М., 2013. С. 24.

жения Закона Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»; Федеральных законов от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»; от 30 апреля 2010 г. № 68-ФЗ «О компенсации за нарушение права на судопроизводство в разумный срок или права на исполнение судебного акта в разумный срок»; от 7 февраля 2011 г. № 3-ФЗ «О полиции»; от 28 декабря 2010 г. № 403-ФЗ «О Следственном комитете Российской Федерации» и др.

Для повышения эффективности Генеральным прокурором Российской Федерации издается ряд организационно-распорядительных документов (приказы, указания, распоряжения, положения и инструкции), положения которых, согласно ч. 1 ст. 17 Закона о прокуратуре, являются обязательными для исполнения. Не менее важное значение для организации надзора за соблюдением прав и законных интересов потерпевших имеют информационные письма, обзоры и методические рекомендации. В указанных документах и материалах конкретизируются процессуальные возможности прокуроров, даются наставления для осуществления действенной и эффективной прокурорской деятельности. В качестве основных необходимо отметить следующие: приказы Генерального прокурора Российской Федерации от 26 ноября 2007 г. № 188 «Об организации прокурорского надзора за исполнением законов о несовершеннолетних и молодежи»; от 27 ноября 2007 г. № 189 «Об организации прокурорского надзора за соблюдением конституционных прав граждан в уголовном судопроизводстве»; от 5 сентября 2011 г. № 277 «Об организации прокурорского надзора за исполнением законов при приеме, регистрации и разрешении сообщений о преступлениях в органах дознания и предварительного следствия»; от 16 января 2012 г. № 7 «Об организации работы органов прокуратуры Российской Федерации по противодействию преступности»; от 28 декабря 2016 г. № 826 «Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия»; от 26 января 2017 г. № 33 «Об организации прокурорского надзора за процессуальной деятельностью органов дознания» и др.

В целях реализации процессуальных функций прокурора уголовно-процессуальный закон наделил прокурора властно-распорядительными *полномочиями*. В соответствии со ст. 30 Закона о прокуратуре полномочия прокурора по надзору за исполнением законов органами дознания и органами предварительного следствия определяются уголовно-процессуальным законодательством и другими федеральными законами. Суд, прокурор, следователь, орган дознания и дознаватель не вправе применять федеральный закон, противоречащий УПК РФ (ч. 1 ст. 7 УПК РФ). УПК РФ не содержит специальных полномочий прокурора по надзору за процессуальной деятельностью по расследованию преступлений в сфере ИКТ, процессуальные полно-

мочия прокурора обуславливаются предметом и задачами прокурорского надзора.

Так, УПК РФ предусмотрены полномочия, принадлежащих исключительно прокурору. Указанные полномочия в своем большинстве закреплены в ч. 2 ст. 37 УПК РФ.

Есть ряд полномочий, которые относят к другим профессиональным участникам уголовного процесса. Как верно указывает А. А. Тушев, полномочия прокурора не могут быть строго подразделены на надзорные, по руководству дознания, уголовному преследования и др., поскольку одни и те же полномочия могут обеспечивать реализацию сразу нескольких функций. Например, право отмены незаконного постановления обеспечивает реализацию и системной правозащитной функции, и руководства процессуальной деятельностью, а в иных случаях — и уголовного преследования[1]. Закон предоставил право судье, руководителю следственного органа, следователю, дознавателю наряду с прокурором выносить законное, обоснованное и мотивированное постановление (п. 25 ст. 5, ч. 4 ст. 7 УПК РФ). Прокурор, а также суд, следователь, дознаватель обязаны разъяснять участникам уголовного судопроизводства их права, обязанности и ответственность и обеспечивать возможность осуществления этих прав (ч. 1 ст. 11 УПК РФ). Прокурор наравне с руководителем следственного органа, следователем, органом дознания и дознавателем имеет право в пределах своих полномочий предъявлять требования, поручения и запросы, которые обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами (ч. 4 ст. 21 УПК РФ).

Полномочия прокурора по предупреждению нарушений закона (полномочия профилактического характера) сводятся преимущественно к инициативному и разрешительному порядку деятельности прокурора в условиях отсутствия установленного факта правонарушения.

Среди наиболее используемых следует указать на право прокурора изымать любые материалы проверки сообщения и уголовное дело у органа дознания и предварительного следствия, передавать его следователю с обязательным указанием оснований такой передачи (п. 11, 12 ч. 2 ст. 37 УПК РФ). В качестве оснований выступают особая значимость устанавливаемых фактов, сложность их исследования, а также неоднократные существенные нарушения требований уголовно-процессуального закона. Как верно указано в литературе, это одна из самых эффективных форм влияния на ход и итоговые результаты предварительного следствия[2] и единственная безусловная

---

[1] *Тушев А. А.* Прокурор в уголовном процессе Российской Федерации. СПб.: Издательство Р. Асланова «Юридический центр Пресс», 2005. С. 59–60.

[2] См.: *Ковтун Н. Н.* К дискуссии об «утраченных» полномочиях прокурора. Есть ли предмет для дискуссий? // Российская юстиция. 2010. № 5. С. 29–34.

процессуальная форма реагирования прокурора на нарушение закона и неисполнение его требований[1]. При реализации данных полномочий в качестве обязательного условия ставится законность, а не целесообразность в интересах следствия. В этой связи данное полномочие нельзя рассматривать как относящиеся к процессуальному руководству предварительным расследованием.

Прокурор вправе давать дознавателю письменные указания о направлении расследования, производстве процессуальных действий (п. 4 ч. 2 ст. 37 УПК РФ). Системный анализ данной нормы позволяет говорить о возможности поручения прокурором проведения любых следственных и процессуальных действий. Вместе с тем анализ положений уголовно-процессуального законодательства показывает, что буквальных полномочий давать указания органам дознания по проведению оперативно-разыскных мероприятий у прокурора нет. Это подтверждает положение ч. 3 ст. 7 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Цель данных указаний может быть различна: если в результате таких действий будут установлены нарушения закона, допущенные при производстве дознания, то данное полномочие будет реализовано с целью надзора. Если же оно позволит установить обстоятельства, подтверждающие причастность конкретного лица к совершению преступления, а также увеличения объема обвинения, то такое полномочие следует отнести к числу тех, которые направлены на осуществление уголовного преследования[2].

Важно отметить, что в настоящее время в перечне процессуальных возможностей прокурора отсутствует введенное в 1999 г. правовое средство — право объявлять в письменной форме должностному лицу (в том числе органов дознания и предварительного следствия) предостережение о недопустимости нарушения закона. Статья 251 Закона о прокуратуре четко устанавливает основания применения прокурором такой превентивной меры — наличие сведений о готовящихся противоправных деяниях, а целью является предупреждение правонарушений (следует отметить, что не любых, а связанных с возможным нарушением закона, что прямо вытекает из названия прокурорского документа). К сожалению, анализ положений Закона о прокуратуре позволяет говорить, что все меры прокурорского реагирования, им предусмотренные, не могут быть использованы в рассматриваемой сфере. Так, согласно указанию Генерального прокурора Российской

---

[1] См.: *Буланова Н. В.* Обеспечение прав человека в уголовном судопроизводстве средствами прокурорского надзора // Законы России: опыт, анализ, практика. 2011. № 11. С. 33–40.

[2] См.: *Халлиулин А. Г.* Уголовное преследование как функция прокуратуры Российской Федерации: дис. ... д-ра юрид. наук. М., 1997. С. 132.

Федерации от 6 июля 1999 г. № 39/7 «О применении предостережения о недопустимости нарушения закона», для профилактики нарушений закона при производстве дознания, предварительного следствия и при рассмотрении дел судами использовать иные средства прокурорского реагирования, предусмотренные п. 1 ст. 30 Закона о прокуратуре, которая является отсылочной к положениям УПК РФ. Также УПК РФ не знает таких актов, как протест, представление (в смысле требований Закона о прокуратуре). И это позволяет говорить о том, что в уголовном судопроизводстве их использование недопустимо с точки зрения положений закона[1], хотя на практике прокуроры такую форму, как представление, достаточно часто используют. В этих условиях указанный пробел восполнил такой не регламентированный законом акт прокурорского реагирования, как информация, который распространился на практике. Установить точное количество фактов, связанных с направление информации в рассматриваемой сфере, также не представляется возможным, так как статистические данные указывают на общее количество внесенных представлений и информаций об устранении нарушений закона[2].

Следует также отметить полномочия по выявлению нарушений закона и причин, их порождающих и способствующих (проверочные полномочия). Данный вид процессуальных полномочий прокурора предполагает активные действия в отношении объектов и предмета надзора при установлении сведений или предположении о потенциальных нарушениях требований закона участниками уголовного судопроизводства. Эта проверка исполнения требований федерального закона при приеме, регистрации и разрешении сообщений о преступлениях является и на практике признается одним из основных полномочий в рассматриваемой сфере (п. 1, 5.1 ч. 2 ст. 37 УПК РФ); право истребования и проверки на законность и обоснованность решений следователя или руководителя следственного органа о приостановлении или прекращении уголовного дела и их отмены при наличии на то оснований (п. 5[1] ч. 2 ст. 37, ч. 6 ст. 148, ч. 1.1 ст. 211, ч. 1 ст. 214 УПК РФ). Важным полномочием является возможность ознакомления с материалами находящегося в производстве уголовного дела при наличии мотивированного письменного запроса прокурора (п. 2.1 ст. 37

---

[1] См., например, *Ергашев Е.* Проблемы правового статуса прокурора в досудебном производстве по уголовному делу // Уголовное право. 2008. № 4. С. 91; *Соколов А.* Проблемы и практика применения прокурором требования об устранении нарушений федерального законодательства в уголовном процессе // Уголовное право. 2009. № 2. С. 124; *Буланова Н. В.* Обеспечение прав человека в уголовном судопроизводстве средствами прокурорского надзора // Законы России: опыт, анализ, практика. 2011. № 11. С. 33–40.

[2] См.: Сводный отчет по Российской Федерации по форме НСиД.

УПК РФ). В общем смысле рассматриваемое полномочие означает, что данный порядок представляется не вполне эффективным, так как полностью исключает возможность прокурора проводить внезапные проверки уголовных дел, находящихся в производстве у следователя, что явно не соответствует задачам надзорной деятельности прокурора и может быть причиной неоднократного нарушения прав и законных интересов участников уголовного процесса[1].

Еще одно из главных полномочий прокурора применительно к рассматриваемой группе — решение прокурора по поступившему к нему уголовному делу с обвинительным заключением (актом, постановлением), согласно которым своим мотивированным постановлением прокурор вправе вернуть уголовное дело для производства дополнительного расследования со своими письменными указаниями (п. 15 ч. 2 ст. 37, п. 2 ч. 1, ч. 3 ст. 221; п. 2 ч. 1 ст. 226; п. 2 ч. 1 ст. 226.8 УПК РФ).

Реформы процессуального положения прокурора, по сути, не коснулись его полномочий в отношении органов, осуществляющих оперативно-разыскную деятельность. Так, по требованию прокуроров руководители данных органов обязаны представлять им оперативно-служебные документы, включающие в себя дела оперативного учета, материалы о проведении оперативно-разыскных мероприятий с использованием оперативно-технических средств, а также учетно-регистрационную документацию и ведомственные нормативные правовые акты, регламентирующие порядок проведения оперативно-разыскных мероприятий (ст. 21 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»).

Полномочия по устранению нарушений закона и обстоятельств, им способствующим, носят превентивный характер и представляют собой меры реагирования прямого или косвенного действия, выносимые надзирающими прокурорами при выявлении нарушений требований закона.

Одно из самых востребованных на практике в данной группе — право прокурора выносить постановление о направлении соответствующих материалов в следственный орган или орган дознания для решения вопроса об уголовном преследовании по фактам выявленных прокурором нарушений уголовного законодательства (п. 2 ч. 2 ст. 37 УПК).

Прокурор вправе требовать от органов дознания и следственных органов устранения нарушений федерального законодательства, допущенных в ходе дознания или предварительного следствия (п. 3 ч. 2 ст. 37 УПК РФ). Необходимо отметить, что процессуальный порядок

---

[1] См.: *Быков В. М.* Права прокурора на стадии возбуждения уголовного дела // Законность. 2013. № 4. С. 49–53.

внесения требования, как и порядок его исполнения, в уголовно-процессуальном законодательстве до настоящего времени остался неопределенным, хотя, как нам представляется, данное полномочие олицетворяет непосредственность и исключительность прокурорской деятельности в уголовном процессе.

До внесения в 2019 г. изменений[1] в УПК РФ на практике с момента знаковых изменений в УПК РФ в 2000 г. отмечался проблемный аспект реализации данной меры прокурорского реагирования о невозможности в ряде случаев буквального толкования данной меры к стадии приема, регистрации и разрешения сообщений о преступлениях. Эти и другие изменения наглядно показывают изначальные поспешные законодательные изменения в отношении прокурора.

Прокурор вправе выносить постановление об отмене незаконного или необоснованного постановления нижестоящего прокурора, а также незаконного или необоснованного постановления дознавателя (п. 6 ч. 2 ст. 37 УПК), отменять незаконные и необоснованные постановления руководителя следственного органа или следователя о приостановлении предварительного следствия, прекращении предварительного следствия (уголовного преследования) (ч. 1.1 ст. 211, ч. 1 ст. 214 УПК РФ).

С учетом специфики расследования преступлений в сфере ИКТ особое внимание следует обращать на соблюдение процессуального порядка обращения и использования (изъятие, копирование, осмотр, использование, признание вещественными доказательствами и др.) в рамках уголовного дела электронных носителей информации (ч. 4 ст. 81, ч. 1, 4 ст. 81.1, ст. 82, 164, 164.1, 166, 185, УПК РФ).

Неоспорим тот факт, что соблюдение законности органами предварительного расследования в существенной мере обеспечивается прокурорским надзором, а качество и эффективность последнего — надлежащей *организацией*[2]. Организация прокурорской деятельности строится на общих началах, с учетом ее значимости и объемов, а также специфики данного направления прокурорской деятельности. Эффективная организация рассматриваемой деятельности предполагает использование как внутрисистемных, так и внешнесистемных ресурсов, когда прокурор управляет рассматриваемой деятельностью, то есть направляет и оперативно руководит ее осуществлением для достижения поставленных целей и задач.

На практике содержание внутрисистемного уровня организации прокурорской деятельности составляют следующие элементы (под-

---

[1] Федеральный закон от 27 декабря 2019 г. № 499-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации».

[2] См.: *Данилова Н. А.*, *Николаева Т. Г.* Анализ прокурором материалов уголовного дела: уголовно-процессуальный и криминалистический аспекты // Вестник Академии Генеральной прокуратуры Российской Федерации. 2014. № 2 (40). С. 67.

ходы), позволяющие в совокупности рассматривать их как единую, образующую систему. Так, используется систематическое изучение практики и анализ состояния законности и правопорядка по определенным периодам времени, например, по полугодиям. Контроль, проверка и оценка исполнения принятых решений позволяют делать обоснованные выводы о состоянии и недостатках прокурорского надзора в рассматриваемой сфере. Для этого используются отчеты подчиненных прокуроров о проделанной работе, изучение иных поступающих от них сведений.

Продуктивная организация деятельности прокурора предполагает управление деятельностью структурных подразделений органов прокуратуры. По результатам выезда с проверками в нижестоящие прокуратуры нередко выявляют многочисленные нарушения и недостатки в организации прокурорского надзора в рассматриваемой сфере. Результатами таких действий становятся, например, отмены незаконных решений по материалам проверки сообщений о преступлениях. Анализ эффективности реального возмещения вреда, причиненного преступлением, может установить непродуктивную деятельность органов предварительного расследовании и органов, осуществляющих оперативно-разыскные мероприятия, несвоевременное планирование мероприятий по установлению, розыску и изъятию похищенного имущества.

Одним из важнейших элементов организации деятельности прокуроров служит выявление и распространение передового опыта. Он предполагает обобщение соответствующей информации, поступающей из органов прокуратуры, и подготовку обзоров, информационно-методических писем (справки, обзоры) о положительном опыте и недостатках такой деятельности, которые имеют для совершенствования надзорной деятельности, в которых аккумулируются эффективные методы надзора или вскрываются причины типичных недостатков (нарушений, просчетов и пр.). Большую роль в получении прокурорами навыков организации эффективной деятельности прокурора играет система повышения их квалификации, в которой первостепенное значение придается учебно-методическому обеспечению выполнения такой работы.

Учитывая сложность расследования преступлений в сфере компьютерной информации, уже отмечавшуюся низкую квалификацию следственных работников, необходимость применения при расследовании специальных знаний, прокурорский надзор за расследованием данных преступлений должен осуществляться на протяжении всего периода расследования. Специфика преступлений в сфере компьютерной информации обуславливает необходимость проведения по уголовным делам данной категории ряда специальных судебных экс-

пертиз. В связи с этим важно осуществлять прокурорский надзор уже на первоначальном этапе расследования[1].

С целью предотвращения нарушений и затягивания сроков следствия прокурору необходимо осуществлять постоянное взаимодействие с руководителем следственного органа, привлекая прокурора, который впредь будет поддерживать государственное обвинение в судебном заседании.

Организовать такое взаимодействие возможно в виде совместных оперативных совещаний по обсуждению хода следствия при прокуроре, проводимых при принятии важных процессуальных решений по уголовному делу, например при оценке достаточности доказательств для предъявления обвинения, при назначении экспертиз и обсуждении их выводов для последующего планирования расследования, при окончании предварительного следствия, при рассмотрении поступающих к прокурору жалоб и заявлений.

Более того, во многих субъектах Российской Федерации изданы межведомственные приказы и иные нормативные документы, регулирующие порядок взаимодействия при расследовании уголовных дел между следственными органами и прокурорами. Это позволяет избежать многих нарушений и недостатков предварительного расследования, которые, в свою очередь, могут повлечь за собой возвращение уголовного дела прокурором для дополнительного расследования или судом прокурору в порядке, установленном ст. 237 УПК РФ.

Для повышения эффективной рассматриваемой деятельности недостаточно использование исключительно внутренних ресурсов системы прокуратуры. Поэтому внешнесистемные подходы организации с учетом координирующей функции прокуратуры используют достаточно разнопланово.

Так, комплексный характер анализа практики в ряде случаев позволяет выявить системные проблемы организации межведомственного взаимодействия, выражающиеся на практике в неустановлении причин и условий, способствующих совершению преступлений.

Прогнозирование и планирование в сфере осуществления деятельности прокурора может дать положительный конечный результат, когда итоги обобщения надзорной практики включаются в проекты координационных совещаний и целевых программ, с возможностью их корректировки и адаптации к изменяющейся обстановке, реализации запланированных мер в полном объеме и в намеченные сроки.

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации / утв. Генеральной прокуратурой Российской Федерации // СПС «КонсультантПлюс» (дата обращения: 13.11.2020).

В качестве потенциально эффективной организационной меры необходимо указать на проведение межведомственных совещаний о взаимодействии правоохранительных органов при осуществлении оперативно-разыскных мероприятий, установление причины неоднократной отмены таких незаконных решений органов предварительного расследования.

Положительно можно оценить совместные организационно-распорядительные документы, регламентирующие вопросы организации осуществления деятельности прокуратуры, органов дознания и органов предварительного следствия.

Важным направлением организации эффективной деятельности прокурора является координационная деятельность. Вынесение на рассмотрения координационных совещаний спорных (коллизионных) вопросов позволяет выработать общий подход в практике расследования и надзора. Логичным и востребованным выглядит ориентирование следователей и дознавателей на признание лиц потерпевшими на первоначальном этапе расследования.

Правильно построенная внешнесистемная организация взаимодействия прокурора и объектов надзора позволяет выявлять проблемы законодательного характера.

Например, как показало обобщение практики расследования преступлений в сфере ИКТ, в последние годы наиболее часто возбуждение уголовных дел этой категории происходит по материалам, содержащим результаты оперативно-разыскных мероприятий специализированных подразделений МВД России и ФСБ России. Решение о возбуждении уголовного дела принимается на основании материалам органов, осуществляющих оперативно-разыскную деятельность при реализации оперативных разработок, результатов оперативно-разыскных действий по выявлению преступлений в сфере ИКТ и лиц, их совершивших. В соответствии со ст. 11 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[1] ее результаты могут служить поводом и основанием для возбуждения уголовного дела и использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства, регламентирующими собирание, проверку и оценку доказательств. Надзирающему прокурору с учетом пределов его деятельности необходимо проверить полноту материалов, легитимность их получения и последующего предоставления в орган предварительного расследования. С учетом п. 2 ст. 1 Федерального закона от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации» уполномоченные прокуроры при-

[1] Далее — Закон об ОРД.

званы осуществлять надзор за исполнением законов органами, осуществляющими ОРД. Таким образом, к числу ключевых вопросов относится запрет на вмешательство в тактику ОРД. Ранее, в соответствии с Законом от 13 марта 1992 г. № 2506-1 «Об оперативно-розыскной деятельности в Российской Федерации»[1], основаниями для проведения ОРМ являлись не только поручения следователя, но и указания прокурора (п. 3 ст. 7).

Результаты надзорной деятельности прокуроров важны, в частности, при оценке законности и обоснованности рассекреченных результатов ОРД, представленных для решения вопроса о возбуждении уголовного дела и доказывания. Это важно при расследовании преступлений, которые совершаются по экстерриториальному принципу, в том числе в сфере ИКТ, с точки зрения допустимости полученных доказательств. В частности, особого внимания прокурора требуют результаты проведения оперативного эксперимента, проверочной закупки, контролируемой поставки, получения компьютерной информации.

Однако на практике само производство оперативно-разыскной деятельности нередко связано со сложностями; как показали проведенные ранее исследования, при выявлении и раскрытии компьютерных преступлений возникает много сложностей, такое оперативно-розыскное мероприятие, как «получение компьютерной информации», до сих пор вызывает у правоприменителей вопросы. В качестве основной причины видится недостаточно эффективный ведомственный контроль.

Особой следует признать роль прокурора в обеспечении законности проведения гласного оперативно-разыскного мероприятия в виде обследования помещений, зданий, сооружений, участков местности и транспортных средств. С позиции Закона об ОРД ограничения для данного мероприятия не предусмотрены. Считаем, что обеспечению законности способствовало бы получение согласия прокурора на проведение данного ОРМ. Этот вывод обусловлен тем, что указанное ОРМ может проводиться в жилище.

Значимым вопросом следует признать предусмотренный законом порядок обжалования действий и решений сотрудников органов, осуществляющих ОРД. С учетом требований ст. 125 УПК РФ обжалование действий и решений органа дознания осуществляется в судебном порядке. Вместе с тем полагаем, что обеспечению законности при осуществлении ОРД способствовало бы обжалование таких действий и решений уполномоченному прокурору в порядке, предусмотренном ст. 124 УПК РФ.

---

[1] Утратил силу в связи с принятием Федерального закона от 12 августа 1995 г. № 144-ФЗ.

3.2. Прокурорский надзор за исполнением законов при выявлении, пресечении и раскрытии преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации

Повышенная общественная опасность компьютерных преступлений выражается в их умышленном и организованном характере, в высокой латентности; с технической точки зрения они являются неочевидными, экстерриториальными и многоуровневыми, что осложняет их выявление, пресечение и раскрытие правоохранительными органами. Специфика данных преступлений предполагает особый подход к оперативно-разыскной деятельности.

Задачи оперативно-разыскной деятельности закреплены в ст. 2 Закона об ОРД и заключаются в выявлении, предупреждении, пресечении и раскрытии компьютерных преступлений, а также в выявлении и установлении лиц, их подготавливающих, совершающих или совершивших; в осуществлении розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания. Нередко оперативная информация, полученная в рамках работы по делу оперативного учета (или иным оперативно-служебным материалам), позволяет раскрыть преступление.

К примеру, при проверке информации, полученной в рамках работы по делу оперативного учета, проведен неотложный осмотр места жительства проверяемого лица, изъяты мобильные средства связи и сим-карты, записи с указанием номеров абонентов субъектов Российской Федерации, способов совершения мошеннических действий[1].

Оперативно значимую информацию на практике получают в ходе оперативно-разыскных мероприятий[2], исчерпывающий перечень которых предусмотрен ст. 6 Закона об ОРД. При этом необходимо иметь в виду, что количество источников получения оперативно значимой информации, особенно технических, активно растет. Это связано, в частности, с введением в обиход так называемых умных вещей, которые содержат устройства ввода-вывода информации, способны хранить, обрабатывать различные данные, осуществлять их обмен с ИКС. К ним можно отнести системы, устанавливаемые в автотранспорте, системы умного дома, бытовые приборы, вспомогательные устройства, работающие в местах общественного пользования, и пр.

Органы, осуществляющие ОРД, проводят многочисленные мероприятия (сбор образцов для сравнительного исследования, проверочную закупку, прослушивание телефонных переговоров, контролируемую

---

[1] По материалам деятельности прокуратуры Краснодарского края.

[2] Далее — ОРМ.

поставку и др.). Например, при выявлении и пресечении преступлений, связанных с незаконным сбытом наркотических средств через сеть Интернет, для установления принадлежности изъятого вещества к наркотическим средствам, психотропным веществам или их аналогам, определения его количества (веса, объема) составляется «отношение», а изъятое направляется в экспертное учреждение на исследование. При получении положительного результата исследования составляется рапорт об обнаружении признаков преступления, который вместе с результатами исследования приобщается к материалам проверки[1].

Федеральным законом от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» ч. 1 ст. 6 закона об ОРД дополнена п. 15 («Получение компьютерной информации»).

Как показывает практика, в силу многочисленности видов носителей компьютерной информации (компьютеры, встроенные и внешние накопители на жестких магнитных дисках, флеш-карты, оптические диски, периферийные устройства в виде принтеров, сканеров, факсов, сетевых серверов, маршрутизаторов, модемов и пр.) процедура обнаружения, фиксации и изъятии компьютерной информации представляет определенную сложность. Для обнаружения этих следов наряду с традиционными оперативно-разыскными мероприятиями используются и специальные, которые «представляют собой совокупность действий по перехвату и исследованию данных трафика, установление логов WEB- и MAIL-серверов, системных логов, доменов, принадлежности адреса электронной почты, исследование кейлогеров»[2].

Наиболее близкие (по сути и по содержанию) к получению компьютерной информации оперативно-разыскные мероприятия «прослушивание телефонных переговоров» (п. 10 ч. 1 ст. 6 Закона об ОРД) и «снятие информации с технических каналов связи» (п. 11 ч. 1 ст. 6 Закона об ОРД). К примеру, получение информации о входящих и исходящих соединениях с указанием базовых станций, IMEI телефонов и сим-карт, а также о движении денежных средств по абонентскому номеру применяется при раскрытии телефонного мошенничества, когда преступник, введя потерпевшего в заблуждение, убеждает его

---

[1] *Скориков Д. Г.*, *Коловоротный А. А.* Особенности выявления и документирования преступлений, связанных с незаконным оборотом наркотических средств // Рос. следователь. 2018. № 3. С. 25–29 // СПС «КонсультантПлюс» (дата обращения: 08.10.2020).

[2] *Егорышева Е. А.*, *Егорышев А. С.* Некоторые вопросы использования специальных знаний при расследовании неправомерного доступа к компьютерной информации // Эксперт-криминалист. 2011. № 3. С. 14–15.

перечислить ему денежные средства. Такое мероприятие вместе со снятием информации с технических каналов связи применяется при выявлении и пресечении преступлений, связанных с незаконным оборотом наркотических средств бесконтактным способом и платой за реализацию на электронный счет (например, QIWI-кошелек).

Важную роль в обеспечении законности оперативно-разыскной деятельности и соблюдения прав, свобод и законных интересов человека и гражданина при осуществлении оперативно-разыскной деятельности играет прокурорский надзор, а также непосредственная деятельность прокуратура по выявлению преступных посягательств.

Проведенными исследованием установлено, что количество материалов прокурорских проверок по фактам противоправных деяний в сфере компьютерной информации, направленных в органы предварительного следствия в порядке, установленном с п. 2 ч. 2 ст. 37 УПК РФ, остается незначительным[1]. Между тем руководящие указания Генерального прокурора Российской Федерации ориентируют прокуроров на необходимость использования в качестве одного из источников информации о правонарушениях информацию из сети Интернет, требуя уделять первоочередное внимание мониторингу сайтов общественных организаций и новостных сайтов[2]. По информации из прокуратур субъектов Российской Федерации за 2018–2019 гг. прокурорами нарабатывается практика эффективной реализации указанных полномочий.

Например, прокуратурой г. Апатиты в рамках надзорной деятельности проведен мониторинг Интернета, по результатам которого выявлена информации порнографического характера. В ходе проверки установлено, что на интернет-ресурсе социальной сети «ВКонтакте» размещена группа «Мурманск ФЕМДОМ...», в которой опубликованы фотографии, видеозаписи мужчин и женщин порнографического содержания. При этом ознакомиться с содержанием вышеуказанной группы социальной сети «ВКонтакте» может любой пользователь сети Интернет, что, в свою очередь, является распространением порнографических материалов посредством информационно-телекоммуникационной сети

---

[1] Информационное письмо Генеральной прокуратуры Российской Федерации от 17 января 2017 г. № 33-15-2017 «Обзор практики прокурорского надзора за соблюдением законности при противодействии преступлениям, совершаемым в Уральском федеральном округе с использованием современных информационно-телекоммуникационных технологий».

[2] См. подробнее: Приказы Генерального прокурора Российской Федерации от 1 июля 2015 г. № 343 «Об организации прокурорского надзора за исполнением законодательства в сфере миграции», от 21 марта 2018 г. № 156 «Об организации прокурорского надзора за исполнением законов о противодействии экстремистской деятельности», от 14 ноября 2017 г. № 774 «Об организации прокурорского надзора за соблюдением прав несовершеннолетних на досудебных стадиях уголовного судопроизводства», от 17 мая 2018 г. № 295 «Об организации прокурорского надзора за исполнением законов о противодействии терроризму» и другие.

Интернет. В связи с выявленными нарушениями уголовного законодательства прокурором г. Апатиты 5 апреля 2019 г. в порядке, установленном п. 2 ч. 2 ст. 37 УПК РФ, в ОД МО МВД России «Апатитский» направлены материалы проверки для решения вопроса об уголовном преследовании по факту незаконной публичной демонстрации и распространения порнографических материалов, совершенных с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть Интернет), то есть по признакам преступления, предусмотренного п. «б» ч. 3 ст. 242 УК РФ. По результатам рассмотрения указанного материала 6 июня 2019 г. ПД МО МВД России «Апатитский» возбуждено уголовное дело по признакам преступления, предусмотренного п. «б» ч. 3 ст. 242 УК РФ[1].

Нередко преступления в сфере ИКТ выявляются прокурорами при анализе и проверках материалов производств по административных правонарушениях.

Так, прокуратурой Советского района г. Липецка в ходе проведения проверки административных материалов по ст. 6.8, 6.9 КоАП РФ выявлен факт незаконного сбыта наркотического средства Л. Установлено, что 28 марта 2019 г. ею было приобретено за 1 тыс. руб. через магазин «Яна Вика» в «Телеграмм» наркотическое средство, известное ей под названием «PVP», оплата производилась через QIWI-кошелек. Данное наркотическое средство получается химическим путем сложного синтеза. В материалах проверки сведений о самостоятельном изготовлении наркотического средства не имелось. По результатам рассмотрения данного постановления прокурора 29 июля 2019 г. в ОРП ОП № 2 СУ УМВД России по г. Липецку возбуждено уголовное дело по признакам преступления, предусмотренного п. «б» ч. 2 ст. 228[1] *УК РФ*[2].

Прокуратурой Харовского района в ходе изучения материалов об административном правонарушении, предусмотренном ст. 7.27 КоАП РФ, установлено, что неустановленное лицо, находясь в неустановленном месте, из корыстной заинтересованности, с целью хищения денежных средств, используя технические устройства с неустановленными IP-адресами, неустановленным способом осуществило копирование компьютерной информации и соответственно получило неправомерный доступ к принадлежащей С. охраняемой законом компьютерной информации с персональными данными последнего, размещенной в сети Интернет в социальной сети «Одноклассники»; в результате которого С., находясь на территории г. Харовск, утратил возможность в течение некоторого времени осуществлять требуемые операции над компьютерной информацией в требуемом режиме; при этом в нее были внесены изменения в виде переписки с пользователями социальной сети «Одноклассники» с целью предоставления номеров телефонов и полученных кодов для списания денежных средств. 9 апреля 2019 г. следователем СО МО МВД России «Харовский» по результатам рассмотрения материалов,

[1] По материалам деятельности прокуратуры Мурманской области.

[2] По материалам деятельности прокуратуры Липецкой области.

направленных в порядке, установленном п. 2 ч. 2 ст. 37 УПК РФ, возбуждено уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 273 УК РФ[1].

Прокуратурой г. Таганрога по результатам проверки 4 февраля 2019 г. протоколов об административных правонарушениях, предусмотренных ст. 12.8 КоАП РФ, выявлен факт незаконного сбыта наркотического средства неустановленным лицом, которое по составленному сотрудниками ОГИБДД УМВД России по г. Таганрогу материалу привлечено к административной ответственности за управление транспортным средством в состоянии наркотического опьянения и потребление наркотического средства без назначения врача. Из материалов административного производства установлено, что наркотическое средство М. приобрел при помощи интернет-сайта «Телеграмм». По результатам рассмотрения внесенного в порядке, установленном п. 3 ч. 2 ст. 37 УПК РФ, требования надзирающего прокурора следователем ОРП на ТО ОП-2 СУ УМВД России по г. Таганрогу возбуждено уголовное дело в отношении неустановленного лица по п. «б» ч. 2 ст. 228.1 УК РФ[2].

Также прокурорами принимаются меры по выявлению новых эпизодов преступлений в сфере ИКТ при осуществлении надзорных полномочий по возбужденным уголовным делам.

Так, при изучении в прокуратуре уголовного дела, возбужденного по п. «г» ч. 3 ст. 158 УК РФ, по факту кражи со счета денежных средств у Р. установлено, что 16 мая 2018 г. около 19 часов неустановленное лицо распространило компьютерную программу на сотовый телефон Р., которая, пройдя по ссылке, указанной в СМС-сообщении, активировала программу, которая подключившись к мобильному банку Р., используя несанкционированный доступ к информации, перевела на неустановленный счет 2950 руб.

При этом, несмотря на показания потерпевшей Р. и свидетеля Д. о том, что неустановленное лицо распространило на их сотовые телефоны компьютерную программу и пыталось похитить денежные средства, следователем МВД меры к выделению и регистрации 2 сообщений о преступлениях, предусмотренных ч. 2 ст. 273 УК РФ, а также сообщения о преступлении, предусмотренном ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ, не приняты.

В этой связи 30 сентября 2018 г. прокурором принятое 25 сентября 2018 г. решение следователя о приостановлении следствия отменено с требованием выделить материалы по указанным фактам. По результатам проведения по выделенным материалам процессуальных проверок возбуждено 2 уголовных дела по ч. 2 ст. 273 УК РФ, 1 по ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ, указанные преступления учтены как укрытые и постановленные на учет по инициативе прокурора[3].

Выявление и раскрытие данных преступлений и надзор сопряжены с рядом трудностей, которые определяются преимущественно спецификой ИКТ.

---

[1] По информации из прокуратуры Вологодской области.

[2] По материалам деятельности прокуратуры Ростовской области.

[3] По информации из прокуратуры Забайкальского края.

Прежде всего, имеется в виду их скрытность и количество соучастников. При этом данные преступления носят, как правило, скоротечный, многоэпизодный (серийный) характер, также в них отсутствует визуальный контакт между потерпевшим и преступником.

Согласно опросам экспертов, к основным причинам низкого уровня выявления и пресечения респонденты отнесли сложность способов и методов совершения преступлений (53%), скрытость для большинства населения (примерно 51%), создание новых IT-технологий, увеличение пользователей сети Интернет, мобильных компьютерных устройств, переход к электронному документообороту (43%); отсутствие эффективного государственного контроля над киберпространством и средствами массовой информации (33%)[1].

Изучение практики выявления и пресечения фактов преступной деяний обобщаемой категории показывает, что органами, осуществляющими оперативно-разыскные мероприятия, ввиду высокой латентности данной категории преступлений зачастую не достигаются цели и задачи уголовного судопроизводства, виновные лица не устанавливаются и не изобличаются, тем самым нарушаются конституционные права и процессуальные гарантии потерпевших на своевременный доступ к правосудию.

Невысокая раскрываемость преступлений, совершенных с ИКТ, обусловлена как **объективными, так и субъективными причинами.**

I. К первым относятся:

1. Крайне динамичное развитие финансовых цифровых продуктов и услуг.

В настоящее время в России имеется достаточно возможностей подключаться к сети Интернет без предоставления своих персональных данных провайдеру. Также следует отметить широкое применение открытых точек доступа WI-FI, к которым можно подключиться анонимно. Выход в сеть преступниками осуществлялся из так называемой зоны свободного WI-FI — участка, где предоставляется Интернет всем желающим бесплатно: территории крупных торговых центров, некоторых кафе, зон отдыха и досуга и пр. Там каждый может воспользоваться услугами Интернет с любого портативного устройства (ноутбук, смартфон).

Кроме того, вызывает сложность и тот фактор, что большинство Wi-Fi-сетей не имеют ограничения в доступе посторонних лиц и не обладают защитными кодами, что также позволяет удаленно работать в сети Интернет без возможности установления собственника электронного устройства, с которого был осуществлен выход в сеть Интернет.

---

[1] См.: Приложение.

При использовании преступниками мобильного Интернета (через USB-модем или сотовый телефон) по известным сотрудникам органов внутренних дел IP-адресам компания-провайдер может предоставить сведения лишь о персональных данных лица, на чье имя заключался договор о предоставлении доступа при оформлении сим-карты.

Развитие продуктов, предлагаемых кредитно-финансовыми учреждениями, платежными сервисами, а также появлением технологии «CardToCard» позволяет осуществлять моментальные онлайн-платежи и переводы между счетами различных банков. Количество организаций, предлагающих данную услугу, велико, однако они не хранят в полном объеме необходимые сведения об обоих участниках транзакции.

2. Совершение преступлений лицами, находящимися за пределами субъекта или иного территориального образования, что, в свою очередь, затрудняет проведение необходимых первоначальных оперативно-разыскных мероприятий по причине сложностей или невозможности оперативной персонализации лиц, совершивших или готовивших совершение преступления.

Например, согласно данным ГСУ ГУ МВД России по Краснодарскому краю, для региона характерен удаленный принцип совершения мошенничеств, 98,7% преступлений (по расследованным уголовным делам) совершены лицами, находившимися за пределами региона, либо денежные средства потерпевших переведены на счета и телефоны, используемые на территории иных субъектов Российской Федерации[1].

В ряде субъектов РФ преступниками нередко используются абонентские номера операторов сотовой связи, которые, как правило, оформлены на третьих лиц. Анализ показал, что наибольшее количество «преступных» телефонных звонков поступает с абонентских номеров, зарегистрированных в крупных субъектах (Москва, Санкт-Петербург, Московская и иные области). Аналогичные проблемы возникают при раскрытии преступлений, совершенных посредством социальных сетей и электронных платежей. Нередко похищенные денежные средства переводятся на счета, зарегистрированные за пределами Российской Федерации.

3. Использование программного обеспечения и ресурсов Интернета, находящегося за пределами российской юрисдикции.

Преступники нередко используют при совершении рассматриваемых преступлений вредоносные программные продукты и распространяют их через различные зарубежные файловые хранилища, находящиеся на территории Европы и США.

---

[1] По материалам деятельности прокуратуры Краснодарского края.

Виртуальное общение осуществляется через почтовые ящики в доменном сегменте @google.com, @yahoo.com, @aol.com, сервера которых находятся только на территории США, либо использованием TOR-сети (браузер), в связи с чем получить необходимые сведения о владельце (пользователе) ресурсов затруднительно или практически невозможно.

4. Перевод похищенных денежных средств на счета банков, расположенных в других субъектах Российской Федерации, где в последующем происходит их снятие, что существенно затрудняет и замедляет получение интересующей информации в рамках таких ОРМ, как «наведение справок».

Установить фактического пользователя абонентским номером либо банковским счетом затруднительно и занимает значительное время. Кроме того, похищенные денежные средства неоднократно переводятся по счетам в разных финансовых организациях, что лишает возможности установить виновное лицо по горячим следам[1].

5. Отсутствие надлежащего взаимодействия со стороны кредитных учреждений, провайдеров, руководства социальных сетей, интернет-магазинов, операторов сотовой связи других субъектов Российской Федерации, нежелание активно и своевременно предоставлять информацию, способствующую раскрытию преступлений, что, в свою очередь, удлиняет сроки получения информации по запросам.

В большинстве случаев запросы правоохранительных органов исполняются необоснованно длительное время, а в ряде случаев — некачественно, что препятствует своевременному документированию противоправной деятельности в данной сфере и установлению лиц, совершивших преступления. Немаловажно отметить то, что кредитные организации далеко не всегда заинтересованы в афишировании таких действий ввиду причинения ущерба их деловой репутации.

6. Отсутствие контроля со стороны операторов сотовой связи за ретейлерами, осуществляющими продажу сим-карт, в связи с чем в большинстве случаев телефонные мошенничества совершаются с использованием сим-карт, зарегистрированных на третьих лиц.

Распространена практика регистрации СИМ-карт, банковских карт и иных устройств, которые регистрируются в различных ИКС, в том числе сети Интернет, на вымышленные данные по утерянным или украденным документам, либо с использованием персональных данных лиц, не осведомленных о преступной деятельности (зачастую карты зарегистрированы на социально неблагополучных граждан), что крайне затрудняет установление реальной личности совершивших преступления. Такие карты используют в телефонных аппаратах или компьютерах посредством мобильных модемов.

---

[1] По материалам деятельности прокуратуры Курганской области.

Единственным рычагом является профилактика таких фактов. Однако ст. 13.29 (заключение договора об оказании услуг подвижной радиотелефонной связи неуполномоченным лицом) и 13.30 КоАП РФ (невыполнение предусмотренных законом требований лицом, действующим от имени оператора связи, или несоблюдение оператором связи установленного порядка идентификации абонентов), предусматривающие ответственность за включение в договор об оказании услуг подвижной радиотелефонной связи недостоверных сведений об абоненте, на практике фактически не работают.

7. Использование преступниками иностранных мессенджеров, в связи с чем IP адреса лиц, совершивших преступления, не соответствуют их месту нахождения.

Анализ оперативной обстановки также свидетельствует о применении мошенниками при осуществлении своей незаконной деятельности анонимизированных средств связи со сквозным шифрованием (Telegram, VI Pole, Jabber) и средств скрытия реального местоположения удаленной системы прокси-серверов сетей TOR, VPN, технологии которых позволяют устанавливать анонимные сетевые соединения, обеспечивающие безопасное и защищенное общение и ввиду нахождения серверов информации за пределами Российской Федерации и отсутствия у оперативных подразделений правоохранительных органов технических ресурсов снятия подобной информации. Сформировано большое количество «зеркал» данного ресурса, что позволяет успешно противодействовать всем попыткам его блокировки.

Ряд компаний не имеют офисов на территории Российской Федерации, в связи с чем получение оперативно значимой информации об их деятельности и оказываемых ими услугах невозможно (Skype, Telegram, Instagram, Google, WhatsApp, Viber).

8. Использование специального программного обеспечения и сетевых технологий.

Стоит отметить, что в 2019 г. в ряде регионов увеличилось количество преступлений, совершенных с использованием так называемой IP-телефонии, с полной подменой абонентского номера на виртуальный, в том числе принадлежащий сегменту сети Интернет иностранных государств, где неизвестные лица представляются сотрудниками службы безопасности различных банков, в связи с чем установление местонахождения IP-адресов зачастую не имеет доказательственного значения.

Как показала практика прокурорского надзора, без проведения технических мероприятий доказать причастность лица к совершенному преступлению становится затруднительным, так как необходимо получение образца голоса звонившего, с целью дальнейшего проведения судебной фоноскопической экспертизы. По этой причине большое количество уголовных дел остается нераскрытыми.

Для сокрытия реальных IP-адресов и уклонения от ответственности преступники используют в качестве последнего звена в цепочке соединений («прокси») посторонний компьютер или сервер. Обычно в качестве «прокси» может быть использован случайный бот из собственного ботнета, также «прокси» могут быть куплены на специализированном сетевом ресурсе. Сложность для выявления и раскрытия преступлений рассматриваемого вида представляет использование «прокси» в моменты совершения хищений либо при осуществлении соединений с какими-либо значимыми ресурсами, информация о которых впоследствии может быть получена при проведении проверок и расследований. В подобных случаях в распоряжении сотрудников органов внутренних дел оказываются реальные IP-адреса совершенно посторонних лиц или организаций, которые необходимо проверять на причастность к совершенным хищениям.

9. Необходимость получения разрешений на ограничение конституционных прав граждан неопределенное количество раз, при каждой смене сим-карты и терминала сотовой связи.

К еще одной проблеме выявления и раскрытия преступлений, совершенных с использованием ИКТ, относится несовершенство механизма получения информации о движении похищенных денежных средств, которое негативно влияет на эффективность раскрытия таких преступлений. Получение сведений может затянуться на срок до одного месяца и более в зависимости от того, сколько платежных платформ и систем было использовано в схеме хищения. По каждой платежной платформе необходим новый запрос, который по срокам своего исполнения привязывается к регламенту организации-исполнителя и, как правило, составляет около 30 рабочих дней.

На практике прокуроры отмечают ряд проблем, связанных с ограниченными возможностями использования контроля телефонных и иных соединений.

Так, в Республике Татарстан существенное влияние также оказывает сложившаяся практика судебного санкционирования оперативно-разыскных мероприятий на срок не более 10 суток. Этого времени явно недостаточно для установления лиц, причастных к совершению высокотехнологичных преступлений (в связи с этим прокуратурой республики в Верховный суд Республики Татарстан подготовлена информация о необходимости корректировки судебной практики). С учетом изложенных обстоятельств раскрываемость названных криминальных посягательств по итогам работы за 12 месяцев 2019 г. достигла всего лишь 10,9% (364 преступления). В целом аналогичная ситуация складывается в части расследования мошенничеств. Из общего числа зарегистрированных преступлений данного вида (7580) две трети (5120, или 67,5%) совершены с использованием ИКТ.

II. Основной **субъективной** причиной низкой раскрываемости является недостаточная готовность оперативных подразделений

к повсеместному внедрению ИКТ в различных сферах цифровой экономики.

Так, на базе УМВД Владимирской области в декабре 2019 г. создан специализированный отдел по раскрытию данных преступлений, включающий 10 оперативных сотрудников в аппарате. Кроме того, в территориальных отделениях полиции выделены конкретные сотрудники либо группы, за которыми закреплена линия по раскрытию дистанционных краж и мошенничеств. При этом указанное подразделение и сотрудники, на которых возложено раскрытие анализируемых преступлений, не обеспечены в достаточном количестве транспортными средствами, компьютерной техникой с доступом в сеть Интернет.

В оперативных подразделениях районных отделов полиции не везде технически возможно установить IMEI-код сотовых телефонов, с помощью которых произошло снятие денежных средств, отслеживание IP-адресов, посредством которых лица, совершившие преступления, выходят в сеть Интернет.

Принимаемые оперативными подразделениями меры по выявлению и раскрытию преступлений несоразмерны оперативной обстановке в данной сфере. Непосредственно заинтересованные в изобличении преступника оперативные сотрудники по месту учета криминального посягательства этого сделать не могут в силу своей загруженности, а также реалий российской географии и финансовых возможностей ведомства. Нередко успешному выявлению и раскрытию преступлений предшествует долгая, затратная и кропотливая оперативная работа.

Например, в 2019 г. сотрудниками УУР ГУ МВД России по Саратовской области осуществлены выезды в служебные командировки в г. Москву, Московскую область, г. Санкт-Петербург, Ленинградскую область, г. Сочи, Волгоградскую, Курганскую, Новосибирскую, Самарскую, Ульяновскую, Челябинскую области, в ходе которых проведены оперативно-разыскные мероприятия в отношении лиц, совершающих мошеннические действия бесконтактным способом. В ходе выездов задержано 17 лиц, причастных к совершению мошеннических действий в отношении жителей Саратовской области.

Трудности и проблемные вопросы также обусловлены недостаточным уровнем технического оснащения оперативных подразделений (например, невозможность оперативного пресечения преступных деяний путем блокировки сайтов, используемых мошенниками и наркосбытчиками).

Например, оперативные подразделения УМВД России по Калужской области имеют достаточное техническое оснащение, вместе с тем при осуществлении звонков посредством IP-телефонии техническая возможность установления конечного абонента и местонахождения станции (устройства) отсутствует.

В процессе раскрытия и расследования преступлений данного вида сотрудниками уголовного розыска используются ресурсы ИБД-Ф «Дистанционное мошенничество», ИБД-Р, АИПС «Мониторинг происшествий», ЦАФАП ОДД ГИБДД «Поток Enterprise», сервисы обеспечения оперативно-служебной деятельности ФИС ГИБДД — М и Следопыт — М.

Однако техническое оснащение оперативных подразделений ГУ МВД России по Нижегородской области в настоящее время недостаточное. Имеется служебная необходимость в приобретении серверного программного обеспечения, предназначенного для проведения автоматического оперативного голосового поиска (идентификации) целевого диктора по образцу речи в потоке поступающих звуковых файлов в режиме реального времени. Программное обеспечение возможно использовать в составе любых систем контроля и регистрации телефонных переговоров. Данное оборудование дает возможность автоматического исследования голоса и речи дикторов, обеспечивает удобное разделение результатов на «совпадающих» и «похожих» дикторов, алгоритмы исследования голоса имеют высокий показатель надежности.

Также для работы с интернет-ресурсами имеется необходимость в приобретении «Поисковых роботов» или «веб-пауков», выполняющих информационно-разведывательную и аналитическую работу в сети Интернет, которая будет анализировать все полученные материалы, опираясь на собственные алгоритмы работы[1].

Сотрудниками поднадзорных ОВД отмечается нехватка специалистов по борьбе с преступлениями, совершаемыми с использованием ИКТ[2].

При этом адаптация криминальных элементов к способам выявления и раскрытия этих преступлений со стороны правоохранительных органов в значительной степени затрудняет установление лиц, их совершивших. Разнообразие имеющихся схем и методов совершения киберпреступлений, постоянное появление их новых видов снижают эффективность применения единых алгоритмов выявления и раскрытия криминальных посягательств, совершаемых с использованием ИКТ.

Исследуемые преступления совершаются хорошо подготовленными субъектами, владеющими различными видами специальных знаний и современными техническими средствами. При этом специальные знания позволяют им предпринимать соответствующие действия для маскировки определенного вида мошенничества под обычную финансово-хозяйственную деятельность законопослушных экономических субъектов. В рамках такой маскировки предпринимаются активные меры конспирации (короткий срок использования телефонных аппаратов, сим-карт, многократные переводы похищенных денежных средств между банковскими счетами и различными сервисами: Яндекс-деньги, QIWI-кошелек и другие), активное использование криптовалют и т.д. Например, при хищения посредством ИКТ используется в случае перечисления денег потерпевшими виртуальная криптовалюта биткоин (лайткоин, праймкоин и т.п.), не имеющая единого центра хранения сведений о владельцах виртуальных счетов,

[1] По материалам работы прокуратуры Нижегородской области.

[2] По материалам прокуратуры Белгородской области.

не рекомендованная Центробанком России к обороту на территории нашего государства и изначально разработанная с функцией анонимности сведений о владельце.

Также значительная часть преступлений совершается с использованием компьютерных вирусов, выявление которых создает определенные временные затраты, затрудняет установление лица, совершившего преступление.

Использование многоуровневого шифрования при осуществлении преступной деятельности, связанной с незаконным оборотом наркотиков, затрудняет установление личности фигурантов, места и способа совершения преступлений, финансовой составляющей и иных обстоятельств преступной деятельности, в связи с чем отследить преступную цепочку (от «закладчиков» до организатора) полностью при существующем программно-технологическом и информационно-аналитическом обеспечении работы не всегда представляется возможным.

На эффективность выявления и пресечения оказывает влияние отсутствие действенных наработок и рекомендаций, недостаточность источников получения информации о возможностях в раскрытии и расследовании преступлений данной категории, низкие навыки и отсутствие компьютерных знаний у сотрудников территориальных органов.

Одной из субъективных причин низкой раскрываемости является **нарушение законодательства об оперативно-разыскной деятельности**, допускаемое сотрудниками оперативных подразделений.

Проведенный анализ результатов прокурорского надзора показал, что во многих случаях места совершения преступлений не установлены, мероприятия в рамках ОРМ по их выявлению не всегда результативны, по делам оперативного учета, заведенным по фактам нераскрытых преступлений, надлежащая работа зачастую не проводится.

Прокурорами неоднократно отмечались недостаточные оперативные позиции подразделений ОВД, шаблонность и безынициативность проводимой оперативной работы, отсутствие эффективного ведомственного контроля со стороны руководства за деятельностью подчиненных. Оперативными подразделениями МВД анализ информации, имеющейся в уголовных делах, надлежащим образом не проводится, ответы на поручения следователей (дознавателей) носят формальный характер, сводятся к проверке на причастность к совершению преступления различных категорий лиц (ранее судимых, совершавших преступления данной категории и т.д.); при этом каких-либо служебных материалов об этом и сведений о совершении конкретными лицами данных преступлений в органах внутренних дел не имеется. Ведомственный контроль за раскрытием преступлений в нарушение

требований ст. 2, 22 Закона об ОРД во многих случаях фактически не осуществляется.

К примеру, в 2018 г. прокуратурой Ленинградского района Краснодарского края в связи с выявленными нарушениями закона об ОРД, выразившимися в бездействии сотрудников уголовного розыска ОМВД России по Ленинградскому району Краснодарского края по делу оперативного учета, заведенному в июне 2017 г. в целях проведения оперативно-разыскных мероприятий, направленных на раскрытие мошенничества с использованием средств мобильной связи путем склонения к перечислению 300 тыс. руб., внесено требование в адрес начальника ОМВД России по Ленинградскому району Краснодарского края. Требование удовлетворено, в результате проведенных по делу оперативно-разыскных мероприятий установлено лицо, причастное к совершению преступления.

Кроме того, прокурорами выявляются нарушения в деятельности органов внутренних дел, связанные с неудовлетворительным качеством оперативного сопровождения по уголовным делам данной категории. Не во всех регионах налажено эффективное использование информационно-поисковых систем «Дистанционные преступления», систематизирующих информацию о фактах мошенничества с использованием сети Интернет, бесконтактного распространения наркотических средств и др.

Исполнение требований закона при проведении оперативно-разыскных мероприятий, правильное оформление и представление их результатов органам предварительного расследования имеют большое значение. От этого во многом зависит возможность постановления судом законного и обоснованного решения, в том числе обвинительного приговора. В случае нарушения требований закона результаты оперативно-разыскной деятельности, закрепленные в качестве доказательств, могут быть признаны недопустимыми, что, в свою очередь, влечет признание незаконными иных доказательств, полученных в ходе предварительного расследования.

Не исключены случаи, когда суд признает результаты оперативно-разыскной деятельности недопустимыми из-за неправильного оформления, несоблюдения процедуры сбора. Чаще всего недопустимыми признаются протоколы осмотра помещений, зданий, участков местности, результаты оперативных экспериментов, прослушивания телефонных переговоров и фонограмм и т.д.

Проведенный анализ результатов прокурорского надзора показал, что по делам оперативного учета, заведенным по фактам нераскрытых преступлений, надлежащая работа зачастую не проводится. Прекращение таких дел в связи с утверждением прокурором обвинительного заключения либо привлечения лица к уголовной ответственности является единичным.

Прокурор не наделен правом отменять незаконные и необоснованные решения органов, осуществляющих оперативно-разыскную

деятельность. Однако он вправе применять меры реагирования, направленные на устранение нарушений закона.

Например, 18 января 2017 г. следственным отделом ОМВД России по г. Нововоронежу Воронежской области возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 2 ст. 272 УК РФ, по факту неправомерного доступа и блокировки компьютерной информации К.

24 января 2017 г. следователем в ОУР направлено поручение об установлении владельца IP-адреса, с которого осуществлялся вход на страницу потерпевшей, о проверке ранее судимых и выполнении иных мероприятий по раскрытию криминального деяния.

6 февраля 2017 г. из оперативного подразделения поступили протокол допроса свидетеля, а также рапорт о проведении оперативно-разыскных мероприятий, не давших положительного результата. При этом документы, подтверждающие проведение конкретных оперативно-разыскных мероприятий, не имелись, что ставило под сомнение достоверность рапорта. Прокурором г. Нововоронежа Воронежской области в адрес начальника ОМВД по г. Нововоронежу Воронежской области направлено требование об устранении нарушений законодательства об оперативно-разыскной деятельности.

Уровень и эффективность внутреннего взаимодействия органов расследования с подразделениями, осуществляющими оперативно-разыскную деятельность, не в полной мере соответствуют предъявляемым требованиям. В то же время налаженное взаимодействие между органами предварительного расследования позволяет выявить и раскрыть совершенное преступное деяние.

К примеру, денежные средства, принадлежащие Е., были похищены под предлогом реализации товара через интернет-магазин, размещенный на сайте «Одноклассники». Благодаря проведенной работе установлено лицо, причастное к совершению преступления, — Б., ранее судимая за совершение аналогичных преступлений. В момент совершения преступления она находилась за пределами Краснодарского края, а именно в Саратове. При расследовании уголовного дела был установлен факт совершения Б. 42 аналогичных преступлений на территории края.

В целях раскрытия указанных преступлений практикуется создание следственно-оперативных групп, в состав которых входят сотрудники оперативных подразделений и БСТМ МВД по субъектам РФ. Однако не всегда прокуроры признают их координирующую роль: не организована надлежащая помощь оперативным подразделениям в проведении занятий и разъяснении организационных вопросов реализации специальных технических мероприятий; не осуществляется эффективный мониторинг средств информационной коммуникации; отсутствие взаимодействия с инициаторами заданий (поручений) в соответствии с требованиями ст. 14 Закона об ОРД (отсутствие обмена значимой оперативной информацией, ненадлежащий контроль со стороны руководителей подразделений).

Поскольку указанные преступления относятся к категории небольшой, средней и тяжким преступлениям, работа осуществляется в рамках выполнения поручений следователей (дознавателей), без заведения дел оперативного учета.

Согласно информации из прокуратуры Республики Алтай, в подавляющем большинстве случаев оперативное сопровождение по уголовным делам анализируемой категории осуществляется без заведения дел оперативного учета, что негативно сказывается на систематизации и планировании работы оперативных служб, затрудняет как прокурорский надзор, так и ведомственный контроль за выявлением и раскрытием преступлений анализируемой категории.

В качестве положительного опыта можно указать на принятые меры на территории Удмуртской Республики[1].

На должном уровне организовано взаимодействие органов дознания МВД по УР с подразделениями, осуществляющими оперативно-разыскную деятельность, при проведении процессуальных проверок и расследовании уголовных дел рассматриваемой категории.

В целях повышения результативности работы в сфере предупреждения, раскрытия и расследования преступлений, совершаемых с использованием информационных технологий, средств мобильной связи, приказом МВД по УР от 3 декабря 2015 г. № 717 создано специализированное оперативное подразделение, штатная численность которого составляет 28 сотрудников.

В целях организации работы по раскрытию и расследованию преступлений, совершенных с использованием ИКТ, в каждом территориальном органе внутренних дел приказами начальников закреплены от 2 до 6 сотрудников подразделений уголовного розыска, дознания и следственных подразделений, которые входят в состав постоянно действующих следственно-оперативных групп.

Распоряжением МВД по УР от 9 апреля 2019 г. № 2/1078 создана следственно-оперативная группа (5 дознавателей и 10 сотрудников уголовного розыска) по раскрытию и расследованию дистанционного мошенничества, предварительное следствие по которому необязательно.

В целях систематизации и обобщения имеющейся по материалам проверок и уголовным делам информации, своевременному выявлению серийных преступлений МВД по УР разработана и введена в эксплуатацию автоматизированная информационно-поисковая система (далее — АИПС) «Мошенник». В каждом территориальном подразделении имеются ответственные сотрудники, которые при поступлении сообщений о преступлениях, а в последующем и при возбуждении уголовного дела в течение дежурных суток вносят всю имеющуюся информацию о фактах мошенничества в АИПС «Мошенник». В указанной системе обобщается вся информация (номера абонентских телефонов, банковских карт, счетов, названия и адреса интернет-сайтов и т.д.), которые используют преступники, что в последующем позволяет выявлять серийность данной преступности.

---

[1] Далее — УР.

С апреля 2019 г. обеспечено подключение подразделений МВД по УР к федеральной поисковой системе АИС «Мобильные мошенничества», организовано внесение в указанную систему необходимой информации.

В рамках заключенных соглашений МВД по УР с Удмуртским отделением № 8618 ПАО «Сбербанк России» и Ижевским филиалом ООО «Т2 Мобайл» осуществляется информационный обмен и организован электронный документооборот.

В целях мониторинга и анализа информации, размещенной в социальной сети «ВКонтакте», с декабря 2018 г. в МВД по УР применяется программное обеспечение «Поисковая система «СЕУС».

В ходе осуществления координационной деятельности прокуроры принимали меры для устранения некоторых из указанных проблемных ситуаций взаимодействия правоохранительных и контролирующих органов, участников экономической деятельности.

Так, в июне 2019 г. проблемы выявления, пресечения и раскрытия уголовно наказуемых деяний, совершенных с использованием ИКТ, являлись предметом обсуждения на межведомственном совещании руководителей правоохранительных органов Белгородской области, по итогам которого выработан комплекс мер по повышению эффективности работы на данном направлении, в том числе по профилактике преступности путем активизации работы по правовому просвещению граждан. Во исполнение решения данного совещания УМВД России по области в ООО «КЕХ еКоммерц» и ООО «Мэйл.ру» направлены предложения о рассмотрении вопроса о размещении в объявлениях на сервисах «Авито» и «Юла» местонахождения абонентского номера (его геолокации), с которого происходила регистрация, исключив при этом размещение объявлений с использованием программ-анонимайзеров. Также УМВД России по области в МВД России направлено предложение об организации электронного документооборота с кредитно-финансовыми организациями в целях сокращения сроков получения ответов на запросы и, соответственно, соблюдения разумных сроков уголовного судопроизводства.

На основе комплексного анализа информации из прокуратур субъектов Российской Федерации видится возможным определить направления по совершенствованию правообеспечительной и правоприменительной практики по эффективному выявлению и раскрытию преступлений в сфере ИКТ; это оперативность получения информации об используемых преступниками технических средствах; неотложное проведение оперативно-разыскных мероприятий, особенно в регионе нахождения подозреваемого; своевременное получение сведений о цифровом следе соединений преступника и потерпевшего, о движении денежных средств и др. Практика показывает, что реализация указанных задач требует особого внимания, выработки и реализации правоохранительными органами дополнительных мер по совершенствованию своей работы на рассматриваемом направлении, повышение результативности которой статистикой до настоящего времени не зафиксировано.

Как нам представляется, первостепенно должны быть урегулированы следующие проблемные вопросы.

1. Фактически отсутствует достаточная нормативно-правовая база для оперативного реагирования на рассматриваемые преступления. Длительная процедура получения расширенных сведений из банков (кроме ПАО «Сбербанк») о log-файлах и IP-адресах ПЭВМ, обращавшихся к расчетным счетам, с которых осуществлено необоснованное списание денежных средств, поскольку во многих случаях интересующие следствие документы готовятся длительное время в офисах кредитных организаций, расположенных в иных по отношению к месту выявления или пресечения преступления (преимущественно Москва и другие крупные города). Указанное обстоятельство крайне негативно отражается на оперативности проведения первоначальных мероприятий по задержанию преступников и изъятию предметов совершения преступлений, так как получение данной информации по судебному решению сказывается на сроках расследования уголовных дел, определении места производства расследования. Следует отметить, что банки (кредитные организации) оказывают пассивную помощь правоохранительным органам в раскрытии и расследовании названных преступлений путем предоставления сведений по запросам и судебным решениям (срок исполнения которых исчисляется месяцами), при этом располагая большей информацией, которую можно предоставить оперативно.

В связи с этим представляется целесообразным рассмотреть на законодательном уровне вопрос упрощения механизма получения сведений о движении денежных средств по банковским счетам, а также сведений о соединении абонентов и их идентификационных данных. Также необходимо усовершенствовать федеральное законодательство путем введения электронного документооборота и установления единого разумного срока для банков при исполнении запросов оперативных подразделений и следственных органов, направляемых в целях раскрытия и расследования преступлений.

2. Помимо этого, необходимо установить ответственность кредитных организаций, не обеспечивающих предусмотренных мер защиты денежных средств и вкладов и допустивших их хищение. Так, изучением уголовных дел о хищениях денежных средств с использованием ИКТ установлено, что данные хищения могли быть предотвращены сотрудниками служб безопасности банков при выявлении подозрительной деятельности на счетах клиентов, а также при обращении к ним граждан и юридических лиц о совершении указанных действий до обращения в правоохранительные органы.

Важнейшей проблемой является оперативное получение информации об операциях клиентов в кредитных организациях. В ряде случаев при рассмотрении обращений граждан для получения информации,

содержащей банковскую тайну, необходимо постановление суда, что значительно затягивает сроки рассмотрения обращений.

В данном случае считаем целесообразным выйти с инициативой в органы законодательной власти и рассмотреть вопрос об упрощении процедуры получения информации оперативными подразделениями, содержащей банковскую тайну в кредитных учреждениях.

3. Изменением существующих подходов взаимодействия может служить закрепление на законодательном уровне минимальных сроков предоставления информации по запросам правоохранительных и контролирующих органов, возможности использования в данном процессе электронного документооборота с целью их сокращения, прежде всего с банковскими структурами, операторами связи, интернет-провайдерами.

4. Для повышения эффективности работы на данном направлении необходимо установить обязательные для исполнения на всей территории РФ правила для интернет-сервисов, операторов мобильной связи, организаций, представляющих доступ к социальным сетям, связанные с запретом анонимной регистрации в социальных сетях, в платежных системах, в сети сотовых операторов мобильной связи; ограничить операторов мобильной связи в количестве регистрируемых на одно лицо сим-карт; усилить ответственность за неисполнение законных требований должностных лиц органов дознания и следствия, связанных с истребованием в учреждениях и организациях информации в рамках проведения оперативно-разыскных мероприятий.

5. Целесообразно на законодательном уровне обязать регистраторов доменных имен, компании, осуществляющие регистрацию электронных почтовых ящиков, IP-, SIP-телефонии, а также электронные платежные системы (АО «КИВИ Банк», ООО НКО «Яндекс. Деньги», ООО «ВебМани.ру», ЗАО «Национальная Сервисная Компания») осуществлять процедуру подтверждения личности с использованием электронной цифровой подписи либо с помощью портала «Госуслуги».

3.3. Прокурорский надзор за исполнением органами дознания и органами предварительного следствия требований федерального закона при приеме, регистрации и разрешении сообщений о преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации

Интеграция современных информационных технологий привела к тому, что с помощью компьютерных средств и систем совершаются преступления, затрагивающие все сферы жизнедеятельности человека, особенно это проявляется в последние годы в сфере цифровых пла-

тежей и иных финансовых услуг. Специфика механизма совершения преступлений в сфере ИКТ влияет на своевременность и законность принятия процессуальных решений при приеме, регистрации и разрешении сообщений о преступлениях.

Важной особенностью рассматриваемой категории преступлений является отсутствие привязки совершения активных преступных действий, то есть дистанционный характер их совершения. Проблемы, связанные с пресечением и выявлением «дистанционных» мошенничеств, заключаются в отсутствии контакта потерпевшего с лицом, совершившим преступление, невозможности надлежащей идентификации пользователя, а также в сравнительно быстром переводе безналичных денежных средств на дальние расстояния или за границу.

Данные прокуратур субъектов Российской Федерации и компаний, специализирующихся на информационной безопасности, также подтверждают, что не менее 80% хищений с использованием ИКТ совершаются посредством так называемой социальной инженерии[1], например с помощью отправки сообщений потенциальным жертвам или звонков с номеров сим-карт, приобретенных без регистрации или оформленных на третье лицо. Выведение похищенных денег осуществляется через подставные банковские карты, счета в интернет-магазинах, лицевые счета мобильного телефона. Действия преступников нацелены на слабости человеческого характера и личности (доверчивость, невнимательность, неграмотность и др.).

Среди наиболее часто встречаемых схем хищений денежных средств выделяются следующие способы, связанные с пластиковыми картами: кража данных банковских карт, когда любое лицо, которому в руки попала карта потерпевшего, может сфотографировать ее, переписать данные или даже запомнить их, используя впредь для осуществления электронных платежей; хищение при бесконтактной оплате, когда похитители оперируют собственными бесконтактными считывателями или терминалами, прислоняя их к карманам и сумкам (обычно посредством оплаты в торговых точках на сумму до 1 тыс. руб., когда не требуется подтверждение операции путем введения PIN-кода); хищения с использованием дубликата сим-карты мобильного телефона, которое осуществляются путем предварительного выяснения номера телефона, с которым синхронизированы карты; изготовление фальшивого аналога с последующим проведением платежей по банковской карте.

---

[1] В контексте современного понимания информационной безопасности и настоящего исследования под социальной инженерией понимается психологическое манипулирование людьми с целью совершения определенных действий.

Не менее часто используемая схема связана с «попавшим в беду близким родственником», когда преступники, информируя потенциального потерпевшего о какой-либо сложной, внезапно возникшей ситуации (ДТП с участием близкого родственника, задержание сотрудниками правоохранительных органов и пр.), требуют незамедлительно перевести крупную сумму денежных средств для якобы неофициального разрешения возникшей ситуации.

К примеру, в производстве СЧ СУ УМВД России по Брянской области находилось уголовное дело по обвинению Х. в совершении 29 преступлений, предусмотренных ч. 2 ст. 159 УК РФ. Расследованием уголовного дела установлено, что в период с февраля по июнь 2018 г. житель г. Самары Х. путем случайного набора абонентских номеров посредством мобильного телефона звонил гражданам и, представляясь сотрудником полиции, сообщал о том, что якобы их родственник совершил дорожно-транспортное происшествие, при котором пострадал человек. За решение проблемы «родственника» он требовал деньги. Таким образом фигурант похитил у 29 жителей Брянской области денежные средства в сумме 1126 тыс. рублей. По результатам расследования 9 января 2019 г. уголовное дело направлено в Новозыбковский городской суд Брянской области, приговором которого Х. назначено наказание в виде 4 лет 6 месяцев лишения свободы с отбыванием наказания в исправительной колонии общего режима. Приговор вступил в законную силу.

С учетом развития за последние годы электронных площадок купли-продажи новых и поддержанных вещей достаточно часто выявляются хищения в виде заведомо ложных предложений об услугах и продаже услуг и товаров или перевода денежных средств в качестве взноса при приобретении автомобиля на сайтах (Avito.ru, Youla.ru, Avto.ru, Drom.ru). Данный способ хищения денежных средств заключается в создании злоумышленниками интернет-магазинов, не продающих ничего в действительности, но привлекающих потенциальных покупателей ценами на товары, значительно отличающимися от рыночных, заманчивыми акциями и скидками. При общении с «сотрудниками» интернет-магазинов покупателю сообщается об оформлении заказа, о необходимости внесения предоплаты, о соответствующих банковских реквизитах. После проведения оплаты заказанный товар покупателю не поставляется, номера телефонов, указанные в качестве контактных, оказываются заблокированными.

Сюда же относятся факты обмана людей, продающих что-либо на популярных интернет-площадках объявлений. В таких случаях злоумышленники в ходе телефонного разговора предлагают внести предоплату на счет банковской карты и просят в связи с этим сообщить номер соответствующей карты, срок ее действия, комбинацию цифр, расположенную на оборотной стороне банковской карты, а также коды доступа, содержащиеся в смс-сообщениях, присылаемых сервисными службами банка. Получив указанную информацию, преступник

получает возможность получить доступ к онлайн-программам, позволяющим дистанционно осуществлять операции по всем банковским счетам, зарегистрированным на пострадавшего.

Распространен также следующий вид телефонного мошенничества. В ходе телефонного разговора неустановленное лицо представляется сотрудником банка или иной кредитной организации, сообщает о якобы выявленных подозрительных транзакциях по банковским счетам потерпевшего и предлагает вывести все денежные средства на «безопасный» банковский счет для их сохранности. В дальнейшем, получив пароли и коды для доступа в «личный кабинет» пострадавшего, злоумышленник похищает денежные средства путем их перечисления на различные банковские счета.

Например, в ходе изучения Тихвинской городской прокуратурой решения об отказе в возбуждении уголовного дела, принятого 5 сентября 2019 г. по заявлению Б. о мошеннических действиях при оформлении кредита, установлено, что злоумышленник, представившись сотрудником службы безопасности ПАО «Сбербанк», введя в заблуждение заявителя относительно своей принадлежности к службе безопасности данного учреждения, получил от нее сведения о ее банковских картах и доступ к мобильному приложению «Сбербанк Онлайн», через которое оформил кредит на сумму 300 тыс. руб. со страховкой на сумму 28 тыс. руб., однако преступление не довел до конца в связи с блокировкой банковских карт. По результатам дополнительной проверки 23 сентября 2019 г. СО ОМВД района возбуждено уголовное дело по признакам преступления, предусмотренного ч. 3 ст. 30 ч. 3 ст. 159 УК РФ[1].

К примеру, в ОП № 2 УМВД России по г. Брянску 26 апреля 2019 г. поступило заявление И. о том, что ему на мобильный телефон позвонила неизвестная женщина, которая представилась сотрудником службы безопасности ПАО «Сбербанк России» и сообщила, что по банковской карте И. происходят несанкционированные списания денежных средств. Неустановленное лицо попросило потерпевшего произвести ряд действий, в результате которых произошло списание денежных средств с банковских карт ПАО «Сбербанк России» и АО «Банк Русский стандарт», принадлежащих И., на общую сумму 26 428 руб.

По данному факту ОП № 2 УМВД России по г. Брянску проведена проверка в порядке ст. 144, 145 УПК РФ, по результатам которой 20 мая 2019 г. в возбуждении уголовного дела отказано. Решение об отказе в возбуждении уголовного дела 20 мая 2019 г. отменено прокурором Володарского района г. Брянска, материал направлен в следственный орган для решения вопроса о возбуждении уголовного дела. По результатам дополнительной проверки 6 июня 2019 г. возбуждено уголовное дело по п. «г» ч. 3 ст. 158 УК РФ.

Преступники изучают странички потерпевших в социальных сетях, после чего создают «фейковые» аккаунты, имитирующие аккаунты их друзей, от имени которых начинают общение с потерпевшими, которые, не замечая подмены, сообщают необходимую злоумышленникам

[1] По материалам деятельности прокуратуры Ленинградской области.

информацию. После они рассылают в личных сообщениях информацию их друзьям с просьбами одолжить деньги, как правило, в силу внезапно возникшей проблемной ситуации (авария, смерть близкого, тяжелая болезнь и пр.). Нередко такие действия не требуют специальных познаний и специального программного обеспечения, поскольку пароли доступа продаются на специализированных сайтах, впрочем, как и программы для взлома.

В случае похищения мобильного телефона с установленными на нем программами оперирования денежными средствами на банковских картах (например, «Сбербанк Онлайн»), если потерпевший не осуществит вовремя блокировку операций по ним, происходит списание или перечисление на другие счета или цепочку счетов.

Методом социальной инженерии совершается также так называемое двойное списание, при котором потерпевшему при покупке с помощью безналичного расчета сообщается о невозможности проведения операции и предлагается снова оплатить товар или услугу. Преступник дублирует уже совершенную операцию, тем самым списывая денежные средства дважды без ведома потерпевшего.

С помощью так называемого фишинга преступник посылает потерпевшему форму, внешне крайне схожую с официальными формами банков, в полях которой необходимо внести номер карты, CCV-код и код подтверждения по СМС-сообщению, после чего получает доступ к банковскому счету или запрашиваемой сумме.

Посредством распространения троянских коней под видом технической информации, как правило поддержки, например обновления программ и приложений, объявления о распродаже с максимально высокими скидками, сообщения о выигрыше, преступники закачивают на компьютер потерпевшего вредоносную программу, после чего злоумышленник получает возможность удаленно управлять банковским счетом, который привязан к номеру сотового телефона или аккаунту.

Прокурорами отмечается еще один способ совершения данных преступлений. На мобильный телефон или иное устройство потерпевшего различными путями устанавливается «вирусная» программа, в том числе позволяющая отслеживать и перехватывать СМС-сообщения, предназначенные для потерпевшего, а также отправлять таковые якобы от его имени. В подобных случаях преступник обладает возможностью осуществлять удаленные банковские операции по переводу денежных средств даже в отсутствие идентификационных данных банковской карты и паролей доступа к системам онлайн-банкинга.

Хищения также совершаются под предлогом компенсации за ранее приобретенные лекарственные препараты или биологически активные добавки, когда преступник, представляющийся сотрудником правоохранительных органов, предлагает потерпевшему получить некое возмещение от государства в связи с задержанием группы преступ-

ников или поставки товара при условии оплаты фискального сбора (государственная пошлина, налоговый сбор).

К «нестандартным» (в плане повсеместности распространения) способам совершения преступлений относятся следующие:

- злоумышленники по телефону представляются сотрудниками служб безопасности различных банков и сообщают потерпевшим о необходимости установления на смартфон, компьютер или планшет различных программ («Anydesk», «Quicksupport», «Teamviever» и др.), выдавая их в том числе за антивирусные, позволяющие мошенникам дистанционно управлять смартфоном, ноутбуком или планшетом, при этом осуществлять онлайн переводы от имени потерпевших через их личный кабинет;
- хищение с банковских карт граждан, когда преступники, используя возможности IP-телефонии, осуществляют подмену реальных номеров, с которых происходят звонки потерпевшим на абонентские номера, схожие или идентичные официальным номерам банков, указанным на оборотной стороне карт, а также с номера «102», принадлежащего дежурной части полиции, и подтверждают, что с ними разговаривали представители данных организаций, что оказывает психологическое давление на потерпевших, и они совершают действия по указанию мошенников;
- мошенничество, совершенное с использованием вредоносных программ на ОС «Android», при котором потерпевшему на сотовый телефон с операционной системой «Android» с неизвестного номера приходят СМС-сообщения с ссылкой, проходя по которой потерпевший загружает на свой телефон вирус (чаще всего «Triada» и «Marcher»), предоставляющий злоумышленнику доступ к СМС-командам. В дальнейшем мошенник похищает деньги, путем направления сообщений на номер «900».

Так, в производстве СЧ ГСУ ГУ МВД России по Ростовской области по находится уголовное дело, выделенное в отдельное производство из уголовного дела по обвинению М. в совершении преступлений, предусмотренных ч. 3 ст. 159.6, ч. 3 ст. 272, ч. 2 ст. 273 УК РФ.

В ходе производства предварительного следствия установлено, что М., З., Ю., Ш., П. М.П., П.И.А. и неустановленные лица, уголовное дело в отношении которых выделено в отдельное производство, действуя в составе организованной преступной группы, в период с 15 июля 2017 г. по 20 марта 2018 г., подыскав вредоносные компьютерные программы, которые позволяли им без ведома и согласия владельцев мобильных телефонов, являющихся держателями банковских карт ПАО «Сбербанк» с подключенной услугой «Мобильный банк», удаленно принимать, просматривать и отправлять от их (владельцев) имени СМС-сообщения на номер «900» с командами о переводе денежных средств посредствам услуги «Мобильный Банк», преследуя единый преступный умысел, совершили хищение

денежных средств в крупном размере у 97 потерпевших, проживающих по всей территории России, на общую сумму 602 935 руб.

К иным преступлениям, не связанным с хищением денежных средств с банковских счетов, относятся использование сети Интернет путем пересылки запретных фото- и видеоматериалов (порнография и т.д.), заказ на интернет-сайтах веществ, запрещенных в свободном гражданском обороте, распространение заведомо ложной информации, порочащей честь и достоинство потерпевших, обман при поиске работы, возврате утраченных вещей; совершение звонков в службы доставки с последующей просьбой пополнить баланс счета сотового телефона, фальсификация платежных документов и др.

Необходимо отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно применяют современные IT-технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей глобальной сети. Очень часто потерпевшие в силу незначительности причиненного вреда не заявляют о правонарушении в правоохранительные органы. Преступники отлично осведомлены об этом и успешно пользуются, вместе с тем посредством незначительного хищения у десятков и сотен потерпевших причиняется в сумме значительный ущерб.

Положительная динамика рассматриваемых преступлений отмечалась во время применения карантинных мер, вызванных глобальным распространением пандемии COVID-19[3]. Ограничения перемещений, изоляция отразились на психологическом состоянии граждан, увеличении спроса на определенные товары, расширении использования онлайн-сервисов для решения повседневных вопросов, а также значительных объемах электронной торговли (преимущественно интернет-магазины). В последнее время в Интернете появилось много фейковых страниц, предлагающих работающую проверенную вакцину от COVID-19.

При совершении вышеуказанных видов преступлений неустановленные лица, как правило, контактируют с потерпевшими с помощью сети Интернет, а также используют множество абонентских номеров, зарегистрированных на несуществующих или подставных лиц, которые не причастны к совершенным правонарушениям. Имеющаяся практика свидетельствует, что аппараты сотовой связи активируются мошенниками для совершения нескольких преступлений, после чего уничтожаются. Ими используется множество счетов платежных карт и различные схемы вывода похищенных денежных средств, что приводит к тому, что ко времени получения информации о конечном выводе денежных средств, если вывод денег происходит через банкоматы или терминалы обслуживания, истекает срок хранения видеозаписей

и дальнейшее установление преступника становится практически невозможным.

В последнее время преобладают различные сайты-однодневки, появление которых и исчезновение достаточно сложно проследить, необходимы технические системы по определению владельцев данных сайтов.

Нередко телефонные мошенники используют съемные квартиры, в которых проживает от 2 до 7 человек, срок аренды квартиры не превышает 3 месяцев. Такие квартиры используются как для совершения мошеннических действий, так и для проживания мошенников, их связей, хранения денежных средств и используемой техники. В качестве последней используются персональные компьютеры с установленным программным обеспечением, позволяющим осуществлять выборку лиц, представляющих криминальный интерес, в том числе предполагаемых жертв из адресной и телефонной базы, где указываются номера телефонов, их местоположение и данные пользователя, что позволяет в процессе разговора с жертвой использовать полученные сведения в преступных целях (установление психологического контакта).

За последние годы характерными **организационными сложностями**, возникающими у органов предварительного расследования при проверках сообщений о компьютерных преступлениях, являются[1]: межрегиональный характер совершения таких преступлений; длительность исполнения запросов интернет-провайдером, кредитными учреждениями и администрациями электронных платежных систем; отсутствие в ряде субъектов Российской Федерации экспертных учреждений, которым может быть поручено производство наиболее востребованных компьютерных экспертиз либо недостаточная их оснащенность и др.

Например, по сведениям из прокуратуры Ненецкого автономного округа, сроки исполнения запросов следователей, направленных в компании операторов сотовой связи, составляют минимум 2–3 месяца, банки — 3–4 недели, владельцам платежных систем (ООО ПС «Яндекс Деньги», ЗАО «QIWI-банк», ООО «Одноклассники», АО «Мобиденьги») — 3–4 недели.

По данным из прокуратуры Краснодарского края, сроки получения информации о владельце абонентского номера, принадлежности IP-адресов, интернет-провайдеров, электронной почты, сайтов составляют от 18 до 90 дней.

По информации из прокуратуры Москвы, направляемые в адреса организаций, предоставляющих финансовые услуги, социальных сетей и мессенджеров, а также операторов сотовой связи и интернет-провайдеров запросы исполняются спустя значительный период времени (от 2 недель до 4 месяцев), запросы нередко приходиться дублировать. Кроме того, ответы на запросы, в некоторых случаях,

[1] Информационно-аналитический обзор «Прокурорский надзор за процессуальной деятельностью органов предварительного следствия при расследовании преступлений в сфере компьютерной информации». Научно-исследовательский институт Университета прокуратуры Российской Федерации, 2018 год.

носят малоинформативный, формальный характер. К примеру, значительная доля мошенничеств совершается с использованием услуги Интернет, предоставляемой ПАО «Мегафон», однако на неоднократные запросы о предоставлении IP-адресов или установочных данных по известному IP-адресу поступает ответ, что требуемая информация не сохранилась или не фиксируется. Информация по запросам от интернет-площадок открытой розничной торговли («Авито», «Юла» и др.) предоставляется по истечении нескольких месяцев и не является уже актуальной.

В ряде регионов России (Республика Саха (Якутия), Калужская и Тюменская области) возможность проведения судебных экспертиз в ходе проверки сообщения о преступлении, в том числе и при проверке сообщений о компьютерных преступлениях, носит ограниченный характер по объективным причинам: высокая загруженность экспертных учреждений, недостаточное количество экспертов и отсутствие необходимых технических средств для производства экспертиз отдельных видов технических устройств.

Кроме того, в связи с оптимизацией расходов банки устанавливают новое оборудование, видеозапись на котором хранится от 3 до 10 дней, вследствие чего информация, необходимая для отождествления лица, совершившего обналичивание денежных средств, утрачивается в короткое время.

Среди **правообеспечительных сложностей** можно выделить следующие.

Невозможность судебного санкционирования получения информации о соединениях между абонентами и абонентскими устройствами в рамках проведения проверки сообщений о преступлениях в сфере ИКТ не позволяет своевременно установить место выхода в эфир лица, подозреваемого в совершении преступления. Руководители филиалов вышеуказанных организаций на территории субъекта Российской Федерации не наделены полномочиями на заключение соглашений об электронном документообороте (банки «Тинькофф», «КивиБанк», социальная сеть «Вконтакте», интернет-холдинг «Яндекс»).

Запросы в финансовые и кредитные учреждения могут направляться только после возбуждения уголовного дела, поскольку в рамках проведения доследственной процессуальной проверки это невозможно ввиду положений Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности».

Правоприменительные сложности. Как и по преступлениям иных категорий, качество проводимых проверок сообщений о преступлениях в сфере ИКТ находится на недостаточном с учетом общественной опасности и распространенности уровне. Прокурорами отмечается, что в целом результаты проверок материалов об отказе в возбуждении уголовного дела свидетельствуют о низком качестве их проведения.

Значительное количество выявленных прокурорами нарушений обусловлены ненадлежащим ведомственным контролем за их проведением

со стороны руководителей. Материалы, находящиеся в производстве следователей, до принятия по ним процессуального решения практически не изучаются. Указания в ходе проверок сообщений о преступлениях, о выполнении конкретных мероприятий с целью предупреждения нарушений и исключения фактов вынесения незаконных решений не даются. Отмечается отсутствие должной последовательной и системной организации работы, низкая эффективность тактики и выработанной методики производства проверочных мероприятий, определение ошибочных и не вытекающих из фактических исследуемых обстоятельств направлений проверки, неправильное применение норм уголовного и уголовно-процессуального законодательства.

Отмечены неединичные факты рассмотрения сообщений о преступлениях не в соответствии с положениями УПК РФ, а по нормам Федерального закона от 2 мая 2016 г. № 59-ФЗ «О порядке рассмотрения обращения граждан Российской Федерации», списания сообщений в номенклатурное дело как не содержащих поводов для проведения процессуальной проверки, возвращения заявителю или перенаправление сообщений в другой орган без регистрации, необоснованного отказа в возбуждении уголовного дела, фальсификации материалов проверки по сообщению о преступлении. Не всегда регистрировались выявленные в ходе проверки новые преступления[1].

В ходе проверки сообщений о преступлении нередко также игнорировалась возможность получения информации из отчетов о результатах расследования компьютерных инцидентов, обязательность проведения которых установлена в отдельных сферах деятельности государственных органов и коммерческих организаций, не истребовались сведения из систем резервной фиксации следов компьютерных инцидентов[2].

Наиболее характерным нарушением законов при проведении процессуальных проверок о преступлениях анализируемого вида является нарушение ст. 6.1, ч. 2 ст. 21, ч. 4 ст. 41, ст. 144, ч. 6 ст. 148 УПК РФ, закрепляющих обязанность правоохранительных органов принимать

---

[1] Информационное письмо Генеральной прокуратуры Российской Федерации «О состоянии законности при принятии органами предварительного расследования решений об отказе в возбуждении уголовного дела, приостановлении предварительного следствия и прекращении производства по уголовным делам» от 10 февраля 2016 г. № 36-11-2016.

[2] См. подробнее: Методические рекомендации о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента (утв. АРБ) // СПС «КонсультантПлюс»; Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств» СТО БР ИББС-1.3-2016 (утв. Приказом Банка России от 30 ноября 2016 г. № ОД-4234) // Вестник Банка России. 2016. № 107 и др.

достаточные и эффективные меры, направленные на своевременное осуществление уголовного преследования и соблюдение разумных сроков уголовного судопроизводства, что влечет за собой нарушение конституционных прав заявителей на защиту и доступ к правосудию в разумные сроки.

Так, в КУСП ОМВД России по Нахимовскому району города Севастополя зарегистрировано заявление А. о хищении ее денег в сумме 6700 руб. под предлогом продажи мобильного телефона через интернет-сайт «Altdel.ru».

По результатам проверки неоднократно принимались решения об отказе в возбуждении уголовного дела по основанию, установленному п. 2 ч. 1 ст. 24 УПК РФ, которые отменялись прокуратурой района в порядке надзора, с указанием на проведение конкретных проверочных мероприятий для принятия законного решения. По результатам дополнительной проверки 17 октября 2019 г. дознавателем возбуждено уголовное дело по признакам преступления, предусмотренного ч. 1 ст. 159 УК РФ.

Нередко основаниями для признания указанных процессуальных решений необоснованными является неполнота проверок, например не устанавливаются все факты по изобличению лиц, виновных в совершении преступления; не опрашиваются все свидетели и очевидцы преступления, отсутствуют сведения о списании денежных средств со счета потерпевшего, о наличии умысла на хищение имущества потерпевшего при покупке товаров дистанционным способом; не выясняются обстоятельства взлома аккаунтов в социальных сетях, возможности использования вредоносной программы и т.д.

Так, в ОМВД России по Ямальскому району 31 октября 2018 г. обратился Т., который сообщил, что у него с банковской карты неизвестные лица списали денежные средства в сумме 1100 руб. По данному сообщению проведена проверка, по результатам которой 9 ноября 2018 г. возбуждено уголовное дело по п. «в» ч. 3 ст. 159.6 УК РФ. Решение о возбуждении уголовного дела 15 ноября 2018 г. отменено руководителем СУ УМВД России по ЯНАО, который посчитал, что действия неустановленного лица в силу ч. 2 ст. 14 УК РФ являются малозначительными и не представляют общественной опасности. Органом дознания ОМВД России по Ямальскому району 23 ноября 2018 г. по тем же основаниям принято решение об отказе в возбуждении уголовного дела.

Вместе с тем на банковской карте Т. находились денежные средства в сумме 2519 руб. Перейдя по ссылке на интернет-ресурс, полученной с неизвестного номера в СМС-сообщении, на мобильный телефон потерпевшего было установлено стороннее приложение (вредоносное программное обеспечение), после чего пришло 2 СМС-сообщения о списании денежных средств в сумме 500 и 600 руб. со счета банковской карты, привязанной к его телефону. Далее услуга «Мобильный банк» была заблокирована службой безопасности банка, а на счете осталось 1419 руб. В этой связи постановление органа дознания об отказе в возбуждении уголовного дела 28 ноября 2018 г. отменено надзирающим прокурором, а 3 декабря 2018 г. возбуждено уголовное дело, производство по которому приостановлено 3 марта 2019 г. на основании, установленном п. 1 ч. 1 ст. 208 УПК РФ.

Органами предварительного расследования при рассмотрении сообщений о рассматриваемых преступлениях также допускаются нарушение правил подследственности, необоснованное направление материалов проверок по территориальности, несвоевременное принятие материалов к производству после отмены прокурорами и руководителями следственных подразделений незаконных решений об отказе в возбуждении уголовных дел[1].

Характерным нарушением законов при проведении процессуальных проверок является их неполнота, приводящая к вынесению необоснованных решений, не соответствующих требованиям ч. 4 ст. 7 УПК РФ, а также неверная оценка органами дознания фактических обстоятельств происшествия.

К примеру, по заявлению Ш. о распространении в социальной сети «Вконтакте» заведомо ложных сведений, порочащих ее честь и достоинство, УУП УМВД России по г. Старому Осколу 15 декабря 2018 г. отказано в возбуждении уголовного дела в связи с отсутствием в действиях М. состава преступления, предусмотренного ст. 128.1 УК РФ. Указанное процессуальное решение отменено 24 января 2019 г. заместителем Старооскольского городского прокурора как незаконное ввиду неполноты проведенной проверки.

По результатам дополнительной проверки 8 февраля 2019 г. ОД УМВД России по г. Старому Осколу с согласия заместителя Старооскольского городского прокурора возбуждено уголовное дело по ч. 1 ст. 128.1 УК РФ, которое в дальнейшем направлено в суд для рассмотрения по существу. Постановлением мирового судьи от 17 июня 2019 г. уголовное дело по обвинению М. в совершении преступлений, предусмотренных ч. 1 ст. 128.1, ч. 4 ст. 128.1 УК РФ, прекращено в связи с примирением сторон[2].

Так, 5 апреля 2019 г. в МО МВД РФ «Ртищевский» поступило заявление В. по факту хищения с ее счета денежных средств в сумме 90 тыс. руб. По данному факту ОУР МО МВД РФ «Ртищевский» проводилась процессуальная проверка, по результатам которой при наличии очевидных признаков преступления, в частности, был установлен способ хищения денежных средств, сотрудниками полиции принято решение об отказе в возбуждении уголовного дела по основанию, установленному п. 1 ч. 1 ст. 24 УПК РФ.

Изучением материалов проверки Ртищевской межрайонной прокуратурой в порядке надзора установлено, что данное решение принято необоснованно, в действиях неустановленного лица имеются признаки преступления, предусмотренного ст. 158 УК РФ. В связи с этим решение об отказе в возбуждении уголовного дела отменено надзирающим прокурором, материал направлен на дополнительную проверку. По результатам дополнительной проверки следователем возбуждено уголовное дело по п. «г» ч. 3 ст. 158 УК РФ[3].

---

[1] Более подробно данный вопрос рассмотрен в разделе 7.

[2] По материалам деятельности прокуратуры Белгородской области.

[3] По материалам деятельности прокуратуры Саратовской области.

Нередки случаи вынесения незаконных процессуальных решений при явных формальных признаках совершенного преступления.

К примеру, 18 декабря 2018 г. в ОМВД поступило заявление В. о том, что неустановленное лицо выложило ее фотографию на сайте «Одноклассники» с надписью оскорбительного характера. Проверкой установлено, что 15 октября 2018 г. В. на сотовый телефон позвонила ее знакомая и сообщила, что на сайте «Одноклассники» на странице, принадлежащей В., в комментариях под ее фотографией размещена информация оскорбительного характера о предложении интимных услуг за долги ее мужа. По результатам проверки 21 декабря 2018 г. УУП и ПДН вынесено постановление об отказе в возбуждении уголовного дела по п. 1 ч. 1 ст. 24 УПК РФ.

Изучением материалов проверки в прокуратуре установлено, что органом дознания нарушены права потерпевших на доступ к правосудию. В действиях неустановленного лица усматривались признаки преступления, предусмотренного ч. 1 ст. 128.1 УК РФ, что подтверждалось объяснениями заявителя и иными материалами проверки. 17 января 2019 г. прокурором района незаконное решение отменено с требованием о возбуждении уголовного дела, 23 января 2019 г. возбуждено уголовное дело по ч. 1 ст. 128.1 УК РФ[1].

Имели место случаи, когда по сообщениям о преступлениях следователями принимались решения об отказе в возбуждении уголовных дел на том основании, что в срок доследственной проверки не получены сведения о движении похищенных денежных средств, собственниках банковских счетов, телефонных номерах, посредством которых осуществлялись мошеннические действия. Указанные решения ввиду очевидной их незаконности в этот же день отменяются руководителем следственного органа; материал возвращается следователю для проведения дополнительной проверки, которая фактически не влияет на установление наличия признаков преступления.

К примеру, 14 октября 2019 г. в ОП № 1 УМВД России по г. Брянску поступило заявление К. о краже 2618 руб. с ее банковской карты, совершенной неизвестным лицом.

По результатам проведенной процессуальной проверки 12 ноября 2019 г. СО СУ УМВД России по г. Брянску вынесено постановление об отказе в возбуждении уголовного дела, которое в этот же день отменено руководителем следственного органа в связи с необходимостью проведения дополнительных проверочных мероприятий.

Вместе с тем в материале проверки на 12 ноября 2019 г. уже имелись достаточные основания для возбуждения уголовного дела, в связи с чем прокуратурой Бежицкого района г. Брянска руководителю следственного органа направлено требование об устранении нарушений федерального законодательства. Данное требование рассмотрено и удовлетворено, по сообщению К. возбуждено уголовное дело по признакам преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ[2].

---

[1] По материалам деятельности прокуратуры Забайкальского края.

[2] По материалам деятельности прокуратуры Брянской области.

Нередко за установленный УПК РФ срок не опрашиваются все участники событий происшествия; не приобщается необходимая документация, подтверждающая размер причиненного ущерба; в большинстве случаев до возбуждения уголовного дела какие-либо мероприятия технического характера не осуществляются.

Прокурорами отмечается несвоевременность проведения первоначальных мероприятий (осмотра места происшествия, установления и опроса лиц), а также неполнота, выраженная в непроведении осмотра компьютерной техники на предмет установления истории соединений интернет-браузера.

Также имеют место факты укрытия сообщений от учета и регистрации путем списания в специальное номенклатурное дело.

Так, 23 декабря 2018 г. в ОП № 4 УМВД России по г. Волгограду обратился П. в связи с хищением у него денежных средств в размере 55 тыс. руб. путем снятия с кредитной карты ПАО «Сбербанк России». В тот же день в отдел полиции поступило заявление инициатора о том, что необходимости в проведении процессуальной проверки не имеется, поскольку он обратился с целью консультации по личным обстоятельствам, которым публичную огласку давать не желает. 23 декабря 2018 г. по рапорту сотрудника полиции материал по заявлению П. списан в специальное номенклатурное дело.

Вместе с тем опрошенный 28 января 2019 г. в прокуратуре Центрального района г. Волгограда П. пояснил, что 22 декабря 2018 г. в вечернее время ранее знакомая ему Ш. тайно похитила у него денежные средства в размере 55 тыс. руб. путем снятия с банковской карты. В подтверждение П. приобщена выписка о движении денежных средств по расчетному счету, открытому на его имя в ПАО «Сбербанк России».

По инициативе прокуратуры района обеспечено проведение процессуальной проверки, по результатам которой 21 марта 2019 г. возбуждено уголовное дело по признакам преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ (направлено в суд, вынесен обвинительный приговор).

Не всегда полно и своевременно выполняются указания прокуроров, данных ими при реализации мер реагирования.

Например, по сообщению о мошеннических действиях Х. в сфере кредитования при оформлении кредита посредством сети Интернет, на протяжении длительного периода времени УУП ОП № 5 МУ МВД РФ «Братское» не выполнялись указания прокурора Братского района, незаконные решения об отказе в возбуждении уголовного дела по материалу отменялись 5 раз, лишь 29 октября 2019 г. возбуждено уголовное дело по признакам преступления, предусмотренного ст. 159.1 ч. 1 УК РФ. Данные нарушения нашли отражение в представлении прокуратуры района, внесенном в адрес начальника МУ МВД РФ «Братское», по результатам рассмотрения которого к дисциплинарной ответственности привлечены два должностных лица[1].

[1] По материалам деятельности прокуратуры Иркутской области.

Также имеют место факты принятия по результатам проведения проверки сообщений о преступлении процессуального решения, не основанного на имеющихся в распоряжении должностного лица материалах.

Так, 7 августа 2019 г. по результатам проведения процессуальной проверки ОУР ОМВД России по г. Горно-Алтайску на основании п. 1 ч. 1 ст. 24 УПК РФ принято решение об отказе в возбуждении уголовного дела по факту блокировки работы сервера МБУ «Централизованная бухгалтерия управления культуры, спорта и молодежной политики». В связи с тем, что данное процессуальное решение было принято без получения результатов компьютерно-технической судебной экспертизы, факта наличия вредоносных программ, а также лица, совершившего блокировку сервера указанного учреждения, решение об отказе в возбуждении уголовного дела отменено прокуратурой г. Горно-Алтайска. По результатам дополнительной проверки 18 сентября 2019 г. СО ОМВД России по г. Горно-Алтайску возбуждено уголовное дело по ч. 2 ст. 272 УК РФ[1].

В некоторых случаях прокурорами при проверке законности принятых процессуальных решений отмечаются многочисленные нарушения требований закона, прежде всего при установлении и проверке обстоятельств проверяемого факта, установление которых не составляет особого труда и временных затрат.

Так, 21 мая 2019 г. в прокуратуру г. Белово поступило постановление следователя от 20 мая 2019 г. о возбуждении уголовного дела по признакам преступления, предусмотренного ч. 3 ст. 159 УК РФ, по факту хищения путем обмана денежных средств в сумме 670 тыс. руб. при заключении договора кредитования от имени Л.

Вместе с постановлением поступили материалы процессуальной проверки, при изучении которых установлено, что постановление следователя является незаконным, подлежит отмене, поскольку в нарушение требований ст. 73, 144 УПК РФ в ходе процессуальной проверки исследованы не все имеющие значение для принятия законного решения обстоятельства.

Не установлено лицо, которому принадлежат деньги в сумме 670 тыс. руб. и которому причинен ущерб. Выводы следователя о том, что пострадавшей является Л., не соответствовали действительности, поскольку денежные средства на ее банковский счет не поступали, с него не списывались. В рамках процессуальной проверки не приняты меры по установлению лица, которому причинен ущерб. Не проверена информация Л. о поступлении в ее адрес сообщения о наличии задолженности по кредиту. С учетом выявленных нарушений 22 мая 2019 г. постановление о возбуждении уголовного дела отменено прокурором[2].

Выявляются нарушения требований УПК РФ об информационном обеспечении заявителя о преступлении, когда ему не направляются уведомление о принятом по результатам проведенной проверки процессуальном решении и сама копия процессуального решения.

---

[1] По материалам деятельности прокуратуры Республики Алтай.

[2] По материалам деятельности прокуратуры Кемеровской области.

Так, 26 января 2016 г. в УМВД России по г. Сыктывкару поступил материал проверки по обращению В. по факту размещения на сайте «darkmoney.cc» сведений об учетных записях в системе «РЖД-Бонус» и неправомерного доступа в указанную систему.

В ходе проведения процессуальной проверки по данному заявлению следователями неоднократно принимались решения об отказе в возбуждении уголовного дела по основанию, установленному п. 2 ч. 1 ст. 24 УПК РФ. Однако в нарушение требований ч. 2 ст. 145, ч. 4 ст. 148 УПК РФ следователями в адрес заявителя не направлялись копии процессуальных решений об отказе в возбуждении уголовного дела от 5 августа 2019 г. и 5 сентября 2019 г. Для устранения указанных нарушений 30 октября 2019 г. в адрес руководителя СУ УМВД России по г. Сыктывкару прокуратурой внесено требование об устранении нарушений федерального законодательства, которое удовлетворено.

Необходимо отметить и то, что должностные лица органов дознания и предварительного следствия не всегда обладают необходимыми познаниями в сфере ИКТ, что влечет недостаточное понимание предмета проверки и, как следствие, не позволяет эффективно производить необходимые процессуальные действия, своевременно направлять мотивированные запросы в адрес организаций, которые располагают значимыми сведениями об обстоятельствах совершенных преступлений, ставить необходимые вопросы перед судебными экспертами.

Например, прокуратурой Красноярского края выявленные на практике факты о том, что следователями не всегда используется возможность получения сведений о телефонных соединениях и их анализ обоснованно расценивались как неполнота проведенных проверочных мероприятий, поскольку раскрытие преступлений, связанных со сбытом наркотиков, совершенных в условиях неочевидности, практически во всех случаях невозможно без анализа соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), установления номеров абонентов, а также других данных, позволяющих идентифицировать абонентов.

Следователями не направляются запросы владельцам социальных сетей с целью установления источника создания и администрирования учетной записи (аккаунта в социальных сетях, запросы на сайты (электронные торговые площадки) по оказанию услуг или продаже товаров о предоставлении информации об объявлениях, где был указан интересующий следствие абонентский номер в качестве контактного.

Еще одной распространенной причиной отмены незаконно вынесенных постановлений об отказе в возбуждении уголовного дела о преступлениях в сфере ИКТ, в том числе совершенных с использованием вредоносных компьютерных программ, является (об этом сообщалось в информационных записках прокуратур Удмуртской Ре-

спублики и Самарской области) непроведение следователем в рамках процессуальной проверки компьютерно-технической экспертизы.

Например, по результатам проверки следователем следственного отдела МВД России по Урицкому району Орловской области сообщения о возможной преступной деятельности, связанной с работой модифицированного программного обеспечения, на автозаправочном комплексе вынесено постановление об отказе в возбуждении уголовного дела по основанию, предусмотренному п. 1 ч. 1 ст. 24 УПК РФ (в связи с отсутствием события преступления, предусмотренного статьей 273 УК РФ). Прокуратурой Урицкого района Орловской области 30 мая 2016 г. постановление следователя было обоснованно отменено в связи с необходимостью проведения исследования изъятых с автозаправочного комплекса программно-запоминающих устройств, сравнения их с официальной версией программного обеспечения. Материал был направлен для проведения дополнительной проверки.

Как показывает практика прокурорского надзора, каких-либо существенных сложностей правообеспечительного характера при проведении органами предварительного расследования проверок сообщений о преступлении в сфере ИКТ не выявлено. Основной причиной низкого качества процессуальной деятельности и процессуальных решений на рассматриваемой стадии уголовного судопроизводства является нарушение требований уголовно-процессуального законодательства в силу не только недостаточной квалификации, но и искусственного регулирования следственной нагрузки. Полагаем, что прокурорам следует более точечно применять предусмотренные законом меры реагирования в комплексе с внешне- и внутрисистемными механизмами взаимодействия и координации борьбы с преступностью.

3.4. Прокурорский надзор за исполнением органами дознания и органами предварительного следствия требований федерального закона при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации

В условиях увеличения количества преступлений в сфере компьютерной информации и преступлений, совершаемых с использованием современных ИКТ, возрастает и роль прокурорского надзора за исполнением законов при расследовании преступлений указанной категории.

Практическими работниками органов прокуратуры и предварительного расследования отмечаются **объективные** проблемы и трудности при расследовании уголовных дел данной категории:

— требует значительных временных затрат процесс установления маршрута движения похищенных денежных средств между электронными платежными системами и учреждениями кредитно-финансовой сферы;
— в связи с непродолжительным сроком хранения утрачиваются видеоматериалы с изображением лиц, осуществляющих обналичивание денежных средств в банкоматах;
— злоумышленники осуществляют частую смену СИМ-карт и сотовых телефонов, используемых при совершении преступлений, что не позволяет провести оперативно-технические мероприятия, направленные на установление их местонахождения;
— необходимость командировок в другие регионы РФ;
— длительное время поступления выписок по движению денежных средств по банковским картам, зачастую неисполнительность запросов банками и организациями;
— длительное исполнение, а также неисполнение мобильными операторами детализаций телефонных переговоров;
— открытие виртуальных банковских счетов, при этом лицо, которое их открывает, дистанционно предоставляет в банк сведения, которые не позволяют идентифицировать владельца;
— совершение мобильных мошенничеств посредством IP-телефонии, когда лицо дистанционно оформляет договор о предоставлении ему линии, при этом предоставляет личные данные, как правило, не свои или несуществующего лица, что затрудняет дальнейшую идентификацию преступника.

В качестве **организационных проблем** выделяются следующие.

Прежде всего, не всегда органами предварительного расследования проводятся необходимые для установления всех обстоятельств совершенного преступления следственные и иные процессуальные действия. В силу разных причин лицо, ведущее расследование, не проявляет необходимой наступательности и инициативности в раскрытии преступлении.

Например, по уголовным делам не допрашиваются сотрудники банков по обстоятельствам, имеющим значение для уголовного дела, наличии в подразделениях банков сведений о совершении конкретных банковских операций, а именно о способе списания денежных средств, заявке на списание, возможности идентификации лица, подавшего указанную заявку, и др.

Не всегда при наличии оснований осуществляются необходимые (исходя из материалов уголовного дела) контроль и запись телефонных переговоров. Следует отметить, что по преступлениям в сфере ИКТ данное следственное действие может выступать достаточно эффективным средством сбора доказательственной информации, когда преступники продолжают использовать одни и те же номера телефонов,

с которых осуществляются соединения. Его цель отличается от цели, которая преследуется при получении информации о соединениях между абонентами и (или) абонентскими устройствами. В результате контроля и записи телефонных переговоров возможно установление соучастников преступления, мест, где они скрываются, данных о механизме преступной деятельности и сведений о других обстоятельствах, подлежащих установлению и доказыванию. Результаты записи телефонных переговоров могут быть исследованы в рамках фоноскопической экспертизы.

Кроме того, не устанавливаются владельцы абонентских номеров, использовавшихся преступниками, IMEI мобильных телефонов, с которых совершаются звонки, номера СИМ-карт, которые помещались в телефоны с вышеуказанными IMEI, а также IMEI иных мобильных телефонов, в которые помещалась СИМ-карта с используемым преступником номером.

В ходе расследования допускаются следующие недостатки при направлении запросов и вынесении постановлений о возбуждении перед судами ходатайств о получении информации: не истребуется в полном объеме информация о соединениях по абонентским номерам СИМ-карты, которые используют лица, совершившие преступления, а также по иным абонентским номерам СИМ-карт, связь с которыми может быть установлена по IMEI мобильного телефона, использовавшегося для совершения преступления; в постановлениях о возбуждении перед судом ходатайств следователями не запрашивается информация об IMEI-номерах мобильных телефонов, в которых использовались СИМ-карты с установленными абонентскими номерами; в постановлениях не запрашивается информация о IMSI-номере СИМ-карты, используемой данным абонентским номером; не запрашивается информация о месторасположении офиса по обслуживанию и продаже СИМ-карты, с которой совершен звонок преступником (при установлении таких офисов необходимо запрашивать информацию о приобретателе карты, истребовать запись камер видеонаблюдения).

Информация о соединениях между абонентами и (или) абонентскими устройствами также является незаменимым доказательством и условием выбора верной тактики для успешного раскрытия и расследования преступления, способствует установлению обстоятельств совершения преступления, его времени, места, характера преступной группы. Сведения, полученные в ходе производства следственного действия, предусмотренного ст. 186.1 УПК, играют роль не только доказательственной, но и криминалистически значимой (ориентирующей) информации и выступают критерием для выдвижения и проверки версий.

По ряду уголовных дел при наличии решения суда о разрешении получения информации о соединениях между абонентами и абонентскими устройствами органами расследования не выполняются требования ст. 186.1 УПК РФ об истребовании у оператора сотовой связи вышеуказанной информации.

В соответствии с требованиями вышеуказанной статьи следователь, дознаватель осматривают представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, с участием специалиста (при необходимости), о чем составляют протокол, в котором должна быть указана та часть информации, которая, по мнению следователя, дознавателя имеет отношение к уголовному делу (дата, время, продолжительность соединений между абонентами и (или) абонентскими устройствами, номера абонентов и другие данные).

Представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, приобщаются к материалам уголовного дела в полном объеме на основании постановления как вещественное доказательство и хранятся в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность.

Вышеуказанные следственные и процессуальные действия органами расследования зачастую в полном объеме не проводятся.

В соответствии с решениями суда получение следователем информации о соединениях между абонентами и (или) абонентскими устройствами установлено, как правило, на срок до 180 суток.

Согласно ч. 4 ст. 186.1 УПК РФ, соответствующая осуществляющая услуги связи организация в течение всего срока производства данного следственного действия обязана предоставлять следователю или дознавателю указанную информацию по мере ее поступления, но не реже одного раза в неделю.

Указанные требования органами дознания и операторами сотовой связи зачастую в полном объеме не выполняются. Соответствующая информация в материалах уголовного дела отсутствует. Меры по привлечению к установленной законом ответственности операторов сотовой связи сотрудниками органа внутренних дел не принимаются.

Основными средствами получения ориентирующей и доказательственной информации о субъектах электронных платежей выступают следственные действия и связанные с ними оперативно-разыскные мероприятия по собиранию и исследованию следов в электронном виде.

Расследование уголовных дел рассматриваемой категории также сопровождается трудностями, связанными с изъятием, фиксацией и сохранностью информации, находящейся на электронных носителях (сотовых телефонах, компьютерах, портативных устройствах GPS и др.). На практике часто встречаются случаи, когда необходи-

мая информация не сохранилась из-за несвоевременных действий сотрудников правоохранительных органов по ее изъятию, была утеряна в результате ненадлежащей фиксации либо неквалифицированного извлечения и хранения.

Например, апелляционным определением Верховного суда Республики Крым отменен приговор в отношении К. по ч. 3 ст. 134, ч. 2 ст. 135 УК РФ, поскольку органом предварительного расследования не был указан способ совершения обвиняемым развратных действий, а именно не установлено, с какого IP-адреса и на какой велась переписка, какие «ники» использовали преступник и жертва.

Кроме того, обвинение по ч. 2 ст. 135 УК РФ относительно направленности умысла обвиняемого, его мотивов и целей при совершении преступления, а также характер этих действий не конкретизированы. По результатам дополнительного расследования уголовное дело вновь направлено в суд, которым в отношении К. постановлен обвинительный приговор[1].

Изучение уголовных дел данной категории в сфере незаконного оборота наркотических средств, показало, что криминалистически значимую информацию при их расследовании можно получить исключительно при осмотре информационной среды средств связи. Вместе с тем не всегда следователями принимаются своевременные меры к изъятию и осмотру различных электронных носителей информации, к которым относятся сотовые телефоны, ноутбуки, смартфоны, планшеты и т.д. В ряде случаев следственными и оперативными подразделениями не устанавливаются лица, на которых зарегистрированы электронные кошельки, на чьи счета зачисляются денежные средства за наркотик, электронные адреса страниц социальных сетей с информацией о сбыте наркотика, IP-адреса пользователей сайтов[2].

По уголовным делам следственные действия фактически ограничиваются получением разрешений судов на истребование сведений, составляющих банковскую тайну; при этом в ряде случаев самостоятельно органами расследования сведения из уполномоченных органов и учреждений не запрашиваются. Кроме того, исполнение данных запросов зачастую не контролируется, несмотря на ориентирование прокурорами начальников отделов дознания и органов следствия на принятие мер воздействия в отношения организаций в виде привлечения к административной ответственности по ст. 17.7 КоАП РФ. Полученная информация не анализируется, требования закона о разумном сроке уголовного судопроизводства не соблюдаются.

---

[1] Обзор Генеральной прокуратуры Российской Федерации состояния прокурорского надзора и практики расследования преступлений против несовершеннолетних, совершенных с использованием информационно-коммуникационной сети «Интернет» от 25 июня 2019 г. № 21/2-21-2019.

[2] По информации прокуратуры Челябинской области.

Прокурорами отмечаются проблемы **взаимодействия** государственных органов при расследовании преступлений в сфере ИКТ.

Прежде всего, это касается особенностей правового регулирования и технических возможностей при обмене информацией между правоохранительными органами и юридическими лицами, оказывающими услуги сотовой связи, банковские и интернет-услуги, администрациями социальных сетей и иных сервисов в сфере ИКТ.

К примеру, в соответствии с Законом о банках и банковской деятельности, дознаватель вправе получить сведения о движении денежных средств по счетам только на основании решения суда. Более того, в соответствии с п. 7 ч. 2 ст. 29 УПК РФ суд дает разрешение на получение такой информации только путем производства выемки, что с практической и технической точек зрения создает серьезные трудности. Следователь же подобные сведения может запросить с согласия руководителя следственного органа.

В настоящее время не со всеми банковскими учреждениями и операторами сотовой связи со стороны территориальных органов МВД России заключено соответствующее соглашение об электронном документообороте. В ряде случаев предложения МВД России о совершенствовании информационного обмена остаются без должного внимания. Вследствие этого необходимые запросы, в том числе в другие регионы, направляются почтовой связью, что наряду с необходимостью получения судебных решений, а также значительным объемом запрашиваемой информации обуславливает их длительное исполнение. Администрациями социальных сетей, особенно ООО «ВКонтакте», запрашиваемая информация фактически не предоставляется либо предоставляется спустя длительное время. В то же время одним из ключевых элементов, существенно повышающим шансы на раскрытие указанного вида преступлений, является оперативное получение правоохранительными органами сведений, которые могут представить указанные лица. Регулирование данных вопросов на федеральном уровне существенно повысит результативность работы по противодействию таким преступлениям.

Например, меры по совершенствованию организации работы по повышению результативности раскрытия и расследования преступлений данной категории преступлений на территории Пермского края принимаются на постоянной основе и стоят на контроле.

Изучением уголовных дел, возбужденных по преступлениям, совершенным с использованием ИКТ, установлено, что в настоящее время остается актуальной проблема длительности исполнения запросов, направляемых следователями в компании сотовой связи, кредитные учреждения, что значительно влияет на сроки предварительного следствия, а также на установление лиц, совершивших преступления. Одной из мер повышения эффективности работы в данном направлении является заключение соглашения об электронном документообороте

с организациями, обладающими информацией, необходимой для раскрытия преступлений. В 2020 г. продолжает действие Соглашение «Об электронном обмене документами и информацией, для выполнения правоохранительным органом возложенных на него функций», заключенного между ГУ МВД России по Пермскому краю и ПАО «Сбербанк России», ПАО «Мегафон»; кроме того, в 2020 г. заключено соглашение с оператором связи ООО «Скартел» («Йота»), в настоящее время прорабатывается алгоритм документооборота.

Для повышения эффективности взаимодействия подразделений следствия, дознания и уголовного розыска территориальных органов МВД России Пермского края при раскрытии и расследовании преступлений в сфере ИКТ, качественного оперативного сопровождения уголовных дел, выявления признаков серийности, реализации мер по возмещению ущерба, причиненного преступлениями, функционирует информационно-поисковая система «Дистанционные преступления» (приказ ГУ МВД России по Пермскому краю от 4 августа 2015 г. № 844), а также вводится в действие информационный банк данных федерального уровня (ИБД-Ф «Дистанционное мошенничество»). Согласно массиву базы, можно проверить совпадение по имеющимся данным лиц, номерам телефонов, IMEI, банковским счетам, адресам электронной почты, с возбужденными уголовными делами, как в Пермском крае, так и в других территориальных субъектах России.

Взаимодействие органов предварительного расследования с подразделениями, осуществляющими оперативно-разыскную деятельность, осуществляется, как правило, путем направления соответствующих поручений. Применительно к уголовным делам о преступлениях в сфере ИКТ поручения даются о производстве конкретных оперативно-разыскных мероприятий, направленных на установление номеров абонентов и данных о телефонных соединениях, контактов преступника, в том числе биллинга, установление обстоятельств регистрации телефонных номеров, контактов, IP-адресов на конкретных лиц, оплаты ими счетов операторов за услуги связи, проверку счетов, установление места открытия и обслуживания счетов, на которые первоначально переведены денежные средства, полученные в результате преступления, в случае обналичивания — места нахождения терминала.

При оценке уровня и эффективности взаимодействия органов расследования с подразделениями, осуществляющими оперативно-разыскную деятельность, надзирающими прокурорами отмечается ряд характерных недостатков.

Как правило, конструктивное и системное взаимодействие в динамике между органами предварительного расследования и оперативными службами не налажено. В частности, поручения дознавателей нередко носят общий, не конкретизированный, шаблонный характер, например «провести ОРМ, направленные на установление лица, совершившего преступление». Не всегда присутствует «обратная связь», запросы оперативных служб о предоставлении дополнительной ин-

формации, необходимой для исполнения поручений, иногда остаются без ответа.

Имеют место факты дачи поручений, исполнение которых следователем не контролируется, ответы на поручения сводятся к констатации факта технического набора проведенных мер и невозможности установления виновных лиц.

Оперативное сопровождение сводилось к представлению органам расследования информации о якобы проведенных оперативно-разыскных мероприятиях, а также проверке на причастность к преступлению лиц, ранее совершавших аналогичные противоправные деяния.

Например, в 2018 г. прокуратурой Хабаровского края выявлялись нарушения следователями требований п. 4 ч. 2 ст. 38 УПК РФ при подготовке поручений о проведении оперативно-разыскных мероприятий, направленных на раскрытие преступлений, предусмотренных ст. 272 и 273 УК РФ. В частности, по ряду уголовных дел следователями направлялись такие поручения непосредственно начальнику отдела «К» УМВД России по краю, который, в свою очередь, не является начальником органа дознания и не обладает полномочиями, указанными в ст. 40.2 УПК РФ, в связи с чем поручения оставались неисполненными.

В ряде случае значимая для раскрытия преступления оперативная информация не использовалась.

Так, Тихвинской городской прокуратурой руководителю следственного органа внесено требование об устранении нарушений по уголовному делу, возбужденному по п. «г» ч. 3 ст. 158 УК РФ, поскольку на протяжении 3 месяцев расследования, несмотря на представленную оперативными службами информацию, не проверен на причастность к совершению данного преступления М. Требование удовлетворено. Оперативные сведения нашли свое подтверждение, М. предъявлено обвинение, и избрана мера пресечения[1].

Надлежащая оперативная работа по раскрытию совершенных преступлений, в том числе взаимодействие с оперативными подразделениями иных регионов, не всегда организована. Взаимодействие по данной категории уголовных дел с правоохранительными органами других регионов характеризуется длительными сроками исполнения направленных в их адрес поручений дознавателей о производстве оперативно-разыскных мероприятий и следственных действий.

Вводимые в действие различные информационные ресурсы находятся в стадии своего становления. Так, введенная в прошлом году в действие единая федеральная информационная база данных по сбору и анализу сведений о преступлениях анализируемой категории «Дистанционное мошенничество» требует усовершенствования. К примеру, в ней до настоящего времени не аккумулируются IP- и ID-адреса, которые использовали злоумышленники для совершения пре-

[1] По материалам работы прокуратуры Ленинградской области.

ступлений. Не указываются данные о принадлежности используемых преступниками абонентских номеров, а также другие значимые сведения, установленные в ходе проверки сообщений о преступлениях и расследовании уголовных дел, то есть база крайне неинформативна. В результате региональные подразделения МВД вынуждены дополнительно их запрашивать в органах МВД других субъектов РФ, при этом не располагая достоверной информацией о наличии либо отсутствии у них таких сведений, что ведет к излишним временным затратам и неэффективному использованию имеющихся ресурсов. Так, правоохранительным органом одного субъекта может быть проведена значительная работа по раскрытию конкретного преступления (получены сведения от операторов сотовой связи, интернет-провайдеров, администрации социальных сетей и др.), однако, поскольку в базе данных информация об этом отсутствует, орган МВД другого субъекта зачастую вынужден дублировать эту работу.

В то же время нельзя говорить о том, что проблемы существуют только у органов предварительного расследования. Качественное оперативное сопровождение уголовных дел о преступлениях данной категории требует кропотливой работы, значительных временных, а иногда и материальных затрат (в частности, поездки в командировки). В итоге оперативное сопровождение в ряде случаев осуществляется бессистемно и эпизодически.

Следует отметить и **координирующую роль прокуроров** в деятельности правоохранительных органов по предупреждению и расследованию преступлений в сфере ИКТ. С целью предупреждения и устранения выявляемых нарушений, а также активизации ведомственного контроля за проведением предварительного следствия по делам названной категории прокурорами регулярно проводятся координационные и межведомственные совещания руководителей правоохранительных органов, создаются межведомственные рабочие группы по противодействию преступности с участием в них представителей правоохранительных органов и органов исполнительной власти.

Целесообразно отметить положительный опыт прокуратуры Тюменской области. Учитывая, что одной из проблем, возникающих при расследовании уголовных дел о компьютерных преступлениях, является выявление лица, совершившего преступление, в 2016 г. с целью систематизации данных о компьютерных преступлениях и выявления причастных к ним виновных лиц прокуратурой Тюменской области и УМВД Тюменской области разработана специальная сетевая многопользовательская база AIPS «Moshennichestva (Region)», которая позволяет анализировать схемы преступлений, связанных с хищением средств с банковских карт и счетов граждан, совершенных с использованием средств коммуникации и в сети Интернет, способы хищения денежных средств, характер и размер причиненного ущерба, место совершения криминальных деяний и иные параметры

и тем самым выявлять однотипные преступления и устанавливать лиц, причастных к их совершению.

При осуществлении надзора за уголовно-процессуальной и оперативно-разыскной деятельностью прокурорами выявляется большое количество **нарушений**. Как правило, одно из самых распространенных нарушений выражается в несоблюдении требования ст. 6.1 УПК РФ, что в ряде случаев грубо нарушало право потерпевших от преступлений, препятствуя их доступу к правосудию. Примеры данных нарушений более всего отмечены прокурорами.

К примеру, 4 сентября 2019 г. следователем СО СУ УМВД России по г. Грозный возбуждено уголовное дело по ч. 2 ст. 159 УК РФ по факту хищения неустановленным лицом путем обмана через интернет-сайт «АВИТО.РУ» денежных средств в сумме 6900 руб., принадлежащих С.

Изучением материалов уголовного дела установлено, что следователем в нарушение требований ст. 6.1, 7, 21, 42, 73, 85–88 УПК РФ должные меры по установлению всех обстоятельств совершенного преступления не приняты, допущены факты несвоевременного проведения следственных действий. В частности, по уголовному делу не была допрошена Ф., чьи паспортные данные использовались на сайте «АВИТО.РУ», соответствующее поручение в следственное подразделение территориальных органов внутренних дел г. Орла о ее допросе не направлено. По имеющейся в деле информации С. через номер «QIWI кошелек» контактировал с неустановленной женщиной, которая представлялась Ф. Вместе с тем владелец указанного номера не установлен, сведения о биллинговых соединениях с базовой станции не получены. С. потерпевшей по делу не была признана и в этом статусе в ходе следствия не допрошена. Изложенные обстоятельства явились основанием для внесения 14 октября 2019 г. прокуратурой Старопромысловского района г. Грозного в СО СУ УМВД России по г. Грозный требования в порядке, установленном п. 3 ч. 2 ст. 37 УПК РФ. Акт прокурорского реагирования рассмотрен, удовлетворен, нарушения закона устранены.

В производстве ОД ОП № 2 УМВД России по г. Воронежу находилось уголовное дело, возбужденное 1 ноября 2019 г. по признакам преступления, предусмотренного ч. 1 ст. 159 УК РФ, по факту хищения путем обмана и злоупотребления доверия имущества ООО «Яндекс.Маркет». При изучении материалов уголовного дела прокурором установлено, что по нему допущена волокита, на протяжении месяца дознавателем не произведено ни одного следственного действия, а также не выполнен ряд необходимых мероприятий, чем допущено грубейшее нарушение уголовно-процессуального законодательства. Кроме того, ООО «Яндекс.Маркет» не признан потерпевшим, представитель данной организации в данном статусе не допрошен. Прокуратурой района внесено требование, которое признано обоснованным и удовлетворено.

Встречались факты повторного нарушения прав потерпевших уже после принятия прокурором мер реагирования.

К примеру, следователем СО ОМВД РФ по Курумканскому району 12 сентября 2019 г. возбуждено уголовное дело по ч. 3 ст. 159 УК РФ по факту хищения бухгалтером централизованной бухгалтерии Финансового управления админи-

страции муниципального образования «Курумканский район» Д. 50 840 руб. путем начисления оплаты по 4 подложным договорам гражданско-правового характера из бюджета района и перечисления денежных средств на счет своего супруга.

При изучении 21 октября 2019 г. прокуратурой Курумканского района уголовного дела установлено, что следственным органом с момента возбуждения дела по нему не произведено ни одного следственного действия. В тот же день начальнику СО ОМВД РФ по Курумканскому району внесено требование, которое рассмотрено и удовлетворено.

В дальнейшем расследование уголовного дела активно и наступательно не осуществлялось. Вопреки требованиям ч. 1 ст. 42 УПК РФ на момент повторного изучения уголовного дела 5 декабря 2019 г. не решен вопрос о признании потерпевшим по уголовному делу.

По выявленным нарушениям требования ст. 6.1 УПК РФ прокурором Курумканского района начальнику СУ МВД по Республике Бурятия 5 декабря 2019 г. внесено представление, которое рассмотрено и удовлетворено, врио начальника СО МВД России по Курумканскому району привлечена к дисциплинарной ответственности. В текущем году уголовное дело передано для дальнейшего расследования в СЧ СУ МВД РФ по Республике Бурятия.

Так, уголовное дело возбуждено 12 июля 2019 г. дознавателем ОД УМВД России по городу Петропавловску-Камчатскому по признакам преступления, предусмотренного ч. 1 ст. 159 УК РФ.

За период расследования уголовного дела дознавателем, в производстве которого оно находилось, не признан потерпевшим Ф., не допрошен в качестве свидетеля Е., не признаны в качестве вещественных доказательств кассовые чеки, телефон, планшетный компьютер.

В связи с выявленными нарушениями закона по данному уголовному делу, в том числе связанными с непроведением следственных действий, отсутствием инициативы и наступательности, в адрес руководства ОД УМВД надзирающим прокурором дважды: 9 августа 2019 г., 25 декабря 2019 г. — вносились меры прокурорского реагирования. По результатам рассмотрения вышеуказанного требования и представления дознаватель ОД УМВД России по городу Петропавловску-Камчатскому привлекался к дисциплинарной ответственности.

Отмечаются факты вынесения заочного постановления о признании лица потерпевшим.

Например, прокурором Липецкого района выявлялись нарушения требований ст. 6.1 УПК РФ по уголовному делу, возбужденному 15 апреля 2019 г. СО ОМВД России по Липецкому району в отношении Б. по признакам преступления, предусмотренного ч. 4 ст. 159 УК РФ, по факту хищения денежных средств в сумме 222 043 руб. с банковского счета, принадлежащего ООО «Правильный автосервис».

Изучение материалов уголовного дела показало, что следователем в нарушение требований ст. 73, 74, 85, 86 УПК РФ не было проведено ни одного следственного и процессуального действия, направленного на установление конкретных обстоятельств хищения денежных средств, за исключением постановления о признании представителя потерпевшего ООО «Правильный автосервис», которое при этом потерпевшему так и не было объявлено; не проведены допросы генераль-

ного директора ООО «Правильный автосервис», сотрудников данного общества, директора филиала магазина «Альта Профиль Липецк», а также самой Б.

На основании изложенного в адрес руководителя следственного органа внесено требование об устранении нарушений федерального законодательства, которое рассмотрено и удовлетворено[1].

Так, по уголовному делу, возбужденному 14 февраля 2019 г. следователем СО ММО МВД РФ «Краснослободский» по ч. 2 ст. 159 УК РФ по факту хищения денежных средств в сумме 25 700 руб. принадлежащих К., установлено, что в нарушение ст. 22 и ст. 42 УПК РФ она на протяжении недели с момента возбуждения уголовного дела не была ознакомлена с постановлением о признании ее потерпевшей и не допрошена по обстоятельствам совершенного в отношении нее преступления, чем было нарушено ее право на доступ к правосудию. С целью устранения указанных нарушений надзирающим прокурором внесено требование в порядке, установленном п. 3 ч. 2 ст. 37 УПК РФ, которое рассмотрено и удовлетворено[2].

Как отмечают прокуроры достаточно часто лица, ведущие предварительное расследование, не проводят очевидных и несложных процессуальных действий, направленных на установление всех необходимых обстоятельств преступного деяния.

В производстве следователя СО ОМВД России по г. Ноябрьску находилось уголовное дело о преступлении, предусмотренном ч. 4 ст. 159 УК РФ, по факту хищения денежных средств, принадлежащих ООО «МП «Стройинвест» и ООО «Сослан86», в сумме 386 080 руб. и 690 620 руб. соответственно.

Изучением уголовного дела в прокуратуре города установлено, что в нарушение требований ст. 6.1 УПК РФ за 3 месяца проведено лишь 2 значимых следственных действия, а принятое процессуальное решение не отвечает требованиям закона.

Из показаний потерпевших следует, что денежные средства в указанных суммах ими были переведены на расчетный счет ООО «Династия» в целях приобретения строительных материалов у ООО «Челстрой Юг». В свою очередь, как им далее стало известно, неустановленное лицо, получив доступ к электронной почте ООО «Челстрой ЮГ», предоставило им подложные платежные реквизиты, тем самым похитив денежные средства, предназначавшиеся для приобретения товаров у данного общества.

Несмотря на это представитель ООО «Челстрой ЮГ» по вопросам «взлома» электронного почтового ящика не допрошен, обстоятельства возникших между ООО «МП «Стройинвест», ООО «Сослан86» и их организацией правоотношений не установлены.

Согласно платежному поручению, счет ООО «Династия», на который были перечислены денежные средства, открыт в ПАО «ФК Открытие». Однако в кредитном учреждении не запрошены выписка о движении денежных средств по счету за интересуемый период, сведения о лицах, имеющих право единоличного

---

[1] По материалам работы прокуратуры Липецкой области.

[2] По материалам деятельности прокуратуры Республики Мордовия.

распоряжения находящимися на нем денежными средствами (копия карточки счета с образцами подписей), о наличии подключенной услуги «банк-клиент», дающей возможность удаленного доступа к нему.

Не приняты меры к установлению и допросу директора ООО «Династия». Выписки о движении денежных средств по счетам юридических лиц, представляющие доказательственное значение, в установленном порядке не истребованы и к материалам дела не приобщены.

С учетом изложенного прокуратурой города 28 марта 2019 г. по факту выявленных нарушений закона начальнику СО ОМВД России по г. Ноябрьску внесено требование, которое рассмотрено и удовлетворено, следователь привлечен к дисциплинарной ответственности[1].

В силу ряда причин у органов предварительного расследования возникали сложности, связанные с эффективным **экспертным сопровождением** при расследовании преступлений в сфере ИКТ.

Одним из основных доказательств по уголовным делам о компьютерных преступлениях является заключение эксперта.

В ряде субъектов отмечается, что экспертное сопровождение и техническое оснащение экспертных подразделений (количество и качество экспертной базы) не соответствует уровню технического развития преступников, в результате чего зачастую не удается установить виновных лиц.

В ходе расследования уголовных дел рассматриваемой категории у следственных органов нередко возникают трудности, связанные с проведением компьютерно-технических экспертиз. В частности, проведение экспертиз занимает длительное время (в среднем 4–5 месяцев), при этом в подавляющем большинстве случаев в своих заключениях эксперты приходят к выводам о невозможности извлечения информации из исследуемых объектов в условиях лаборатории судебных компьютерных экспертиз ЭКЦ УМВД России по территориальному субъекту[2].

В ряде субъектов отмечается недостаточная штатная численность экспертов, имеющих допуск для проведения компьютерно-технических экспертиз для подтверждения программного воздействия на устройства потерпевших[3], ограниченные технические возможности исследовать обстоятельства внедрения, распространения, использования вредоносного программного обеспечения, в том числе на различного рода объектах (смартфоны, планшеты и т.п.)[4].

В частности, в докладной записке прокуратуры Республики Саха (Якутия) отмечается, что на территории республики действует только одно экспертное

---

[1] По материалам деятельности прокуратуры Ямало-Ненецкого автономного округа.

[2] По материалам работы прокуратуры Хабаровского края.

[3] По материалам работы прокуратуры Кировской области.

[4] По материалам работы прокуратуры Республики Татарстан.

учреждение, которое может давать заключение по результатам компьютерных экспертиз, — ЭКЦ МВД по Республике Саха (Якутия), в котором, в свою очередь, право проведения таких экспертиз имеют только три эксперта. Данное обстоятельство приводит к тому, что из-за загруженности экспертов исследования проводятся необоснованно длительное время, что приводит к продлению сроков предварительного следствия.

В деятельности следственных органов отмечены затруднения, связанные с отсутствием или недостаточной численностью экспертов, осуществляющих определенные виды судебных экспертиз.

Так, судебно-компьютерные экспертизы проводятся ЭКЦ МВД по республике Бурятия, в штате которого имеются лишь два аккредитованных эксперта, либо негосударственными экспертными учреждениями, которые осуществляют свою деятельность на платной основе. Судебные экспертизы по вопросу отнесения оборудования, использованного при проведении азартных игр, к категории игорного в регионе не проводятся, что влечет необходимость подыскивания организаций, которые могут проводить такие экспертизы, в других субъектах Российской Федерации[1].

При производстве предварительного расследования также возникали сложности с проведением компьютерных экспертиз по причине отсутствия научно обоснованных методик в экспертных учреждениях области для решения поставленных вопросов, необходимого оборудования и программного обеспечения.

Современные способы совершения преступлений в сфере ИКТ требуют зачастую проведения бухгалтерских исследований и соответствующих экспертиз. Вместе с тем существующий ревизионный аппарат явно не справляется с нагрузкой, о чем свидетельствуют имеющиеся очереди[2].

Так, по данным ГУ МВД России по Нижегородской области остается проблемным вопрос о назначении компьютерно-технических экспертиз по вредоносным (вирусным) программам, которые проводятся лишь в МВД России, экспертном подразделении ФСБ и лаборатории «Касперского». Сроки их проведения составляют несколько месяцев, что увеличивает сроки дознания. В ЭКЦ ГУ МВД России по Нижегородской области технические средства и программно-аппаратные комплексы, используемые для проведения компьютерных экспертиз по мобильным телефонам с операционной системой «Android», отсутствуют.

Важно отметить, что прокурорами отмечались неединичные факты, когда должностные лица органов предварительного расследования используют проведение судебно-экспертных исследований в качестве способов затягивания сроков предварительного расследования.

Так, изучением в рамках осуществления надзорных действий прокурором уголовного дела, возбужденного 18 апреля 2019 г. СО ОМВД России по Черекскому району по ч. 2 ст. 159 УК РФ по факту хищения денежных средств у Ч., уста-

---

[1] По материалам деятельности прокуратуры Республики Бурятия.

[2] По материалам работы прокуратуры Тверской области.

новлено, что дело фактически не расследовалось, без каких-либо обоснованных причин оно затягивается, следственные действия проводились эпизодически. В частности, следователем 22 апреля 2019 г. вынесено постановление о назначении судебной дактилоскопической экспертизы, которое эксперту фактически направлено лишь 7 июня 2019 г. По выявленным нарушениям федерального законодательства надзирающим прокурором в адрес руководства СО ОМВД России по Черекскому району внесено представление и по результатам его рассмотрения следователю объявлен выговор[1].

К примеру, в производстве УРОВД ГСУ СК РФ по Республике Крым находится уголовное дело о совершении преступлений, предусмотренных ч. 3 ст. 171.2, ч. 1, 2 ст. 210 УК РФ. В ходе расследования следственным органом допущены грубые нарушения требований уголовно-процессуального законодательства, в том числе о разумном сроке уголовного судопроизводства.

Несмотря на то, что производство предварительного расследования по уголовному делу с момента его возбуждения осуществляется следственно-оперативной группой в составе 33 следователей, в нарушение ч. 3 ст. 163 УПК РФ руководитель следственной группы ее работу должным образом не организовал. Оргтехника, изъятая 29 марта 2019 г. по местам нахождения игровых клубов в г. Севастополе и г. Керчи, осмотрена только 15 августа 2019 г., в результате чего лишь 16 августа 2019 г., по минованию более 4 месяцев с момента ее изъятия, назначены судебные компьютерно-технические экспертизы. В нарушение п. 11 ч. 4 ст. 47 УПК РФ обвиняемые по уголовному делу с постановлениями о назначении экспертиз не ознакомлены, их право на постановку вопросов экспертам следователем не обеспечено.

В связи с изложенным прокуратурой республики 27 августа 2019 г. в адрес и.о. руководителя ГСУ СК РФ по Республике Крым внесено требование, которое рассмотрено и удовлетворено с принятием конкретных мер по активизации расследования, устранению допущенных нарушений уголовно-процессуального законодательства[2].

Также выявлены нарушения положений УПК РФ при ознакомлении участников уголовного процесса с заключениями экспертов.

Так, при изучении прокурором материалов уголовного дела, возбужденного в отношении Л. по признакам преступления, предусмотренного ч. 2 ст. 228 УК РФ, выявлены нарушения требований ст. 6.1 УПК РФ, выразившиеся в несвоевременном предъявлении Л. обвинения и неознакомлении его с заключениями проведенных по уголовному делу экспертиз, что привело к необоснованному продлению сроков расследования до 3 месяцев[3].

Как правило, экспертизы проводятся в ЭКЦ субъектов Российской Федерации. Однако в случае их загруженности проведение экспертизы поручалось образовательным организациям. Например, в целях преодоления сложившейся ситуации в некоторых регионах (Владимир-

[1] По материалам деятельности прокуратуры Кабардино-Балкарской Республики.

[2] По материалам деятельности прокуратуры Республики Крым.

[3] По материалам работы прокуратуры Республики Мордовия.

ская, Кировская, Тюменская области) для производства экспертных исследований привлекались представители научных и образовательных организаций.

Например, по уголовному делу, возбужденному 24 мая 2017 г. СЧ СУ УМВД Тюменской области по признакам предусмотренного ч. 2 ст. 272 УК РФ преступления в отношении неустановленного лица по факту неправомерного доступа к охраняемой законом компьютерной информации, содержащейся на сервере мониторинга систем видеонаблюдения компании ООО «Ин Нова», повлекшего блокирование и модификацию компьютерной информации, проведение компьютерно-технической судебной экспертизы было поручено экспертам кафедры информационной безопасности института математики и компьютерных наук Тюменского государственного университета.

В ходе предварительного расследования немаловажным остается и вопрос о **возмещении причиненного компьютерными преступлениями ущерба.**

В целом прокуроры оценивают деятельность органов предварительного следствия по обеспечению ущерба по данной категории уголовных дел как достаточную.

В ходе расследования с обвиняемыми (подозреваемыми) проводится работа, направленная на инициирование добровольного возмещения причиненного преступлением ущерба, разъясняются положения действующего уголовного и уголовно-процессуального законодательства о правовых последствиях, смягчающих положение виновного лица при добровольном возмещении причиненного ущерба[1]. В добровольном порядке ущерб, как правило, возмещался лишь частично.

Так, в докладной записке прокуратуры Республики Алтай отмечается, что по оконченным следователями МВД по Республике Алтай в 2015 г. уголовным делам анализируемой категории установлен ущерб на сумму 610 тыс. руб., из которых в добровольном порядке возмещено 346 тыс. руб. В первом полугодии 2016 г. сумма ущерба по оконченным уголовным делам составила 262 тыс. руб., в добровольном порядке погашена задолженность на 97 тыс. руб.

С целью обеспечения гражданского иска и исполнения наказания в виде штрафа следователи обращаются в суд с ходатайствами о наложении ареста на имущество обвиняемых. В ряде регионов прокурорами налажена комплексная работа по обеспечению возмещения вреда от преступлений в сфере ИКТ.

Так, в целях обеспечения прав потерпевших на возмещение вреда, причиненного преступлением, а также исполнения приговора в части возможной конфискации и иных взысканий по уголовным делам следователями территориальных органов СУ УМВД России по Ярославской области проводились обыски по месту жительства обвиняемых, запрашивались сведения о наличии у привлекаемых к ответственности лиц имущества (в частности недвижимости, автотранспорта, оружия и др., подлежащего обязательной регистрации имущества), счетов в банках,

[1] По материалам деятельности прокуратуры Магаданской области.

на которые может быть наложен арест, направлялись поручения в подразделения МВД России, уполномоченные проводить оперативно-разыскные мероприятия.

Работа в рассматриваемой сфере организована в соответствии с совместным приказом прокуратуры Ярославской области, СУ СК России по Ярославской области, УФСБ России по Ярославской области, УМВД России по Ярославской области, УФССП России по Ярославской области, ГУ МЧС России по Ярославской области № 40/36/30/223/209/211 от 25 апреля 2019 г. «Об организации межведомственного взаимодействия при возмещении причиненного преступлениями ущерба».

Вопросы возмещения причиненного преступлениями ущерба обсуждены 23 апреля 2019 г. на заседании межведомственного совещания руководителей правоохранительных органов Ярославской области «О результатах анализа состояния работы правоохранительных и иных уполномоченных органов по возмещению ущерба, причиненного преступлениями».

В соответствии с решением указанного межведомственного совещания прокуроры, изучая уголовные дела, поступившие с обвинительным заключением (актом, постановлением), устанавливают полноту принятых правоохранительными органами мер по возмещению ущерба, причиненного преступлениями, а также пресечению фактов возможной легализации (отмывания) денежных средств или иного имущества, приобретенного преступным путем. Нарушение прав потерпевших на возмещение причиненного преступлением ущерба рассматривается как самостоятельное основание для возвращения уголовного дела на дополнительное расследование.

На особом контроле у прокуроров находится исполнение требований УПК РФ относительно обеспечительных мер гражданского иска, иных мер процессуального принуждения.

Так, при изучении уголовного дела, возбужденного 18 февраля 2019 г. СУ МУ МВД России «Рыбинское» по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ, по факту хищения путем обмана имущества М. с использованием сети Интернет, установлено, что следователем не выполнены требования ст. 73, ч. 3 ст. 42 и ст. 160.1 УПК РФ. Установлено, что подозреваемым в совершении указанного преступления является несовершеннолетний Ч., который обратился в правоохранительные органы с явкой с повинной. В качестве его законного представителя допущен К. Вместе с тем следователем в разумный срок достаточные меры к установлению имущества подозреваемого или его законного представителя, за счет которого возможно обеспечение возмещения причиненного имущественного вреда, не приняты. Розыск такого имущества фактически не осуществлялся, запросы в органы регистрации движимого и недвижимого имущества, а также в банки о наличии счетов не направлялись, обыск в жилище не производился.

В связи с выявленными нарушениями закона 9 июля 2019 г. в адрес начальника СУ МУ МВД России «Рыбинское» прокурором в порядке, установленном п. 3 ч. 2 ст. 37 УПК РФ направлено требование об устранении нарушений закона, которое рассмотрено и удовлетворено, расследование активизировано.

Работа по возмещению ущерба, причиненного преступлениями, ведется в тесном взаимодействии с органами, осуществляющими оперативно-разыскную деятельность.

Например, в целях обеспечения возмещения ущерба на стадии предварительного расследования сотрудниками ОД УМВД Камчатского края осуществляется взаимодействие с контролирующими органами и учреждениями для получения информации об имуществе, ценностях и денежных средствах путем направления соответствующих запросов в учреждение Федеральной службы государственной регистрации, кадастра и картографии (Росреестр), БТИ для установления сведений о правах подозреваемых (обвиняемых) на недвижимое имущество, земли, региональное подразделение Федеральной налоговой службы России о наличии регистрации подозреваемых (обвиняемых) в качестве индивидуальных предпринимателей, юридических лиц, долей в уставном капитале, Межрегиональное управление Федеральной службы по финансовому мониторингу по Дальневосточному федеральному округу, ФКУ «Центр Государственной инспекции по маломерным судам МЧС России по Камчатскому края», Инспекцию Государственного технического надзора Камчатского края для установления сведений о транспортных средствах и специальной техники, подразделения лицензионно-разрешительной работы Управления Росгвардии по Камчатскому краю, государственные и коммерческие банки на наличие валютных и рублевых вкладов на имя фигурантов уголовных дел.

Для повышения эффективности работы по установлению имущества подозреваемых, обвиняемых и иных лиц, несущих по закону материальную ответственность, на которое может быть обращено взыскание в счет возмещения ущерба, причиненного преступлением, штрафа или конфискации, прокуратурой края, СУ СК России, УМВД России, УФСБ России, УФСКН России, ГУ МЧС России, УФССП России по Камчатскому краю 29 марта 2016 г. издан и исполняется совместный приказ № 50/28/40/98/106/16/108/88 «Об организации взаимодействия правоохранительных органов Камчатского края в целях повышения эффективности работы по возмещению ущерба, причиненного преступлениями».

Данным приказом подробно регламентированы действия правоохранительных органов по установлению указанного имущества в ходе осуществления оперативно-разыскной деятельности, проведения проверок по сообщениям о преступлениях, предварительного расследования по уголовным делам.

Отмечается положительный опыт деятельности некоторых прокуратур.

Так, реализуя представленные уголовно-процессуальным законом полномочия, следователями по всем уголовным делам анализируемой категории направлялись запросы о предоставлении сведений об имущественном положении подозреваемых и обвиняемых в управление Федеральной службы государственной регистрации, кадастра и картографии по Вологодской области, управление Федеральной налоговой службы России по Вологодской области, УГИБДД УМВД России по Вологодской области, ГУ Вологодской области «Вологдатехинвентаризация», а также в банковские и иные учреждения и организации, расположенные как на территории Вологодской области, так и в других субъектах Российской Федерации.

В ходе предварительного расследования по уголовным делам наряду с установлением имущества, подлежащего конфискации в соответствии со ст. 104.1 УК РФ, принимаются меры к установлению иного имущества подозреваемого (обвиняемого) или лиц, несущих по закону материальную ответственность за их действия, на которое может быть наложен арест в целях обеспечения исполнения приговора в части заявленного гражданского иска, взыскания штрафов, других имущественных взысканий.

Во исполнение приказа руководителя следственного управления СУ СК России по Вологодской области от 14 августа 2014 г. № 73 «О мерах по повышению эффективности работы следственного управления в сфере возмещения ущерба, причиненного преступлением», по каждому сообщению, уголовному делу о преступлении анализируемой категории принимаются исчерпывающие меры к возмещению ущерба, причиненного государству, в том числе обеспечению гражданского иска по уголовным делам. В этой связи перед судом возбуждаются ходатайства об аресте имущества в качестве обеспечительной меры, прокурорами исключено направление с обвинительным заключением уголовных дел, по которым не приняты меры по возмещению причиненного ущерба.

Вопросы возмещения ущерба, причиненного преступлениями, находятся на постоянном контроле прокуратуры Республики Башкортостан.

Для повышения эффективности и качества работы по возмещению ущерба, причиненного преступлениями коррупционной направленности, прокуратурой республики совместно с МВД по РБ, СУ СК РФ по РБ, УФСБ РФ по РБ и УФСИН РФ оп РБ разработан и утвержден совместный приказ от 28 февраля 2017 г. «О межведомственном взаимодействии при установлении имущества, за счет которого возможно возмещение ущерба, причиненного преступлениями коррупционной направленности, а также полученного в результате преступной деятельности и подлежащего конфискации».

В целях обеспечения возмещения ущерба, причиненного данным видом преступлений государству, прокуратурой республики подготовлено указание «Об организации исполнения Указания Генерального прокурора Российской Федерации от 3 апреля 2017 г. № 236/8 «Об организации работы по возмещению ущерба, причиненного Российской Федерации, субъектам Российской Федерации, муниципальным образованиям, государственным и муниципальным унитарным предприятиям преступлениями».

В аппарате и на местах функционируют рабочие группы по вопросам возмещения ущерба, причиненного преступлениями, каждые полгода утверждается план работы, исполнение которого контролируется.

В целом в ходе расследования уголовных дел для отыскания имущества подозреваемых и обвиняемых запрашиваются необходимые сведения в органах Росреестра о наличии у подозреваемого прав на недвижимое имущество и земельные участки; в органах ГИБДД — о наличии зарегистрированных транспортных средств, прицепов; в органах Гостехнадзора — о наличии прав на спецтехнику; в Инспекции по маломерным судам — о наличии прав на плавсредства; в органах Федеральной налоговой службы Российской Федерации — о том, является ли лицо

руководителем либо учредителем юридического лица, индивидуальным предпринимателем; в организациях, оказывающих услуги держателей реестра акционеров, — о наличии у лица в собственности акций; в банках — о наличии счетов, банковских карт, а также банковских ячеек.

В целях повышения эффективности возмещения ущерба органами следствия принимаются меры к своевременному проведению обысков и выемок; устанавливается имущество, на которое возможно наложить арест. Потерпевшим при наличии данных о причинении им преступлением имущественного вреда разъясняется порядок заявления иска[1].

Вместе с тем анализ следственной и судебной практики демонстрирует ряд примеров, когда принимаемые органами предварительного расследования меры по возмещению материального ущерба, причиненного преступлением, являются недостаточными.

По некоторым уголовным делам наличие недвижимости, банковских вкладов не проверяется, отдельные поручения о проведении соответствующих проверок не даются. В планах расследования уголовных дел не указываются мероприятия, направленные на розыск похищенного и установление наличия имущества у подозреваемых и обвиняемых с учетом их связей. Кроме того, дознаватели пренебрегают такой важной процессуальной мерой, как наложение ареста на имущество, хотя своевременное ее применение дает возможность обеспечить сохранность разысканного имущества преступника и возместить материальный ущерб потерпевшим[2].

Меры к установлению имущества, за счет которого может быть возмещен причиненный ущерб, предпринимаются не на стадии предварительных оперативных мероприятий, а в ходе проведения процессуальной проверки или расследования уголовного дела, когда имущество уже легализовано[3].

Также прокурорами констатировалось отсутствие инициативы в работе следственных органов по направлению запросов об оказании международной правовой помощи, относящихся к установлению имущества обвиняемых по уголовным делам, находящегося за рубежом.

По результатам проведенного в октябре 2019 г. анализа работы органов дознания УМВД России по Ивановской области по возмещению ущерба, причиненного преступлениями, выявлены нарушения требований ст. 115 УПК РФ, связанные с недостаточностью принимаемых мер по наложению ареста на имущество подозреваемых (обвиняемых).

Проведенный анализ уголовных дел показал, что при их расследовании дознаватели не принимают мер, направленных на установление имущества подо-

---

[1] По материалам прокуратуры Кемеровской области.

[2] По материалам деятельности прокуратуры Ставропольского края.

[3] По материалам деятельности прокуратуры Тверской области.

зреваемых (обвиняемых), на которое может быть наложен арест, а показатели возмещенного ущерба сформированы из данных о добровольном возмещении имущественного ущерба и за счет стоимости изъятого имущества. По результатам проведенной проверки 5 ноября 2019 г. прокурором области в адрес начальника УМВД России по Ивановской области внесено представление, по результатам рассмотрения которого приняты дополнительные меры по повышению эффективности работы органов дознания на данном направлении, виновные должностные лица привлечены к дисциплинарной ответственности.

Нельзя не отметить также объективные сложности, присущие всем категориям уголовных дел: на момент раскрытия преступления и установления лица, совершившего преступление, похищенные денежные средства израсходованы; отсутствие у виновных лиц какого-либо дохода либо имущества, на которое возможно наложение ареста[1].

Прокурорами и руководителями правоохранительных органов в целях оптимизации работы по возмещению ущерба, причиненного преступлением физическим и юридическим лицам, а также государству, издаются совместные организационно-распорядительные акты.

Например, прокуратурой Владимирской области и руководителями правоохранительных органов области издано совместное указание № 35/15/23/1/31 3/2/224/129/10/73 от 30 марта 2018 г. «О порядке взаимодействия правоохранительных и иных государственных органов на досудебной стадии уголовного судопроизводства в сфере возмещения ущерба, причиненного преступлениями», в котором регламентирована деятельность должностных лиц органов расследования по выполнению требований п. 4 ч. 1 ст. 73 УПК РФ, а также определен порядок взаимодействия следственных органов и надзирающих прокуроров для реализации последними полномочий, установленных ч. 3 ст. 44 УПК РФ. Вопросы возмещения имущественного вреда, причиненного преступлениями, рассматриваются на полугодовых, годовых коллегиях, межведомственных, координационных совещаниях.

Так, в 2019 г. прокуратурой Удмуртской республики проведено координационное совещание руководителей правоохранительных органов «О дополнительных мерах, принимаемых по возмещению ущерба, причиненного преступлениями», на котором выработаны дополнительные меры по повышению эффективности работы правоохранительных органов на данном направлении.

Вопросы эффективности работы правоохранительных и иных уполномоченных органов по возмещению ущерба, причиненного преступлениями, рассмотрены 25 апреля 2019 г. на коллегии прокуратуры Камчатского края, 25 июня 2019 г. и 19 декабря 2019 г. на заседании межведомственной рабочей группы по противодействию преступлениям в сфере экономики с выработкой мероприятий, направленных на повышение качества указанной деятельности, исполнение которых находится на контроле прокуратуры края. Рассмотрение вопросов, связанных с возмещением причиненного ущерба, в том числе полноты и своевременности принятия мер к наложению ареста на имущество подозреваемых (обвиняемых),

[1] По материалам прокуратур Забайкальского края, Иркутской области.

запланировано на Координационном совещании в первом полугодии 2020 г. в соответствии с пунктом 2.1 плана основных мероприятий по координации деятельности правоохранительных органов края.

Практика изучения прокурорами **приостановленных** уголовных дел в сфере ИКТ показывает, что как правило следователями и дознавателями не проводится необходимый перечень следственных и иных процессуальных действий в отсутствие лица, подлежащего привлечению в качестве обвиняемого.

Практика прокурорского надзора свидетельствует, что одной из основных причин низкой эффективности раскрытия данных преступлений является отсутствие наступательности при производстве предварительного расследования со стороны следователей и дознавателей, низкая интенсивность расследования, а также ненадлежащий ведомственный контроль руководства органов расследования за своевременностью производства следственных и процессуальных действий.

К примеру, 2 августа 2018 г. дознавателем ОД ОМВД России по г. Усинску возбуждено уголовное дело по признакам преступления, предусмотренного ч. 1 ст. 159.1 УК РФ. По данному делу неоднократно принимались решения о приостановлении дознания, которые признавались как прокурором города, так и начальником дознания незаконными и отменялись, поскольку дознавателем не принимались меры по привлечению лица в качестве подозреваемого, при этом в материалах дела имелись сведения о причастности к данному преступлению З. В связи с выявленными нарушениями прокурором в адрес начальника ОМВД России по г. Усинску внесено требование, по результатам рассмотрения которого привлечен к дисциплинарной ответственности дознаватель, в чьем производстве находилось дело. После отмены незаконного решения и дополнительного расследования 19 августа 2019 г. уголовное дело направлено в суд для рассмотрения по существу[1].

Не во всех случаях, особенно на первоначальном этапе расследования, истребуются сведения из банковских организаций о движении денежных средств, похищенных с применением электронных платежных систем, устанавливали расчетные счета, на которые перечисляются денежные средства, а при хищении имущества с использованием мобильных устройств принимали своевременные меры к установлению региона, в котором зарегистрирован абонент, к получению номеров сотовых компаний, сведений о соединении абонентских номеров и определению IP-адреса абонентов, назначали необходимые судебные экспертизы.

Так, при проверке в прокуратуре установлено, что поднадзорным органом внутренних дел при производстве расследования преступлений рассматриваемой категории не принимаются меры к установлению владельцев, указываемых потерпевшим телефонных номеров. В суды не направляются ходатайства на получение разрешения на снятие информации о соединениях между абонентами и абонентскими устройствами с указанием географического местоположения

[1] По материалам деятельности прокуратуры Республики Коми.

в момент осуществления телефонного звонка, данных, на кого зарегистрирован телефонный номер, и последующего направления оператору связи для предоставления сведений о местонахождении лица и произведенных им соединениях[1].

Следует отменить, что с целью установления лиц, совершивших такие преступления, необходимо оперативно по судебным решениям, полученным в порядке, установленном ст. 165 УПК РФ, истребовать в различных кредитных учреждениях, находящихся, как правило, за пределами территориального субъекта, сведения о движении денежных средств по счетам потерпевшего и других лиц, а также сведения у интернет-провайдеров, владельцев ресурсов социальных сетей об IP-адресах устройств, с использованием которых посредством удаленного доступа совершались банковские операции с последующим установлением владельцев указанных устройств.

Однако анализ повторных отмен постановлений о приостановлении предварительного расследования по таким делам показал, что следователи не всегда своевременно получают в порядке ст. 165 УПК РФ соответствующие разрешения суда, зачастую с ходатайством обращаются уже после второй или даже третьей отмены незаконных решений прокурором[2].

Несмотря на длительные сроки представления ответов, сами запросы фактически направляются непосредственно перед приостановлением расследования, а не сразу после возбуждения уголовного дела. После приостановления расследования контроль за поступлением ответов на запросы, их изучение и возобновление производства по уголовным делам должным образом не осуществляются. При поступлении сведений, требующих проведения дальнейшего расследования, дела длительное время не возобновляются, следственные действия не проводятся[3].

При условии выполнения первоначальных, необходимых следственных и процессуальных действий следователями (дознавателями) принимаются решения о приостановлении расследования, а дальнейший анализ поступившей информации по уголовным делам в нарушение требований ст. 209 УПК РФ следователями и руководителями следственных органов не проводится. Только после периодических запросов прокурора о направлении дел для изучения в порядке надзора работа по таким уголовным делам начинает проводиться[4].

Так, 16 августа 2019 г. дознавателем ОД ОМВД России по Елизовскому району принято решение о приостановлении по п. 1 ч. 1 ст. 208 УПК РФ уголовного дела, возбужденного 17 июля 2019 г. по признакам преступления, предусмотренного ч. 1 ст. 159 УК РФ. Изучением уголовного дела установлено, что все следственные

---

[1] По материалам работы прокуратуры Ростовской области.

[2] По материалам деятельности прокуратуры Алтайского края.

[3] По материалам деятельности прокуратуры Ненецкого автономного округа.

[4] По материалам деятельности прокуратуры Архангельской области.

действия, выполнение которых возможно без лица, подлежащего привлечению в качестве обвиняемого, не выполнены. Телефоны, на которые поступали звонки, не изъяты, не осмотрены и не приобщены к материалам уголовного дела; детализация абонентских номеров потерпевшей не истребована и не проанализирована. Не приняты в ходе расследования исчерпывающие меры с целью установления личности лица, совершившего данное преступление следственным путем. В связи с изложенным постановление о приостановлении расследования прокурором отменено, уголовное дело направлено начальнику ОД ОМВД России по Елизовскому району для организации дополнительного расследования. После устранения выявленных недостатков дознавателем ОД ОМВД России по Елизовскому району вновь принято решение о приостановлении расследования, признанное прокурором законным[1].

Прокурорами отмечались факты нарушения прав и законных интересов потерпевших, препятствующих их доступу к правосудию.

Например, прокуратурой Ленинского района г. Иваново 22 октября 2019 г. отменено незаконное постановление от 18 октября 2019 г. о приостановлении предварительного расследования на основании п. 1 ч. 1 ст. 208 УПК РФ по уголовному делу о преступлении, предусмотренном ч. 1 ст. 128[1] УК РФ. При проверке законности принятого решения о приостановлении предварительного расследования установлено, что в нарушение требований ст. 6.1, 42, 73, ч. 5 ст. 208 УПК РФ в ходе проведенного дознания при наличии сведений о лице, которому преступлением причинен моральный вред, постановление о признании потерпевшим не вынесено, данное лицо в качестве потерпевшего не допрошено, свидетели, о которых в материалах уголовного дела имелись данные, не допрошены, мер для получения сведений о лице, использовавшем аккаунт «ВКонтакте» для совершения преступления, не принято.

По факту покушения на хищение денежных средств ООО МКК «Монеза» ОД ОП № 4 МУ МВД России «Оренбургское» возбуждено уголовное дело по ч. 3 ст. 30, ч. 1 ст. 159.1 УК РФ. По результатам расследования дознавателем дважды выносились постановления о приостановлении производства дознания, которые прокуратурой района отменялись как незаконные и необоснованные. В ходе расследования не признан потерпевшим и по обстоятельствам совершенного преступления не допрошен представитель ООО МКК «Монеза», сведения об исполнении поручения о проведении соответствующих следственных действий, направленного в ОМВД России по Пресненскому району г. Москвы, к уголовному делу не приобщены. В ООО МКК «Монеза» не истребованы сведения, имеющие значения для раскрытия уголовного дела. В связи с выявленными нарушениями прокуратурой района начальнику ОП внесено представление, которое рассмотрено и удовлетворено, виновные должностные лица привлечены к ответственности[2].

Анализ надзорной деятельности на стадии изучения уголовных дел, поступивших с обвинительным заключением, показал, что основными причинами их **возвращения для производства дополнительного расследования** являются: неполнота следствия, в том числе наличие

---

[1] По материалам деятельности прокуратуры Камчатского края.

[2] По материалам работы прокуратуры Оренбургской области.

неустраненных противоречий в показаниях допрошенных лиц; отсутствие достоверных доказательств размера причиненного ущерба, несоответствие обвинения фактически установленным в ходе расследования обстоятельствам совершения преступления; невыясненные, имеющие значение для уголовного дела обстоятельств; неверное применение уголовного закона.

Неполнота предварительного следствия заключалась в том, что не были установлены все обстоятельства, подлежащие доказыванию в соответствии со ст. 73 УПК РФ, с учетом специфики рассматриваемых преступлений: не проводился осмотр компьютерной техники на предмет установления истории соединений браузера, осмотр мобильных телефонов потерпевших, не запрашивались необходимые сведения о движении денежных средств по счетам потерпевших; не истребовались сведения из кредитных учреждений и т.д.

Прокурорами в качестве оснований также отмечаются нарушения формальных требований УПК РФ. Среди данных нарушений указаны ошибки при составлении процессуальных документов.

К примеру, в прокуратуру Ленинского района г. Оренбурга от следователя отдела по расследованию преступлений № 5 СУ МУ МВД России «Оренбургское» с обвинительным заключением поступило уголовное дело по обвинению Р. в совершении преступления, предусмотренного ч. 2 ст. 159.3 УК РФ.

Изучение уголовного дела показало, что при описании в постановлении о привлечении в качестве обвиняемого и обвинительном заключении в отношении Р.А.М. объективной стороны мошенничества следователем не указан признак причинения потерпевшей Р.О.С. значительного материального ущерба. Кроме того, в предъявленном обвинении и обвинительном заключении Р.А.М. инкриминируется хищение денежных средств, в том числе в ресторане быстрого питания «Burger King» по адресу: г. Оренбург, пр. Гагарина, 29/1. Вместе с тем установлено, что фактически данный ресторан по адресу, указанному в постановлении о привлечении в качестве обвиняемого и обвинительном заключении, не располагается. Таким образом, в нарушение требований ст. 73 УПК РФ место совершения преступления не установлено[1].

В материалах уголовного дела отсутствуют сведения о проведении обязательных процессуальных действий и принятия процессуальных решений.

Так например, уголовное дело по обвинению Т. в совершении преступлений, предусмотренных п. «б» ч. 2 ст. 165, ч. 3 ст. 33, ч. 1 ст. 173.1, ч. 3 ст. 160, ч. 1 ст. 187 УК РФ возвращено прокурором в порядке, установленном ст. 221 УПК РФ в связи с допущенными по уголовному делу процессуальными нарушениями, выразившимися, в том числе, в непризнании лица в качестве потерпевшего по эпизоду преступной деятельности по ч. 3 ст. 160 УК РФ[2].

---

[1] По материалам работы прокуратуры Оренбургской области.

[2] По материалам деятельности прокуратуры Тверской области.

Отмечались факты неполноты предъявленного обвинения с учетом представленных прокурору материалов уголовного дела.

Так, постановлением прокурора для производства дополнительного следствия, изменения объема обвинения, квалификации действий обвиняемого и составления обвинительного заключения заново возвращено уголовное дело по обвинению П. в совершении преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ.

Основанием для возврата уголовного дела послужило отсутствие в предъявленном П. обвинении дополнительного квалифицирующего признака кражи, предусмотренного п. «г» ч. 2 ст. 158 УК РФ, — тайное хищение чужого имущества, совершенное из одежды (похищенная банковская карта, с которой впоследствии обвиняемым были сняты денежные средства, находилась в кармане брюк потерпевшего).

Вместе с тем П., изначально обладая информацией о местонахождении банковской карты потерпевшего С. и PIN-кодом, обеспечивающим доступ к расчетному счету, похитил кошелек с находившейся там электронной банковской картой из кармана брюк спящего С. с прямым умыслом на последующее снятие и хищение денежных средств, находящихся на расчетном счете, а не на хищение кошелька и электронной банковской карты.

Кроме того, предмет кражи не обладал экономическими признаками и не имел потребительской и меновой стоимости (потерпевший С. показал, что кошелек, в котором находилась банковская карта, материальной ценности для него не представляет). Сама же электронная банковская карта является лишь средством для безналичного оборота и обналичивания денежных средств, является собственностью банка и самостоятельной стоимости не имеет, в связи с чем не может являться предметом хищения.

В связи с изложенным незаконное постановление о возвращении уголовного дела 18 октября 2018 г. отменено заместителем прокурора республики, обвинительное заключение утверждено и уголовное дело направлено в суд для рассмотрения по существу, в отношении П. вынесен обвинительный приговор[1].

Не устанавливались размер и характер вреда, причиненного преступлением.

Заместителем прокурора г. Костромы 19февраля 2019 г. для производства дополнительного расследования возвращено уголовное дело по обвинению в совершении преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ, М., который незаконно завладел мобильным телефоном Р., совершил хищение денежных средств с расчетного счета потерпевшей.

Основанием для возвращения уголовного дела послужили допущенные в ходе предварительного расследования нарушения уголовно-процессуального законодательства: факт хищения М. мобильного телефона Р. незаконно выделен следователем в отдельное производство как не связанный с расследуемым преступлением, в результате чего объем похищенного у Р. имущества, сумма причиненного потерпевшей материального ущерба в обвинении, предъявленном М., занижены, стоимость похищенного телефона не установлена. По результатам дополни-

[1] По материалам деятельности прокуратуры Республики Чувашия.

тельного расследования недостатки устранены, уголовное дело направлено в суд для рассмотрения по существу.

Имелись факты непринятия следователем обеспечительных мер по гражданскому иску.

Так, в прокуратуру Кемеровской области 7 марта 2019 г. для утверждения обвинительного заключения поступило уголовное дело по обвинению О. в совершении девяти преступлений, предусмотренных ч. 2 ст. 159 УК РФ.

Изучение материалов уголовного дела показало, что обвинительное заключение не подлежало утверждению вследствие установленных нарушений уголовно-процессуального закона. Так, в нарушение требований ч. 3 ст. 152, ч. 1 ст. 160.1 УПК РФ к материалам уголовного дела не приобщено решение вышестоящего руководителя следственного органа об определении территориальной подследственности; следователем не приняты меры по установлению имущества О., стоимость которого обеспечивает взыскание штрафа, а также меры по наложению ареста на такое имущество.

Заместителем прокурора области 14 марта 2019 г. уголовное дело возвращено следователю следственной части ГСУ ГУ МВД России по Кемеровской области для производства дополнительного следствия и устранения выявленных недостатков. По результатам дополнительного следствия в июне 2019 г. уголовное дело направлено для рассмотрения по существу в Юргинский городской суд.

Прокурорами устанавливались факты направления органами предварительного расследования уголовного дела с обвинительным заключением с многочисленными нарушениями требований уголовно-процессуального законодательства.

Так, заместителем прокурора Нижегородской области возвращено уголовное дело по обвинению С. по п. «в» ч. 3 ст. 286, ч. 2 ст. 272, ч. 3 ст. 291 УК РФ. Основаниями для возвращения уголовного дела в порядке, установленном ст. 221 УПК РФ, послужило то, что при описании преступного деяния не приведены сведения о месте совершения преступления, не конкретизирован мотив преступного посягательства. Квалифицирующий признак «с наступлением тяжких последствий» должным образом не раскрыт. Также не разрешен ряд ходатайств обвиняемого, чем нарушено его право на защиту. Кроме того, в обвинительном заключении не отражено содержание ряда полученных по уголовному делу доказательств, в частности результатов осмотра предметов и документов. К уголовному делу не приобщены ответы на ряд направленных в ходе следствия запросов[1].

Обобщение практики прокурорского надзора за процессуальной деятельностью органов предварительного расследования позволяет говорить о том, что каких-либо существенных факторов правообеспечительного характера, препятствующих эффективно и в разумный срок осуществлять расследования преступлений в сфере ИКТ, в настоящее время нет. В абсолютном большинстве случаев формальные нарушения требований уголовно-процессуального закона связаны с отсутствием наступательности и инициативности следователей и до-

[1] По материалам деятельности прокуратуры Нижегородской области.

знавателей при проведении уголовных процедур. Как и по уголовным делам иных категорий, ведомственный контроль не несет существенной компенсационной функции, а создает дополнительную организационную нагрузку на надзирающих прокуроров.

Полагаем, что, если имеются основания считать уровень знаний сотрудников того или иного органа предварительного следствия МВД России в области компьютерных технологий недостаточным, а также при наличии данных, указывающих на особую сложность расследования преступлений, в том числе в сфере ИКТ, и (или) их высокую общественную значимость, прокурор может реализовывать предоставленные ему п. 12 ч. 2 ст. 37 УПК РФ полномочия по передаче материалов проверки сообщения о преступлении и уголовных дел из органа предварительного расследования федерального органа исполнительной власти следователю Следственного комитета России[1]. При этом приемлемым представляется привлечение прокурорами для получения консультаций специалистов в сфере информационной безопасности, например для получения разъяснений по техническим аспектам обработки компьютерной информации. Последнее, как представляется, является предпосылкой к постановке вопроса о возрождении института прокуроров-криминалистов в системе органов прокуратуры Российской Федерации.

Видится возможным предложить изменения действующего законодательства, которые, как нам представляется, исключили некоторые сложности в работе органов предварительного расследования.

На законодательном уровне следует предусмотреть:

— варианты межведомственного взаимодействия между операторами социальных сетей, банками, операторами сотовой связи и правоохранительными органами, решить вопрос о возможности быстрого обмена информации об IP-адресах владельцев аккаунтов в социальных сетях, их географическом местоположении. Также следует предусмотреть взаимодействие правоохранительных органов, расположенных на разных территориях для быстрого установления лиц, получивших доступ к банковским картам потерпевших, возможности создания программного обеспечения, позволяющего находить лиц, фактически похитивших денежные средства;
— открытие банковских счетов только с обязательным личным присутствием лица в банке, на которого открывается счет. В качестве предложения представляется необходимым заключать договор о предоставлении услуг связи при личном присутствии

[1] Пункт 1.5 указания Генерального прокурора Российской Федерации от 19 декабря 2011 г. № 433/49 «Об усилении прокурорского надзора за исполнением требований закона о соблюдении подследственности уголовных дел».

клиента, с копированием всех документов личности. Также актуальным является возмещение причиненного материального ущерба по делам данной категории — в законе отсутствует процессуальное право на временное блокирование банковских счетов преступника по постановлению следователя, во избежание возможности завладения денежными средствами преступником;

— включение в Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» дознавателя в перечень должностных лиц, правомочных получать без судебного решения информацию о вкладах и счетах физических лиц, операциях и счетах юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица.

В настоящее время экспертное сопровождение при раскрытии и расследовании преступлений рассматриваемой категории нуждается в комплексном совершенствовании.

Приведенные статистические данные свидетельствуют о том, что в целом органами предварительного расследования принимаются определенные меры для обеспечения возмещения причиненного преступлениями имущественного вреда.

Однако объективной причиной неудовлетворительной работы по обеспечению возмещения потерпевшим имущественного вреда остается несовершенство действующего законодательства, не позволяющего оперативно обнаруживать имущество и денежные средства, за счет которых должно осуществляться возмещение. Прежде всего, действующее нормативно-правовое регулирование не позволяет создать единую систему учета наличия имущества, вкладов (счетов) в банках и т.п. (например, для отыскания вклада (счета) в банковских учреждениях сотрудникам органов предварительного расследования необходимо направлять соответствующие запросы в десятки банков, филиалов и отделений банков; для отыскания недвижимости — в территориальные регистрирующие органы, которыми учет объектов недвижимости и их собственников ведется не в полном объеме, а только с момента создания соответствующих структур).

Необходимость и длительность получения судебных решений о наложении ареста на расчетные счета организаций, куда были перечислены похищенные денежные средства, что в итоге приводит к невозможности своевременно заблокировать их перечисление и, соответственно, вернуть потерпевшим. Эта особенность хорошо известна преступникам, например, по данным прокуратуры Республики Татарстан, пик совершения хищений приходится на четверг, как предпоследний рабочий день.

К числу проблем по возмещению ущерба можно отнести отсутствие правовых возможностей у правоохранительных органов по

принятию обеспечительных мер на стадии процессуальной проверки. В связи с этим представляется необходимым внесение в уголовно-процессуальное законодательство нормы, разрешающей производить выемку до возбуждения уголовного дела.

3.5. Прокурорский надзор за процессуальной деятельностью органов предварительного расследования при принятии процессуального решения о направлении сообщений о преступлениях и уголовных дел по подследственности

Следует отметить, что за последние годы проблемы законного и обоснованного определения подследственности уголовных дел о преступлениях, совершенных в сфере ИКТ, отмечается многими прокурорами. Как правило, сложности возникают в ситуации, когда потерпевший и злоумышленник находятся в различных административно-территориальных образованиях, а также в разных субъектах Российской Федерации.

Правоохранительные органы эффективно противодействовать этому виду правонарушениям не всегда способны в силу сложившейся и пока непреодоленной в стране практики их расследования. Причиной этого являлось отсутствие в территориальных субъектах единого подхода при определении подследственности с учетом процессуально установленных фактических данных, что, в свою очередь, приводило к многократному и зачастую необоснованному направлению материалов проверок по сообщениям о преступлениях и уголовных дел по территориальной и ведомственной подследственности, что отрицательно сказывалось на соблюдении разумных сроков уголовного судопроизводства, а также приводило к утрате доказательств и усложняло ход расследования уголовного дела.

Помимо принятия незаконных решений об отказе в возбуждении уголовного дела характерным нарушением является практика необоснованного неоднократного перенаправления таких сообщений о преступлениях из одного территориального подразделения органов внутренних дел в другое, что, в свою очередь, позволяет виновным уйти от уголовной ответственности, поскольку в большинстве случаев такие решения принимаются без выполнения каких-либо проверочных мероприятий.

К примеру, 27 июля 2019 г. в ОП № 2 в составе МУ МВД РФ «Энгельсское» Саратовской области поступило заявление С. по факту совершения неустановленным лицом противоправных действий в отношении ее малолетней дочери Х.

Данный материал органами полиции в соответствии с требованиями действующего законодательства 19 августа 2019 г. направлен по подследственности в СО по г. Энгельс СУ СК РФ по Саратовской области. В нарушение требований ст. 151 УПК РФ следственным отделом незаконно материал без регистрации

и проведения процессуальной проверки возвращен в МУ МВД РФ «Энгельсское». Сотрудниками органа дознания 29 августа 2019 г. по результатам процессуальной проверки вынесено постановление об отказе в возбуждении уголовного дела по основанию, предусмотренному п. 2 ч. 1 ст. 24 УПК РФ.

При проверке принятого процессуального решения с целью уточнения обстоятельств произошедшего надзирающим прокурором опрошены малолетняя Х. и ее законный представитель С., которые пояснили, что неустановленное лицо путем шантажа принуждало Х. присылать фотографии сексуального характера через сеть Интернет.

В связи с установленными обстоятельствами прокуратурой г. Энгельса 7 октября 2019 г. процессуальное решение об отказе в возбуждении уголовного дела отменено, а материал направлен в СО по г. Энгельс СУ СК РФ по Саратовской области для проведения процессуальной проверки, по результату которой следственным органом возбуждено уголовное дело по признакам состава преступления, предусмотренного п. «б» ч. 4 ст. 132 УК РФ.

Прокурорами отмечаются неединичные факты незаконного направления сообщений о преступлении в пределах одного или смежных административно-территориальных делений.

Так, в территориальный орган внутренних дел поступил материал по заявлению Л. о мошеннических действиях неустановленного лица, похитившего у него денежные средства на сумму 12 тыс. руб., что для него явилось значительным ущербом. Постановлением оперативного уполномоченного органа внутренних дел вынесено постановление о передаче материала по указанному факту по территориальности в орган внутренних дел смежного района. Данное решение надзирающим прокурором признано незаконным и необоснованным, отменено ввиду наличия признаков преступления. Материал передан в орган предварительного следствия, которым возбуждено уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ[1].

6 мая 2019 г. в ОП № 6 в составе УМВД России по г. Саратову зарегистрировано заявление Н. о мошеннических действиях неизвестного лица, которое под предлогом приобретения в сети Интернет запчастей для автомобиля похитило денежные средства в размере 19 тыс. руб. Сотрудниками территориального отдела полиции необоснованно данный материал проверки без согласования с прокуратурой района 7 июня 2019 г. направлен по территориальности в ОП № 3 в составе УМВД России по г. Саратову, откуда впоследствии 20 июня 2019 г. возвращен в ОП № 6 в составе УМВД России по г. Саратову. Прокурором Фрунзенского района г. Саратова 17 июля 2019 г. в ходе проверки материалов, находящихся в производстве сотрудников ОП № 6 в составе УМВД России по г. Саратову, обнаружен указанный материал, который повторно планировался к направлению по территориальности. С целью пресечения факта принятия незаконного решения надзирающим прокурором по материалу даны письменные указания о направлении материала в ОД ОП № 6 в составе УМВД России по г. Саратову с требованием о возбуждении уголовного дела по ч. 1 ст. 159 УК РФ.

[1] По материалам деятельности прокуратуры Томской области.

17 июля 2019 г. возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 1 ст. 159 УК РФ.

Также имеются факты многократного незаконного направления материалов проверки сообщения о преступлении.

Так, при наличии в материале проверки данных, указывающих на наличие в действиях Л. признаков преступления, предусмотренного ч. 1 ст. 137 УК РФ, следователем 24 января 2019 г. было вынесено незаконное и необоснованное постановление о передаче заявления о преступлении и материала проверки по подследственности в отделение МВД России по Беляевскому району. При этом фактически материал проверки передан в отделение МВД России по Беляевскому району лишь 6 февраля 2019 г.

Отделением МВД России по Беляевскому району указанный материал проверки 9 февраля 2019 г. вновь направлен в Саракташский МСО СУ СК РФ по Оренбургской области по подследственности. Между тем следователем в установленный ч. 1 ст. 144 УПК РФ срок проверка сообщения о преступлении не проведена.

19 марта 2019 г. следователем вновь вынесено незаконное постановление о передаче заявления о преступлении и материала проверки по подследственности в отделение МВД России по Беляевскому району. Отделением МВД России по Беляевскому району указанный материал проверки 23 марта 2019 г. вновь направлен в Саракташский МСО СУ СК РФ по Оренбургской области по подследственности.

В связи с тем, что в ходе изучения указанного материала были выявлены нарушения требований ст. 6.1 и ст. 144–145 УПК РФ, прокуратурой района 25 марта 2019 г. в адрес руководителя Саракташского МСО СУ СК РФ по Оренбургской области направлена информация, по результатам рассмотрения которой за нарушения по указанному материалу проверки следователь приказом руководителя следственного управления Следственного комитета Российской Федерации по Оренбургской области привлечена к дисциплинарной ответственности в виде объявления выговора[1].

Отмечаются факты направления материалов проверки сообщения о преступлении с грубым нарушением предметной подследственности.

Например, в ОД МО МВД необоснованно передано сообщение органами следствия заявление К., поступившее 9 сентября 2019 г., о том, что 9 сентября 2019 г. ею утеряна карта «МИР», с которой неизвестные лица совершили покупки на сумму 6 тыс. руб. 11 сентября 2019 г. начальником СО МО МВД России «Эхирит-Булагатский» вынесено постановление о передаче материала в ОД МО МВД России «Эхирит-Булагатский». При наличии в действиях М. признаков преступления, предусмотренного ст. 158 ч. 3 п. «г» УК РФ, расследование которых осуществляется следователями, материал по формальным основаниям передан в отдел дознания, которым далее было принято решение об отказе в возбуждении уголовного дела. Данное решение отменено прокуратурой района как незаконное

[1] По материалам деятельности прокуратуры Оренбургской области.

и необоснованное, материал передан в следственный отдел, которым возбуждено уголовное дело по ст. 158 ч. 3 п. «г» УК РФ[1].

В ряде субъектов нарушения требований законодательства выявлялись прокурорами уже на этапе направления уголовного дела с обвинительным заключением для утверждения.

Так, 1 ноября 2019 г. в прокуратуру г. Южно-Сахалинска для утверждения обвинительного заключения в порядке, установленном ст. 220 УПК РФ, поступило уголовное дело по обвинению несовершеннолетнего М. в совершении преступления, предусмотренного п. «в» ч. 3 ст. 158 УК РФ, по факту хищения денежных средств в размере 2900 руб., принадлежащих К. Изучение материалов уголовного дела показало, что следственным органом при предъявлении обвинения были нарушены требования ст. 73, 171 УПК РФ в части отсутствия сведений о месте совершения преступления.

Так, в ходе расследования установлено, что обвиняемый М. в период времени с 9 ноября 2018 г. по 19 ноября 2018 г. с мобильного телефона К. с помощью услуги «Мобильный банк» путем перевода с банковского счета последнего похитил 2900 руб., которые перевел на банковский счет Б. По общему правилу преступление, предусмотренное ст. 158 УК РФ, считается оконченным с момента изъятия имущества и наличия реальной возможности им пользоваться и распоряжаться по своему усмотрению. При этом в случае, если предметом преступления являются безналичные денежные средства, в том числе электронные денежные средства, такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб.

Вместе с тем при предъявлении обвинения М. следственным органом не указаны наименование и адрес банка, с которого были похищены денежные средства потерпевшего, а также наименование и адрес банка, в котором открыт счет Б., на который были переведены денежные средства потерпевшего и которыми обвиняемый получил реальную возможность распорядиться по своему усмотрению. По результатам дополнительного расследования нарушения устранения 19 декабря 2019 г. уголовное дело направлено для рассмотрения по существу в Южно-Сахалинский городской суд.

Основные проблемы, указанные прокурорами, связаны с неоднозначностью практической реализации положений федерального законодательства, регламентирующих вопросы определения места совершения преступления и места (момента) окончания преступления.

При отсутствии в материалах проверки информации о месте совершения преступления и месте его окончания далеко не всегда органы предварительного расследования незамедлительно возбуждают уголовные дела.

Так, 30 января 2019 г. в прокуратуру Центрального района г. Воронежа поступил материал проверки по факту совершения противоправных действий в отношении Б. с постановлением следователя МВД о направлении указанного

[1] По материалам прокуратуры Иркутской области.

материала проверки в ОП № 3 УМВД России по г. Воронежу. Изучением материала проверки в прокуратуре района установлено, что из объяснения последнего объективно не усматривается, что он отправлял товары из места своего проживания, то есть место совершения указанного преступления не установлено, а его регистрация произошла в ОП № 6 УМВД России по г. Воронежу. Таким образом, решение следователя о направлении указанного материала проверки в ОП № 3 явилось незаконным. Материал проверки возвращен в следственный орган, 8 марта 2019 г. следователем возбуждено уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ.

В соответствии с положениями постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», если предметом преступления при мошенничестве являются безналичные денежные средства, такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца, в результате которого владельцу этих денежных средств причинен ущерб. Таким образом, местом совершения преступления является место открытия банковского счета, с которого похищены денежные средства потерпевших. Однако по уголовным делам данной категории преступлений нередки случаи, когда уголовное дело расследуется по месту нахождения виновного лица; при этом банковские счета, с которых похищаются денежные средства, открыты в разных субъектах Российской Федерации. В таких случаях в порядке, установленном ст. 152 УПК РФ, по каждому уголовному делу необходимо определить место производства предварительного расследования, что влияет на сроки предварительного следствия.

Как показало проведенное исследование, практически в абсолютном большинстве территориальных субъектов в деятельности органов предварительного расследования имеются существенные проблемы с определением места расследования преступлений по сообщениям о совершении хищений в сфере ИКТ денежных средств с банковских карт потерпевших. Рассматриваемые преступления, как правило, имеют трансграничный и высокотехнологичный характер, не позволяющий своевременно и однозначно определить точное место его совершения.

Так, возникает вопрос места производства предварительного расследования в случаях, когда с банковской карты происходит несанкционированный владельцем (держателем) данной карты перевод денежных средств путем услуг «Мобильный банк» либо интернет-банкинг на банковскую карту злоумышленника или счет его мобильного телефона.

В таких ситуациях практически невозможно определить место нахождения злоумышленника. При этом, если в случае перевода денежных средств на счет мобильного телефона можно определить место

и время его выхода в эфир в момент непосредственного зачисления на счет, то в случае перевода денежных средств с одной банковской карты на другую практически невозможно определить конкретное место проведения активных действий по принудительному (помимо воли потерпевшего) электронному переводу.

Также следует отметить, что в случае обналичивания денежных средств, переведенных помимо воли потерпевшего, возможно определить место нахождения в данный момент злоумышленника.

Однако на практике возникает вопрос о месте окончания преступления в случае, если обналичивание произошло спустя продолжительное (более суток) время после перевода денежных средств потерпевшего либо не происходило вообще (совершен перевод денежных средств на третью банковскую карту, в QIWI, Yandex кошелек, либо произведена оплата за услугу или товар в интернет-магазине и т.п.).

Аналогичные вопросы (денежные средства не обналичивались либо обналичивались через продолжительное время) возникают и в случаях хищения путем обмана и злоупотребления доверием денежных средств, переведенных потерпевшими со своих банковских карт.

Положения п. 7 ч. 3 Положения о едином порядке организации приема, регистрации и проверки сообщений о преступлениях, утвержденного приказом Генпрокуратуры РФ № 39, МВД РФ № 1070, МЧС РФ № 1021, Минюста РФ № 253, ФСБ РФ № 780, Минэкономразвития РФ № 353, ФСКН РФ № 399 от 29 декабря 2005 г. «О едином учете преступлений», в случае, если не представляется возможным определить место совершения *преступления,* оно подлежит учету по месту его выявления, по понятным причинам не всегда применяются на практике: следователи после поступления к ним сообщения о преступлении вместо незамедлительного проведения необходимых процессуальных действий необоснованно направляли его в другой орган предварительного расследования.

Так, прокурором Пензенского района установлен факт необоснованной передачи по территориальности сообщения о мошеннических действиях в отношении М. В ходе проведенной доследственной проверки установлено, что М. зарегистрировался на сайте suprafn.com и перечислил через платформу сайта денежные средства в сумме 2203 тыс. руб.

При этом денежные средства перечислялись с банковской карты ПАО «Сбербанк России», счет которой открыт в дополнительном офисе, расположенном на территории оперативного обслуживания ОМВД России по Пензенской области.

Вместе с тем 24 января 2019 г. по сообщению вынесено постановление о передаче сообщения в ОП № 5 УМВД России по г. Пензе, которое мотивировано невозможностью установления места совершения преступления.

Указанное постановление прокурором района отменено; по выявленным нарушениям начальнику ОМВД России по Пензенскому району направлено требование, которое рассмотрено и удовлетворено, 3 должностных лица привлечены

к дисциплинарной ответственности. По результатам дополнительной проверки возбуждено уголовное дело по ч. 4 ст. 159 УК РФ.

На практике отмечается несколько подходов определения органами дознания и предварительного следствия места производства расследования преступления.

Одним из вариантов является определение места предварительного расследования по месту нахождения потерпевшего.

К примеру, 2 августа 2019 г. в ОП № 3 УМВД России по г. Тюмени поступило заявление М. о хищении денежных средств с банковского счета. По результатам доследственной проверки начальником смены дежурной части ОП № 3 УМВД России по г. Тюмени вынесено постановление о передаче сообщения о преступлении по территориальности в ОП № 4 УМВД России по г. Тюмени, мотивированное местонахождением М. в момент хищения денежных средств с банковского счета по адресу: г. Тюмень, ул. Ленина, остановочный комплекс «Центральный рынок». 5 августа 2019 г. данное решение заместителем прокурора Ленинского АО г. Тюмени отменено, поскольку местонахождение заявительницы в момент обнаружения хищения денежных средств не определяет места совершения преступления. Материалы проверки направлены в СО ОП № 3 СУ УМВД России по г. Тюмени для организации дополнительной проверки и принятия законного решения. По результатам проверки 19 августа 2019 г. по факту хищения денежных средств с банковского счета М. возбуждено уголовное дело по п. «г» ч. 3 ст. 158 УК РФ, производство по которому 19 октября 2019 г. приостановлено на основании п. 1 ч. 1 ст. 208 УК РФ в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого.

В 2018 г. ОМВД России по Октябрьскому району г. Рязани зарегистрировано заявление З., из которого следовало, что она посредством сети Интернет забронировала проживание в доме отдыха, находящемся в Республике Абхазия, после чего ей посредством электронной почты высланы реквизиты для оплаты брони, по которым заявитель осуществила перевод денежных средств на общую сумму 127,5 тыс. руб. Однако сайт, на котором осуществлялось бронирование, оказался фиктивным и использовался неустановленными лицами в целях хищения денежных средств.

Однако вместо принятия незамедлительных мер к установлению лиц, завладевших денежными средствами заявителя, органом дознания в нарушение требований ст. 151, 152 УПК РФ и п. 7 Положения о едином порядке регистрации уголовных дел и учета преступлений, утвержденного совместным приказом Генпрокуратуры России, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России, ФСКН России от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399 «О едином учете преступлений», принято решение о направлении материала в ОМВД России по Советскому району г. Рязани на основании того, что в момент перечисления денежных средств заявитель находилась на территории обслуживания указанного территориального органа внутренних дел.

В течение 2018 г. материал проверки неоднократно передавался по территориальной подследственности между указанными органами внутренних дел, во всех случаях по одним и тем же основаниям. По результатам очередной дополнитель-

ной проверки органом дознания ОМВД России по Советскому району г. Рязани принято решение о передаче данного сообщения о преступлении по территориальной подследственности в МО МВД России «Касимовский» на основании того, что банковский счет, с которого заявителем переведены денежные средства, открыт в отделении ПАО «Сбербанк России», находящемся в г. Касимов Рязанской области. После вмешательства прокурора местом производства процессуальной проверки определено в ОМВД России по Октябрьскому району г. Рязани.

Следующим достаточно распространенным вариантом является определение места совершения преступления по месту открытия банковского счета.

Так, 1 октября 2018 г. в ГУ МВД России Кемеровской области поступил материал по факту мошеннических действий в отношении П. Из материала проверки следует, что 23 февраля 2018 г. в дежурную часть ГУ МВД России по г. Москве обратилась П., которая сообщила, что она по предложению неустановленного лица зарегистрировалась на сайте «Fxnet.trade», после пополнения счета не принимала участия в торгах. Все торговые операции производились неустановленным лицом, назвавшимся «Ждановым Сергеем». Самостоятельно П. не имела возможности вывести денежные средства со счета, а также производить с данными денежными средствами какие-либо операции, что свидетельствует о том, что лицо под именем «Жданов Сергей» имело свободный доступ в личный кабинет клиента П.

Из вышеизложенного следует, что с момента, когда денежные средства были переведены П. с банковских счетов на торговый счет, злоумышленники получили реальную возможность распоряжаться денежными средствами, при этом П. фактически утратила возможность распоряжения деньгами. Таким образом, с момента изъятия денежных средств со счета П. преступление — хищение безналичных денежных средств путем обмана или злоупотребления доверием является оконченным, а местом совершения данного преступления является место открытия (нахождения) счета потерпевшего. Принимая во внимание, что последнее зачисление денежных средств на торговый счет осуществлено П. с банковского счета, открытого в г. Новокузнецке, в соответствии с требованиями ст. 152 УПК РФ предварительное расследование преступления должно производиться в г. Новокузнецке.

На определение места совершения преступления по месту открытия банковского счета ориентированы и поднадзорные органы предварительного расследования.

Так, по материалу проверки по сообщению о хищении денежных средств со счета О. вынесено постановление об отказе в возбуждении уголовного дела. Указанное решение принято с нарушением требований ст. 150–151 УПК РФ органом дознания, а не органом следствия. Кроме того, в соответствии с указанием МВД РФ № 1/5562 от 13 июля 2015 г. «Об организации работы по противодействию отдельным видам мошенничества», при поступлении заявления (сообщения) о совершении мошеннических действий с использованием мобильных средств связи принимать решение о возбуждении уголовного дела обязан территориальный орган, принявший заявление (сообщение). По сложившейся

практике, местом преступления является место открытия счета, с которого похищены денежные средства. В ОМВД России по Краснокамскому городскому округу материал со стороны органа дознания ОП № 1 был направлен необоснованно. Постановление об отказе в возбуждении уголовного дела отменено 6 августа 2019 г., по результатам дополнительной проверки 2 сентября 2019 г. материал направлен в ОП № 1 УМВД РФ по г. Перми[1].

На практике встречаются процессуальные решения, в основу которых положены факты, не связанные с местом открытия счета и с местом совершения преступления.

В 2019 г. МО МВД России «Куменский» для принятия решения в порядке ст. 144–145 УПК РФ из МО МВД России «Слободской» поступил материал по сообщению о хищении у Л. неустановленным лицом денежных средств в сумме 5500 руб. В частности, Л. на сайте «Авито» нашел объявление о сдаче в наем квартиры в г. Слободском и после разговора с риелтором по телефону внес предоплату за съем квартиры. Материал по территориальности возвращен в МО МВД России «Слободской», которым он снова перенаправлен в МО МВД России «Куменский». При его изучении в прокуратуре района установлено, что перечисление Л. денежных средств на счет злоумышленника происходило с банковского счета, который открыт и обслуживается в отделении ПАО «Сбербанк», расположенном в п. Кумены. Место совершения преступления, личность преступника, а также место обналичивания похищенных денежных средств установлены не были[2].

Также на практике принимались процессуальные решения, по которым принимался во внимание не тот территориальный субъект, где открыт банковский счет, а тот счет, куда переведены деньги потерпевших.

Например, прокуратурой Республики Ингушетия проведена проверка законности направления материала проверки по территориальной подследственности в ГУ МВД России по Ростовской области по факту мошеннических действий в отношении Б.

Оперуполномоченным УЭБ и ПК МВД России по Республике Ингушетия принято решение о передаче материалов проверки по территориальной подследственности в ГУ МВД России по Ростовской области в связи с тем, что денежные средства в размере 913 822 руб., принадлежащие Б., в интересах последнего перечислены ООО «Нектар» на расчетный счет ООО «Дон-Продукт», открытый в Юго-Западном банке ПАО «Сбербанк», расположенном в г. Ростов-на-Дону.

Учитывая, что расчетный счет ООО «Нектар», с которого осуществлен перевод денежных средств, открыт в Ингушском региональном филиале АО «Россельхозбанк» в г. Назрани, то местом окончания преступления является г. Назрань. Данные обстоятельства свидетельствовали о наличии в действиях неустановленного лица признаков преступления, предусмотренного ч. 3 ст. 159 УК РФ, в связи с чем 17 января 2019 г. постановление оперуполномоченного УЭБ и ПК России по Республики Ингушетия отменено в прокуратуре республики. Дополнительная проверка по материалу поручена ОМВД России по

---

[1] По материалам деятельности прокуратуры Пермского края.

[2] По материалам деятельности прокуратуры Кировской области.

г. Назрань, где 5 февраля 2019 г. возбуждено уголовное дело по признакам преступления, предусмотренного ч. 3 ст. 159 УК РФ.

Место открытия банковского счета не всегда являлось безусловным основанием для направления материалов проверки сообщения о преступлении по территориальности, на что надзирающие прокуроры обращали внимание.

Так, установлено, что Г. в 2018 г. перевел за покупку вариатора по объявлению, размещенному в сети Интернет, от автомагазина денежные средства в сумме 8500 руб. на карту неустановленного лица, представившегося продавцом, однако товар не получил, в связи с чем обратился в орган внутренних дел другого субъекта, сотрудниками которого сообщение передано в территориальный орган внутренних дел Томской области со ссылкой на положения п. 5 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». Основанием для направления материала послужили сведения о месте открытия счета Г. на территории Томской области. В то же время изучением материала установлено, что лица, имеющие отношение к произошедшему, проживают на территории иного субъекта, не в Томской области, они не опрошены; кроме того не установлены сведения о счете, на который Г. переведены денежные средства, а также о лице, с которым заявитель осуществлял контакт. С учетом изложенного, а также на основании ч. 4 ст. 152 УПК РФ сообщение по данному факту возвращено для организации дальнейшей проверки.

Место предварительного расследования определялось надзирающим прокурором по месту снятия денежных средств потерпевшего через банкомат.

К примеру, изучением в аппарате прокуратуры области материала по заявлению К. о хищении его денежных средств, поступившего из прокуратуры Краснодарского края и неоднократно направлявшегося по территориальной подследственности между правоохранительными органами Краснодарского края и г. Санкт-Петербурга, установлено, что 24 декабря 2018 г. К., находясь на территории г. Санкт-Петербурга, утратил портмоне с банковскими картами, а 25 декабря 2018. с одной из них неустановленным лицом были похищены денежные средства в сумме 50 тыс. руб.; при этом их снятие произошло через банкомат, расположенный на территории Ленинградской области. По результатам проверки СУ УМВД России по Всеволожскому району возбуждено уголовное дело[1].

Следует также указать на решение прокурора, «привязанное» к месту изъятия банковской карты, используемой в процессе совершения преступления.

Например, 17 сентября 2019 г. первым заместителем прокурора области заместителю прокурора Смоленской области направлен материал проверки сообщения о совершении мошеннических действий в отношении В. Из материала проверки следует, что сотрудники Управления МВД России по Смоленской области в ходе проведения оперативно-разыскных мероприятий установили, что к совершению

[1] По материалам деятельности прокуратуры Ленинградской области.

преступления причастны лица, проживающие на территории Смоленской области, которые под предлогом осуществления выплаты компенсации вкладчикам ООО «МММ» совершали мошенничества в отношении граждан. Потерпевшие, будучи введенными в заблуждение, перечисляли денежные средства на банковскую карту, на которую также перевела деньги В. Данная банковская карта была изъята сотрудниками Управления МВД России по Смоленской области в ходе проведения ОРМ. Принимая во внимание изложенное, в соответствии с требованиями ч. 4 ст. 152 УПК РФ материал обоснованно был направлен в прокуратуру Смоленской области для организации проверки сообщений о преступлении.

Место проведения расследования определено по месту реальной возможности использовать похищенное имущество.

Так, 16 октября 2019 г. в ОП № 3 УМВД России по г. Владимиру поступило заявление Ш. о совершении в отношении него мошеннических действий, выразившихся в завладении имуществом при выполнении перевозки груза. По результатам проверки в порядке ст. 144, 145 УПК РФ ОУР УМВД России по г. Владимиру 21 октября 2019 г. принято решение о передаче сообщения о преступлении по территориальной подследственности в ОМВД России по району Метрогородок г. Москвы.

Данное постановление 25 октября 2019 г. отменено заместителем прокурора г. Владимира, поскольку злоумышленник осуществлял связь с покупателем и продавцом посредством телефона и получил реальную возможность распоряжаться грузом при его вывозе со склада в г. Владимире. По результатам дополнительной проверки СО ОП № 3 УМВД России по г. Владимиру 31 октября 2019 г. возбуждено уголовное дело по ч. 3 ст. 159 УК РФ, производство предварительного расследования по которому 31 декабря 2019 г. приостановлено на основании п. 1 ч. 1 ст. 208 УПК РФ.

Встречаются примеры, когда на определение места расследования повлияли установленные в ходе проверки сообщения о преступлении обстоятельства о месте открытия банковского счета и места проживания виновных лиц.

Так, 29 марта 2019 г. в МО МВД России «Завьяловский» зарегистрировано заявление Ш. по факту хищения сотового телефона «Honor-7A» и денежных средств в сумме 271 800 руб. с его банковского счета с помощью мобильного приложения «Сбербанк Онлайн». Установлено, что Ш. 26 марта 2019 г. находился по адресу: г. Новосибирск, пер. 1-й Петропавловский, 14–1, где распивал спиртные напитки с неизвестными лицами. В связи с плохим самочувствием Ш. был госпитализирован в больницу. В это время неустановленными лицами из указанного адреса был похищен его сотовый телефон «Honor-7A». Впоследствии с его банковского счета, открытого в офисе ПАО «Сбербанк» в г. Новосибирске, с помощью мобильного приложения «Сбербанк Онлайн» были похищены денежные средства в сумме 271 800 руб., которые переведены на счета банковских карт жителей г. Новосибирска И., П.А.А., П.С.А., а также на абонентские номера, принадлежащие оператору сотовой связи «ТЕЛЕ 2» и ООО «Скартел». Поскольку преступление совершено на территории г. Новосибирска, материалы проверки направлены в прокурату-

ру Новосибирской области для организации проверки в порядке, установленном ст. 144–145 УПК РФ.

Как видно из приведенных примеров на практике возникают многочисленные сложности с определением места совершения преступления. Справедливости ради следует отметить, что далеко не всегда на практике можно с очевидностью определить территориальную «привязку» подследственности материалов по сообщению о преступлении, в которых фигурирует открытый банковский счет.

К примеру, в июне 2019 г. надзирающим прокурором изучен материал проверки, проведенной по факту оформления неустановленным лицом с использованием паспортных данных М. микрозайма в ООО «МКУФ в размере 5600 руб. Органом дознания изучены сведения, представленные ООО «МКУФ», в том числе договор микрозайма, из содержания которого следует, что расчетный счет ООО «МКУФ» открыт в филиале банка ВТБ (ПАО) в г. Ростове-на-Дону. В этой связи с учетом положений п. 5 постановления Пленума Верховного суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате органом дознания сделан вывод, что денежные средства неустановленному лицу, действовавшему от имени М., переведены с расчетного счета ООО «МКУФ», открытого в филиале банка ВТБ (ПАО) в г. Ростове-на-Дону. С учетом изложенного, 17 июня 2019 г. начальником полиции ОМВД России по г. Магадану принято процессуальное решение о передаче сообщения о преступлении по подследственности в УМВД России по г. Ростов-на-Дону.

Надзирающим прокурором установлено, что постановление о передаче сообщения о преступлении по подследственности от 17 июня 2019 г. не отвечает требованиям УПК РФ, обстоятельства произошедшего в ходе проверки в полном объеме не установлены, факт указания ООО «МКУФ» в договоре микрозайма номера расчетного счета, открытого в филиале банка ВТБ (ПАО) в г. Ростове-на-Дону, сам по себе не свидетельствует о том, что указанный счет Общества является единственным и именно с него осуществлен перевод денежных средств неустановленному лицу, действовавшему от имени М. Кроме того, из информации ООО «МКУФ» следовало, что выдача микрозайма осуществлена микрофинансовой организацией с помощью платежной системы ООО НКО «Яндекс.Деньги», что позволяет прийти к выводу о том, что денежные средства списаны не с расчетного счета, открытого в филиале банка ВТБ (ПАО) в г. Ростове-на-Дону, а с электронного кошелька ООО «МКУФ», открытого в платежной системе «Яндекс.Деньги».

Таким образом, объективных данных, позволяющих судить о том, что денежные средства в размере 5600 руб. перечислены со счета, открытого в филиале банка ВТБ (ПАО) в г. Ростове-на-Дону, не имелось, в связи с чем 20 июня 2019 г. постановление о передаче сообщения о преступлении по подследственности отменено, материал проверки возвращен в орган дознания для проведения дополнительных проверочных мероприятий. ОД ОМВД России по г. Магадану по данному

факту по признакам преступления, предусмотренного ч. 1 ст. 159.1 УК РФ возбуждено уголовное дело[1].

Это также касается примеров из практики, когда место действия потерпевшего в момент совершения преступления и местонахождения открытия счета не идентично.

Так, 29 августа 2019 г. в ОМВД России по Чернышевскому району поступил материал проверки из ОП «Центральный» УМВД России по г. Туле о том, что в ноябре 2018 г., находясь в г. Тула, П. на сайте «Сравни.ru» оставила заявку на кредит. Через некоторое время ей поступил звонок, неизвестный представился сотрудником Московского коммерческого банка «Госкредит», который пояснил, что ее заявка одобрена банком и ей готовы выплатить кредит. При этом заявительнице необходимо было оплатить транспортировку денежных средств в сумме 5 тыс. руб. Данную сумму П. перевела через терминал, расположенный в магазине «Спар» по адресу: г. Тула, ул. М. Горького, 7. Затем потерпевшей неоднократно поступали звонки о необходимости оплаты различных услуг за получение кредита (страховка, курьер). В общей сложности у заявительницы похищены денежные средства в сумме 150 тыс. руб.

Изучением материала в прокуратуре края установлено, что 21 августа 2018 г., П., будучи введенной в заблуждение неустановленным лицом, перевела денежные средства в размере 150 тыс. руб. за предоставления кредита со своего банковского счета ПАО «Сбербанк России», открытого в подразделении ПАО «Сбербанк России», расположенном по адресу: Забайкальский край, пгт. Чернышевск ул. Центральная д. 23, что является территорией административного обслуживания ОМВД России по Чернышевскому району Забайкальского края.

По смыслу абзаца 1, 2 п. 5 постановления Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» «мошенничество, то есть хищение чужого имущества, совершенное путем обмана или злоупотребления доверием, признается оконченным с момента, когда указанное имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность (в зависимости от потребительских свойств этого имущества) пользоваться или распорядиться им по своему усмотрению. Таким образом, в действиях неустановленного лица усматривались признаки преступления, предусмотренного ч. 2 ст. 159 УК РФ. Кроме этого, П. после совершения в отношении нее преступления переехала на постоянное место жительства в Забайкальский край.

На основании изложенного процессуальное решение о возбуждении уголовного дела по заявлению П. должно было быть принято сотрудником ОМВД России по Чернышевскому району, однако вместо этого было вынесено постановление о передаче материала по подследственности в г. Тулу, тем самым укрывалось от учета преступление путем незаконной передачи по подследственности. После принятия мер прокурорского реагирования в адрес начальника отдела полиции

[1] По материалам деятельности прокуратуры Магаданской области.

24 октября 2019 г. по заявлению П. возбуждено уголовное дело по ч. 2 ст. 159 УК РФ[1].

Встречались сложности с определением места совершения преступления с учетом невозможности определения места открытия банковского счета.

Например, 23 апреля 2019 г. в ОМВД России по Александровскому району из ОМВД России по Комсомольскому району Ивановской области поступил материал проверки по заявлению представителя ООО МФК «Смартмани.ру» о привлечении к ответственности Т. по ст. 159.1 УК РФ. Установлено, что 30 марта 2018 г. через официальный сайт ООО МФК «Смартмани.ру» Т. заполнена заявка на получение займа в сумме 7 тыс. руб. со сроком погашения 16 июля 2018 г., после чего заемщику переведены денежные средства, которые не возвращены. Основанием для направления материала являлось установление факта подачи заявления на займ с IP-адреса в г. Александрове.

Однако в соответствии с п. 5 постановления Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г., если предметом преступного деяния при мошенничестве являются безналичные (электронные) денежные средства, его следует считать оконченным с момента их изъятия с банковского счета их владельца, в результате которого последнему причинен ущерб.

Поскольку сведений о месте открытия расчетного счета, с которого Т. переведены денежные средства, не имелось, органом дознания 17 июня 2019 г. принято решение о возвращении материала в ОМВД России по Комсомольскому району Ивановской области как необоснованно направленное.

Также прокурорами обращается внимание на сложности в определении момента окончания преступления. Отмечаются примеры, когда момент окончания преступления определяется с момента зачисления денежных средств на счет преступника.

Органы предварительного расследования ориентировались прокурорами на то, что моментом окончания дистанционного мошенничества следует считать момент зачисления денежных средств на счет мошенника — на его телефон либо QIWI-кошелек, то есть тот момент, когда у него появляется реальная возможность распоряжаться полученными денежными средствами.

Кроме того, в ходе надзора следует учесть, что, согласно п. 4, 12 постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате», мошенничество, то есть хищение чужого имущества, совершенное путем обмана или злоупотребления доверием, признается оконченным с момента, когда указанное имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность (в зависимости от потребительских свойств этого

[1] По материалам деятельности прокуратуры Забайкальского края.

имущества) пользоваться или распорядиться им по своему усмотрению. В соответствии со ст. 140 Гражданского кодекса Российской Федерации платежи на территории Российской Федерации осуществляются путем наличных и безналичных расчетов, то есть находящиеся на счетах в банках денежные суммы могут использоваться в качестве платежного средства.

Исходя из этого, с момента зачисления денег на банковский счет лица, оно получает реальную возможность распоряжаться поступившими денежными средствами по своему усмотрению, например осуществлять расчеты от своего имени или от имени третьих лиц, не снимая денежных средств со счета, на который они были перечислены в результате мошенничества.

Так, в ОМВД России по Колпинскому району зарегистрировано заявление представителя ООО МКФ «Смартмани.ру» о том, что П. 4 апреля 2019 г. путем акцепта публичной оферты заключен договор займа 14 тыс. руб. на 73 дня. Договор заключен через официальный сайт «smartcredit.ru». В связи с непогашением задолженности по договору и утратой связи заявитель полагает, что заемщик получил денежные средства, не намереваясь их возвращать.

В ходе проверки по данному заявлению установлено, что выдача займа осуществлялась с банковского счета в АО «Альфа Банк» (ДО «Дорогомиловский»), расположенного по адресу: Москва, ул. Дорогомиловская, д. 1.

Согласно п. 5 постановления Пленума Верховного Суда Российской Федерации от 30 января 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» следует, что мошенничество признается оконченным с момента, когда имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность пользоваться или распоряжаться им по своему усмотрению. Если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб. В данной связи местом происшествия является территория оперативного обслуживания ОМВД России по району Дорогомилово г. Москвы, в связи с чем 26 декабря 2019 г. принято решение о передаче сообщения о преступлении в ОМВД России по району Дорогомилово г. Москвы[1].

Имелись сложности при определении места окончания преступления посредством определения места открытия и обслуживания банковского счета потерпевшего.

Например, по заявлению М. о хищении принадлежащих ей денежных средств с банковской карты в размере 14 тыс. руб. органом дознания УМВД России по г. Кирову вынесено постановление о направлении сообщения о преступлении в ОП № 7 УМВД России по г. Новосибирску. При проверке материала в прокуратуре Ле-

[1] По материалам деятельности прокуратуры Санкт-Петербурга.

нинского района г. Кирова установлено, что расчетный счет банковской карты, откуда похищены денежные средства заявительницы, открыт и обслуживается в ПАО «Сбербанк России» в г. Кирове, который и будет являться местом окончания преступления. Постановление о передаче сообщения отменено, по требованию прокурора 16 мая 2019 г. возбуждено уголовное дело по ч. 2 ст. 159 УК РФ[1].

Прокуратурой г. Астрахани возвращено для дополнительного расследования уголовное дело по обвинению генерального директора управляющей компании А. в совершении преступлений, предусмотренных ч. 4 ст. 160, ч. 3 ст. 159 УК РФ, и бывшего генерального директора Б. в совершении преступлений, предусмотренных ч. 3 ст. 33, ч. 4 ст. 160, ч. 3 ст. 159 УК РФ, которые похитили денежные средства в размере 1 703 918 руб. с расчетного счета ООО «Дом-Сервис», принадлежащие собственникам домов по ул. Дзержинского и Жилая г. Астрахани. Основанием для возвращения уголовного дела явилось отсутствие в материалах дела сведений об открытии расчетного счета ООО «Дом-Сервис» именно в дополнительном офисе ПАО «Сбербанк России», расположенном на территории Кировского района г. Астрахани, что не позволило достоверно утверждать, что местом окончания преступления являлся указанный адрес.

Прокурорами отмечаются нарушения, связанные с определением территориальной подследственности уголовных дел.

Например, невзирая на указание МВД России от 13 июля 2015 г. № 1/5562 «Об организации работы по противодействию отдельным видам мошенничества» и приказ Министерства внутренних дел Российской Федерации от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений», предписывающий практику расследования дел по месту совершения мошеннических действий, а не наступления их последствий Следственный департамент МВД России возвращает в СУ УМВД России ранее переданные им по территориальной подследственности уголовные дела с указаниями на неполноту следствия, устранить которую можно только по месту совершения объективной стороны преступления.

Имеют место и случаи возвращения по мотивам невозобновления следствия уголовных дел, направленных по подследственности после приостановления их расследования, что, на наш взгляд, противоречит закону, поскольку ч. 3 ст. 209 УПК РФ запрещает после приостановления предварительного следствия производство только следственных действий, тогда как постановление о приостановлении следствия является, согласно п. 33 ст. 5 УПК РФ, процессуальным решением[2].

Таким образом, основными причинами отмены руководителями следственных органов решений о передаче сообщений по подследственности (территориальности) по требованиям прокуроров являлись неполнота проверки, а также отсутствие единообразной практики применения положений п. 5 постановления Пленума Верховного Суда РФ

[1] По материалам деятельности прокуратуры Кировской области.

[2] По материалам деятельности прокуратуры Архангельской области.

от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

В одном случае местом окончания хищений, предметом которых являются безналичные денежные средства, судом определяется место открытия счета, в другом — место, где непосредственно выполнялись действия, входящие в объективную сторону состава преступления, вне зависимости от того, что последствия наступили на другой территории, а также по месту наступления общественно опасных последствий или обращения потерпевшего в правоохранительные органы.

Невозможность установления места совершения преступления является достаточно распространенным основанием возвращения судом уголовного дела прокурору в порядке, установленном ст. 237 УПК РФ (такие решения принимались судами Краснодарского края, Амурской, Брянской, Томской областей, г. Москвы и др.).

Например, Октябрьским районным судом Амурской области 13 ноября 2018 г. в порядке, установленном ст. 237 УПК РФ, прокурору возвращено уголовное дело по обвинению М. в совершении преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ.

Свое решение суд обосновал тем, что в обвинительном заключении не отражено место открытия банковского счета, а также отсутствуют сведения о расчетном счете (в обвинительном заключении указан лишь номер банковской карты, с которой произведено хищение), в связи с чем место совершения преступления не установлено и определить территориальную подсудность рассмотрения уголовного дела не представляется возможным.

В то же время в Республике Бурятия аналогичное решение суда первой инстанции на основании представления прокурора отменено апелляционной коллегией по уголовным делам Верховного Суда Республики Бурятия отменено.

Заиграевским районным судом Республики Бурятия 27 февраля 2019 г. уголовное дело в отношении С, обвиняемой в совершении преступлений, предусмотренных п. «з» ч. 2 ст. 111, п. «в» ч. 2 ст. 158, п. «б, в» ч. 2 ст. 158 УК РФ, возвращено прокурору на основании п. 1 ч. 1 ст. 237 УПК РФ.

С. обвинялась в краже денежных средств с банковского счета в сумме 8 тыс. руб. посредством услуги «мобильный банк», ее действия квалифицированы по п. «в» ч, 2 ст. 158 УК РФ как кража, совершенная с причинением значительного ущерба гражданину.

Свое решение о возвращении уголовного дела суд обосновал тем, что, формулировка статьи уголовного закона, по которой квалифицировано указанное деяние, не соответствовала описанию способа хищения безналичных денежных средств, приведенного в обвинительном заключении. В описании преступного деяния не указано наименование банка и его адрес, где был открыт счет, с которого похищены денежные средства, поэтому нельзя сделать вывод о месте совершения преступления.

Апелляционной инстанцией Верховного суда Республики Бурятия решение суда первой инстанции отменено, уголовное дело направлено в тот же суд для рассмотрения по существу.

Также в 2019 г. Борзинским городским судом Забайкальского края прокурору возвращено уголовное дело по обвинению В. по п. «г» ч. 3 ст. 158 УК РФ в связи с нарушением правил территориальной подследственности. На решение суда прокурором принесено апелляционное представление, которое удовлетворено апелляционной инстанцией Забайкальского краевого суда, постановление суда отменено, дело направлено в суд для рассмотрения по существу.

Таким образом, как видно из приведенных примеров, судебная практика складывается неоднозначно, что позволяет сделать вывод о том, что по-прежнему сохраняется проблема определения территориальной подследственности в связи с тем, что, как правило, банк, в котором открыт счет потерпевшего, и сам потерпевший находятся по адресам, относящимся к разной территориальной подследственности.

Представляется необходимым указать на позицию Генеральной прокуратуры Российской Федерации в данных ей разъяснениях по рассматриваемому вопросу.

В соответствии с ч. 1,2 ст. 152 УПК РФ предварительное расследование производится по месту совершения преступного деяния, содержащего признаки преступления, независимо от времени наступления общественно опасных последствий.

В то же время законодатель в целях обеспечения полноты и объективности расследования, соблюдения процессуальных сроков предусмотрел возможность изменения территориальной подследственности в случаях, предусмотренных в ч. 4 и 4.1 ст. 152 УПК РФ.

В частности, расследование уголовных дел допускается как по месту совершения большинства преступных деяний или наиболее тяжкого из них, месту нахождения обвиняемого или большинства свидетелей, так и по месту жительства или пребывания потерпевшего в Российской Федерации.

Поскольку преступления рассматриваемого вида нередко имеют трансграничный и высокотехнологичный характер, не позволяющий своевременно установить место их совершения и обеспечить объективное расследование в установленные законом процессуальные сроки, правомерным является признание территориальной подследственности в субъекте Российской Федерации, где непосредственно выполнялись действия, входящие в объективную сторону преступления, вне зависимости от того, что последствия наступили на другой территории.

Таким образом, передача уголовных дел в органы расследования, находящиеся в различных административно-территориальных образованиях субъекта, а также субъектах Российской Федерации, возможна лишь при достоверном установлении в ходе расследования местонахождения злоумышленника при осуществлении им действий, входящих в объективную сторону состава преступления.

С учетом складывающий ситуации в территориальных субъектах прокурорами приняты меры для организации эффективного взаимодействия со стороны прокуроров.

В ряде субъектов Российской Федерации на межведомственных совещаниях руководителей прокуратуры и органов внутренних дел приняты решения, в соответствии с которыми признано недопустимым направление материалов по заявлениям и сообщениям о преступлениях в иные подразделения правоохранительных органов в целях опроса лиц, приобщения предметов и документов, проведения иных процессуальных действий[1].

Прокурорами с учетом сложности данного участка работы принимались предупредительные меры.

Так, прокуратурой Саратовской области активно используется практика проверки и изучения документов и материалов, находящихся, что называется, «на руках» у сотрудников полиции. Это приводит к положительным результатам по выявлению укрытых от учета преступлений. Так, проверка непосредственно в ОП № 3 в составе УМВД России по г. Саратову КУСП и других материалов показала, что по ряду зарегистрированных сообщений нет отметок об их разрешении. Было установлено, что, несмотря на наличие явных признаков преступлений, материалы неоднократно необоснованно направлялись по территориальности в другие отделы полиции ГУ МВД России по Саратовской области и иных субъектов Российской Федерации. Например, материал по заявлению А. о хищении ее денежных средств с банковской карты в сумме 17 тыс. руб., зарегистрированный в отделе полиции 27 октября 2016 г., 13 раз необоснованно направлялся по территориальности. По указанию прокуратуры области по данному сообщению 19 марта 2019 г. возбуждено уголовное дело по признакам преступления, предусмотренного п. «в» ч. 2 ст. 158 УК РФ. Всего в указанном отделе полиции установлено более 40 таких материалов, по 33 из которых по требованию прокуратуры области возбуждены уголовные дела.

В качестве иных предупредительных мер предусмотрено направление проектов постановления о направлении сообщения о преступлении надзирающим прокурорам.

Например, прокурором Кемеровской области и начальником ГУ МВД России по Кемеровской области издано совместное указание от 16 апреля 2019 г. № 65/49/1/266 «О порядке передачи сообщений о преступлениях по подследственности», в соответствии с которым в целях исключения фактов необоснованного

---

[1] См.: Указание Прокурора Волгоградской области и Главного управления МВД России по Волгоградской области от 1 октября 2014 г. № 97/15-1/2707; указание Прокурора Республики Карелия и МВД по Республике Карелия от 30 декабря 2014 г. № 82/15/1/2255 «О порядке разрешения сообщений о происшествиях, по которым возник спор о территориальной подследственности, в органах МВД по Республике Карелия»; Совместный приказ Прокурора Ивановской области и начальника УМВД России по Ивановской области от 21 июня 2015 г. № 72/467 «Об утверждении Инструкции о порядке принятия решений по сообщениям о происшествиях, по которым возник спор о территориальной подследственности».

направления материалов по территориальности в правоохранительные органы других субъектов Российской Федерации начальники территориальных органов ГУ МВД России по Кемеровской области направляют надзирающим прокурорам для согласования проекты постановления о передаче сообщений о преступлениях по подследственности с приложением материалов проверки.

Вопросы передачи уголовных дел по территориальной подследственности находятся на контроле руководства прокуратуры области. Прокуроры ориентированы на передачу подобных уголовных дел сразу после их возбуждения и производства неотложных следственных действий по месту реализации объективной стороны преступления, то есть совершения обманных действий, исходя из положений ч. 4 ст. 152 УПК РФ о производстве предварительного расследования по месту нахождения обвиняемого или большинства свидетелей в целях обеспечения его полноты, объективности и соблюдения процессуальных сроков[1].

Прокурорами на постоянной основе анализируется состояние законности при передаче органами предварительного расследования сообщений о преступлениях по подследственности, в том числе в другие регионы Российской Федерации.

Например, в связи с выявляемыми ранее упущениями в организации работы на указанном направлении с 31 октября 2017 г. действует изданное совместно с УМВД России по Орловской области, СУ СК России по Орловской области, УФССП России по Орловской области, ГУ МЧС России по Орловской области указание № 255/15 «Об усилении прокурорского надзора и ведомственного контроля за законностью процессуальных решений и направлении сообщений о преступлениях по подследственности (территориальности)». Данным указанием закреплена обязанность соответствующих должностных лиц территориальных подразделений правоохранительных органов организовать учет материалов, переданных по подследственности (территориальности), с отметками о законности принятых решений, обеспечить проведение незамедлительной (в течение суток) проверки законности решений о передаче сообщения о преступлении по подследственности (территориальности); в случае установления факта возвращения материала проверки из другого правоохранительного органа в пределах области или из другого субъекта Российской Федерации, а также спора о подследственности обеспечить незамедлительное изучение поступившего материала, при наличии оснований принимать меры прокурорского реагирования.

В целях обеспечения законности и обоснованности решений о передаче сообщений по подследственности либо по территориальности, соблюдения процессуальных сроков разрешения материалов проверок сообщений о преступлениях, выработки единообразной правоприменительной практики, усиления ведомственного контроля и прокурорского надзора за этой деятельностью прокуратурой Кабардино-Балкарской Республики и МВД по Кабардино-Балкарской Республике издан совместный приказ от 21 мая 2015 г. № 33/384 «Об утверждении Инструкции о порядке передачи заявлений (сообщений) о преступлениях по территориальной подследственности и направления заявлений (сообщений) об адми-

[1] По материалам деятельности прокуратуры Архангельской области.

нистративных правонарушениях и происшествиях в другие субъекты Российской Федерации» (с изменениями от 9 октября 2019 г. № 60/744).

Проверки по переданным сообщениям проводятся путем ежемесячного направления соответствующих писем в динамике с реестрами (перечнем переданных сообщений) в прокуратуры других субъектов, в которых содержатся сведения, представленные штабом МВД по Кабардино-Балкарской Республике и прокурорами городов и районов республики о сообщениях (материалах), направленных по территориальности, по которым в установленном порядке не возвращены талоны-уведомления.

В целях совершенствования механизма контроля и надзора, исключения фактов незаконной передачи по подследственности в ряде территориальных субъектов введен порядок направления материалов только через аппарат надзирающих прокуратур.

С июля 2016 г. действует изданное совместно с УМВД России по Брянской области, СУ СК России по Брянской области, УФССП России по Брянской области, ГУ МЧС России по Брянской области указание «О мерах по укреплению законности при передаче сообщений о преступлениях по подследственности». Указанием закреплена обязанность соответствующих должностных лиц территориальных подразделений правоохранительных органов области в случае вынесения постановления о передаче сообщения о преступлении по территориальной подследственности в другой регион Российской Федерации предоставлять материалы проверки надзирающему прокурору в суточный срок с момента принятия такого решения. Только после проверки прокурором законности данного постановления осуществляется направление указанных сообщений в другие регионы. Разработанный в регионе механизм позволил полностью исключить факты необоснованного направления сотрудниками правоохранительных органов сообщений о преступлениях по подследственности в иные субъекты Российской Федерации.

Например, положительное влияние на состояние законности в указанной сфере оказало и совместное указания прокуратуры области и ГУ МВД России по области от 17 марта 2015 г. № 35/373 «О повышении эффективности прокурорского надзора и ведомственного контроля за исполнением законов при приеме, регистрации и разрешении сообщений о преступлениях», который направлен на исключение фактов необоснованной передачи сообщений о преступлениях между органами внутренних дел вместо принятия решения, предусмотренного п. 1, 2 ч. 1 ст. 145 УПК РФ. В соответствии с ним сообщения о преступлениях по подследственности передаются исключительно через надзирающего прокурора, которым проверяется законность и обоснованность принятого решения. Результатом организованного таким образом надзора за законностью принятия сотрудниками органа дознания решений в порядке п. 3 ч. 1 ст. 145 УПК РФ стало увеличение с 62 до 111 числа восстановленных на учет преступлений, ранее укрытых путем необоснованной передачи сообщения о преступлении по подследственности[1].

С целью контроля обоснованности передачи материалов проверок по подследственности (территориальности) 5 июля 2018 г. прокуратурой Алтайского края совместно с ГУ МВД издан приказ № 532/380 «О порядке передачи сообще-

[1] По материалам деятельности прокуратуры Ростовской области.

ний о преступлениях по территориальности», согласно которому направление таких материалов в другие субъекты федерации осуществляется через аппарат прокуратуры края.

В Вологодской области продолжается реализация совместного указания региональной прокуратуры и Главка МВД от 1 октября 2014 г. № 97/15/1/2707 «О дополнительных мерах, направленных на обеспечение законности при приеме, регистрации и разрешении сообщений о преступлениях», которым регламентирован обязательный порядок согласования с прокурором постановлений о передаче сообщений о преступлениях по подследственности (территориальности). Положения названного организационно-распорядительного документа во многом предвосхитили новеллы Федерального закона от 27 декабря 2019 г. № 499-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации», связанные с обязательным уведомлением прокурора о передаче сообщения по подследственности. В территориальных прокуратурах организована работа по согласованию таких процессуальных решений, а также ведение накопительных дел.

Заслуживает внимания и опыт организации работы по соблюдению установленного порядка учета преступлений по уголовным делам, переданным для дальнейшего расследования в иные субъекты Российской Федерации либо поступивших из других регионов, в органах прокуратуры Пермского края и Пензенской области, согласно которому реестры таких уголовных дел формируются в районных прокуратурах[1].

Отсутствие единообразия в применении норм закона о территориальной подследственности является существенным препятствием в соблюдении прав участников уголовного процесса на осуществление уголовного судопроизводства в разумный срок.

В целях принятия законного, обоснованного и мотивированного процессуального решения о направлении материалов проверки сообщения о преступлении в сфере ИКТ и уголовных дел органы предварительного расследования, прокуроры и суды должны руководствоваться положениями УПК РФ, ГК РФ, постановлением Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», различными организационно-распорядительными актами. Реагируя на общественно опасные деликты, уголовные дела о таких преступлениях, как правило, возбуждаются по месту изъятия денежных средств с банковского счета их владельца, однако, представляется, что расследование не может быть эффективным по месту окончания преступления, когда установлена территория, откуда действовал злоумышленник.

---

[1] Информационное письмо Генеральной прокуратуры Российской Федерации от 27 декабря 2017 г. № 11-07-2017/Ип12304 «О состояние законности при учете преступлений по уголовным делам, переданным (поступившим) по подследственности (территориальности) в иные субъекты Российской Федерации».

Направляемые в другие регионы уголовные дела в соответствии с ч. 4 ст. 152 УПК РФ для производства расследования по месту нахождения обвиняемого и большинства свидетелей в целях обеспечения полноты, объективности и соблюдения процессуальных сроков по-прежнему не во всех случаях принимаются к производству по месту совершения объективной стороны преступления, как правило, со ссылкой на п. 5 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», что с учетом распространенности нарушений в рассматриваемой сфере свидетельствует о необходимости издания Генеральной прокуратурой Российской Федерации, Следственным комитетом России, Министерством внутренних дел Российской Федерации и другими заинтересованными ведомствами совместного организационно-распорядительного документа.

Внесенные Федеральным законом от 27 декабря 2019 г. № 499-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» изменения подтверждают приведенные нами исследования о роли прокурора в механизме доступа потерпевших от преступления к правосудию, о чем свидетельствует практика ряда прокуратур территориальных субъектов.

Вместе с тем, как представляется, направление копии процессуального решения о передаче сообщения о преступлении по подследственности не содержит механизма оперативного устранения нарушений требований закона, когда материал проверки незамедлительно направлен адресату (логично было бы внести в закон слова «после получения прокурором копии постановления о направлении ...»). Кроме того, вызывает вопрос порядок реализации новой ч. 4 ст. 145 УПК РФ, когда споры о подследственности возникают не только между прокурором и должностными лицами органов предварительного следствия, но и прокурорами одного уровня. Нельзя также однозначно ответить, с какого момента начинает течь этот срок и каков порядок его продления.

Оптимальным вариантом видится установление в УПК РФ обязанности следователей и дознавателей согласовывать с надзирающим прокурором постановление о передаче сообщения о преступлении и сам материал по подследственности перед фактическим исполнением данного процессуального действия. Изложенное логично вытекает из устоявшихся в УПК РФ положений ч. 7, 8 ст. 151 УПК РФ, согласно которым, во-первых, при соединении уголовных дел о компьютерных преступлениях, относящихся к органам предварительного расследования разных ведомств, необходимо исходить из того, что определение подследственности возложено на прокурора; во-вторых, все споры о подследственности разрешает прокурор — в случае, когда следо-

ватель принимает решение о направлении материалов проверки по подследственности, по делам рассматриваемой категории фактически имеет место спорная ситуация.

Также перспективным выходом из сложившейся ситуации представляется запланированное создание специального сервиса, доступного в том числе на мобильных устройствах, с помощью которого каждый гражданин сможет подать заявление о преступлении в правоохранительные органы в электронном виде, которое далее автоматически будет направляться по подследственности[1].

3.6. Деятельность прокурора по устранению обстоятельств, препятствующих рассмотрению уголовных дел о преступлениях, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации в суде

Как уже указывалось в предыдущих главах, в последние годы в Российской Федерации отмечается крайне негативная динамика преступлений, связанных с использованием ИКТ. В связи с этим неслучайно Президент Российской Федерации В. В. Путин, выступая 17 марта 2020 г. на заседании коллегии Генеральной прокуратуры Российской Федерации, указал на необходимость проанализировать, насколько эффективно построена работа правоохранительных органов по этому направлению, как используются имеющиеся у них процессуальные возможности и выработать систему, комплекс мер по снижению числа подобного рода преступлений.

Деятельность прокурора по устранению обстоятельств, препятствующих рассмотрению судом уголовных дел о компьютерных преступлениях, бесспорно, является одной их тех «процессуальных возможностей», эффективное использование которых непосредственно влияет на качество и длительность предварительного расследования, а следовательно, и на разрешение судом в разумный срок основного вопроса — о виновности обвиняемого и мере его уголовной ответственности.

Согласно принятому в России типу уголовного судопроизводства в ходе предварительного расследования выявляется и исследуется большинство доказательств по делу, формируется обвинение, которое будет предметом судебного разбирательства и определит его пределы. Предварительное расследование, являясь основой будущего судебного разбирательства, одновременно призвано служить цели всестороннего и объективного рассмотрения дела судом. И потому, если в процессе

[1] Интервью Генерального прокурора Российской Федерации Чайки Ю. Я. газете «Известия» // URL: https://goo.gl/kvHMV6 (дата обращения: 20.02.2018).

досудебного производства дознавателем, следователем или прокурором допущены нарушения требований закона, которые не могут быть устранены в судебном заседании, это может препятствовать постановлению судом законного, обоснованного и справедливого итогового решения по делу, а поступившее в суд уголовное дело может быть возвращено в досудебное производство.

Возложив бремя доказывания обвинения по поступившему в суд уголовному делу исключительно на прокурора и отделив функцию разрешения уголовного дела от функции обвинения и защиты, УПК РФ установил, что судья, принимая решение о передаче поступившего уголовного дела для рассмотрения его в судебном заседании, не должен рассматривать (пусть даже и в форме предварительного вывода) вопрос о достаточности собранных органами предварительного расследования доказательств для признания предъявленного лицу обвинения обоснованным. Решение этого вопроса фактически возложено на прокурора при утверждении им обвинительного заключения (обвинительного акта, постановления) перед направлением уголовного дела в суд (ст. 221, 226 и 226.8 УПК РФ), поскольку именно на этом этапе «прокурор впервые берет на себя ответственность за качество обвинения, которое ему в дальнейшем придется поддерживать в суде»[1]. Учитывая характер деятельности прокурора при поступлении к нему уголовного дела, достаточно широкий круг полномочий, которыми он при этом обладает, наличие только у него права направить уголовное дело в суд для разбирательства его по существу, некоторые ученые, на наш взгляд, не без оснований предлагают считать этап утверждения прокурором обвинительного заключения, обвинительного акта или обвинительного постановления самостоятельной стадией уголовного судопроизводства, задачей которой является «формирование государственного обвинения»[2].

Одновременно нельзя не отметить, что, поскольку в судебном заседании восполнить недостатки и пробелы предварительного расследования и устранить ранее допущенные нарушения закона возможно далеко не всегда, прокурорский надзор за законностью процессуальной деятельности органов предварительного расследования, в том числе при составлении ими заключительного обвинительного документа (обвинительного заключения, обвинительного акта, обвинительного постановления), имеет исключительно важное значение.

Возвращение же судом поступившего от прокурора уголовного дела чаще всего означает, что решение прокурора о направлении

---

[1] *Смирнов А. В.* Уголовный процесс: учебник. М., 2017. С. 466–467.

[2] *Ковтун Н. Н.* Формирование государственного обвинения как самостоятельная стадия уголовного судопроизводства России // Журнал российского права. 2019. № 9. С. 123–135.

дела в суд было принято им без достаточных оснований. В случае возвращения дела процедура предварительного расследования, а также некоторые правовые выводы по делу должны быть приведены в соответствие с требованиями, установленными уголовным и уголовно-процессуальным законом, с тем чтобы после устранения выявленных процессуальных нарушений, не устранимых в судебной стадии, дело могло быть вновь направлено в суд для рассмотрения по существу и принятия по результатам его рассмотрения правосудного итогового решения[1].

Институт возвращения судом уголовного дела в досудебное производство — один из дискуссионных в уголовно-процессуальной науке, а предусматривающая его ст. 237 УПК РФ — одна из тех статей, которые с момента введения в действие УПК РФ неоднократно подвергались кардинальным изменениям, отражающим, по сути, этапы реформирования российского уголовно-процессуального законодательства (за прошедшие после принятия УПК РФ годы изменения в ст. 237 УПК РФ вносились 15 раз).

В настоящее время эта статья (части 1, 1.1 и 1.2) содержат 9 пунктов, в которых перечисляются основания возвращения судом уголовного дела прокурору для устранения обстоятельств, препятствующих судебному разбирательству. Конкретных же причин, в силу которых суд может принять такое решение, в общей сложности 12. Перечислим их, разделив для удобства анализа на три группы.

1. **Обстоятельства, касающиеся в целом проведения предварительного расследования по данному делу:**

имеются перечисленные в ст. 153 УПК РФ основания для соединения уголовных дел, за исключением случаев, когда суд сам принял такое решение по ходатайству стороны (п. 4 ч. 1);

по уголовному делу, по которому дознание проводилось в сокращенной форме, возникла какая-либо из следующих ситуаций: а) выявились предусмотренные ст. 226.2 УПК РФ обстоятельства, исключающие производство дознания в такой форме; б) поступили возражения какой-либо из сторон против рассмотрения уголовного дела в особом порядке; в) судьей выявлены обстоятельства, препятствующие постановлению законного, обоснованного и справедливого приговора (ч. 1.1).

2. **Обстоятельства, связанные с окончанием предварительного расследования и направлением уголовного дела в суд:**

нарушение прав обвиняемого при ознакомлении с материалами дела, когда по окончании предварительного следствия обвиняемому не были разъяснены права, предусмотренные ч. 5 ст. 217 УПК РФ, то есть

---

[1] Определение Конституционного Суда Российской Федерации от 1 ноября 2012 г. № 2001-О.

право ходатайствовать в установленном законом порядке о рассмотрении уголовного дела с участием присяжных заседателей, коллегией из трех судей федерального суда общей юрисдикции, с вынесением судебного решения в особом порядке, а также о проведении предварительного слушания (п. 5 ч. 1);

составление итогового документа предварительного расследования (обвинительного заключения, обвинительного акта, обвинительного постановления) с нарушением требований УПК РФ (п. 1 ч. 1 с. 237 УПК РФ);

выявление необходимости составления обвинительного заключения либо обвинительного акта по уголовному делу, направленному в суд с постановлением о применении принудительной меры медицинского характера (п. 3 ч. 1);

нарушение требования об обязательном вручении прокурором обвиняемому копии обвинительного заключения (акта, постановления) перед направлением дела в суд (п. 2 ч. 1).

3. **Обстоятельства, указывающие на наличие оснований для квалификации деяния, в совершении которого обвиняется лицо, по закону о более тяжком преступлении, если:**

фактические обстоятельства, изложенные в обвинительном заключении, обвинительном акте, обвинительном постановлении, постановлении о направлении уголовного дела в суд для применения принудительной меры медицинского характера, свидетельствуют о наличии оснований для квалификации действий обвиняемого, лица, в отношении которого ведется производство о применении принудительной меры медицинского характера, как более тяжкого преступления, общественно опасного деяния (п. 6 ч. 1);

фактические обстоятельства, указывающие на наличие оснований для квалификации действий указанных выше лиц как более тяжкого преступления, общественно опасного деяния, установлены в ходе предварительного слушания или судебного разбирательства (п. 6 ч. 1);

после направления уголовного дела в суд наступили новые общественно опасные последствия инкриминированного обвиняемому деяния, которые являются основанием для предъявления обвинения в совершении более тяжкого преступления (п. 1 ч. 1.2);

ранее вынесенные по уголовному делу приговор, определение или постановление отменены ввиду новых или вновь открывшихся обстоятельств (глава 49 УПК РФ), а послужившие для такой отмены обстоятельства являются основанием для предъявления обвиняемому обвинения в совершении более тяжкого преступления (п. 2 ч. 1.2).

Проведенное исследование позволило выделить наиболее распространенные причины и виды нарушений, ставшие основанием для возвращения уголовных дел о преступлениях, совершенных в сфере ИКТ.

Во-первых, это нарушение требований закона при составлении обвинительного заключения, обвинительного акта или обвинительного постановления (не было установлено или не указывалось фактическое место совершения преступления; описание преступного деяния не соответствовало диспозиции статьи УК РФ, по которой квалифицировалось деяние; в итоговом обвинительном документе не было отражено время и способ совершения преступления; обвинительное заключение, обвинительный акт не соответствовали постановлению о привлечении в качестве обвиняемого и др.).

Например, Центральным районным судом г. Читы 18 декабря 2018 г. уголовное дело по обвинению Р. в совершении преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ, возвращено прокурору в порядке, установленном ст. 237 УПК РФ, в связи с нарушением ст. 220 УПК РФ, так как изложенные в фабуле обвинения обстоятельства противоречили фактическим обстоятельствам, содержащимся в показаниях потерпевшего Г., подсудимой, а также в других имеющихся в деле доказательствах. Кроме того, в обвинительном заключении не были описаны конкретные действия Р., которые, исходя из диспозиции п. «г» ч. 3 ст. 158 УК РФ, входили в предмет доказывания (действия по переводу денежных средств и их снятию со счетов, не указаны реквизиты счетов).

Во-вторых, в ходе предварительного расследования нарушалось право обвиняемого на защиту.

Выборгский районный суд Санкт-Петербурга возвратил прокурору уголовное дело по обвинению несовершеннолетней Г. в совершении преступлений, предусмотренных п. «г» ч. 4 ст. 228.1 и ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ (обвиняемая в составе группы лиц по предварительному сговору, используя информационно-телекоммуникационную сеть Интернет, незаконно сбыла наркотические средства и психотропные вещества в крупном размере, а кроме того, покушалась на сбыт таких средств в крупном размере). Судом установлено, что в ходе предварительного следствия в качестве законного представителя несовершеннолетней обвиняемой была привлечена ее мать, лишенная 12 апреля 2006 г. родительских прав решением Выборгского районного суда Санкт-Петербурга, в связи с чем право на защиту несовершеннолетней Г. было нарушено.

Основанием для возвращения Тихвинским городским судом прокурору уголовного дела в отношении Б., обвинявшегося в краже мобильного телефона и банковской карты ПАО «Сбербанк России», со счета которой он впоследствии похитил принадлежащие потерпевшему 2782 руб. (п. «г» ч. 3 ст. 158 УК РФ), послужило нарушение права обвиняемого на защиту, выразившееся в том, что Б. и его защитник были ознакомлены не со всеми материалами уголовного дела, а также в отсутствии в предъявленном обвинении указания на способ хищения денежных средств с банковского счета.

В-третьих, в судебном заседании выявлялась необходимость квалификации действий подсудимого по закону о более тяжком преступлении.

В частности, изучение докладных записок прокуроров субъектов Российской Федерации о судебной практике рассмотрения уголовных

дел о преступлениях, посягающих на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации, показало, что не единичны случаи, когда квалификация преступления, указанная в обвинительном заключении (акте), утвержденном прокурором, была неправильной.

Анализ конкретных причин возвращения судом уголовных дел прокурору подтверждает вывод о том, что как в целом по возвращенным судом делам, так и по возвращенным делам о преступлениях в сфере ИКТ, допущенные в ходе предварительного следствия нарушения в абсолютном большинстве случаев могли быть выявлены, а следовательно, и устранены прокурорами до направления дела в суд. В этой связи еще раз подчеркнем исключительную важность деятельности прокурора на этапе утверждения обвинительного заключения (акта, постановления). Прокурор должен принимать решение о направлении дела в суд при условии, что обстоятельств, препятствующих судебному разбирательству, он не выявил, а собранных органами предварительного расследования доказательств в совокупности достаточно для обоснования события преступления и виновности лица в совершении деяния. При этом очевидно, что особенности собирания доказательств (а следовательно, и их последующая оценка) и возникающие подчас сложности юридической оценки деяния, инкриминируемого обвиняемому, во многом предопределяются отличительными свойствами категории преступлений, к которой относится совершенное обвиняемым деяние. Иными словами, у стоящей перед прокурором при поступлении к нему уголовного дела с обвинительным заключением (актом, постановлением) задачи — ответить на вопрос, установлены ли в ходе расследования все обстоятельства, подлежащие доказыванию по уголовному делу в соответствии со ст. 73 УПК РФ, и не были ли допущены органами предварительного расследования нарушения, являющиеся препятствием рассмотрения дела судом, много составляющих. В числе таких составляющих играют далеко не последнюю роль особенности состава преступления, инкриминируемого обвиняемому, специфика собирания и проверки доказательств, сложности юридической оценки содеянного.

Однако прежде чем анализировать эти особенности, а равно деятельность прокурора на этапе утверждения итогового обвинительного акта по уголовным делам о компьютерных преступлениях, важно отметить, что объем правомочий прокурора на досудебных стадиях уголовного судопроизводства зависит от формы предварительного расследования — дознания или предварительного следствия. Учитывая это, Генеральный прокурор Российской Федерации деятельность прокуроров в досудебном производстве регламентировал двумя приказами: «Об организации прокурорского надзора за процессуальной

деятельностью органов дознания» и «Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия»[1]. В то же время оба приказа обязывают прокурора на этапе утверждения обвинительного заключения или обвинительного акта (постановления) определить: 1) соответствуют ли выводы дознавателя, следователя установленным в ходе расследования обстоятельствам дела, 2) правильно ли органы предварительного расследования квалифицировали содеянное обвиняемым, 3) соблюдены ли уголовно-процессуальные нормы при производстве следственных действий, 4) соответствуют ли имеющиеся в деле процессуальные документы требованиям УПК РФ.

В целом по России прокуроры в последние годы направляют в суды значительное количество уголовных дел о преступлениях, совершенных в сфере ИКТ.

Согласно данным, содержащимся в докладных записках прокуроров, в 2018 г. суды рассмотрели 11 799 дел в отношении 13 510 лиц, совершивших преступления с использованием информационно-телекоммуникационных сетей. В 2019 г. количество рассмотренных судами дел о преступлениях названной категории увеличилось на 62,7%: рассмотрено 19 198 дел в отношении 21 537 лиц. В абсолютном большинстве случаев (почти 90%) судебное разбирательство завершилось постановлением обвинительных приговоров; прекращались же уголовные дела, как правило, по не реабилитирующим обстоятельствам.

Одновременно отметим, что некоторые правоприменители подчас относили к преступлениям, совершенным в сфере ИКТ, любые общественно опасные деяния, при изложении обстоятельств которых упоминались те или иные электронные технологии.

Например, прокуратурой Республики Дагестан к таким преступлениям отнесено хищение денежных средств, совершенное Г., главным бухгалтером ОМВД России по Кайтагскому району, который обвинялся в том, что, используя электронную подпись руководителя, перечислил на свои расчетные счета и счета знакомых денежные средства, поступившие на счет ОМВД, в размере 1 991 177 руб. (ч. 4 ст. 160 УК РФ)[2].

Не имея возможности с учетом объема данного раздела подробно анализировать деятельность прокурора на этапе утверждения итогового обвинительного акта применительно к каждому виду преступлений, совершенных в сфере ИКТ, проанализируем общий алгоритм его действий по названным делам. Цель этой деятельности очевидна — не

---

[1] Приказы Генерального прокурора Российской Федерации от 28 декабря 2016 г. № 826 «Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия», от 26 января 2017 г. № 33 «Об организации прокурорского надзора за процессуальной деятельностью органов дознания».

[2] По материалам деятельности прокуратуры Республики Дагестан.

пропустить имевшие место в ходе предварительного расследования нарушения закона, которые могут повлечь возвращение судом уголовного дела прокурору, а равно исключить направление в суд таких уголовных дел, по которым лицу предъявлено необоснованное, неподтвержденное доказательствами обвинение.

1. Прежде всего, в ходе изучения материалов поступившего уголовного дела прокурор должен выяснить, *полно ли проведено предварительное следствие или дознание*. В частности, подтверждены ли материалами дела время, место, способ и другие юридически значимые обстоятельства совершения обвиняемым деяния; доказана ли его вина, установлены ли мотивы совершения им преступления; каков характер и размер вреда, причиненного противоправным деянием обвиняемого. Очевидно, что невозможность получить из материалов уголовного дела ответы на эти (и другие, указанные в ст. 73 УПК РФ) вопросы и означает неполноту предварительного расследования. Такая ситуация, в частности, может возникнуть, если органами предварительного расследования не исследованы и не вменены в вину обвиняемому последствия преступления или в ходе досудебного производства по делу не были исследованы обстоятельства, свидетельствующие о более активной роли обвиняемого в совершении группового преступления либо дополнительные обстоятельства, отягчающие наказание или влекущие увеличение размера причиненного преступлением вреда.

Предварительное расследование следует признать неполно проведенным, если, например, по уголовному делу о мошенничестве в сфере компьютерной информации (ст. 159.6 УК РФ) должным образом не установлено, каким способом обвиняемый похитил чужое имущество или приобрел право на него (путем ввода, удаления, блокирования, модификации компьютерной информации и др.); по уголовным делам об использовании вредоносных программ для ЭВМ (ст. 273 УК РФ) не исследован и вследствие этого в постановлении о предъявлении обвинения и в обвинительном заключении при описании обстоятельств совершения преступлений не указан конкретный способ использования обвиняемым вредоносных компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации.

В уголовном деле о компьютерном преступлении, совершенном группой лиц (группой лиц по предварительному сговору, организованной группой или преступным сообществом), должны содержаться доказательства, подтверждающие характер соучастия в преступлении каждого из обвиняемых. В частности, при обвинении в незаконном сбыте наркотических средств с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет), совершенном группой лиц по предварительному сговору, организованной группой или преступным сообществом, в обвини-

тельном заключении следует указывать, какие конкретно обязанности выполнял тот или иной соучастник: организатора преступной группы, вербовщика, межрегионального либо регионального курьера, «раскладчика» наркотических средств и т.д. При этом прокурору важно иметь в виду следующее: тот факт, что привлекаемые к ответственности по одному уголовному делу обвиняемые или большинство из них чаще всего не знакомы друг с другом, сложившейся правоприменительной практикой (при условии, что из текста предъявленного обвинения следует совершение преступления группой лиц и видна роль каждого из соучастников) не рассматривается в качестве обстоятельства, исключающего квалификацию деяния как совершенного группой лиц по предварительному сговору (организованной группой, преступным сообществом). Этот вывод обусловлен тем, что только совместные действия соучастников приводят к достижению преступного результата — распространению наркотических средств; при этом каждый из соучастников выполняет действия, составляющие объективную сторону преступления, предусмотренного ст. 228.1 УК РФ.

Следует также иметь в виду, что с июня 2018 г. подсудные судам районного уровня уголовные дела о незаконном производстве, сбыте или пересылке наркотических средств, психотропных веществ или их аналогов, совершенном в особо крупном размере (ч. 5 ст. 228.1 УК РФ), в том числе с использованием ИКТ, могут рассматриваться с участием присяжных заседателей. Очевидно, что только наличие в материалах дела достоверных доказательств, полученных с соблюдением уголовно-процессуальных процедур и подтверждающих участие каждого из обвиняемых в совершении предусмотренного ст. 228.1 УК РФ деянии, позволят государственному обвинителю квалифицированно поддержать обвинение перед коллегией присяжных заседателей и рассчитывать на обвинительный вердикт присяжных заседателей.

Органом предварительного следствия З., П. и С. обвинялись в покушении на незаконный сбыт наркотических средств в крупном размере, совершенный организованной группой с использованием электронных и информационно-телекоммуникационных сетей (включая Интернет), а К. — в покушении на совершение такого деяния в особо крупном размере. Действия обвиняемыми совершались под контролем сотрудников оперативно-разыскных служб. Результаты оперативно-разыскной деятельности были приобщены к материалам дела в установленном процессуальным законом порядке

Доказательствами по делу явились: размещенные в мобильных телефонах незнакомых друг с другом обвиняемых фотографии одних и тех же ничем не примечательных мест (мест закладки наркотических средств), записи с камер видеонаблюдения, переписка соучастников преступления с помощью различных компьютерных программ и другие доказательства, позволившие прокурору направить уголовное дело для судебного разбирательства. Эти доказательства были признаны судом допустимыми.

По ходатайству обвиняемого К. уголовное дело рассматривалось Волжским городским судом Волгоградской области с участием присяжных заседателей, которые признали доказанным, что подсудимые З., П., С. и К. участвовали в деятельности устойчивой группы лиц, заранее объединившихся с целью распространения наркотических средств на территории города Волгограда и Волгоградской области; при этом З., П., С. выполняли в группе функцию розничных раскладчиков, а К. — функцию межрегионального курьера. На основании обвинительного вердикта присяжных заседателей 5 декабря 2019 г. постановлен приговор, в соответствии с которым подсудимые осуждены к длительным срокам лишения свободы.

К нарушениям, препятствующим направлению прокурором уголовного дела в суд, следует отнести отсутствие в материалах уголовного дела точных данных о размере причиненного преступлением ущерба. Ведь нередко обвиняемые совершают компьютерные преступления именно с целью хищения чужого имущества (например, с помощью компьютерного вируса получают доступ к банковской информации о расчетных счетах потерпевших и, проводя модификацию информации, переводят денежные средства потерпевших на указанные ими счета). Особо отметим и важность принятия органами предварительного расследования необходимых мер по обеспечению исполнения приговора в части гражданского иска, взыскания штрафа, других имущественных взысканий или возможной конфискации имущества. В соответствии с предусмотренными ч. 1 ст. 115 УПК РФ положениями следователь, дознаватель с целью обеспечения гражданского иска и исполнения наказания в виде штрафа обязаны принять меры по установлению имущества подозреваемого, обвиняемого или лиц, которые в соответствии с законодательством Российской Федерации несут ответственность за вред, причиненный подозреваемым, обвиняемым, а также принять меры по наложению ареста на такое имущество. Согласно же ч. 3 ст. 115 УПК РФ арест может быть наложен и на имущество, находящееся у других лиц, если в материалах имеются достаточные основания полагать, что оно получено в результате преступных действий обвиняемого либо использовалось или предназначалось для использования в качестве средства совершения преступления или для финансирования терроризма, экстремистской деятельности, организованной группы, незаконного вооруженного формирования, преступного сообщества.

По многим уголовным делам о преступлениях, совершенных в сфере ИКТ, предварительное расследование нельзя признать полным без проведения судебной экспертизы (компьютерно-технической, информационно-технической, верификации электронной подписи и т.д.). В частности, для выяснения, не содержат ли изображения или видеофайлы призывы к распространению терроризма, экстремизма, не носят ли они порнографический характер и т.д., целесообразно (чаще необходимо) проведение не только компьютерно-технической,

но и иных судебных, в том числе комплексных, экспертиз (лингвистической, психологической, психолого-лингвистической и др.). По делам о создании, использовании и распространении вредоносных программ для ЭВМ (ст. 273 УК РФ), как представляется, только в ходе экспертного исследования можно определить, какие изменения и когда внесены в исследуемые программы, к каким последствиям привело использование и распространение вредоносных программ, что позволит предъявить обвиняемому конкретное обвинение и составить отвечающий требованиям закона итоговый обвинительный документ. Эксперт может также установить способ преодоления программной и аппаратной защиты (подбор ключей и паролей, отключение блокировки, использование специальных программных средств). При этом прокурору следует иметь в виду, что в случае загруженности территориальных подразделений ЭКЦ МВД России и судебно-экспертных учреждений Минюста России производство экспертизы может поручаться образовательным организациям либо представителям коммерческих организаций, специализирующимся в сфере информационной безопасности[1].

Между тем в работе органов предварительного расследования по делам о компьютерных преступлениях не единичны случаи проведения осмотра предметов (электронных носителей информации, ЭВМ, сетевых ресурсов) с участием специалиста вместо назначения и проведения компьютерно-технической или иной экспертизы, тогда как Верховный Суд Российской Федерации разъяснил, что заключение специалиста не может подменять заключение эксперта, если оно требуется по делу[2].

2. Отвечая на предыдущий вопрос, прокурору одновременно важно определить, что доказательства, приведенные в подтверждение обвинения, соответствуют *требованию относимости, допустимости и достоверности,* а также установить, что их *совокупность достаточна* для принятия итогового процессуального решения по делу (в том числе с учетом особенностей собирания доказательств по делам о компьютерных преступлениях).

По общему правилу доказательства признаются полученными с нарушением закона, то есть недопустимыми, если при их собирании и закреплении были нарушены гарантированные Конституцией Российской Федерации права человека и гражданина или установленный

---

[1] Постановление Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам».

[2] Пункт 16 постановления Пленума Верховного Суда Российской Федерации от 19 декабря 2017 г. № 51 «О практике применения законодательства при рассмотрении уголовных дел судом первой инстанции (общий порядок судебного разбирательства)».

уголовно-процессуальным законодательством порядок собирания и закрепления доказательств, а также если собирание и закрепление доказательств осуществлялось ненадлежащим лицом или органом либо в результате действий, не предусмотренных процессуальными нормами[1].

Что касается оценки достоверности сведений, полученных с электронных носителей информации при проведении процессуальных действий, то нельзя не отметить, что результаты такой оценки могут быть обусловлены рядом обстоятельств: неквалифицированными действиями следователя либо дознавателя при изъятии информации, в том числе без участия специалиста; искажением информации в результате воздействия помех (нарушение условий хранения, копирования); ошибками при выборе способов фиксации компьютерной информации (в том числе способов ее формализации) и т.д.

Проведенное исследование показало, что по уголовным делам о компьютерных преступлениях суды подчас соглашались с позицией защиты и признавали значимые для разрешения дела доказательства недопустимыми. Причинами для таких выводов являлись: нарушение порядка проведения личного досмотра лица сотрудниками, осуществляющими оперативно-разыскную деятельность, нарушение уголовно-процессуального законодательства при проведении осмотра жилища, нарушение законодательства об оперативно-разыскной деятельности при проведении оперативно-разыскных мероприятий по обнаружению наркотических средств, неразъяснение предусмотренных законом прав лицу при оформлении протокола явки с повинной и др.

Полагаем, что для правоприменителей будет полезен следующий пример из судебной практики.

В апелляционном порядке изменен приговор Кировского районного суда г. Курска в отношении С., осужденного за покушение на незаконный сбыт наркотического средства группой лиц по предварительному сговору с использованием ИКТ в крупном размере; при этом в ходе рассмотрения уголовного дела в апелляционном порядке некоторые доказательства признаны недопустимыми.

Постановляя приговор, суд первой инстанции в обоснование принятого решения о виновности С. сослался на «беседу», проведенную с ним сотрудниками полиции М. и Б. с использованием скрытой видеозаписи, а также на показания указанных сотрудников о содержании данной «беседы». Однако согласно ст. 74 УПК РФ такая «беседа» не относится к числу доказательств. Как следует из содержания «беседы» с С., перед ее началом С., заявил о своем желании воспользоваться правом, предусмотренным ст. 51 Конституции Российской Федерации, не свидетельствовать против самого себя. Беседа была проведена в отсутствие защитника, что, безусловно, является нарушением его права на защиту. По-

[1] Пункт 16 постановления Пленума Верховного Суда РФ от 31 октября 1995 г. № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия».

казания сотрудников полиции о сведениях, полученных от С., в том числе о совершении последним преступления с неустановленным лицом и использовании при совершении преступления сети Интернет, также признаны недопустимыми доказательствами и исключены из приговора, поскольку были получены вопреки требованиям п. 1 ч. 2 ст. 75 УПК РФ в отсутствие защитника и не подтверждены обвиняемым в суде.

В связи признанием ряда доказательств недопустимыми из обвинения С. был исключены квалифицирующие признаки «группой лиц по предварительному сговору» и «с использованием информационно-телекоммуникационных сетей (включая сеть Интернет)», наказание осужденному было снижено.

В отдельных случаях признание доказательств недопустимыми может привести к постановлению оправдательного приговора, если иных доказательств, подтверждающих виновность подсудимого, не имеется

Некоузским районным судом Ярославской области Б. оправдан по предъявленному обвинению в совершении преступлений, предусмотренных ч. 3 ст. 228, п. «б» ч. 4 ст. 229.1 УК РФ, в связи с отсутствием в его действиях состава преступления. Б. обвинялся в незаконном перемещении через таможенную границу Таможенного союза в рамках ЕврАзЭС наркотического средства в особо крупном размере, а также в незаконном приобретении и хранении без цели сбыта наркотических средств в особо крупном размере.

Суд признал недопустимым доказательством протокол личного досмотра Б., так как личный досмотр подсудимого произведен в нарушение положений ст. 4, 6–8, 13–15 и 17 Федерального закона № 144-ФЗ от 12 августа 1995 г. «Об оперативно-розыскной деятельности» и ст. 48 Федерального закона № 3-ФЗ от 8 января 1998 г. «О наркотических средствах и психотропных веществах». Кроме того, в нарушение требований УПК РФ произведен осмотр жилища несовершеннолетнего Ф. и обыск в его квартире, в связи с чем соответствующий протокол также был признан недопустимым доказательством, вследствие чего из числа допустимых доказательств суд исключил протоколы осмотра ноутбука и системного блока, а также заключения экспертов по результатам исследования сотового телефона, ноутбука и системного блока, веществ, изъятых при личном досмотре. Поскольку каких-либо допустимых доказательств, подтверждающих вину Б., не имелось, суд подсудимого Б. оправдал.

Анализируя обстоятельства, подтверждающие необходимость тщательной проверки прокурором материалов уголовного дела перед направлением его в суд, напомним, что поддержание в суде государственным обвинителем предъявленного подсудимому обвинения, то есть продолжение уголовного преследования, возможно только в случае твердого убеждения прокурора в законности и обоснованности обвинения. Как совершенно справедливо отмечал еще А. Ф. Кони, «поддержание обвинения во что бы то ни стало являлось бы действием не только бесцельным, но и нравственно недостойным».

В соответствии с приказом Генерального прокурора Российской Федерации от 25 декабря 2012 г. № 465 «Об участии прокуроров в судебных стадиях уголовного судопроизводства» государственному обви-

нителю необходимо учитывать, что отказ от уголовного преследования невиновных и их реабилитация в той же мере отвечают назначению уголовного судопроизводства, что и поддержание обоснованного обвинения. Разумеется, отказ от обвинения допускается только после всестороннего исследования доказательств.

Между тем в некоторых случаях прокуроры направляли в суд уголовные дела о преступлениях, совершенных в сфере ИКТ, при отсутствии бесспорных доказательств виновности обвиняемого либо при недостаточно обоснованной квалификации содеянного, в связи с чем по таким делам суды постановляли оправдательные приговоры либо прекращали их по реабилитирующим основаниям. Всего в 2019 г. по реабилитирующим основаниям суды прекратили уголовное преследование в отношении 7 лиц, совершивших такие преступления, и в отношении 14 лиц постановили оправдательные приговоры. Для сравнения: в 2018 г. по направленным прокурорами в суд уголовным делам о преступлениях в сфере ИКТ оправдано 6 лиц, прекращено уголовное преследование по реабилитирующему основанию в отношении 1 лица[1].

Судом апелляционной инстанции отменен обвинительный приговор Кызылского городского суда (Республика Тыва) в отношении Ц., обвинявшейся в совершении преступления, предусмотренного ч. 2 ст. 273 УК РФ, и вынесен новый приговор, в соответствии с которым Ц. оправдана в связи с отсутствием в деянии состава преступления. Причиной оправдания послужил тот факт, что совокупность исследованных в суде доказательств не подтверждала обстоятельства, изложенные в описательной части обвинительного заключения, поскольку доступ к личному паролю и компьютеру Ц. был и у других лиц, а отождествить действия, производимые с компьютерной информацией, с конкретной личностью физически невозможно, если даже на флеш-накопителе фигурирует конкретная фамилия. Таким образом, не были выяснены обстоятельства доступа в программу в условиях, когда предыдущий пользователь не завершил процесс.

По другому уголовному делу — в отношении К. (г. Барнаул) в связи с изменением квалификации деяния в судебном заседании государственный обвинитель сам отказался от обвинения. Подсудимый К. обвинялся в совершении совместно с двумя иными лицами тайного хищения денежных средств с банковского счета потерпевшего путем расчета бесконтактным способом (банковской картой потерпевшего) через терминалы в магазинах, при этом деяние К. органом следствия было ошибочно квалифицировано по п. «г» ч. 3 ст. 158 УК РФ. Направляя уголовное дело в суд, прокурор согласился с такой юридической оценкой содеянного. Между тем в соответствии с позицией Пленума Верховного Суда Российской Федерации, изложенной в постановлении от 30 ноября 2017 г. № 48 «О судеб-

[1] Справка Главного уголовно-судебного управления Генеральной прокуратуры Российской Федерации о результатах анализа практики рассмотрения судами в 2018–2019 гг. уголовных дел о преступлениях в сфере компьютерной информации, а также совершенных с использованием информационно-компьютерных технологий.

ной практике по делам о мошенничестве, присвоении и растрате», действия К. надлежало квалифицировать как мошенничество с использованием электронных средств платежа, совершенное по предварительному сговору группой лиц (ст. 159.3 УК РФ). Учитывая это, а также то, что К. на момент совершения преступления исполнилось только 14 лет, а уголовная ответственность за совершение мошенничества, согласно ст. 20 УК РФ, наступает с 16 лет, государственный обвинитель отказался от обвинения К. в связи с отсутствием в его действиях состава преступления. Суд уголовное дело в отношении К. прекратил на основании п. 2 ст. 254 УПК РФ.

Как показало исследование, непосредственными причинами постановления оправдательных приговоров по делам о преступлениях, совершенных в сфере ИКТ, явились: малозначительность деяния; наличие в деянии подсудимого не уголовного, а административного правонарушения; отсутствие доказательств, подтверждающих вину подсудимого (в том числе после признания доказательств недопустимыми); недоказанность умысла на совершение преступления; провокация со стороны сотрудников, осуществляющих оперативно-разыскную деятельность. Очевидно, что при принятии решения о направлении в суд названных уголовных дел прокуроры надлежащим образом не оценили обоснованность обвинения, предъявленного органом предварительного расследования обвиняемому.

Фрунзенским районным судом Санкт-Петербурга К., обвиняемый в совершении преступлений, предусмотренных ч. 2 ст. 146, ч. 2 ст. 146 и ч. 1 ст. 273 УК РФ, оправдан в связи с отсутствием в его деяниях состава преступления.

Свое решение суд мотивировал тем, что в ходе предварительного расследования и судебного следствия не выявлено объективных доказательств, безусловно свидетельствующих о том, что К. до обращения к нему Е. занимался или намеревался заниматься противоправной деятельностью, направленной на незаконное использование объектов авторского права и распространение компьютерной информации, заведомо предназначенной для нейтрализации средств защиты компьютерной информации, и о том, что его умысел на незаконное использование объектов авторского права и распространение компьютерной информации, заведомо предназначенной для нейтрализации средств защиты компьютерной информации, сформировался вне зависимости от деятельности органа, осуществляющего оперативно-разыскную деятельность. Свои действия К. совершил под влиянием сотрудников правоохранительных органов, которые сформировали его умысел на незаконное использование объектов авторского права и на распространение компьютерной информации, заведомо предназначенной для нейтрализации средств защиты компьютерной информации. Судебной коллегией по уголовным делам Санкт-Петербургского городского суда приговор оставлен без изменения.

3. Существенным нарушением уголовно-процессуального закона, которое, бесспорно, будет препятствовать рассмотрению уголовного дела судом, является *нарушение гарантированных законом прав участников уголовного судопроизводства*. Перед направлением уголовного

дела в суд прокурор должен не только проверить, соблюдены ли в досудебном производстве положения закона, регламентирующие права участников уголовного судопроизводства, но и (это важно отметить) обеспечена ли органами предварительного расследования реальная возможность осуществления этих прав. Прежде всего, это касается обеспечения права обвиняемого на защиту. Как уже отмечалось, нарушение этого права является одним из наиболее распространенных оснований возвращения судом уголовного дела прокурору. Вот почему прокурору при поступлении к нему уголовного дела надлежит:

- проверить, были ли соблюдены требования ст. 51 УПК РФ, определяющей случаи обязательного участия защитника в уголовном судопроизводстве, а также установить, обеспечили ли органы предварительного расследования условия для фактической реализации права обвиняемого на получение квалифицированной юридической помощи (ст. 52 УПК РФ) и не было ли обстоятельств, исключающих участие защитника в производстве по уголовному делу (ст. 72 УПК РФ);
- по уголовному делу в отношении несовершеннолетнего выяснить, выполнено ли требование об обязательном участии в деле законных представителей обвиняемого (ст. 48 УПК РФ);
- установить, не относится ли обвиняемый к категории лиц, в отношении которых должен применяться особый порядок производства по уголовным делам, и если да, то были ли соблюдены положения гл. 52 УПК РФ.

По делам о компьютерных преступлениях вопросы обеспечения прав участников уголовного процесса нередко возникают в связи с производством судебных компьютерно-технических и других экспертиз (соблюдение права обвиняемого, потерпевшего на ознакомление с постановлением о назначении судебной экспертизы и заключением эксперта, право ходатайствовать о производстве дополнительной или повторной судебной экспертизы (особенно если она проведена до возбуждения уголовного дела) и т.д. Прокурор должен также выяснить, обеспечено ли органами предварительного расследования право потерпевшего на доступ к правосудию и компенсацию причиненного ущерба (ст. 42 УПК РФ).

Если из материалов дела следует, что участники процесса не владеют или недостаточно владеют языком, на котором ведется уголовное судопроизводство, важно выяснить, было ли обеспечено при проведении расследования их право делать заявления, давать объяснения и показания, заявлять ходатайства, приносить жалобы, знакомиться с материалами уголовного дела на родном языке или другом языке, которым они владеют, а также бесплатно пользоваться помощью переводчика (ст. 18 УПК РФ).

В ходе предварительного расследования органы предварительного расследования, как уже отмечалось, должны принять меры по возмещению причиненного преступлением ущерба, а потому належит проверить, разъяснялось ли потерпевшим право на предъявление гражданского иска (ч. 1, 2 ст. 44 УПК РФ) и приняты ли меры по обеспечению возмещения ущерба, причиненного преступлением.

4. Особо укажем на необходимость проверки *соблюдения прав обвиняемого на этапе окончания предварительного расследования,* поскольку невыполнение следователем обязанности после окончания ознакомления разъяснить обвиняемому его права, предусмотренные ч. 5 ст. 217 УПК РФ, отнесено законом к самостоятельным основаниям возвращения уголовного дела прокурору (п. 5 ч. 1 ст. 237 УПК РФ).

В отношении обвиняемого, содержащегося под стражей, важно определить, соблюдено ли в досудебном производстве требование ч. 5 ст. 109 УПК РФ, обязывающей следователя предъявлять материалы оконченного расследованием уголовного дела обвиняемому и его защитнику не позднее чем за 30 суток до окончания предельного срока содержания под стражей, установленного законом. Если это требование было нарушено, а на момент поступления к прокурору материалов уголовного дела предельный срок содержания обвиняемого под стражей истек, прокурор должен отменить данную меру пресечения (ч. 2 ст. 221 УПК РФ).

Согласно требованиям ч. 5 ст. 217 УПК РФ по окончании ознакомления с материалами уголовного дела следователь должен разъяснить обвиняемому право ходатайствовать о рассмотрении уголовного дела судом с участием присяжных заседателей, коллегией из трех судей федерального суда общей юрисдикции о постановлении приговора без проведения судебного разбирательства и о проведении предварительного слушания (по основаниям, предусмотренным законом). Учитывая практику возвращения судом уголовного дела прокурору по основаниям, предусмотренным п. 5 ч. 1 ст. 237 УПК РФ, особо отметим, что прокурору следует удостовериться, что обвиняемый не просто проинформирован о наличии у него названных прав, но ему было разъяснено их содержание, а также убедиться в наличии соответствующей записи в протоколе ознакомления обвиняемого и его защитника с материалами уголовного дела, где должно быть отражено желание обвиняемого воспользоваться этим правом или отказаться от него (ч. 2 ст. 218 УПК РФ).

Если участники уголовного процесса по окончании ознакомления с материалами уголовного дела заявили ходатайство о дополнении материалов уголовного дела и в удовлетворении такого ходатайства им было отказано, прокурору следует проверить обоснованность соответствующего постановления следователя, дознавателя.

Считаем также важным обратить внимание на следующее обстоятельство. В соответствии с п. 5 ч. 1 ст. 237 УПК РФ возможно возвращение уголовного дела в досудебное производство, если следователь по окончании предварительного следствия не разъяснил обвиняемому его права, предусмотренные ч. 5 ст. 217 УПК РФ, которые в том числе включают в себя право ходатайствовать о применении особого порядка судебного разбирательства и о проведении предварительных слушаний. Но ведь названными правами, бесспорно, обладают и лица, в отношении которых проводилось не следствие, а дознание, и когда права должны разъясняться дознавателем при ознакомлении обвиняемого с обвинительным актом и материалами уголовного дела в порядке, предусмотренном ст. 225 УПК РФ, поэтому полагаем обоснованным уже высказывавшееся некоторыми исследователями предложение о необходимости внесения в ст. 237 УПК РФ соответствующих дополнений.

5. *Нарушения процессуального порядка возбуждения уголовного дела и общих условий производства предварительного расследования* также препятствуют направлению уголовного дела в суд.

Как свидетельствует практика, в процессе предварительного расследования не единичны нарушения, которые непосредственно не направлены на лишение либо ограничение прав участников уголовного судопроизводства, но предопределяют невозможность составления органами предварительного расследования соответствующего требованиям закона итогового обвинительного документа и, следовательно, вынесения судом законного и обоснованного приговора. К таким нарушениям относятся:

а) несоблюдение процессуального порядка возбуждения уголовного дела, проведение дознания вместо предварительного следствия, несоблюдение правил подследственности, производство дознания или предварительного следствия лицом, не уполномоченным на то законом либо подлежащим отводу, и др. В частности, возбуждение уголовного дела вопреки установленному ч. 1 ст. 448 УПК РФ порядку ненадлежащим лицом явится бесспорным основанием для возвращения дела прокурору, если вопреки допущенному нарушению такое дело будет направлено прокурором в суд[1].

Поскольку во многих случаях уголовные дела о компьютерных преступлениях возбуждаются на основании материалов, содержащих результаты оперативно-разыскной деятельности, а результаты такой

---

[1] Определение Конституционного Суда Российской Федерации от 13 мая 2010 г. № 623-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Слюсаренко Владимира Терентьевича на нарушение его конституционных прав пунктом 1 части первой статьи 237 и статьей 254 Уголовно-процессуального кодекса Российской Федерации».

деятельности нередко представляются органам предварительного расследования на электронном носителе информации, очень важно убедиться, что был соблюден порядок представления названной информации[1] и результаты оперативно-разыскной деятельности отвечают требованиям, предъявляемым к доказательствам уголовно-процессуальным законом (ст. 89 УПК РФ)[2]. Иными словами, для того чтобы представляемая по результатам оперативно-разыскной деятельности компьютерная информация обладала свойствами допустимости и относимости и получила статус уголовно-процессуального доказательства, необходимо выполнить три группы последовательных действий: проведение мероприятия (поиск, выявление, фиксация информации); представление результатов органу предварительного расследования (хранение, передача, защита информации от модификации и утечки, обеспечение целостности и неизменности информации); легализация в уголовно-процессуальные доказательства (сохранение свойств относимости и допустимости, рассекречивание сведений, трансформация информации)[3]. Как свидетельствует практика, чаще всего из-за неправильного оформления, несоблюдения процедуры сбора признаются недопустимыми доказательствами составленные по результатам оперативно-разыскной деятельности протоколы следующих действий: осмотра помещений, оперативных экспериментов, прослушивания телефонных переговоров и фонограмм.

б) нарушение процедуры производства процессуальных действий, установленной ст. 164–170 УПК РФ. По делам о компьютерных преступлениях проверка законности таких действий должна производиться с учетом особенностей, характерных для общественно опасных деяний, совершенных в сфере ИКТ. В частности, особенность осмотра места совершения компьютерного преступления заключается в том, что необходимо обнаружить, зафиксировать и изъять компьютерную информацию с электронных носителей. При этом к следам преступления относятся: электронные документы; лог-файлы журналов и отчетов операционной системы; файлы программного обеспечения, используемого преступниками для сканирования, декодирования, модификации, копирования,

---

[1] Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России от 27 сентября 2013 г. № 68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд».

[2] Алгоритм деятельности следователя при рассмотрении сообщения о компьютерном преступлении более подробно изложен в пособии «Методика борьбы с компьютерными преступлениями. М., 2020».

[3] *Драпезо Р. Г.*, *Шелестюков В. Н.* Особенности использования результатов оперативно-розыскного мероприятия «получение компьютерной информации» // Рос. следователь. 2018. № 9. С. 65–72.

записи и хранения информации; данные телекоммуникационных сервисов, мессенджеров, приложений VoIP и т.д.[1]

Поскольку уголовно-процессуальный закон не установил форму фиксации размещенной в сети Интернет информации, содержимое и реквизиты цифровой информации подлежат обязательному описанию в протоколе осмотра, обыска или заключении эксперта (специалиста). В текст процессуального документа рекомендуется вносить или прикладывать к нему скриншоты, распечатки логов, выдержки из внутренней или внешней аналитики и статистики по сайту и т.п. К участию в осмотре и обыске целесообразно привлекать понятых и специалиста, который может уточнить технические детали и терминологию. В частности, согласно ч. 2 ст. 164.1 УПК РФ электронные носители информации должны изыматься с обязательным участием специалиста. На практике в качестве специалистов чаще всего привлекаются сотрудники той организации, в которой производится выемка или обыск. Между тем специалистом должно выступать незаинтересованное лицо. Поэтому в случае, когда с учетом конкретных обстоятельств дела объективность и незаинтересованность привлеченного в качестве специалиста сотрудника организации, в отношении которой совершено преступление, вызывает обоснованные сомнения, полученное с его участием доказательство прокурор может признать недопустимым. Следует также иметь в виду, что законодатель установил дополнительные гарантии при производстве следственных действий по уголовным делам о преступлениях, совершенных в сфере предпринимательской деятельности, в том числе с использованием электронно-информационных технологий. В частности, по таким делам запрещается необоснованное применение мер, способных привести к приостановлению законной деятельности юридических лиц или индивидуальных предпринимателей, в том числе изъятие электронных носителей информации (ст. 164.1 УПК РФ).

в) нарушения требований закона, предъявляемых к форме и содержанию уголовно-процессуальных документов. Такие нарушения, как известно, многообразны, но именно они, как свидетельствует практика, нередко являются основанием возвращения уголовного дела прокурору. В частности, в процессуальном документе неправильно указываются данные лица, привлекаемого в качестве обвиняемого; неверно отражаются сведения о времени, месте, способе, мотиве совершения преступления, а также иные обстоятельства, подлежащие доказыванию; не конкретизируется предъявленное обвинение в части описания преступных действий обвиняемого; изложенная в постановлении о при-

[1] *Вехов В. Б.* О понятии, механизме образования и классификации электронно-цифровых, оптических и магнитных следов // Криминалистика в системе правоприменения: материалы конференции. М., 2008. С. 103.

влечении в качестве обвиняемого фабула обвинения не соответствует юридической квалификации деяния; неправильно излагаются диспозиция уголовно-правовой нормы и квалифицирующие признаки состава преступления; отсутствует подпись следователя и т.д.

Постановлением Невского районного суда уголовное дело в отношении Р., обвиняемого в совершении преступления, предусмотренного ч. 1 ст. 282 УК РФ, возвращено прокурору на основании ст. 237 УПК РФ в связи с тем, что в обвинительном заключении не было приведено содержание высказываний обвиняемого, а описание преступления Р. представляло собой полный текст диспозиции ч. 1 ст. 282 УК РФ, без указания на конкретные элементы состава, имеющие отношение к действиям Р. В апелляционном порядке постановление Невского районного суда не пересматривалось и вступило в законную силу[1].

г) *несоблюдение регулируемой ст. 171–173, 223.1 УПК РФ процедуры предъявления обвинения и уведомления о подозрении в совершении преступления*. Закон требует, чтобы обвинение было предъявлено не позднее 3 суток со дня вынесения постановления о привлечении в качестве обвиняемого и обязательно в присутствии защитника, если он участвует в уголовном деле. При производстве по делу дознания вручение подозреваемому письменного уведомления о подозрении в совершении преступления и разъяснении ему прав, предусмотренных ст. 46 УПК РФ, должно быть оформлено протоколом с отметкой о вручении копии уведомления.

В связи с тем, что несоблюдение названных требований закона, как правило, предполагает производство следственных и иных процессуальных действий (предъявление нового обвинения, допрос обвиняемого, ознакомление его с материалами уголовного дела и др.), прокурор, выявив ошибки следователя или дознавателя, должен возвратить уголовное дело для производства дополнительного расследования.

6. Согласно ч. 2 ст. 252 УПК РФ изменение обвинения в судебном разбирательстве допускается, только если этим не ухудшается положение подсудимого и не нарушается его право на защиту. В связи с этим при изучении материалов уголовного дела прокурору очень важно определить, *правильна ли уголовно-правовая оценка содеянного обвиняемым и нет ли оснований для изменения квалификации его действий*. Ошибочное применение в ходе предварительного расследования закона о менее тяжком преступлении, как уже отмечалось, влечет за собой возвращение судом уголовного дела прокурору. При этом такое решение может быть принято еще до разбирательства дела по существу, на этапе предварительного слушания, если изложенные в обвинительном заключении, обвинительном акте или обвинительном постановлении фактические обстоятельства указывали на наличие оснований для квалификации содеянного как более тяжкого преступления.

---

[1] По материалам деятельности прокуратуры Санкт-Петербурга.

При утверждении обвинительного акта по уголовному делу в отношении В., обвиняемого в совершении преступления, предусмотренного ч. 3 ст. 30, ч. 1 ст. 158 УК РФ, прокурор не учел, что обвиняемый пытался завладеть денежными средствами потерпевшего путем совершения покупки с использованием похищенной банковской карты, чем ввел работника торговой организации в заблуждение относительно правомерности владения ею (ст. 159.3 УК РФ). Возвращая дело, судья обоснованно указал на необходимость квалификации содеянного как более тяжкого преступления, то есть как покушение на мошенничество с использованием электронных средств платежа (Архангельская область)[1].

Исследования показывают, что в досудебном производстве по уголовным делам о преступлениях в сфере ИКТ ошибки при квалификации тех или иных деяний допускаются нередко. Чаще всего они выражаются либо во вменении не той, которую следовало, статьи УК РФ, либо в неполной юридической оценке содеянного. Например, сложности возникали при квалификации посягательств на имущественные права потерпевших, в частности при разграничении таких преступлений, как мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и кража (ст. 158 УК РФ).

Объект предусмотренного ст. 159.6 УК РФ деяния сложный, поскольку оно посягает на два непосредственных объекта: основной — отношения собственности и дополнительный — безопасность в сфере компьютерной информации, а предметом преступления выступают не только имущество или право на имущество, но и компьютерная информация. В этой связи мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или ст. 274.1 УК РФ[2].

В то же время, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к этим данным (например, обвиняемый тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «Мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица), такие действия подлежат квалификации как кража, если виновным не было оказано незаконное воздействие на программ-

---

[1] Обзор состояния законности на стадии утверждения прокурорами обвинительных актов (постановлений), направлен заместителем Генерального прокурора Российской Федерации прокурорам субъектов Российской Федерации, приравненным к ним прокурорам специализированных прокуратур 4 октября 2019 г., исх. № 69-09-2019.

[2] Пункт 20 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

ное обеспечение серверов, компьютеров или на информационно-телекоммуникационные сети. Изменение данных о состоянии банковского счета и (или) о движении денежных средств в результате использования виновным учетных данных потерпевшего не является таким воздействием[1].

По поступившему к нему уголовному делу решение прокурора, выявившего ошибку в юридической оценке деяния обвиняемого, различаются в зависимости от того, расследовано уголовное дело в форме дознания или предварительного следствия.

По уголовному делу с обвинительным актом или обвинительным постановлением прокурор вправе исключить отдельные пункты обвинения либо переквалифицировать обвинение на менее тяжкое (ч. 2 ст. 226, ч. 2 ст. 226.8 УПК РФ). Он может также исключить из обвинения отдельные квалифицирующие признаки или избыточные ссылки на нормы УК РФ, изменить квалификацию деяния в соответствии с нормой, предусматривающей более мягкое наказание. Прокурор вправе без изменения квалификации исключить из фабулы обвинения отдельные действия обвиняемого, если они не подтверждаются собранными по делу доказательствами, уменьшить размер причиненного преступлением вреда.

Вместе с тем, если в досудебном производстве были собраны достаточные доказательства, дающие основани**е** для обвинения лица в совершении более тяжкого преступления или предъявления обвинения, существенно отличающегося по фактическим обстоятельствам от ранее предъявленного, прокурор возвращает уголовное дело для производства дополнительного дознания. В том случае, когда квалификация действий обвиняемого по уголовному закону о более тяжком преступлении влечет изменение подследственности, уголовное дело подлежит направлению для производства предварительного следствия (п. 4 ч. 1 ст. 226 УПК РФ).

В отличие от уголовных дел, расследованных в форме дознания, выявление ошибок при квалификации содеянного по делу, поступившему с обвинительным заключением, всегда влечет принятие прокурором решения о возвращении его следователю для изменения объема обвинения или квалификации действий обвиняемых либо для производства дополнительного следствия, если ошибка в уголовно-правовой оценке деяния является следствием неполноты исследования обстоятельств дела (п. 2 ч. 1 ст. 221 УПК РФ). Это обусловлено характером правомочий прокурора: закон не предоставляет ему право самостоятельно изменить обвинение в сторону смягче-

[1] Пункт 20 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». П. 21.

ния на этапе утверждения обвинительного заключения, что, на наш взгляд, не согласуется с принципом уголовного судопроизводства в разумный срок.

Вопрос о юридической оценке совершенного обвиняемым деяния неотделим от вопроса о том, содержит ли деяние состав преступления. В частности, не является преступлением действие (бездействие), хотя формально и содержащее признаки какого-либо преступления, но в силу малозначительности не представляющее общественной опасности (ч. 2 ст. 14 УК РФ). Фактические обстоятельства совершенного обвиняемым деяния должны оцениваться прокурором всесторонне и объективно, в том числе и с учетом этой правовой нормы. Направление же для судебного разбирательства уголовного дела о заведомо малозначительном деянии, а потому подлежащего прекращению не согласуется как с назначением уголовного судопроизводства, так и с требованием о его разумном сроке.

Показателен следующий пример. Несовершеннолетний Ж. обвинялся в том, что ввел на сайте «Дневник.ру» логин и пароль администратора системы электронного журнала МБОУ «Гимназия № 5», осуществил неправомерный доступ к охраняемой законом компьютерной информации и модифицировал ее, изменив, удалив или добавив оценки по учебным дисциплинам себе и некоторым другим учащимся гимназии, то есть в совершении преступления, предусмотренного ч. 1 ст. 272 УК РФ.

В ходе судебного разбирательства государственный обвинитель признал, что в силу малозначительности действия Ж. не представляют общественной опасности, и отказался от обвинения, в связи с чем суд 12 февраля 2019 г. уголовное дело в отношении Ж. прекратил на основании п. 2 ст. 254 УПК РФ (г. Новосибирск).

7. При проверке *соответствия обвинительного заключения, обвинительного акта, обвинительного постановления требованиям ст. 220, 225, 22.7[1] УПК РФ* необходимо учитывать разъяснение Пленума Верховного Суда Российской Федерации, согласно которому исключается, в частности, возможность вынесения судебного решения в случаях, когда обвинение, изложенное в обвинительном заключении или обвинительном акте, не соответствует обвинению, изложенному в постановлении о привлечении лица в качестве обвиняемого; обвинительное заключение, обвинительный акт или обвинительное постановление не подписаны следователем (дознавателем), обвинительное заключение не согласовано с руководителем следственного органа либо не утверждено прокурором, обвинительный акт или обвинительное постановление не утверждены начальником органа дознания или прокурором; в обвинительном заключении, обвинительном акте или обвинительном постановлении отсутствуют указание на прошлые неснятые и непогашенные судимости обвиняемого,

данные о месте нахождения обвиняемого, данные о потерпевшем, если он был установлен по делу[1].

Разумеется, приведенный перечень нарушений не может быть исчерпывающим, и не единичны случаи, когда и другие ошибки следователей и дознавателей суды признают основанием возвращения уголовного дела прокурору в соответствии с п. 1 ч. 1 ст. 237 УПК РФ (невключение квалифицирующих признаков состава преступления в юридическую формулировку предъявленного обвинения, составление итогового процессуального документа неправомочным лицом, слишком общая формулировка обвинения и т.д.).

Выявив нарушения, прокурор должен вернуть уголовное дело *для составления заново* обвинительного заключения, обвинительного акта или обвинительного постановления (п. 2 ч. 1 ст. 221, п. 2 ч. 1 ст. 226, п. 2 ч. 1 ст. 226.8 УПК РФ), поскольку, как уже отмечалось, прокурор не вправе сам составить новое обвинительное заключение, обвинительный акт, обвинительное постановление, даже если такая необходимость была обусловлена выявлением в документе технических или стилистических ошибок, которые также могут быть признаны препятствием для рассмотрения дела в суде. Если же для устранения нарушений требуется провести следственные или иные процессуальные действия, например предъявить новое обвинение и допросить обвиняемого, прокурор должен вернуть уголовное дело для производства дополнительного расследования.

8. Направляя уголовное дело в суд, прокурор должен *копию утвержденного им обвинительного заключения (акта, постановления) вместе с приложениями вручить обвиняемому*, а также защитнику и потерпевшему, если они об этом ходатайствовали (ч. 2 ст. 222, ч. 3 ст. 226, ч. 3 ст. 226.8 УПК РФ). Поскольку обязанность вручить обвиняемому копию обвинительного заключения (акта, постановления) возлагается на прокурора, получение органом предварительного расследования расписки обвиняемого о получении такого документа сразу по окончании ознакомления с материалами уголовного дела, то есть до утверждения документа прокурором, противоречило бы закону.

Невыполнение прокурором требования о вручении обвиняемому копии итогового обвинительного акта может послужить основанием для возвращения судом уголовного дела прокурору (п. 2 ч. 1 ст. 237 УПК РФ), за исключением случаев, когда обвиняемый сам отказался от получения копии процессуального документа, не явился по вы-

---

[1] Постановление Пленума Верховного суда Российской Федерации от 22 декабря 2009 г. № 28 «О применении судами норм уголовно-процессуального законодательства, регулирующих подготовку уголовного дела к судебному разбирательству». П. 14.

зову либо иным образом уклонился от его получения, о чем прокурор должен уведомить суд, указав конкретные причины, по которым копия обвинительного заключения (акта, постановления) не была вручена обвиняемому. При этом отказ получить копию итогового обвинительного акта должен быть оформлен письменно, а факт неявки подтвержден документально. В то же время закон (ч. 4 ст. 222 УПК РФ) не содержит указания на то, в каком процессуальном документе прокурор должен привести причины, в связи с которыми обвиняемому не была вручена копия названного процессуального акта. По сложившейся прокурорской практике эти причины указываются в подписанном прокурором сопроводительном письме, с которым уголовное дело направляется в суд. Однако, по нашему мнению, которое мы высказывали и ранее, в тех случаях, когда обвиняемый отказался или уклонился от получения копии обвинительного заключения, решение о направлении дела в суд с указанием причин, по которым этот документ не был вручен обвиняемому, следовало бы оформлять мотивированным постановлением, как это и требуется в соответствии с ч. 4 ст. 7 УПК РФ. Это позволило бы, с одной стороны, участникам уголовного судопроизводства обжаловать решение прокурора, а с другой — способствовало бы началу судебного разбирательства без необоснованных задержек[1].

9. Препятствия к вынесению судебного решения возникают и при рассмотрении уголовных дел, направленных в суд с постановлением *о применении принудительных мер медицинского характера*. Необходимость составления обвинительного заключения или обвинительного акта по таким делам (п. 3 ч. 1 ст. 237 УПК РФ) в определенных случаях может являться следствием ошибок органов предварительного следствия при доказывании обстоятельств, имеющих значение для уголовного дела, и предусмотренных не только ст. 73, но и ст. 434 УПК РФ. Как известно, в предмет доказывания по данной категории дел наряду с обстоятельствами совершенного деяния, характером и размером причиненного деянием вреда входят вопросы о наличии у лица психических расстройств в прошлом, характере психического заболевания в момент совершения деяния, запрещенного уголовным законом, или во время производства по уголовному делу; также должно быть установлено, связано ли психическое расстройство лица с опасностью для него или других лиц либо возможностью причинения им иного существенного вреда (ст. 434 УПК РФ). В случае, если указанные обстоятельства не были установлены либо недостаточно исследованы при производстве предварительного следствия или нарушены иные

[1] *Решетова Н. Ю.*, *Баева Т. Н.*, *Оксюк Т. Л.* Деятельность прокурора по устранению обстоятельств, препятствующих рассмотрению уголовного дела судом. М., 2009. С. 134.

требования, предъявляемые к содержанию итогового постановления следователя, прокурор должен направить уголовное дело для производства дополнительного расследования (п. 2 ч. 5 ст. 439 УПК РФ), ибо в противном случае дело возвратит суд.

Важно также отметить, что, решая вопрос о возможности направления такого уголовного дела в суд, прокурор должен убедиться, что органы предварительного следствия не только собрали необходимые доказательства для подтверждения предусмотренных законом обстоятельств, но и предоставили лицу, страдающему психическим заболеванием, возможность самостоятельно реализовывать свои процессуальные права, если заболевание этому не препятствовало (ч. 1 ст. 437 УПК РФ).

Подводя итог, прежде всего, отметим, что допущенные в ходе предварительного расследования нарушения закона, которые не были выявлены прокурором перед направлением дела в суд и которые невозможно устранить в судебном заседании, затрудняют осуществление правосудия в разумный срок. Они также существенно осложняют поддержание государственного обвинения в суде, а в некоторых случаях приводят к невозможности продолжения уголовного преследования. Очевидно, что только наличие в материалах уголовного дела достоверных доказательств, полученных в соответствии с требованиями уголовно-процессуального закона и подтверждающих факт совершения обвиняемым преступления, позволит государственному обвинителю квалифицированно и эффективно поддержать обвинение, а суду вынести законный, обоснованный и справедливый приговор.

В то же время отсутствие у прокурора правомочия при поступлении к нему уголовного дела с обвинительным заключением самостоятельно исправлять допущенные следователем ошибки в квалификации содеянного и определении объема обвинения (если, разумеется, внесение изменения в обвинительное заключение не повлечет ухудшение положения обвиняемого), по нашему мнению, не согласуется с принципом разумного срока уголовного судопроизводства, в связи с чем целесообразно внесение соответствующих дополнений в положения УПК РФ, определяющие полномочия прокурора.

Учитывая особенности и разнообразие преступлений, совершаемых в сфере ИКТ, полагаем, что для принятия обоснованного решения о направлении в суд уголовного дела о таком преступлении прокурор, помимо наличия у него профессиональных знаний, должен быть осведомлен о возможностях современной компьютерной техники, об основах функционирования Интернета и компьютерных программ (приложений), созданных для использования в мобильных устройствах, и т.д.

Квалифицированная и целенаправленная деятельность прокуроров по своевременному выявлению и устранению обстоятельств, препятствующих рассмотрению судом уголовных дел о преступлениях, совершаемых в сфере ИКТ, позволяет повысить эффективность уголовно-процессуальных процедур, способствует достижению целей уголовного судопроизводства при осуществлении правосудия в разумный срок и тем самым — предупреждению названных преступлений.

Глава 4

МЕЖДУНАРОДНЫЕ ПОДХОДЫ К ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

4.1. Зарубежный опыт противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации

К настоящему времени в зарубежных странах накоплен значительный опыт противодействия преступлениям в сфере ИКТ, представляющий несомненный интерес для российского законодателя и правоприменителя.

Ввиду глобальных процессов информатизации, происходящих в современном мире, вышеуказанные деяния уже вышли за рамки одного из видов общеуголовной преступности и превратились в глобальную угрозу, как для основ существующего международного правопорядка, так и для национальной безопасности отдельных государств. Если на заре своего появления компьютерные преступления выступали чаще всего как способ хищения или как проявление хулиганства, то теперь все чаще приходится сталкиваться с таким феноменом, как «кибертерроризм» и организованными хакерскими атаками, носящими диверсионный, антигосударственный характер.

Поэтому борьба с такими преступлениями рассматривается теперь не только в русле уголовной политики, но и в рамках стратегии обеспечения национальной безопасности.

К настоящему моменту стратегии кибербезопасности приняты в Австралии (2011 г.) Индии (2011 г.), Канаде (2010 г.), Новой Зеландии (2011 г.), Норвегии (2012 г.), США (2011 г.), Швейцарии (2012 г.), ЮАР (2010 г.), Японии (2013 г.) и многих других государствах.

В ряду стран — членов Евросоюза такие стратегии приняли: Швеция (2008 г.), Эстония (2008 г.), Финляндия (2008 г., 2013 г.), Словакия (2008 г.), Великобритания (2009 г., 2011 г.), Германия (2011 г.), Литва (2011 г.), Люксембург (2011 г.), Нидерланды (2011 г.), Польша (2011 г.), Румыния (2011 г.), Франция (2011 г.), Чехия (2011 г.), Австрия (2012 г.).

Этот список стран наглядно показывает, что проблема кибербезопасности признается важной во всем мире.

Так, во **Франции** в 2008 г. была разработана Стратегия по защите и безопасности «Белая книга»[1], в которой защита информационных систем была определена как сфера, в которой необходимо полностью реализовывать суверенитет Франции. В рамках указанной Стратегии и целях укрепления национального потенциала в сфере кибероборонь в 2009 г. Главное управление компьютерной безопасности (DCSSI) было преобразовано в Национальное агентство безопасности информационных систем (Agence Nationale la Sécurité des Systèmes d'Information, ANSSI). Оно служит межведомственным органом под прямым руководством премьер-министра, ответственным за координацию деятельности по обеспечению кибербезопасности в национальном масштабе для ключевых предприятий и государственных органов, включая Вооруженные силы. С 2011 г. ANSSI является также национальным органом, несущим ответственность за оборону информационных систем и сетей как в государственном, так и в частном секторах.

В **Германии** в 2011 г. правительство публиковало первую версию документа «Стратегия кибербезопасности для Германии», в котором выделяется несколько стратегических областей и целей для более успешной борьбы с киберугрозами. Кроме того, указанный документ определил Федеральный офис информационной безопасности Министерства внутренних дел (Bundesamt für Sicherheit in der Informationstechnik, BSI) органом, ответственным за кибербезопасность страны, а также ответственным за реализацию указанной стратегии. BSI был создан в 1991 г. для предоставления услуг в области IT-безопасности федеральному правительству, ИКТ-компаниям, частным и коммерческим пользователям, а также интернет-провайдерам Германии.

В июне 2011 г. министр внутренних дел ФРГ официально открыл в Бонне Национальный центр киберзащиты (Nationales Cyber-Abwehrzentrum, NCAZ), который призван координировать работу целого ряда федеральных ведомств в борьбе с киберпреступностью[2]. Новая структура работает под эгидой вышеупомянутого Федерального

---

[1] Défense et Sécurité nationale: le Livre blanc. 2008 // URL: https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000341.pdf (дата обращения: 16.06.2020).

[2] URL: https://www.securitylab.ru/news/405957.php (дата обращения: 17.06.2020).

ведомства по безопасности в сфере информационной техники (BSI). К работе центра киберзащиты подключены Федеральное ведомство по охране Конституции, Федеральное ведомство по защите населения и чрезвычайным ситуациям, а также Федеральное ведомство по уголовным делам (BKA), Федеральная разведслужба (BND) и бундесвер.

В соответствии с Национальной стратегией кибербезопасности от 2011 г. был также создан Национальный совет кибербезопасности, целью которого было позволить секретариатам всех министерств внести вопросы кибербезопасности в стратегии реализации всех политических направлений деятельности в стране. Совет также координирует применение единых для государственного и частного секторов превентивных мер и междисциплинарных подходов в области кибербезопасности. Помимо представителей центрального правительства и земель Германии в Совет входят также представители каждого министерства (в том числе обороны, внутренних дел, экономики и технологий и других). На заседания в качестве ассоциированных членов часто приглашаются представители частного бизнеса[1].

В июле 2015 г. в Германии был принят Акт об информационной безопасности (IT Security Act), целью которого является предотвращение ущерба важнейшим IT-системам, таким, например, как системы Министерства внутренних дел (BSI), провайдеров телекоммуникационных услуг, операторов критически важных элементов инфраструктуры и др.[2]

В **Италии** полиция по охране почты и телекоммуникаций является ведущим правоохранительным органом, ответственным за профилактику киберпреступлений и охрану критически важных элементов инфраструктуры в Италии. Почта Италии в течение десятилетий предоставляет онлайн-услуги миллионам своих клиентов и уже разработала и ввела в действие сложную систему мониторинга и защиты своих сетей от кибератак.

В 2008 г. Министерство внутренних дел своим указом создало специализированный Центр по борьбе с киберпреступностью и защите критически важной инфраструктуры (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, CNAIPIC), который является подразделением почтовой полиции, напрямую ответственным за все мероприятия по профилактике, локализации, борьбе и расследованиям киберпреступлений и других вредоносных кибердействий в отношении критически важных элементов инфраструктуры. CNAIPIC, являясь правоохранительным органом, работает

---

[1] URL: https://digital.report/kibergotovnost-germanii-2-0-natsionalnaya-strategiya/ (дата обращения: 17.06.2020).

[2] URL: https://digital.report/kibergotovnost-germanii-2-0-kiber-prestupnost-i-ohrana-pravoporyadka/ (дата обращения: 17.06.2020).

в круглосуточном режиме и состоит из оперативного, технического и следственного отделов.

В Италии существуют и другие правоохранительные органы, призванные бороться с киберпреступностью. Итальянская полиция и Карабинеры — национальная жандармерия, исполняющая одновременно полицейские и военные функции, — создали специальные подразделения, занимающиеся борьбой с киберпреступностью, а также компьютерной криминалистикой и научными исследованиями. Кроме того, Финансовая полиция (Guardia di Finanza, GdF) несет ответственность за реализацию решений по блокировке веб-ресурсов, нарушающих авторское право либо совершающих иные правонарушения[1].

В 2013 г. утвержден «Декрет Премьер-министра, содержащий стратегическое руководство по национальной киберзащите и информационной безопасности», на основе которого в том же году в Италии были опубликованы «Национальный стратегический рамочный план безопасности киберпространства» и прилагаемый к нему план реализации, «Национальный план защиты киберпространства и безопасности ИКТ». Декретом 2013 г. был создан Отдел кибербезопасности (Nucleo per la sicurezza cibernetica, NSC), постоянный орган при Канцелярии Премьер-министра, который состоит из представителей Министерств иностранных дел, внутренних дел, юстиции, обороны, экономики и финансов, экономического развития, Департамента защиты гражданских прав и некоторых других ведомств.

Великобритания опубликовала свою национальную Стратегию кибербезопасности в 2009 г. и внесла в нее изменения в 2011 г. В соответствии с этим документом в 2014 г. был создан Центр оценки киберситуации и первая Национальная команда киберреагирования (CERT-UK).

В октябре 2016 г. в Лондоне начал функционировать Национальный центр кибербезопасности Великобритании (National Cybersecurity Center, NCSC) — организация правительства Великобритании, которая оказывает консультативную помощь и поддержку государственному и частному секторам в вопросах предотвращения угроз компьютерной безопасности.

В 2013 г. сформировано Национальное подразделение по вопросам киберпреступности (National Cyber Crime Unit, NCCU) при Национальном агентстве по борьбе с преступностью (National Crime Agency), которое призвано нести ответственность за координацию национальных действий в области реагирования на наиболее серьезные киберугрозы и оказывать экспертную поддержку партнерам в этой области; а также созданы киберкоманды при каждом из девяти региональных агентств по борьбе с организованной преступностью (ROCU).

---

[1] URL: https://digital.report/kibergotovnost-italii-2-0-kiberprestupnost-i-ohrana-pravoporyadka/ (дата обращения: 17.06.2020).

В **США** в 2018 г. президент утвердил новую Национальную стратегию кибербезопасности — 2018, в которой перечисляются шаги, предпринимаемые федеральным правительством, для обеспечения открытого, безопасного, интероперабельного и надежного киберпространства[1].

Еще в 2008 г., в рамках Комплексной национальной инициативы по кибербезопасности (CNCI), экс-президент Джордж Буш постановил, что Министерство юстиции и ФБР будут являться «ведущими организациями в области расследования киберпреступлений и преследования преступников». Для реализации этой задачи создавалась Совместная национальная оперативная группа кибериссследований (NCIJTF).

В 2014 г. Министерство юстиции США сообщило о формировании нового отдела, который будет специализироваться на расследовании компьютерных преступлений[2]. Отдел создан при уголовном подразделении министерства, в секции «Компьютерные преступления и интеллектуальная собственность» (Computer Crime and Intellectual Property). Его задачей станет сотрудничество с компаниями частного сектора и правоохранительными органами для повышения эффективности мер кибербезопасности в общественном и частном секторах.

В ФБР создано собственное специализированное Кибер-подразделение (Cyber Division, CyD), которое реализует свою деятельность с использованием ресурсов NCIJTF и координирует работу специальных киберкоманд в 56 региональных офисах на всей территории США.

При Секретной службе США (United States Secret Service — USSS) также создана специальная структура по расследованию электронных и финансовых преступлений. Секретная служба создала Целевую группу по электронным преступлениям, работающую в национальном и международном масштабах, основная цель которой — обнаружение и определение личностей киберпреступников, связанных с преступной деятельностью в киберпространстве, банковским мошенничеством, взломом баз данных, а также другими преступлениями в IT-сфере. Секция киберразведки (Cyber Intelligence Section) Секретной службы напрямую участвовала в аресте международных киберпреступников, ответственных за кражу сотен миллионов номеров кредитных карт и последующую кражу более 600 млн долларов со счетов финансовых и торговых организаций. Кроме того, Секретная служба является учредителем Национального

---

[1] URL: https://tass.ru/mezhdunarodnaya-panorama/5588614 (дата обращения: 17.06.2020).

[2] URL: https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-cybercrime-2020-symposium (дата обращения: 17.06.2020).

института компьютерных расследований (National Computer Forensic Institute), который предоставляет обучение и информацию по борьбе с киберпреступностью офицерам правоохранительных органов, прокурорам и судьям[1].

В **Японии** правительство постоянно обновляет свою стратегию кибербезопасности. С момента публикации в 2006 г. «Первой национальной стратегии информационной безопасности» в нее несколько раз вносились изменения и дополнения. Так, уже в 2009 г. в Японии опубликовали «Вторую национальную стратегию информационной безопасности», а в 2013 г. Совет по политике в области информационной безопасности выпустил в свет первую национальную «Стратегию кибербезопасности». В 2015 г. Японский кабинет министров одобрил вторую «Стратегию кибербезопасности», разработка которой велась на основе положений «Основного закона о кибербезопасности» 2014 г. В Стратегии-2015 также определен орган, ответственный за ее реализацию, — Стратегический штаб по обеспечению кибербезопасности. Образованная в 2014 г. посредством реорганизации Совета по политике в области информационной безопасности новая организация действует как командный и контрольный орган в вопросах, связанных с национальной кибербезопасностью, а также как орган, наделенный полномочиями давать рекомендации в сфере кибербезопасности другим госучреждениям. Стратегический штаб по обеспечению кибербезопасности возглавляется Главным секретарем кабинета министров; в него также входят Министр иностранных дел, Министр обороны, Министр торговли и экономики, Министр внутренних дел, Председатель Комиссии по национальной безопасности, а также другие участники и специалисты, назначаемые лично премьер-министром[2]. В настоящий момент действует Стратегия кибербезопасности 2019 г.

Конечно, в основе любой системы противодействия инфор-мационно-телекоммуникационным и компьютерным преступлениям лежит **уголовное законодательство, устанавливающее ответственность за соответствующие деяния.**

Первый специальный закон, касающийся информационных преступлений, были издан в Швеции в 1973 г.

В США такие законы стали появляться во второй половине 1970-х годов. Далее соответствующие изменения и дополнения в уголовное законодательство были внесены Канадой в 1985 г., Германией в 1986 г., Японией в 1987 г., Англией и Францией в 1990 г., Ирландией, Порту-

---

[1] URL: https://digital.report/kibergotovnost-ssha-2-0-kiberprestupnost-i-ohrana-pravoporyadka/ (дата обращения: 17.06.2020).

[2] URL: https://digital.report/kibergotovnost-yaponii-2-0-natsionalnaya-strategiya/ (дата обращения: 17.06.2020).

галией и Турцией в 1991 г., Люксембургом и Нидерландами в 1993 г., Израилем в 1995 г., Бельгией в 2000 г.

Специальные нормы или даже разделы о компьютерных преступлениях содержат все новые уголовные кодексы, принимаемые в мире начиная с 1992 г., в том числе уголовные кодексы всех стран СНГ и Балтии.

К настоящему времени законодательная база для борьбы с информационными и компьютерными преступлениями существует уже почти во всех странах мира; в некоторых из них соответствующие нормы содержатся не в УК, а в специальных законах (Индия, Израиль, Малайзия, Пакистан, Португалия, Филиппины, Чили).

В современных национальных законодательствах имеют место два основных подхода к криминализации компьютерных преступлений.

Согласно первому из них ряд преступлений, связанных с использованием компьютерной техники и информации, выделяется в специальную главу, исходя из того, что главным Объектом посягательства для всех них является информационная безопасность. При этом остальные деяния, имеющие компьютерную технику и информацию в качестве предмета преступления или способа совершения, преследуются на основании статей о преступлениях, имеющих иной родовой и видовой объект посягательства.

Второй подход заключается в том, что у любого из «компьютерных» преступлений свой конкретный объект посягательства (собственность, права личности, общественная безопасность и т.д.), поэтому составы рассматриваемых деяний рассредоточены по соответствующим разделам Особенной части уголовного закона.

Первый подход принят в странах СНГ, Андорре, Литве, Монголии, Польше, Румынии, Сербии, Черногории.

Основная проблема первого подхода состоит в том, что полностью выделить компьютерные преступления из общей массы других деяний просто невозможно, так как между ними отсутствуют четкие границы. Поэтому в ряде постсоветских стран совершение деяния в информационно-телекоммуникационных сетях (включая сеть Интернет) или с их использованием предусмотрено в качестве квалифицирующего или альтернативного признака тех или иных преступлений. Нельзя не отметить, что указанные признаки появились в уголовном законодательстве всего несколько лет назад, что отражает общую тенденцию: по мере информатизации современного общества использование телекоммуникационных технологий становится все более универсальным способом совершения широкого круга «традиционных» преступлений, нередко существенно повышая их общественную опасность.

Второй подход, при котором составы компьютерных преступлений не выделяются по общему объекту посягательства, имеет место в уголовных кодексах Австрии, Германии, Испании, Эстонии, Японии.

Во Франции, Хорватии, Швейцарии и Эстонии специальные составы компьютерных преступлений отнесены к преступным деяниям против имущества.

Анализ современных уголовных законодательств позволяет выделить следующие **основные составы компьютерных преступлений**:

1) несанкционированный доступ в компьютерные сети (СНГ, Австралия, Бельгия, Боливия, Великобритания, Германия, Дания, Ирландия, Канада, КНР, Колумбия, Латвия, Мексика, Нидерланды, Норвегия, Польша, Португалия, Румыния, Сербия, Словения, США, Франция, Хорватия, Швейцария, Эстония);

2) создание и распространение компьютерных вирусов (страны СНГ и Балтии, Бельгия, Вьетнам, Гватемала, Индия, Италия, КНР, Монголия, Нидерланды, Сербия, США, Швейцария);

3) компьютерный саботаж (Армения, Беларусь, Германия, Кыргызстан, Нидерланды, Парагвай, Польша, Португалия, Сербия, Таджикистан, Узбекистан, Эстония);

4) изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной информации, системе или сети (Армения, Беларусь, Великобритания, Италия, Канада, КНР, Монголия, США, Таджикистан, Украина, Хорватия);

5) нарушение правил эксплуатации компьютерной системы или сети (Азербайджан, Армения, Беларусь, Вьетнам, Грузия, Кыргызстан, Латвия, Молдова, Таджикистан, Украина);

6) хищение путем использования компьютерной техники (Армения, Беларусь, Боливия);

7) компьютерное мошенничество (Австрия, Сербия, Хорватия, Черногория, Эстония, Япония).

Наряду с вышеперечисленными в отдельных странах в последние годы появляются и другие составы преступлений, которые можно отнести к компьютерным: кибертерроризм (Грузия, США), распространение спама (США, Украина), компьютерный подлог (Бельгия, Хорватия), использование компьютерных данных и технологий в корыстных целях извлечения прибыли путем создания финансовых и других «пирамид» (Канада).

В **Германии** преступления, совершенные с использованием информационно-коммуникационных технологий, входят в различные разделы Уголовного кодекса.

Уголовно-правовому преследованию подвергаются такие деяния, как шпионаж данных (§ 202a), нарушение телекоммуникационной тайны (§ 206), изменение данных (§ 303a), компьютерный саботаж (§ 303b), компьютерное мошенничество (§ 263a), фальсификация данных, имеющих доказательственное значение (§ 269), обман в право-

применительной деятельности путем использования результатов переработки данных (§ 270) и другие.

Шпионаж данных (§ 202a) представляет собой преступление, нарушающее неприкосновенность и тайну частной жизни, и заключается в незаконном получении и передаче данных, не принадлежащих этому лицу и особо охраняемых от незаконного доступа. При этом под данными (Daten) понимается информация, сохраненная или передаваемая электронным, магнитным или иным, непосредственно визуально не воспринимаемым способом.

Противоправное аннулирование, уничтожение, приведение в непригодность или изменение данных является признаком состава преступления, предусмотренного § 303a.

Предметом компьютерного саботажа являются данные, которые имеют существенное значение для чужого предприятия, чужой фирмы или государственного органа. Уголовную ответственность влечет совершение с ними действий, указанных в § 303a, а также повреждение программы обработки (установки) данных либо носителя данных.

Фальсификация данных, имеющих доказательственное значение (§ 269), предполагает их сохранение или изменение с помощью ЭВМ, путем обмана, приводящее к восприятию документов как сфальсифицированных или поддельных, либо использование такого рода сохраненных или измененных данных.

В качестве самостоятельного вида мошенничества УК ФРГ выделяет компьютерное мошенничество, закрепляя в § 263a ответственность лица, причиняющего вред имуществу другого лица, путем воздействия на результат обработки данных неправильным созданием программ, использованием неправильных или неполных данных или иным неправомочным воздействием на результат обработки данных с целью получения имущественной выгоды для себя или третьего лица.

В отличие от основного состава мошенничества компьютерное мошенничество включает обман, направленный не на человека, а на программу, а ущерб в таком случае является результатом воздействия на процесс переработки информации. Исследователи германского уголовного права выделяют следующие формы компьютерного мошенничества: 1) мошенничество с товарами, приобретенными на онлайн-аукционах или в интернет-магазинах; 2) мошенничество с кредитными картами, в том числе в банкоматах; 3) новые методы мошенничества со счетами и отмыванием денег, например создание компаний по депонированию денежных средств; 4) рекламное мошенничество путем наиболее типичных обманных схем с адресными книгами; 5) мошенничество в сфере добросовестной конкуренции, в частности направленное на обманное предоставление конкурент-

ного преимущества; 6) клик-мошенничество, когда используется интернет-реклама (или «спонсорские списки») услуг, к примеру страхования в «один клик»[1].

Во **Франции** ответственность за информационные и компьютерные преступления предусмотрена в Уголовном кодексе[2]. Так, в главе № 6 (тома № 2) предусмотрена уголовная ответственность за публикацию информации любыми средствами, без согласия заинтересованного лица (ст. 226-8) — 1 год тюремного заключения. Здесь же в разделе 5, касающемся нарушения прав человека в результате использования компьютерных файлов или обработки данных, предусмотрены наказания в виде штрафов до 300 тыс. евро или тюремного заключения до 5 лет за сбор данных обманным, самоуправным или запрещенным законом способом, обработка персональных данных (ст. 226-16—226-18); ввод или хранение на компьютере без согласия заинтересованного лица и помимо случаев, предусмотренных законом, именной информации (ст. 226-19).

Также УК Франции содержит уголовные нормы (ст. 323-1–323-4), предусматривающие санкции — штраф до 300 тыс. евро или до 5 лет тюремного заключения за посягательство на системы автоматизированной обработки данных, незаконный доступ к автоматизированной системе обработки данных, изменение или уничтожение содержащихся в автоматизированной системе данных.

До 10 лет тюремного заключения, штраф до 225 тыс. евро предусмотрены в разделе 1 тома № 4 «Преступления против нации, государства и общественного порядка», предусматривающие ответственность за сбор или передачу компьютерных файлов иностранному государству; уничтожение, хищение, изъятие или копирование данных, носящих характер секретов национальной обороны.

Уничтожение, порча или незаконное присвоение любого документа, оборудования, сооружения, снаряжения, установки, аппарата, технического устройства или системы автоматизированной обработки информации либо внесение неполадок в их работу, если эти деяния способны причинить вред основополагающим интересам нации, наказываются 15 годами тюремного заключения или штрафом до 300 тыс. евро (ст. 411-9); террористические акты в области информатики (глава 2, том № 4) — до 30 лет тюремного заключения.

В **Великобритании** ответственность за компьютерные преступления установлена в статутах, принятых Парламентом. Преступность деяний непосредственно в сфере компьютерной информации установлена

---

[1] *Семыкина О. И.* Компаративистские исследования уголовного права, криминологии и уголовно-исполнительного права // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6. С. 109.

[2] URL: https://www.legifrance.gouv.fr/ (дата обращения: 11.06.2020).

Законом о злоупотреблении компьютерами 1990 г.[1] В соответствии с названным законом к уголовно наказуемым отнесены:

— умышленный незаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам (ст. 1);
— умышленный, незаконный доступ к компьютеру или содержащимся в нем информации и программам с намерением совершить или облегчить совершение другого преступления (ст. 2);
— незаконные действия, в результате которых произошло ухудшение работы компьютера (ст. 3);
— несанкционированные действия, причинившие значительный ущерб (ст. 3 ZA);
— незаконный оборот программ или данных, хранящихся в электронной форме для совершения компьютерного преступления (ст. 3A).

По ст. 1 ответственность наступает за сам факт несанкционированного доступа при осознании лицом незаконности своих действий; при этом не имеет значения, было ли у лица намерение получить доступ к конкретной программе или данным; программе или данным определенного вида либо программе или данным, хранящимся на определенном компьютере.

Незаконный доступ квалифицируется по ст. 2 при направленности действий на совершение или облегчение совершения другого преступления самим виновным или другими лицами. Причем факт совершения последующего преступления не имеет значения для уголовно-правовой оценки деяния по признакам неправомерного доступа.

В ст. 3 ответственность установлена за совершение любых незаконных действий в отношении компьютера, приводящих умышленно или по неосторожности к нарушению работы компьютера, созданию препятствий для доступа к любой программе или данным, хранящимся на нем.

Причинение значительного ущерба или угроза его причинения в результате неправомерного доступа является признаком преступления, предусмотренного в ст. 3 ZA. Под ущербом в данной статье понимается ущерб благосостоянию людей (вред жизни, здоровью, нарушение обеспечения продуктами питания, водой, энергией или топливом, нарушение системы связи, разрушение объектов транспорта), вред окружающей среде, ущерб экономике страны либо национальной безопасности.

К незаконным действиям, криминализированным в ст. 3 A, относятся разработка, модификация, распространение и получение вредо-

[1] Computer Misuse Act 1990 // URL: http://www.legislation.gov.uk/ukpga/1990/18 (дата обращения: 17.06.2020).

носных программ или данных в электронной форме, предназначенных для совершения преступления.

В 2015 г. вышеназванный закон 1990 г. был обновлен принятием «Акта о серьезных преступлениях», который: 1) ввел новое наказание за неавторизированные действия, приводящие к серьезному вреду, 2) привел в действие Директивы ЕС об Атаках на информационные системы, а также 3) дал ясные трактовки, необходимые для работы правоохранительных органов.

Кроме указанного закона в Великобритании отношения в информационной сфере регулируются следующими актами Парламента, устанавливающими ответственность за компьютерные преступления и преступления, связанные с Интернетом: Законом о защите персональных данных (1998 г.), Законом об электронных коммуникациях (2000 г.).

Указанными актами к числу уголовно наказуемых отнесены легализация (отмывание) денежных средств или иного имущества, приобретенных преступным путем, совершенная с использованием компьютера; распространение детской порнографии с помощью компьютера или компьютерных сетей; несанкционированный перехват данных, передающихся по каналам связи (телекоммуникаций); незаконное разглашение персональных данных, в том числе с использованием компьютерных технологий; разглашение конфиденциальной информации, передающейся по электронным средствам коммуникации; незаконное проникновение в компьютеры, их системы или сети с целью использования полученной таким образом компьютерной информации для организации массовых насильственных действий.

Кроме того, Законом о телекоммуникациях (мошенничестве) (1997 г.) установлен запрет на владение и поставку другим лицам предметов в целях обманного получения закрытой информации путем использования телекоммуникационной системы. Схожая норма содержится в Законе о мошенничестве (2006 г.), криминализирующем владение, разработку, переработку и распространение программ или хранящихся в электронной форме данных, используемых для совершения мошенничества.

Закон о терроризме 2000 г. устанавливает, что незаконное проникновение в компьютеры, их системы или сети с целью организации массовых беспорядков или повлекшее значительный ущерб может быть приравнено к актам террора и влечь за собой повышенную ответственность.

В **США** сложилась одна из самых развитых систем противодействия киберпреступности. Уже в 1984 г. в этой стране был принят Закон о мошенничестве и злоупотреблении с использованием компьютеров — нормативный правовой акт, устанавливающий уголовную ответственность за преступления в сфере компьютерной информации.

Претерпев неоднократные изменения и дополнения, в настоящее время он включен в виде § 1030 Титула 18 Свода законов США[1].

Данный закон установил ответственность за деяния, предметом посягательств которых является «защищенный компьютер» (находящаяся в нем компьютерная информация). Под ним понимается:

1) компьютер, находящийся в исключительном пользовании правительства или финансовой организации, либо компьютер, функционирование которого было нарушено при работе в интересах правительства или финансовой организации;

2) компьютер, являющийся частью системы или сети, элементы которой расположены более чем в одном штате США.

Уголовная ответственность наступает в случаях:

1) несанкционированного доступа — когда посторонний по отношению к компьютеру или компьютерной системе человек вторгается в них извне и пользуется ими;

2) превышение санкционированного доступа — когда законный пользователь компьютера или системы осуществляет доступ к компьютерным данным, на которые его полномочия не распространяются.

Данный закон устанавливает ответственность за следующие противоправные деяния:

- намеренный несанкционированный доступ к компьютеру, превышение пределов санкционированного доступа, а также получение информации, которая может быть использована в ущерб США или в интересах иностранного государства (§ 1030 (a)(1));
- намеренный несанкционированный доступ к компьютеру либо превышение пределов санкционированного доступа к финансовым отчетам финансовых учреждений, эмитентов карт, департаментов и агентств США, а равно к иным защищенным компьютерам (§ 1030 (a)(2));
- умышленный несанкционированный доступ к компьютеру, находящемуся в исключительном пользовании правительственного ведомства США, или нарушение функционирования компьютера, используемого полностью или частично Правительством США (§ 1030 (a)(3));
- сознательный с намерением обмана несанкционированный доступ (или превышение пределов санкционированного доступа) к защищенному компьютеру в целях обманного получения какого-либо имущества, за исключением обмана, состоящего в использовании компьютера, если стоимость такого использования не превышала 5000 долл. США в срок до одного года (§ 1030 (a)(4));

---

[1] Federal Criminal Code and Rules/ Title 18 — Crimes and Criminal Procedure // URL: https://www.law.cornell.edu/uscode/text (дата обращения: 17.06.2020).

— несанкционированные преднамеренные получение, передача программ, информации, компьютерных кодов, команд и иных сведений о доступе к защищенному компьютеру, причинившие ущерб, то есть любое нарушение целостности или доступности данных, программы, системы или информации, а также причинение ущерба в результате несанкционированного преднамеренного доступа к защищенному компьютеру (§ 1030 (a)(5));
— мошенничество путем торговли компьютерными паролями или аналогичной информацией, позволяющей получить несанкционированный доступ к информации, если такая торговля влияет на торговые отношения между штатами и с другими государствами, или на компьютер, используемый правительством США (§ 1030 (a)(6));
— передача электронных сообщений, содержащих угрозы повреждения защищенного компьютера, несанкционированного получения информации и нарушения конфиденциальности сведений, совершенная в целях вымогательства денежных средств или иного имущества, а равно содействия такому вымогательству (§ 1030 (a)(7)).

В § 1029 Титула 18 Свода законов США предусмотрена ответственность за торговлю похищенными или поддельными устройствами доступа, которые могут быть использованы для получения денег, товаров или услуг.

Кроме того, в США к уголовно наказуемым деяниям относятся посягательства на неприкосновенность частной жизни, совершенные с применением информационно-коммуникационных технологий. К этой группе преступлений можно отнести перехват и разглашение сведений, передаваемых по телеграфу, устно или электронным способом (§ 2511), незаконный доступ к хранимым сообщениям, заключающийся в получении, изменении или создании препятствий для санкционированного доступа к сообщению, находящемуся в электронном хранилище (§ 2701).

В правоприменительной практике как компьютерные обманы квалифицируются следующие деяния: кража информации с компьютеров, принадлежащих финансовым учреждениям или федеральным агентствам, а также используемых в государственной торговой деятельности; кража средств электронного кошелька путем изменения учетных данных; несанкционированный доступ к информации, находящейся в государственных компьютерных системах; обманные почтовые лотереи (например, реализация схем, так называемых финансовых пирамид); перехват информации об одобренном кредите; получение PIN-кодов кредитных карт путем подглядывания, отслеживания или использования подслушивающих устройств; использование фальсифицированных средств телемаркетинга в целях получения частной

информации о клиентской базе (фишинг); предложения фиктивных вакансий, направленные по электронной почте; сбор конфиденциальной информации и ее последующее использование для получения выгоды; трафик похищенных паролей; угрозы повреждения компьютеров в целях вымогательства. Для совершения компьютерных обманов используются различные способы, например: несанкционированное изменение входа в компьютерную систему; модификация и удаление электронных сведений; несанкционированный перехват электронной передачи частной информации (паролей, данных кредитных карт и иных конфиденциальных сведений); умышленное или неосторожное повреждение электронных систем или баз данных; создание программных кодов и загрузка их в компьютерные системы банков в целях получения доступа к базам данных клиентов дистанционной системы обслуживания (информации по кредитным картам); компьютерные вирусы и черви[1].

Хотя в УК **КНР** нет специальной главы о преступлениях против информационной безопасности, однако путем логического анализа можно прийти к выводу, что к данной категории относятся деяния, предусмотренные в следующих 5 статьях: 285, 286, 286.1, 287.1, 287.2. При этом основные составы компьютерных преступлений соответствуют (в нашей терминологии) категории средней тяжести и тяжких.

Незаконное вторжение в компьютерно-информационные системы; незаконное получение компьютерно-информационных системных данных и т.д., а также предоставление специальных программ или инструментов, предназначенных для доступа и незаконного управления компьютерно-информационными системами (ст. 285) наказывается лишение свободы до 3 лет, а при особо отягчающих обстоятельствах — на срок от 3 до 7 лет.

Любое незаконное воздействие (включая создание и распространение компьютерных вирусов), приведшее к невозможности нормального функционирования компьютерной информационной системы, если это повлекло серьезные последствия, наказывается лишением свободы на срок до 5 лет, а при наличии особо серьезных последствий — на срок свыше 5 лет (ст. 286).

Специфической чертой китайского уголовного закона является установление ответственности за незаконное завладение каналами связи других людей, дублирование чужого номера электронной почты или пользование заведомо похищенными, дублированными электронными оборудованием и устройствами с целью извлечения прибыли (ст. 265), а также за невыполнение интернет-провайдером

[1] Цит. по: *Семыкина О. И.* Компаративистские исследования уголовного права, криминологии и уголовно-исполнительного права // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6. С. 108.

общественной обязанности по управлению кибербезопасностью информационной сети (ст. 286.1), незаконное использование информационных сетей (ст. 287.1) и содействие преступной деятельности в информационных сетях (ст. 287.2).

С особой тщательностью в Китае проработана система законодательного противодействию экстремизму и терроризму в информационных системах. Согласно ст. 18 Закона КНР о противодействии терроризму (принят 27 декабря 2015 г., вступил в силу 1 января 2016 г.) операторы телекоммуникаций и поставщики интернет-услуг должны в соответствии с законом предоставлять технические интерфейсы, расшифровку и оказывать другую техническую поддержку органам общественной безопасности и органам государственной безопасности, проводящим предотвращение и расследование террористической деятельности.

В соответствии со ст. 19 того же закона операторы электросвязи и провайдеры интернет-услуг в соответствии с положениями законодательства и административных правил применяют на практике системы сетевой безопасности и системы мониторинга информационного содержания, технические меры профилактики и безопасности, чтобы избежать распространения информации с террористическим или экстремистским содержанием. Если обнаружена информация с террористическим или экстремистским содержанием, ее распространение немедленно прекращается, соответствующие записи сохраняются и удаляется соответствующая информация, а также направляется отчет в органы общественной безопасности или соответствующие департаменты.

Несмотря на то, что угрозы информационно-телекоммуникационной и компьютерной безопасности объективно носят общий характер для всех современных государств, в области их криминализации между национальными законодательствами наблюдаются многочисленные и существенные расхождения.

Это связано не только с особенностью юридической техники, о чем говорилось выше, но и с высоким динамизмом развития данной сферы правового регулирования, не всегда поспевающим за быстрыми изменениями в технологиях и появлением новых способов их общественно-опасного использования. Часть расхождений объясняется и различиями в социально-политических системах, степени их открытости и приверженности соблюдению гражданских свобод.

Основную роль в борьбе с киберпреступностью в КНР играет Министерство общественной безопасности (аналог МВД), совместно с которым в этой сфере действуют Народный банк Китая, Верховная народная прокуратура, Верховный народный суд и Министерство промышленности и информационных технологий[1].

[1] URL: https://bits.media/pyat-ministerstv-kitaya-budut-borotsya-s-kiberprestupnostyu/ (дата обращения: 17.06.2020).

В **Индии** уголовная ответственность за преступления в сфере ИКТ предусмотрена Законом № 21 от 2000 г. «Об информационных технологиях»[1], который содержит 8 составов таких деяний.

В данном акте дается разъяснение терминов «информация» и «данные». Первый включает в себя «данные, сообщение, текст, изображения, звук, голос, коды, компьютерные программы, программное обеспечение и базы данных или микрофильм, или компьютерную микропленку». Под «данными» понимается «представление информации, знаний, фактов, концепций или инструкций, которые подготавливаются или были подготовлены формализованным образом и предназначены для обработки, обрабатываются или были обработаны в компьютерной системе или компьютерной сети, и могут быть в любой форме (включая компьютерные распечатки магнитных или оптических носителей информации, перфокарты, перфоленты) или храниться внутренне в памяти компьютера».

Компьютерные преступления с основным составом влекут наказание в виде лишения свободы сроком до 3 лет, в то время как совершение актов кибертерроризма наказуемо вплоть до пожизненного заключения.

В индийской полиции на местном уровне действуют отделы по борьбе с киберпреступностью. В 2001 г. в штате Бангалор открылся Участок полиции киберпреступности (Cyber Crime Police Station) — первое в стране самостоятельное ведомство подобного рода. В последующие годы подобные учреждения появились и в других штатах и крупных городах Индии (где именуются также Cyber Crime Investigation Cell или Cyber Crime Cell).

В **Пакистане** уголовная ответственность за рассматриваемые деяния (в количестве 11 составов) предусмотрена Законом № XL от 2016 г. «О предотвращении электронных преступлений»[2]. В нем подробно раскрывается только термин «информация», в то время как дефиниция понятия «данные» носит лаконичный характер (указано только, что данные могут относиться к контенту и к трафику). «Информация» включает в себя текстовое сообщение, данные, голос, звук, базу данных, видео, сигналы, программное обеспечение, компьютерные программы, различные формы интеллекта, определенные в соответствии с Законом о телекоммуникации (реорганизация) Пакистана 1996 г. (XVII от 1996 г.), и коды, включая объектный код и исходный код».

Злонамеренное незаконное проникновение в чужую информационную систему или повреждение ее данных наказуемо лишением

---

[1] URL: https://www.meity.gov.in/content/information-technology-act-2000 (дата обращения: 17.06.2020).

[2] URL: http://nasirlawsite.com/laws/peca1.htm (дата обращения: 17.06.2020).

свободы на срок до 2 лет, а в случае совершения аналогичных актов в отношении информационных систем или данных критической инфраструктуры — до 3 лет. Максимальный размер наказания за преступление кибертерроризма составляет 14 лет лишения свободы.

В 2007 г. в Пакистане был создан специальный центральный орган для координации борьбы с «электронными» преступлениями — Национальный центр противодействия киберпреступности (National Response Centre for Cyber Crime (NR3C)), который действует в системе Федерального бюро расследований (Federal Investigation Agency (FIA)) под эгидой министра внутренних дел.

В государствах на территории бывшего СССР основная ответственность за борьбу с киберпреступностью возложена на специальные подразделения министерств внутренних дел. В некоторых из этих стран, как и в России, это подразделение сокращенно именуется управлением «К» МВД. В Республике Беларусь его полное название — Управление по раскрытию преступлений в сфере высоких технологий (создано в 2002 г.).

В Казахстане в 2004 г. в структуре МВД было создано специализированное подразделение *(Управление «К» Департамента криминальной полиции)*, которое в январе 2019 г. преобразовано в Центр по борьбе с киберпреступностью с территориальными подразделениями (в структуре *Департамента криминальной полиции* МВД).

В 2009 г. специальный отдел МВД по борьбе с киберпреступностью организован в Кыргызской Республике.

В 2013 г. в структуре УБОП МВД Республики Таджикистан создано специализированное оперативное подразделение, задачей которого является выявление и раскрытие преступлений против информационной безопасности[1].

В мае 2017 г. подразделение Организация по борьбе с преступностью в сфере информационных технологий создано в составе Главного управления уголовного розыска МВД Узбекистана[2].

На **Украине** с 2015 г. действует Департамент киберполиции Национальной полиции Украины, созданный в результате трансформации управления МВД по борьбе с киберпреступностью. В его штате насчитывается около 400 сотрудников. У этой структуры есть собственный портал в сети Интернет[3].

---

[1] *Окилов С. Ю.* К вопросу о некоторых проблемах оперативно-розыскной деятельности органов внутренних дел Республики Таджикистан по борьбе с преступлениями против информационной безопасности, в том числе посягающими на банковскую сферу // Труды Академии управления МВД России. 2018. № 3. С. 163.

[2] URL: https://www.pv.uz/ru/newspapers/kiberprestupnost-vyzov-vremeni (дата обращения: 18.06.2020).

[3] URL: https://cyberpolice.gov.ua/ (дата обращения: 18.06.2020).

Можно предположить, что в связи с распространением киберпреступности будет повышаться и правовой статус специальных органов по борьбе с ней, которые из небольших оперативных подразделений в недрах МВД будут постепенно преобразовываться в самостоятельные структуры с системой территориальных отделений.

В последние годы в бывших советских республиках стали принимать документы программно-концептуального характера, посвященные информационной безопасности.

Так, можно упомянуть Стратегию кибербезопасности Кыргызской Республики на 2019–2023 гг., утвержденную постановлением Правительства Кыргызской Республики от 24 июля 2019 г. № 369, включающую раздел о противодействии компьютерной преступности.

В Казахстане постановлением Правительства Республики Казахстан от 30 июня 2017 г. № 407 утверждена Концепция кибербезопасности («Киберщит Казахстана»). Кроме того, постановлением правления Национального банка Казахстана от 29 октября 2018 г. утверждена Стратегии кибербезопасности финансового сектора Республики Казахстан на 2018–2022 гг.

В Беларуси постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 утверждена Концепция информационной безопасности Беларуси.

Как указывалось выше, в странах СНГ ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации, установлена в специальных главах уголовных кодексов (где родовым и видовым Объектом выступает информационная безопасность), однако в последние годы все шире применяется и другой подход, при котором совершение деяния с использованием телекоммуникационных сетей рассматривается в качестве элемента объективной стороны или квалифицирующего признака различного рода преступных посягательств (оскорбления, клеветы, экстремистских призывов, порнографии, мошенничества, хищения и т.д.).

В Уголовном кодексе **Республики Беларусь** от 9 июля 1999 г. (далее — УК Беларуси)[1] имеется глава 31 «Преступления против информационной безопасности», включающая 7 статей: несанкционированный доступ к компьютерной информации (ст. 349), модификация компьютерной информации (ст. 350), компьютерный саботаж (ст. 351), неправомерное завладение компьютерной информацией (ст. 352), изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353), разработка, использование либо распространение вредоносных программ

[1] Текст в ред. от 11 ноября 2019 г. в БД «Законодательство стран СНГ» (с) 2003–2019 СоюзПравоИнформ // URL: http://spinform.ru/ (дата обращения: 18.06.2020).

(ст. 354), нарушение правил эксплуатации компьютерной системы или сети (ст. 355).

Кроме того, в главе о преступлениях против собственности УК Беларуси содержится ст. 212 «Хищение путем использования компьютерной техники», под которым понимается хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации. В 2015 г. на долю этих деяний приходилось более 83% всей компьютерной преступности в Беларуси[1].

В зависимости от своего состава деяния, предусмотренные в гл. 31 УК Беларуси, относятся к преступлениям, как не представляющим большой общественной опасности, так и более тяжким. Например, общий и квалифицированный состав несанкционированного доступа к компьютерной информации (ст. 349) отнесены к первой категории, а особо квалифицированный — к последней (если деяние повлекло по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия).

Наиболее сурово (лишением свободы на срок от 3 до 10 лет) карается компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия (ч. 2 ст. 351), а также разработка, использование либо распространение вредоносных программ, повлекшие тяжкие последствия (ч. 2 ст. 354).

В качестве альтернативного признака объективной стороны использование глобальной компьютерной сети Интернет, иной сети электросвязи общего пользования или выделенной сети электросвязи предусмотрено в УК Беларуси для таких деяний, как клевета (ст. 188), оскорбление (ст. 189), клевета в отношении Президента Республики Беларусь (ст. 367).

В Уголовном кодексе **Республики Казахстан** от 3 июля 2014 г. (далее — УК Казахстана)[2] рассматриваемым деяниям посвящена гл. 7 «Уголовные правонарушения в сфере информатизации и связи», в которой предусмотрена ответственность за неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205), неправомерные уничтожение или модификация информации (ст. 206), нарушение работы информационной системы или сетей

---

[1] Обзор законодательства Республики Беларусь: Борьба с киберпреступностью // URL: https://digital.report/obzor-zakonodatelstva-respubliki-belarus-kiberprestupnost/ (дата обращения: 18.06.2020).

[2] Текст в ред. от 25 мая 2020 г. в БД «Законодательство стран СНГ» (с) 2003–2019 «СоюзПравоИнформ» // URL: http://spinform.ru/ (дата обращения: 18.06.2020).

телекоммуникаций (ст. 207), неправомерное завладение информацией (ст. 208), принуждение к передаче информации (ст. 209), создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210), неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211), предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212), неправомерные изменения идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213).

Категории преступлений в сфере компьютерной информации варьируются от небольшой тяжести до тяжких. Наиболее строго караются преступные деяния в отношении критически важных объектов информационно-коммуникационной инфраструктуры. Этот признак выступает квалифицирующим в шести составах из девяти. В отдельных случаях такие преступления (с учетом других квалифицирующих признаков) влекут наказание в виде лишения свободы на срок до 10 лет. Так, создание, использование или распространение вредоносных компьютерных программ и программных продуктов, если это деяние совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры, наказываются ограничением свободы на срок от 3 до 7 лет либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового. А если такое деяние совершено преступной группой или повлекло тяжкие последствия, за него предусмотрено лишение свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью (ст. 210).

По иным составам преступлений гл. 7 за совершение преступлений преступной группой либо повлекших тяжкие последствия также предусмотрено безальтернативное наказание в виде лишения свободы от 3 до 7 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок от 3 до 5 лет или без такового.

Кроме того, санкции за преступления в сфере информатизации и связи предусматривают наказания в виде штрафа, исправительных или общественных работ, ареста, ограничения свободы, а также лишения свободы и лишения права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет.

В **Кыргызстане** новый Уголовный кодекс Кыргызской Республики от 2 февраля 2017 г. № 19, вступивший в силу 1 января 2019 г. (далее —

УК Кыргызстана)[1], включает в себя главу 42 «Преступления против информационной безопасности». Кроме того, вступивший в силу также 1 января 2019 г. Кодекс Кыргызской Республики о проступках от 1 февраля 2017 г. № 18[2] содержит главу 29 «Проступки против информационной безопасности».

В гл. 42 УК Кыргызстана содержится всего 3 статьи: неправомерный доступ к компьютерной информации (ст. 304), создание вредоносных компьютерных программ (ст. 305) и компьютерный саботаж (ст. 306).

Все преступления в сфере компьютерной безопасности (включая квалифицированные составы) относятся к категории менее тяжких. Наиболее строгое наказание предусматривают нормы, закрепляющие квалифицированные составы неправомерного доступа к компьютерной информации (ч. 2 ст. 304), создания вредоносных компьютерных программ (ч. 2 ст. 305) и компьютерного саботажа, под которым понимается умышленные изменение, уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы без права на это либо вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы, а также вывод из строя компьютерного оборудования либо разрушение компьютерной системы или сети (ч. 2 ст. 306). За эти деяния установлено максимальное наказание в виде лишение свободы на срок от 2 лет 6 месяцев до 5 лет. При этом все статьи главы 42 УК Кыргызстана в качестве альтернативной санкции предусматривают штраф, в том числе за деяния с квалифицированным составом.

В Уголовном кодексе **Республики Таджикистан** от 21 мая 1998 г. № 574 (далее — УК Таджикистана)[3] глава 28 «Преступления против информационной безопасности» содержит 7 основных составов: неправомерный доступ к компьютерной информации (ст. 298), модификация компьютерной информации (ст. 299), компьютерный саботаж (ст. 300), незаконное завладение компьютерной информацией (ст. 301), изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 302), разработка, использование и распространение вредоносных программ (ст. 303), нарушение правил эксплуатации компьютерной системы или сети (ст. 304).

---

[1] Текст в ред. от 3 апреля 2020 г. в БД «Законодательство стран СНГ» (с) 2003–2019 СоюзПравоИнформ // URL: http://spinform.ru/ (дата обращения: 18.06.2020).

[2] Текст в ред. от 3 апреля 2020 г. в БД «Законодательство стран СНГ» (с) 2003–2019 СоюзПравоИнформ // URL: http://spinform.ru/ (дата обращения: 18.06.2020).

[3] Текст в ред. от 2 января 2020 г. в БД «Законодательство стран СНГ» (с) 2003–2019 СоюзПравоИнформ // URL: http://spinform.ru/ (дата обращения: 18.06.2020).

Рассматриваемые деяния в основной своей массе относятся к преступлениям небольшой тяжести, поскольку влекут наказание в виде лишения свободы сроком до 2 или 3 лет либо наказание, не связанное с лишением свободы. Наиболее строго карается незаконное завладение компьютерной информацией, совершенное повторно, организованной группой или повлекшее по неосторожности смерть человека либо иные тяжкие последствия (влечет безальтернативное лишение свободы на срок от 7 до 10 лет — ч. 4 ст. 301 УК Таджикистана). Напротив, изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети, а также разработка, использование и распространение вредоносных программ влекут штраф либо ограничение свободы на срок до 2 лет (ст. 302, ч. 1 ст. 303 УК Таджикистана).

Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру (аналог ст. 274.1 УК РФ) не установлена, хотя в статьях используется понятие «особо ценная информация» как оценочная категория.

В трех статьях допускается назначение исправительных работ, в одной — арест. Среди наказаний в основном предусмотрена альтернатива между штрафом и лишением свободы либо штрафом и ограничением свободы.

В Уголовном кодексе **Республики Узбекистан** от 22 сентября 1994 г. № 2012-XI (далее — УК Узбекистана)[1] в главе XX-1 «Преступления в сфере информационных технологий» также 7 основных составов: нарушение правил информатизации (ст. 278-1), незаконный (несанкционированный) доступ к компьютерной информации (ст. 278-2), изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций (ст. 278-3), модификация компьютерной информации (ст. 278-4), компьютерный саботаж (ст. 278-5), создание, использование или распространение вредоносных программ (ст. 278-6), незаконный (несанкционированный) доступ к сети телекоммуникаций (ст. 278-7).

Все преступления против информационных технологий отнесены к категории «не представляющих большой общественной опасности» (максимальное наказание составляет менее 3 лет лишения свободы), за исключением квалифицированного состава незаконного (несанкционированного) доступа к сети телекоммуникаций (ст. 278-7): данное преступление относится к категории менее тяжких преступлений (максимальное наказание — от 3 до 5 лет лишения свободы).

---

[1] Текст в ред. от 26 марта 2020 г. в БД «Законодательство стран СНГ» (с) 2003–2019 СоюзПравоИнформ // URL: http://spinform.ru/ (дата обращения: 18.06.2020).

В большинстве указанных выше стран СНГ в последние годы наблюдалась тенденция к ужесточению ответственности за преступления против информационной безопасности за счет введения новых квалифицирующих признаков.

Общим для рассматриваемой группы постсоветских государств является установление ответственности за два деяния: неправомерный доступ к компьютерной информации и создание, использование и распространение вредоносных программ. УК Беларуси (ст. 351), Таджикистана (ст. 300) и Кыргызстана (ст. 306) содержат сходные по своим признакам составы «компьютерный саботаж». В УК Узбекистана это понятие (ст. 278-5) касается только повреждения компьютерного оборудования, тогда как за порчу программного обеспечения и данных ответственность предусмотрена в ст. 278-4 «Модификация компьютерной информации». В УК Казахстана ответственность за аналогичные действия предусмотрена также двумя статьями: 206 «Неправомерные уничтожение или модификация информации» и 207 «Нарушение работы информационной системы или сетей телекоммуникаций». С учетом наличия в обеих статьях квалифицирующего признака «в отношении критически важных объектов информационно-коммуникационной инфраструктуры» они отчасти корреспондируют со ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» УК РФ.

В УК Таджикистана и УК Казахстана предусмотрена ответственность за принуждение к передаче компьютерной информации путем шантажа (ч. 2 ст. 301 УК Таджикистана и ст. 209 УК Казахстана). Аналогичная норма в УК Беларуси, Кыргызстана и Узбекистана отсутствует.

Помимо «специализированных» составов преступлений в информационной сфере уголовное законодательство Беларуси, Казахстана, Таджикистана, Узбекистана предусматривает использование компьютерной техники и информационных сетей как **квалифицирующий признак** ряда других преступных деяний.

Наиболее часто он встречается в УК Казахстана: квалифицирующий признак «с использованием телекоммуникационных сетей» предусмотрен в 17 статьях. Использование сетей телекоммуникаций признается квалифицирующим признаком клеветы (ст. 130), оскорбления (ст. 131), нарушения неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите (ст. 147), пропаганды или публичных призывов к развязыванию агрессивной войны (ст. 161), возбуждения социальной, национальной, родовой, расовой, сословной или религиозной розни (ст. 174), пропаганды или публичных призывов к захвату или удержанию власти (ст. 179), сепаратистской деятельности (ст. 180), пропаганды терроризма или публичные призывы к совершению акта

терроризма (ст. 256), распространения заведомо ложной информации (ст. 274), оскорбления представителя власти (ст. 378) и некоторых других деяний. Совершение деяния путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций, является квалифицирующим признаком кражи (ст. 188), причинения имущественного ущерба путем обмана или злоупотребления доверием (ст. 195).

По УК Таджикистана совершение деяния с использованием средств компьютерной техники признается квалифицирующим признаком подделки, изготовления или сбыта поддельных документов, государственных наград, штампов, печатей, бланков (ст. 340). Использование средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть Интернет), — квалифицирующим признаком незаконных изготовления и оборота порнографических материалов или предметов (ст. 241), изготовления и оборота порнографических материалов или предметов с изображениями несовершеннолетних (ст. 241(1)), использования несовершеннолетнего в целях изготовления порнографических материалов или предметов (ст. 241(2)).

По УК Узбекистана совершение деяния с использованием средств компьютерной техники признается квалифицирующим признаком хищения путем присвоения и растраты (ст. 167) и мошенничества (ст. 168), а совершение деяния с несанкционированным проникновением в компьютерную систему — квалифицирующим признаком кражи (ст. 169). Использование сетей телекоммуникаций, а также всемирной информационной сети Интернет выступает квалифицирующим признаком таких деяний, как доведение до самоубийства (ч. 2 ст. 103), склонение к самоубийству (ч. 2 ст. 103-1), незаконная деятельность по привлечению денежных средств и (или) иного имущества (ч. 2 ст. 188-1), изготовление, хранение, распространение или демонстрация материалов, содержащих угрозу общественной безопасности и общественному порядку (ч. 3 ст. 244-1). Предоставление услуг в сетях телекоммуникации, в том числе провайдерами всемирной информационной сети Интернет, тиражирование, размножение, распространение соответствующего программного обеспечения для организации или проведение азартных и других основанных на риске игр, совершенные после применения административного взыскания за такие же действия, является одним из альтернативных составов такого преступления, как организация и проведение азартных и других основанных на риске игр (ст. 278).

По УК Беларуси использование глобальной компьютерной сети Интернет, иной сети электросвязи общего пользования или выделенной сети электросвязи предусмотрено в качестве квалифицирующего признака при совершении преступлений порнографии (ст. 343), дет-

ской порнографии (ст. 343–1), призывах к действиям, направленным на причинение вреда национальной безопасности Республики Беларусь (ст. 361).

По УК Кыргызстана только для одного преступления, организация финансовых пирамид, предусмотрен квалифицирующий признак «совершенные путем осуществления незаконных операций с использованием компьютерных, информационных или телекоммуникационных систем либо сетей или систем электронных платежей» (ч. 2 ст. 214).

Вышеуказанные квалифицирующие и альтернативные признаки появились в уголовном законодательстве постсоветских стран всего несколько лет назад, что отражает общую тенденцию: по мере информатизации современного общества использование телекоммуникационных технологий становится все более универсальным способом совершения широкого круга «традиционных» преступлений (против личности, собственности, общественной безопасности, конституционного строя и т.д.), нередко существенно повышая их общественную опасность.

4.2. Проблемы международно-правового сотрудничества при выявлении, расследовании и предупреждении преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации

Компьютерная преступность является одной из самых специфических, сложно устроенных и динамично развивающихся видов преступности. Современная киберпреступность — серьезная угроза как для отдельных государств, так и для всего мирового сообщества[1].

Как отмечалось, преступления в сфере высоких технологий имеют глобальный характер и элементы транснациональности, что делает международное сотрудничество ключевым фактором принятия эффективных мер противодействия.

Основными целями международного сотрудничества являются:

— совершенствование международного-правового регулирования в соответствующей области;
— гармонизация на основе международных норм и рекомендаций национальных законодательств;
— достижение единства действий государств в лице национальных правоохранительных органов при расследовании преступлений.

Как и в других сферах, сотрудничество государств в борьбе с компьютерными преступлениями базируется на конвенционном

[1] *Бессонов С. А.* История и зарубежный опыт правовой регламентации компьютерной преступности // Территория науки. 2013. № 2. С. 232.

(договорно-правовом) и институциональном (в рамках международных организаций) механизмах.

Современное состояние международного сотрудничества в борьбе с киберпреступлениями характеризуется следующими особенностями:

— тенденцией к фрагментации сотрудничества в рамках региональных организаций и интеграционных объединений, создающих свои механизмы сотрудничества;
— отсутствием четкого понимания явления и общих определений основных используемых понятий, в том числе в научном дискурсе;
— наличием обстоятельств, при которых развитие законодательной деятельности существенно отстает от развития информационных технологий, в том числе новых форм киберпреступности;
— противоречиями между государствами по вопросам процедур сотрудничества, затрагивающих принцип суверенитета[1].

Традиционно целями международного сотрудничества выступают совершенствование международного правового пространства, а также слаженная координация действий компетентных органов иностранных государств при выявлении, расследовании и предупреждении преступлений.

Универсальным международным документом в рассматриваемой области выступила Конвенция Совета Европы о киберпреступности, заключенная в Будапеште 23 ноября 2001 г. Данная конвенция является самым первым международным договором о преступлениях, совершенных через Интернет и другие компьютерные сети, и касается, в частности, нарушений авторских прав, компьютерных мошенничеств, детской порнографии и нарушений безопасности сети. Она также содержит ряд полномочий и процедур, таких как обыск компьютерных сетей и перехват. Протокол к ней от 28 января 2003 г.[2] добавил в перечень преступлений распространение информации расистского и другого характера, подстрекающей к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающимся на расовой, национальной, религиозной или этнической принадлежности.

Несмотря на название указанных документов, к их реализации присоединились также более 20 государств — не членов Совета Европы: Австралия, Аргентина, Гана, Израиль, Маврикий, Канада, Колумбия, Перу, США, ЮАР, Япония и др. Таким образом, по состоянию на июнь 2020 г. Конвенцию и протокол к ней ратифицировали 65 государств.

Россия в этом договоре не участвует в силу распоряжения Президента Российской Федерации от 22 марта 2008 г. № 144-рп «О при-

---

[1] *Шматкова Л. П.* Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. 2016. № 28. С. 720–723.

[2] URL: https://www.coe.int/ru/web/conventions/full-list (дата обращения: 11.06.2020).

знании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности»[1]. Хотя при его подписании Россия оставляла за собой право определиться с участием в Конвенции при условии возможного пересмотра положений пункта «b» ст. 32, которые «могут причинить ущерб суверенитету и безопасности государств — участников конвенции и правам их граждан». Согласно этому пункту договаривающаяся сторона может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему.

Таким образом, в настоящий момент Россия не имеет единого специального договора с ведущими зарубежными странами о борьбе с компьютерными преступлениями, несмотря на тот факт, что наше государство последовательно выступает с инициативой разработки универсальной конвенции по международному противодействию информационной преступности под эгидой ООН[2], однако перспективы принятия такого акта остаются пока крайне проблематичными из-за противодействия западных государств.

Вместе с тем имеется ряд резолюций Генеральной Ассамблеи ООН, касающихся вопросов защиты информации ресурсов в контексте международного взаимодействия в борьбе с преступлениями в сфере компьютерных технологий:

- резолюция RES/55/28 от 20 ноября 2000 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»;
- резолюция RES/56/121 от 19 декабря 2001 г. «Борьба с преступным использованием информационных технологий»;
- резолюция RES/65/141 от 20 декабря 2010 г. «Использование информационно-коммуникационных технологий в целях развития»;
- резолюция A/RES/64/211 от 21 декабря 2009 г. «Создание глобальной кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур»;

---

[1] СЗ РФ. 2008. № 13. Ст. 1295.

[2] Проект конвенции ООН «О сотрудничестве в сфере противодействия информационной преступности» был подготовлен Россией как альтернатива Будапештской конвенции Совета Европы о Конвенции о киберпреступности и передан в Генассамблею ООН (письмо Постоянного представителя Российской Федерации при Организации Объединенных Наций на имя Генерального секретаря от 11 октября 2017 г.).

— резолюция A/RES/64/25 от 2 декабря 2009 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»;
— резолюция A/RES/65/141 от 20 декабря 2010 г. «Использование информационно-коммуникационных технологий в целях развития» и др.[1]

В этих условиях правовым основанием для международного взаимодействия при выявлении, расследовании и предупреждении преступлений, совершенных с использованием ИКТ, можно рассматривать узкопрофильные конвенциальные документы, которые могут быть применимы в случаях, когда данные виды преступлений совершены с использованием ИКТ. К таким конвенциям можно отнести, к примеру, Конвенцию Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16 мая 2005 г. (ст. 7)[2]; Конвенцию ООН против транснациональной организованной преступности от 15 ноября 2000 г. (ст. 29)[3]; Протокол против незаконного ввоза мигрантов по суше, морю и воздуху, дополняющий Конвенцию Организации Объединенных Наций против транснациональной организованной преступности[4] (принят 15 ноября 2000 г. Резолюцией 55/25 Генеральной Ассамблеи ООН).

В рамках СНГ договорно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий базируется на Соглашении о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г.[5] (далее — СПКИ), которое вступило в силу для России 17 октября 2008 г.[6] Договаривающимися сторонами являются Азербайджан, Армения, Беларусь, Казахстан, Киргизия, Молдова, Россия, Таджикистан, Узбекистан, Украина.

В СПКИ определены четыре состава преступления, которые государства — участники Соглашения обязуются закрепить в своем уголовном законодательстве, если они совершены умышленно: неправомерный доступ к охраняемой законом компьютерной информации; создание, использование или распространение вредоносных программ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети; незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права.

---

[1] URL: https://www.un.org/ru/development/ict/res.shtml (дата обращения: 28.06.2020).

[2] СЗ РФ. 2018. № 8. Ст. 1091.

[3] СЗ РФ. 2004. № 40. Ст. 3882.

[4] СЗ РФ. 2004. № 40. Ст. 3883.

[5] СЗ РФ. 2009. № 13. Ст. 1460.

[6] Бюллетень международных договоров. 2009. № 6.

Наиболее детальную регламентацию в СПКИ получила процедура направления и исполнения запроса об оказании содействия (ст. 6–8).

СПКИ основано на традиционном представлении о правовой помощи. Так, В. П. Талимончик справедливо относит данный факт к числу недостатков указанного Соглашения: «Вызывает удивление, что система электронных запросов на оказание правовой помощи не нашла своего применения в рамках СНГ. Поразительным является тот факт, что СПКИ... основано также на традиционном представлении о правовой помощи. Оно вкратце упоминает о новых технологиях при направлении запроса о правовой помощи, не упоминая о них при ответе»[1].

В научной литературе отмечены и другие явные недочеты СПКИ:

— в договоре, координирующем международное сотрудничество в борьбе с преступлениями в сфере компьютерной информации, не учтена природа данного вида преступлений, хотя такой документ должен содержать нормы, закрепляющие специальные процессуальные формы сотрудничества;
— не называются компетентные органы для работы с запросами. В части 1 ст. 4 СПКИ говорится, что сотрудничество между сторонами в рамках настоящего Соглашения осуществляется между компетентными органами непосредственно. В то же время установление четкого списка уполномоченных для сотрудничества органов могло бы упростить применение Соглашения[2];
— в статье 7 СПКИ, которая посвящена процедуре исполнения запросов, во-первых, не содержится четко определенных случаев, когда исполнение запроса может быть приостановлено. Во-вторых, несмотря на специфику преступлений в сфере высоких технологий, ст. 6 требует обязательного письменного подтверждения запроса;
— соглашением не рассматривается такая перспективная процессуальная форма сотрудничества, как создание совместных следственных групп;
— наконец, СПКИ не предусматривает положений для решения ряда вопросов, затрагивающих суверенитет государства (вопросы конкурирующей юрисдикции, передачи уголовного производства)[3].

---

[1] *Талимончик В. П.* Конвенция о киберпреступности и унификация законодательства // Информационное право. 2008. № 2. С. 29.

[2] В соответствии с Нотой МИД России от 3 августа 2015 г. № 6839/1дснг и Нотой Исполнительного комитета СНГ от 10 августа 2015 г. № 3-1/919 Следственный комитет Российской Федерации является компетентным органом.

[3] *Мороз Н. О.* Актуальные вопросы международного сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ // Международное уголовное право и международная юстиция. 2016. № 3. С. 12.

Как видно, договорно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках СНГ нуждалось в совершенствовании.

Учитывая правовые недочеты СПКИ 28 сентября 2018 г. было заключено Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий[1].

Договаривающимися сторонами в данном Соглашении выступают Армения, Беларусь, Казахстан, Киргизия, Россия, Таджикистан, Узбекистан. Как видно, существенно сужен состав участников по сравнению с СПКИ.

В настоящее время[2] в Российской Федерации проходит процедура ратификации. С момента вступления в силу этого документа для ратифицировавших его государств утратит силу СПКИ 2001 г. (в отношениях между государствами — участниками Соглашения).

В новом Соглашении устранен ряд недостатков предыдущего документа: название акта более точно отражает предмет регулирования, более полно даны определения всех значимых терминов, расширен круг уголовно наказуемых деяний в сфере информационных технологий.

Так, согласно ч. 1 ст. 3 нового Соглашения, стороны признают в соответствии с национальным законодательством в качестве уголовно наказуемых следующие деяния в сфере информационных технологий, если они совершены умышленно:

а) уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия;

г) хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации;

---

[1] СПС «КонсультантПлюс» (дата обращения: 15.09.2019).

[2] По состоянию на 2020 год.

д) распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего;

е) изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети;

ж) незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб;

з) распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма.

Сохраняя общее правило о письменной форме запроса об оказании содействия, Соглашение 2018 г. (в ч. 2 ст. 6) все же допускает, что «запрос и материалы исполненного запроса могут передаваться по техническим каналам связи в случае, если об этом есть двусторонняя договоренность между компетентными органами Сторон либо эти каналы определены иными международными договорами, участниками которых являются Стороны».

В рамках СНГ также была принята Программа сотрудничества государств — участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий на 2016–2020 годы (одобрена Исполнительным комитетом СНГ 4 декабря 2015 г.). Основными задачами Программы обозначены:

- дальнейшее развитие международно-правовой базы взаимодействия;
- совершенствование и сближение национального законодательства;
- проведение комплексных совместных, согласованных межведомственных профилактических, оперативно-разыскных мероприятий и специальных операций;
- информационное и научное обеспечение сотрудничества;
- осуществление сотрудничества в подготовке кадров, повышении квалификации специалистов;
- развитие сотрудничества с международными организациями.

В целях всестороннего взаимодействия в борьбе с компьютерными преступлениями была разработана Стратегия сотрудничества государств — участников СНГ в построении и развитии информационного общества на период до 2025 года и План действий по ее реализации,

которые были утверждены на заседании Совета глав правительств СНГ в Минске 28 октября 2016 г.

Благодаря указанным документам появилась система мер межгосударственной защиты безопасности ИКТ для государств — участников СНГ. Так, План действий по реализации указанной Стратегии содержит более 50 мероприятий, направленных на создание благоприятной среды для развития и укрепления сотрудничества в области ИКТ, гармонизацию законодательства и нормативно-технической базы, развитие цифровой экономики и «промышленного Интернета», разработку и внедрение конкретных проектов в рамках актуальных направлений ИКТ (электронное правительство, электронная торговля, электронная наука) и др.[1]

Перспективным для России является развитие международного сотрудничества в борьбе с компьютерными преступлениями в формате ШОС. В этой связи можно упомянуть соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009). В числе основных направлений сотрудничества (ст. 3) в этом документе названы противодействие угрозам использования информационно-коммуникационных технологий в террористических целях и противодействие информационной преступности. После вступления соглашения в силу стороны приступили к его практической реализации: была начата работа по выстраиванию комплексного механизма взаимодействия шести стран-участников (помимо России это соглашение подписали Казахстан, Китай, Кыргызстан, Таджикистан, Узбекистан).

В 2018 г. страны — участники ШОС договорились об организации мониторинга террористических угроз в Интернете в рамках работы Совета региональной антитеррористической структуры (РАТС).

Международное взаимодействие России с иностранными государствами по вопросам сотрудничества в борьбе с преступлениями в сфере высоких технологий осуществляется также на основании двусторонних межправительственных соглашений. К числу таких документов можно отнести соглашение между правительством Российской Федерации и правительством Французской Республики о сотрудничестве в борьбе с преступностью и в области внутренней безопасности

---

[1] *Ревин В. П.* Актуальные проблемы сотрудничества государств — участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий // Международное сотрудничество Евразийских государств: политика, экономика, право. Научно-аналитический и информационный журнал Института проблем безопасности СНГ. 2017. № 1. С. 85.

от 10 февраля 2003 г.[1], в ст. 1 которого прямо предусмотрено техническое и оперативное сотрудничество в борьбе с преступлениями в сфере компьютерной информации, в том числе связанной с использованием Интернета и других средств связи.

Выражая озабоченность угрозами, связанными с возможностями использования компьютерных технологий в целях, не совместимых с задачами обеспечения международного мира, безопасности и стабильности, правительство Российской Федерации и правительство Туркменистана заключили соглашение о сотрудничестве в области обеспечения международной безопасности (5 июня 2019 г.)[2].

Сотрудничество в области информационной безопасности и вопросов, касающихся киберпреступности, предусмотрено соглашением между правительством Российской Федерации и правительством Малайзии о сотрудничестве в области информационных и коммуникационных технологий от 5 августа 2003 г.[3]

Отмечая значительный прогресс, достигнутый в развитии и внедрении новейших информационно-коммуникационных технологий, Российская Федерация и Республика Индия заключили в 2016 г. межправительственное соглашение о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий[4].

Сотрудничество в целях расследования дел, связанных с использованием информационно-коммуникационных технологий в террористических и криминальных целях, закреплено также в соглашении между правительством Российской Федерации и правительством Социалистической Республики Вьетнам о сотрудничестве в области обеспечения международной информационной безопасности от 6 сентября 2018 г.[5]

Взаимодействие компетентных органов иностранных государств в борьбе с преступлениями в сфере компьютерной информации предусмотрено также соглашением между правительством Российской Федерации и правительством Королевства Бельгия о сотрудничестве в борьбе с преступностью от 20 декабря 2000 г.[6] К сожалению, до настоящего времени это соглашение не вступило в силу в соответствии со ст. 19, предусматривающей направление и получение сторонами уведомлений о выполнении внутригосударственных процедур, необходимых для его вступления в силу.

---

[1] Бюллетень международных договоров. 2005. № 8. С. 62.

[2] Бюллетень международных договоров. 2019. № 10. С. 63.

[3] Бюллетень международных договоров. 2004. № 1. С. 77.

[4] Бюллетень международных договоров. 2017. № 4.

[5] Официальный сайт МИД России (дата обращения: 25.06.2020).

[6] СПС «КонсультантПлюс» (дата обращения: 26.02.2020).

По тем же основаниям не вступило в силу (ст. 11) соглашение между правительством Российской Федерации и правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности от 14 мая 2010 г., разработанное сторонами в русле *реализации* положений *резолюции* Генеральной Ассамблеи ООН от 2 декабря 2009 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[1], а также в целях противостояния угрозам международной информационной и коммуникационной безопасности.

Соглашение между правительством Российской Федерации и правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности (4 сентября 2017 г.) предусматривает широкий спектр форм взаимодействия, но не вступило в силу[2].

В правовом пространстве международного взаимодействия государств в борьбе с преступлениями в сфере высоких технологий важное место занимают и межведомственные договоренности с компетентными органами иностранных государств.

В их числе можно упомянуть следующие документы:

Соглашение между правительством Российской Федерации и правительством Греческой Республики о сотрудничестве Министерства внутренних дел Российской Федерации и Министерства общественного порядка Греческой Республики в области борьбы с преступностью (Афины, 6 декабря 2001 г.)[3];

Меморандум о взаимопонимании между Следственным комитетом Российской Федерации и Полицией Государства Израиль (Тель-Авив, 15 ноября 2012 г.);

Меморандум о взаимопонимании между Следственным комитетом при прокуратуре Российской Федерации и Министерством внутренней безопасности Соединенных Штатов Америки в лице Службы иммиграционных и таможенных расследований США (Вашингтон, 26 марта 2010 г.)[4].

В первом из них предусмотрено, что компетентные органы сторон будут осуществлять взаимодействие в предупреждении, выявлении, пресечении и раскрытии «преступлений в сфере высоких технологий, включая компьютерные преступления».

---

[1] URL: https://undocs.org/ru/A/RES/64/25 (дата обращения: 17.04.2020).

[2] Официальный сайт МИД России (дата обращения: 25.06.2020).

[3] Бюллетень международных договоров. 2004. № 12. С. 61–66.

[4] СПС «Консультант Плюс» (дата обращения: 02.10.2019).

В втором и третьем в качестве одной из областей, в которой стороны выражают стремление к сотрудничеству, названа борьба с «мошенничеством, совершаемым с использованием компьютерной техники».

Международные организации, такие как ОЭСР, Совет Европы, РАТС, Европейский союз, ООН и Интерпол, играют важную роль в выработке единого подхода, координации международных усилий и выстраивании международного сотрудничества в борьбе с преступлениями в сфере высоких технологий.

Так, например, первое всестороннее исследование проблемы киберпреступности и уголовно-правовых мер по борьбе с ней в международном масштабе было предпринято Организацией экономического сотрудничества и развития (ОЭСР), которая проанализировала возможности гармонизации норм, предусматривающих уголовную ответственность за киберпреступления, а также представила криминологическое определение компьютерного преступления[1].

Интерпол ввел в обиход кодификатор компьютерных преступлений и способов их совершения, которым присвоил каждому компьютерному преступлению определенный буквенный индекс, расположив их в порядке уменьшения общественной опасности совершенного деяния[2].

Формирование единого решения проблемы компьютерной преступности на региональном уровне было реализовано Комитетом министров Совета Европы[3], который определил минимально необходимый к включению в национальное законодательство список киберпреступлений. Кроме того, в рамках Совета Европы успешно действуют Европейская группа по обучению и борьбе с киберпреступностью и Европейский комитет по проблемам преступности, основными задачами которых являются оказание содействия государствам-участникам в гармонизации законодательств в сфере киберпреступности и электронных доказательствах, расширение возможностей для эффективного международного сотрудничества в этой области.

Деятельность Межправительственной группы экспертов открытого состава по киберпреступности в рамках ООН также направлена на наращивание потенциала в борьбе с киберпреступностью путем информационной и консультативной поддержки национальных компетентных органов и их взаимодействия с зарубежными партнерами.

---

[1] Computer — Related Crime: Analysis of Legal Polici. Paris: OECD, 1986. 86 p.

[2] *Русскевич Е. А.* Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Международное уголовное право и международная юстиция. 2018. № 3. С. 113.

[3] Recommendation of the Committee of Ministers to member states Rec (89) 9 on computer-related crime // URL: https://www.coe.int/en/web/cdpc/resolutions-recommendations (дата обращения: 10.02.2020).

Вместе с тем Управление ООН по наркотикам и преступности использует свой специализированный опыт в области реагирования систем уголовного правосудия для оказания технической помощи в наращивании потенциала, предупреждении и повышении осведомленности, международном сотрудничестве, а также в сборе данных, исследованиях и анализе в области киберпреступности.

Успешность борьбы по противодействию компьютерным преступлениям заключается не только в наличии нормативной базы, но также в скоординированном и оперативном взаимодействии компетентных органов государств в данном направлении.

Таким образом, представляется, что создание специализированных внутригосударственных и международных органов является одной из форм сотрудничества государств в борьбе с киберпреступлениями.

В настоящее время государства активно расширяют и создают специальные подразделения, которые должны обеспечивать развитие наступательных возможностей в киберпространстве. Например, группа безопасности электронной коммуникации при Центре правовой связи при МИД и подразделение Министерства обороны по защите от виртуальных угроз в Великобритании; Специальная группа при МВД ФРГ; аналитический и исследовательский отделы внешней разведки и разведывательное бюро внутренней разведки в Индии; Центр национальной кибербезопасности, Объединенное кибернетическое командование Вооруженных сил США и др. В США наряду с уже функционирующим Центром национальной кибербезопасности (National Cyber Security Center) в составе Вооруженных сил сформировано Объединенное кибернетическое командование (Unified U. S. Cyber Command), которое в глобальном масштабе должно координировать усилия всех структур Пентагона. В Великобритании реализуются программы по созданию кибероружия, которые обеспечат способность властей противостоять растущим угрозам из киберпространства. В Австралии создана группа координации безопасности электронной почты (ESCG). Основной задачей этой группы является создание безопасного и надежного электронного оперативного пространства как для общественного, так и для частного секторов.

Также большое значение во взаимодействии государств — участников Европейского союза имеет деятельность Европола и Евроюста, принимающих непосредственное участие в борьбе с киберпреступностью на пространстве Европейского союза. В работе Европола используется система аналитических рабочих картотек (analys work files), формируемых из сосредоточенных в его информационной системе данных в целях анализа, определяемого как обработка или использование данных для поддержки уголовных расследований. Система

действующих аналитических картотек включает картотеки по киберпреступности Cyborg[1].

Евроюст осуществляет в том числе координацию действий правоохранительных органов различных государств по вопросам расследования киберпреступлений, предоставляет правоохранительным органам этих стран информацию о проводимых расследованиях в отношении киберпреступников[2].

Помимо указанных органов, обладающих юрисдикционной компетенцией в рассматриваемой сфере, Европейским союзом создаются и вспомогательные органы. Так, 18 января 2013 г. в Гааге официально открыт Европейский центр по борьбе с киберпреступностью. Целями его создания являются сбор и обработка данных по киберпреступлениям, проведение экспертных оценок интернет-угроз, разработка и внедрение передовых методов профилактики и расследования киберпреступлений, подготовка новых кадров, оказание помощи правоохранительным и судебным органам, а также координация совместных действий заинтересованных сторон, направленных на повышение уровня безопасности в европейском киберпространстве[3].

Представляется, что основные меры по борьбе с преступностью в сфере высоких технологий, предпринимаемые на международном уровне, должны быть связаны с действиями по реформированию законодательства на национальном уровне. Национальные и международные усилия должны дополнять друг друга, обеспечивая тем самым координацию шагов по борьбе с киберпреступностью и гармонизацию национальных законодательств.

Однако на этом пути остается пока немало нерешенных проблем. Как справедливо отмечает Т. Л. Тропина, имеющиеся международные инструменты, направленные на обеспечение кибербезопасности, характеризуются мозаичностью, являются фрагментарными и, скорее, конкурируют между собой, что не способствуют гармонизации уголовного и уголовно-процессуального законодательства государств[4].

Также следует согласиться с утверждением, что международно-правовые механизмы, позволяющие отстаивать суверенное право государств на регулирование информационного пространства, в том числе в национальном сегменте сети Интернет, не установлены. Боль-

---

[1] *Якимова Е. М.*, *Нарутто С. В.* Международное сотрудничество в борьбе с киберпреступностью // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10. № 2. С. 371–372.

[2] URL: http://www.eurojust.europa.eu

[3] URL: http://www. arms-expo.ru/news/archive/kibertmezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/mezhdunarodnoy-bez opasnosti14-03-2013-18-35-00/

[4] *Тропина Т. Л.* Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3. С. 86.

шинство государств вынуждены на ходу адаптировать государственное регулирование сферы информации и информационных технологий к новым обстоятельствам[1].

Таким образом, можно констатировать, что международно-правовая база для борьбы с преступлениями, совершаемыми с использованием ИКТ, на сегодня носит недостаточный, фрагментарный характер и нуждается в совершенствовании как на универсальном, так и на региональном уровне. Основным препятствием на этом пути является несогласованность позиций государств по ряду вопросов, наиболее существенным из которых является допустимая степень ограничения национального суверенитета в сфере регулирования киберпространства.

Безусловно, что даже при наличии многообразия и четких правовых основ международного взаимодействия остаются опасности и риски глобализации совершения преступлений в сфере компьютерных технологий, поскольку нормативно-правовая база предупреждения, выявления и борьбы с преступлениями в этой сфере не успевает за развитием новых форм киберпреступлений, поскольку формы и способы совершения преступлений, создающих угрозу информационной безопасности, постоянно изменяются и модифицируются.

Тем не менее при выработке средств и методов борьбы с киберпреступностью следует помнить о латентности данного вида преступлений. По оценкам экспертов, латентность «компьютерных преступлений» в США достигает 80%, в Великобритании — 85%, в ФРГ — 75%, в России — более 90%. По данным международной службы по обеспечению безопасности в области киберугроз Symantec Security, «каждую секунду в мире подвергаются кибератаке 12 человек, а ежегодно в мире совершается около 556 млн киберпреступлений, ущерб от которых составляет более 100 млрд дол. США»[2].

Кроме того, очень важно понимать глобальность проблемы киберпреступности. Кибератаки парализуют работу не только частных структур, но и государственных органов; в мире не существует государства, которое было бы защищено от подобного рода атак. В качестве вероятных источников киберугроз рассматриваются не только хакеры или их группы, но также отдельные государства, террористические организации[3].

---

[1] Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203. П. 17 // URL: http://www.kremlin.ru/acts/bank/41919/page/3 (дата обращения: 10.05.2020).

[2] *Карпова Д. Н.* Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46.

[3] *Якимова Е. М.*, *Нарутто С. В.* Указ. соч. С. 371.

В борьбе с киберпреступлениями, носящий глобальный транснациональный характер, важная роль отведена государствам. Однако результативность борьбы с компьютерными преступлениями будет максимальной при проработанной и обширной договорной базе, а также хорошо скоординированной работе правоохранительных органов иностранных государств и международных организаций. Очевидно, что международное сотрудничество должно осуществляться по нескольким направлениям и предполагать не только создание нормативных основ, но и выработку общих рекомендаций, внедрение эффективных моделей организационного взаимодействия между компетентными органами иностранных государств при выявлении, расследовании и предупреждении преступлений, совершенных с использованием высоких технологий.

ЗАКЛЮЧЕНИЕ

Анонимность, отсутствие реальных границ, быстрая адаптация к новым условиям – это те выявляемые и латентные факторы, которые делают киберпространство привлекательной средой для совершения многочисленных преступлений. Реальность такова, что установить сейчас реальный уровень правонарушаемости в сети Интернет практически невозможно. Количество зарегистрированных преступных посягательств дает приблизительную картину.

Общественная опасность компьютерных преступлений заключается в том, что они становятся способом совершения других преступлений, облегчения их совершения и уничтожения следов преступной деятельности. Вопросы противодействия таким преступлениям приобретают все большую актуальность.

Характерными особенностями данных преступлений является ярко корыстный характер: в последние годы компьютерная преступность приобрела экономические черты, так как большинство компьютерных преступлений совершается в банковско-финансовом или экономическом секторе, и политическую окраску, что связано с активацией в «киберпространстве» хактивистских движений, доступность специализированного программного обеспечения. Не уменьшается активность международных экстремистских и террористических организаций. Если на заре своего появления компьютерные преступления выступали чаще всего как способ хищения или как проявление хулиганства, то теперь все чаще приходится сталкиваться с таким феноменом, как «кибертерроризм» и организованные хакерские атаки, носящие диверсионный, антигосударственный характер.

1. Основываясь на результатах проведенного исследования можно выделить основные **детерминанты** данной преступности: насыщение компьютерными информационными технологиями всех современных правоотношений; реальная возможность получения значительной экономической выгоды посредством противоправных деяний с использованием компьютерной техники; низкая эффективность работы правоохранительных органов, создающая ощущение безнаказанности; ненадлежащее отношение к вопросу обеспечения информационной

гигиены и безопасности; отсутствие необходимости в наличии специальных знаний и навыков для совершения большинства преступлений с использованием информационно-телекоммуникационных сетей; новые риски кибербезопасности, возникшие вследствие распространения новых инфекционных заболеваний в 2019–2020 гг. и изоляции граждан.

Высокая латентность преступлений в сфере компьютерной информации также обусловлена сложностью их выявления, внедрением новых информационных технологий, высоким образовательным уровнем лиц, совершающих данные преступления.

2. Проведенный анализ актуальных вопросов **квалификации** преступлений демонстрирует необходимость разъяснения единых подходов: для определения терминов «охраняемая законом информация», «кража, совершенная с банковского счета, а равно в отношении электронных денежных средств»; квалификации по рассматриваемой совокупности преступных деяний; квалификации преступных действий лица в случае хищения части денежных средств с использованием банковской карты потерпевшего путем их обналичивания через терминал и с последующей оплатой этой картой различных покупок путем прикладывания карты к терминалу с использованием функции «pay-pass» (например, снял наличные в размере 1000 руб. и оплатил картой товар на сумму менее 2500 руб.) и при наличии формальных требований малозначительности.

3. Обязательным условием достижения положительных результатов в сфере **противодействия экстремизму и терроризму** является активизация мероприятий по информационному противодействию радикализации населения и адресному профилактическому воздействию, включая проведение культурно-просветительской работы, направленной на формирование общественного мнения по неприятию идеологии экстремизма, с привлечением представителей различных религиозных конфессий, освещение в средствах массовой информации негативных последствий экстремистской деятельности и результатов работы прокуратуры по пресечению экстремистской деятельности, пресечение распространения экстремистской идеологии в сети Интернет. Кроме того, целесообразно на законодательном уровне усилить полномочия органов прокуратуры в сфере координации деятельности правоохранительных органов по борьбе с распространением идеологии экстремизма и терроризма в сети Интернет.

4. Основные направления по совершенствованию правообеспечительной и правоприменительной практики по эффективному **выявлению и раскрытию преступлений** в сфере ИКТ — это оперативность получения информации об используемых преступниками технических средствах; неотложное проведение оперативно-разыскных мероприятий, особенно в регионе нахождения подозреваемого; своевременное

получение сведений о цифровом следе соединений преступника и потерпевшего, о движении денежных средств и др. Практика показывает, что реализация указанных задач требует реализации правоохранительными органами дополнительных мер по совершенствованию своей работы на рассматриваемом направлении.

Основные проблемы выявления и пресечения преступных деяний относятся не к процессуальной, а к оперативно-разыскной деятельности, к сфере предварительного обеспечения сохранности электронных следов, оперативного взаимодействия с поставщиками услуг в области ИКТ, шифрования (в особенности сквозного в мессенджерах, Dark net и т.д.) и анонимизации в сети Интернет и мессенджерах.

Следует признать, что в условиях высокого уровня латентности компьютерной преступности, опережающего развитие способов совершения преступлений в сфере компьютерной информации по отношению к механизмам обеспечения информационной безопасности, выявление и пресечение преступлений не в полной мере соответствует существующим угрозам: современный уровень развития науки и техники не соответствует субъективным ожиданиям общества к готовности их внедрения и применения в деятельности правоохранительных органов.

С учетом повсеместного быстрого распространения цифровых технологий необходимость создания центров реагирования на компьютерные инциденты и правонарушения в качестве структурного подразделения специализированных государственных органов более чем очевидна (создание специализированных подразделений по расследованию компьютерных преступлений). Как нам представляется, такой подход позволит направлять в органы предварительного расследования качественные материалы с необходимым перечнем документов и мотивированной правовой оценкой, выполненной профильными специалистами. Данное предложение обусловлено спецификой выявления компьютерных преступлений.

Фактические отсутствует достаточная нормативно-правовая база для оперативного реагирования на преступления. Повсеместно отмечается длительная процедура получения сведений из банков и поставщиков телекоммуникационных услуг. Указанное обстоятельство крайне негативно отражается на оперативности проведения первоначальных оперативных мероприятиях. Следует отметить, что нередко банки (кредитные организации) оказывают пассивную помощь правоохранительным органам в раскрытии и расследовании названных преступлений путем предоставления сведений по запросам и судебным решениям (срок исполнения которых исчисляется месяцами), при этом располагая большей информацией, которую можно предоставить оперативно.

В связи с этим представляется целесообразным рассмотреть на законодательном уровне вопрос упрощения механизма получения све-

дений о движении денежных средств по банковским счетам, а также сведений о соединении абонентов и их идентификационных данных. Также необходимо усовершенствовать федеральное законодательство путем введения электронного документооборота и установления единого разумного срока для банков при исполнении запросов оперативных подразделений и следственных органов, направляемых в целях раскрытия и расследования данных преступлений (оперативный обмен информации об IP-адресах владельцев аккаунтов в социальных сетях, их географическом местоположении; установление лиц, получивших доступ к банковским картам потерпевших; создание и внедрение программного обеспечения, позволяющего находить лиц, фактически похитивших денежные средства, и др.).

Для повышения эффективности работы на данном направлении необходимо установить обязательные для исполнения на всей территории РФ правила, связанные с запретом анонимной регистрации в социальных сетях, в платежных системах, в сети сотовых операторов мобильной связи. Например, открытие банковских счетов только с личным присутствием лица в банке, на которого открывается счет, с копированием всех документов личности. Подтверждение личности возможно также посредством использования электронной цифровой подписи либо с помощью портала «Госуслуги».

5. Как показывает практика прокурорского надзора, каких-либо существенных сложностей правообеспечительного характера при проведении органами предварительного расследовании **проверок сообщений о преступлении** в сфере ИКТ не выявлено. Основная причина низкого качества процессуальной деятельности и процессуальных решений в рассматриваемой стадии уголовного судопроизводства — нарушение требований уголовно-процессуального законодательства в силу не только недостаточной квалификации, но и искусственного регулирования следственной нагрузки. Полагаем, что прокурорам следует более точечно применять предусмотренные законом меры реагирования в комплексе с внешне- и внутрисистемными механизмами взаимодействия и координации борьбы с преступностью.

6. То же самое касается и стадии **предварительного расследования**. Обобщение практики прокурорского надзора за процессуальной деятельностью органов предварительного расследования позволяет говорить о том, что каких-либо существенных факторов правообеспечительного характера, препятствующих эффективно и в разумный срок осуществлять расследования преступлений в сфере ИКТ, в настоящее время нет. В абсолютном большинстве случаев формальные нарушения требования уголовно-процессуального закона связаны с отсутствием наступательности и инициативности следователей и дознавателей при проведении уголовных процедур. Как и по уголовным делам иных категорий, ведомственный контроль не всегда выполняет

существенной компенсационной функции, а создает дополнительную организационную нагрузку на надзирающих прокуроров.

Одним из основных факторов, способствующих совершению рассматриваемого вида преступлений, является низкая информированность населения при использовании электронных средств и платежей об уровне и степени необходимой информационной безопасности и цифровой гигиене. В этой связи особую роль играет профилактика, направленная на дополнительное информирование и проведение разъяснительной работы с населением. Зачастую потерпевшие не понимают необходимости сокрытия конфиденциальной информации и сами способствуют совершению преступления, позволяющей злоумышленникам беспрепятственно осуществлять незаконные операции с их счетами и вкладами в банковских учреждениях; при этом разъяснительная и иная профилактическая работа среди населения органами правопорядка практически на данном направлении не ведется.

Изучение практики внесения и рассмотрения представлений об устранении причин и условий, способствующих совершению преступления, направленных на предупреждение повторной и новой виктимизации, свидетельствует о формальном подходе в отдельных случаях ответственных должностных лиц органов предварительного расследования к выполнению требований данной нормы закона; как следствие, они не оказывают какого-либо профилактического воздействия на уровень и состояние преступности.

Также актуальным является возмещение причиненного материального ущерба по делам данной категории. Для повышения эффективности процессуальной деятельности в данной сфере необходимо: создание единой системы учета наличия имущества, вкладов (счетов) в банках и т.п. (например, для отыскания вклада (счета) в банковских учреждениях сотрудникам органов предварительного расследования необходимо направлять соответствующие запросы в десятки банков, филиалов и отделений банков; для отыскания недвижимости — в территориальные регистрирующие органы, которыми учет объектов недвижимости и их собственников ведется не в полном объеме, а только с момента создания соответствующих структур); внедрение возможности оперативной блокировки расчетных счетов, куда были перечислены похищенные денежные средства (действующий в настоящее время порядок нередко приводит к невозможности своевременно заблокировать их перечисление и, соответственно, вернуть потерпевшим (эта особенность хорошо известна преступникам; например, по данным прокуратуры Республики Татарстан, пик совершения хищений приходится на четверг, как предпоследний рабочий день); включение в УПК РФ правовых возможностей по принятию обеспечительных мер на стадии процессуальной проверки.

7. Отсутствие единообразия в применении норм закона о территориальной **подследственности** является существенным препятствием в соблюдении прав участников уголовного процесса на осуществление уголовного судопроизводства в разумный срок и доступа к правосудию. Внесенные Федеральным законом от 27 декабря 2019 г. № 499-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» изменения подтверждают приведенные нами исследования о роли прокурора в механизме доступа потерпевших от преступления к правосудию, о чем свидетельствует практика ряда прокуратур территориальных субъектов.

Вместе с тем, как представляется, оптимальным вариантом видится установление в УПК РФ обязанности следователей и дознавателей согласовывать с надзирающим прокурором постановление о передаче сообщения о преступлении и сам материал по подследственности перед фактическим исполнением данного процессуального действия. Изложенное логично вытекает из устоявшихся в УПК РФ положений ч. 7, 8 ст. 151 УПК РФ, согласно которым, во-первых, при соединении уголовных дел о компьютерных преступлениях, относящихся к органам предварительного расследования разных ведомств, необходимо исходить из того, что определение подследственности возложено на прокурора; во-вторых, все споры о подследственности разрешает прокурор — в случае, когда следователь принимает решение о направлении материалов проверки по подследственности, по делам рассматриваемой категории фактически имеет место спорная ситуация.

Также перспективным выходом из сложившейся ситуации представляется запланированное создание специального сервиса, доступного в том числе на мобильных устройствах, с помощью которого каждый гражданин сможет подать заявление о преступлении в правоохранительные органы в электронном виде, которое далее автоматически будет направляться по подследственности[1].

8. Допущенные в ходе предварительного расследования нарушения закона существенно затрудняют **поддержание государственного обвинения в суде**, а в некоторых случаях приводят к невозможности продолжения осуществления уголовного преследования. Очевидно, что только наличие в материалах уголовного дела достоверных доказательств, подтверждающих факт совершения обвиняемым преступления, а по преступлениям, совершенным несколькими лицами, участие каждого из обвиняемых в совершении деяния, полученных в соответствии с требованиями уголовно-процессуального закона, позволит государственному обвинителю квалифицированно поддержать обвинение, а суду вынести обвинительный приговор.

---

[1] Интервью Генерального прокурора Российской Федерации Чайки Ю. Я. газете «Известия» // URL: https://goo.gl/kvHMV6 (дата обращения: 20.02.2018).

В то же время очевидно, что для принятия обоснованного решения о направлении в суд уголовного дела о преступлении, совершенном в сфере ИКТ, прокурор должен быть осведомлен о возможностях современной компьютерной техники, об основах функционирования Интернета и компьютерных программ (приложений), созданных для использования в мобильных устройствах, и т.д.

Как нам представляется, квалифицированная и целенаправленная деятельность прокуроров по своевременному выявлению и устранению обстоятельств, препятствующих рассмотрению судом уголовных дел о преступлениях в сфере ИКТ, позволяет повысить эффективность уголовно-процессуальных процедур, способствует достижению целей уголовного судопроизводства и тем самым — предупреждению названных преступлений. Представляется необходимым повышение квалификации сотрудников, выявляющих и расследующих данные преступления, прокуроров, осуществляющих надзор за следствием, и государственных обвинителей, впоследствии поддерживающих обвинение в суде.

9. Несмотря на то, что угрозы информационно-телекоммуникационной и компьютерной безопасности объективно носят общий характер для всех современных государств, в области их криминализации между национальными законодательствами наблюдаются многочисленные и существенные расхождения. Это связано не только с особенностью юридической техники, но и с высоким динамизмом развития данной сферы правового регулирования, не всегда поспевающим за быстрыми изменениями в технологиях и появлением новых способов их общественно-опасного использования. Часть расхождений объясняется и различиями в социально-политических системах, степени их открытости и приверженности соблюдению гражданских свобод.

Имеющиеся международные инструменты, направленные на обеспечение кибербезопасности, характеризуются мозаичностью, являются фрагментарными и, скорее, конкурируют между собой, что не способствует гармонизации уголовного и уголовно-процессуального законодательства государств.

Кроме того, международно-правовые механизмы, позволяющие отстаивать суверенное право государств на регулирование информационного пространства, в том числе в национальном сегменте сети Интернет, не установлены. Большинство государств (в том числе Россия) вынуждены на ходу адаптировать государственное регулирование сферы информации и информационных технологий к новым вызовам и угрозам.

В борьбе с киберпреступлениями, носящими глобальный транснациональный характер, важная роль отведена государствам. Однако результативность борьбы с компьютерными преступлениями будет максимальной при проработанной и обширной договорной базе, а также

хорошо скоординированной работе правоохранительных органов иностранных государств и международных организаций. Очевидно, что международное сотрудничество должно осуществляться по нескольким направлениям и предполагать не только создание нормативных основ, но и выработку общих рекомендаций, внедрение эффективных моделей организационного взаимодействия между компетентными органами иностранных государств при выявлении, расследовании и предупреждении преступлений, совершенных с использованием высоких технологий. В настоящий момент Россия не имеет единого специального договора с ведущими зарубежными странами о борьбе с компьютерными преступлениями, несмотря на тот факт, что наше государство последовательно выступает с инициативой разработки универсальной конвенции по международному противодействию информационной преступности под эгидой ООН[1], однако перспективы принятия такого акта остаются пока крайне проблематичными из-за противодействия западных государств.

Представляется, что основные меры по борьбе с преступностью в сфере высоких технологий, предпринимаемые на **международном уровне**, должны быть также связаны с действиями по реформированию законодательства на национальном уровне. Национальные и международные усилия должны дополнять друг друга, обеспечивая тем самым координацию шагов по борьбе с киберпреступностью и гармонизацию национальных законодательств.

Практика создания на уровне субъектов РФ специализированных оперативно-следственных групп не только доказала свою эффективность, но и основана на опыте многих цивилизованных стран.

Например, в 2014 г. США сформировали новый отдел, который будет специализироваться на расследовании компьютерных преступлений[2]. Отдел создан при уголовном подразделении министерства, в секции «Компьютерные преступления и интеллектуальная собственность» (Computer Crime and Intellectual Property). Его задачей станет сотрудничество с компаниями частного сектора и правоохранительными органами для повышения эффективности мер кибербезопасности в общественном и частном секторах.

В 2011 г. в ФРГ открыт Национальный центр киберзащиты (Nationales Cyber-Abwehrzentrum, NCAZ), который призван коор-

---

[1] Проект конвенции ООН «О сотрудничестве в сфере противодействия информационной преступности» был подготовлен Россией как альтернатива Будапештской конвенции Совета Европы о Конвенции о киберпреступности и передан в Генассамблею ООН (письмо Постоянного представителя Российской Федерации при Организации Объединенных Наций на имя Генерального секретаря от 11 октября 2017 г.).

[2] URL: https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-cybercrime-2020-symposium (дата обращения: 17.06.2020).

динировать работу целого ряда федеральных ведомств в борьбе с киберпреступностью[1]. В структуре итальянской полиции и Карабинеров функционируют специальные подразделения, занимающиеся борьбой с киберпреступностью, а также компьютерной криминалистикой и научными исследованиями. Кроме того, Финансовая полиция (Guardia di Finanza, GdF) несет ответственность за реализацию решений по блокировке веб-ресурсов, нарушающих авторское право либо совершающих иные правонарушения.

В качестве **общих предложений** видим возможным отметить, что для повышения уровня и состояния законности в рассматриваемой сфере следует сосредоточиться на понимании компьютерной преступности, предполагающем противодействие как систему мероприятий, включающую в себя анализ объективных условий, порождающих преступление, механизмов их совершения, способов выявления, пресечения, расследования, опыт правоприменения и судебного рассмотрения.

Устранение рассмотренных причин компьютерной преступности должно носить политический, правовой, социально-экономический, организационно-технический, то есть комплексный характер (государство в лице правоохранительных органов должно занять более жесткую позицию по отношению к интернет-провайдерам, электронным и печатным СМИ, размещающим информацию преступного характера; совершенствование законодательства; развитие экономики; более качественная подготовка сотрудников правоохранительных органов в сфере информационной безопасности; развитие отечественной электроники и программного обеспечения; привлечение талантливых программистов на государственную службу; правовое просвещение населения и т.д.).

Необходимо также создать эффективные механизмы внедрения результатов уголовно-правовых и криминологических изысканий в законодательную и нормотворческую практику и обучение сотрудников правоохранительных органов.

[1] URL: https://www.securitylab.ru/news/405957.php (дата обращения: 17.06.2020).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Монографии, пособия, методические рекомендации

1. *Агапов П. В.*, *Борисов С. В.*, *Меркурьев В. В.* и др. Противодействие киберпреступности в аспекте обеспечения национальной безопасности. М., Акад. Ген. прокуратуры Рос. Федерации, 2014.
2. *Вехов В. Б.* Компьютерные преступления: способы совершения и раскрытия / под ред. Б. П. Смагоринского. М.: Право и Закон, 1996.
3. *Гузеева О. С.* Квалификация преступлений в сфере компьютерной информации. М., 2016.
4. *Евдокимов Е. Н.* Проблемы квалификации и предупреждения компьютерных преступлений: монография. Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2009.
5. *Ефремова М. А.* Прокуратура в системе обеспечения информационной безопасности: монография / М. А. Ефремова, Э. Б. Хатов; Ун-т прокуратуры Рос. Федерации. М., 2019. 128 с.
6. *Коимшиди Г. Ф.*, *Черникова И. А.*, *Камаев Б. Г.* Анализ рядов динамики (методы математической статистики в криминологии и социологии): учебно-методическое пособие. М.: ВНИИ МВД России, 2007.
7. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // СПС «КонсультантПлюс».
8. Организация экстремистского сообщества: проблемы квалификации и доказывания: пособие / П. В. Агапов и др.; под. ред. В. В. Меркурьева; Акад. Ген. прокуратуры Рос. Федерации. М., 2013.
9. Противодействие киберпреступности в аспекте обеспечения национальной безопасности: монография / П. В. Агапов и др.; Акад. Ген. прокуратуры Рос. Федерации. М., 2014.
10. *Реуцкий Д. В.* Информационные материалы в проект сборника тезисов касательно вопроса противодействия распространению идеологии терроризма в информационно-телекоммуникационной сети «Интернет» (материалы Департамента информационной без-

опасности Минкомсвязи России) // Борьба с криминальными рынками в России: законодательные и правоприменительные проблемы: реализация положений Конвенции ООН против транснациональной организованной преступности: сб. материалов межведомственной науч.-практ. конф. (Москва, 28 апреля 2020 г.) / под общ. ред. О. С. Капинус. Ун-т. прокуратуры Рос. Федерации. М., 2020.

11. *Смирнов А. В.* Уголовный процесс: учебник. М. 2017.
12. Теоретические основы предупреждения преступности на современном этапе развития российского общества: монография / под общ. ред. Р. В. Жубрина; Академия Генеральной прокуратуры Российской Федерации. М.: Проспект, 2016.

Авторефераты, диссертации

1. *Доронин А. М.* Уголовная ответственность за неправомерный доступ к компьютерной информации: автореф. дис. ... канд. юрид. наук. М., 2003.
2. *Кесареева Т. П.* Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: автореферат дис. ... канд. юрид. наук. М., 2002.
3. *Малышенко Д. Г.* Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. ... канд. юрид. наук. М., 2002.
4. *Шарков А. Е.* Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук. Ставрополь, 2004.

Зарубежные источники

1. Catching the virus — cybercrime, disinformation and the COVID-19 pandemic. European Union Agency for Law Enforcement Cooperation, 2020.
2. Computer — Related Crime: Analysis of Legal Polici. Paris: OECD, 1986. 86 p.
3. Exploiting isolation: offenders and victims of online child sexual abuse during the Covid-19 pandemic. European Union Agency for Law Enforcement Cooperation, 2020.
4. The Global Risks Report 2020, 15th Edition, World Economic Forum.
5. Pandemic profiteering: how criminals exploit the Covid-19 crisis. European Union Agency for Law Enforcement Cooperation, 2020.

Статьи

1. *Бессонов С. А.* История и зарубежный опыт правовой регламентации компьютерной преступности // Территория науки. Воронеж, 2013. № 2.

2. *Богданова Т. Н.* Причины и условия совершения преступлений в сфере компьютерной информации // Вестник Челябинского государственного университета. 2013. № 11 (302). Право. Вып. 36. С. 64–67.
3. *Вехов В. Б.* О понятии, механизме образования и классификации электронно-цифровых, оптических и магнитных следов // Криминалистика в системе правоприменения: материалы конференции. М., 2008.
4. *Гурин А. Д.* Обеспечение достоверности официальных статистических данных о преступлениях в сфере информационных технологий // Законность. 2020. № 2 (1024).
5. *Драпезо Р. Г.*, *Шелестюков В. Н.* Особенности использования результатов оперативно-розыскного мероприятия «получение компьютерной информации» // Рос. следователь. 2018. № 9. С. 65–72.
6. *Дремлюга Р. И.* Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // Уголовное право. 2018. № 4. С. 52–57.
7. *Евдокимов К. Н.* Новые угрозы информационной безопасности России: от компьютерной преступности к анекселенктотичной технотронной преступности (частная научная теория) // Основные направления государственной политики России в сфере обеспечения национальной безопасности Материалы международной научно-практической конференции. С. 57–65.
8. *Евдокимов К. Н.* Некоторые особенности уголовно-правовой квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела // Российский следователь. 2017. № 4. С. 39–44.
9. *Егорышева Е. А.*, *Егорышев А. С.* Некоторые вопросы использования специальных знаний при расследовании неправомерного доступа к компьютерной информации // Эксперт-криминалист. 2011. № 3.
10. *Ефремов К. А.* Личность преступника, совершающего преступления в сфере компьютерной информации // Общество: политика, экономика, право. 2016. № 6.
11. *Земцова С. И.* Интернет-магазины, осуществляющие незаконный сбыт синтетических наркотических средств: дифференциация и характерные признаки // Вестник Сибирского юридического института МВД России. 2019. № 1 (34).
12. *Ковтун Н. Н.* Формирование государственного обвинения как самостоятельная стадия уголовного судопроизводства России» // Журнал российского права. 2019. № 9. С. 123–135.
13. *Крылов В. В.* Информационные преступления — новый криминалистический объект // Российская юстиция. 1997. № 4.
14. *Кулешова Г. П.*, *Капитонова Е. А.*, *Романовский Г. Б.* Правовые основы противодействия кибертерроризму в России и за рубежом

с позиции общественно-политического измерения // Всероссийский криминологический журнал. 2020. Т. 14. № 1. С. 156–165.

15. *Ляпунов Ю. В.*, *Максимов В. Ю.* Ответственность за компьютерные преступления // Законность. 1997. № 1.
16. *Меркурьев В. В.* Задачи прокуратуры Российской Федерации по противодействию экстремизму и терроризму в контексте обеспечения национальной безопасности // Вестник Академии Генеральной прокуратуры Российской Федерации 2016. № 3. С. 44–53.
17. *Мороз Н. О.* Актуальные вопросы международного сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ // Международное уголовное право и международная юстиция. 2016. № 3.
18. *Окилов С. Ю.* К вопросу о некоторых проблемах оперативно-розыскной деятельности органов внутренних дел Республики Таджикистан по борьбе с преступлениями против информационной безопасности, в том числе посягающими на банковскую сферу // Труды Академии управления МВД России. 2018. № 3.
19. *Ревин В. П.* Актуальные проблемы сотрудничества государств — участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий // Международное сотрудничество Евразийских государств: политика, экономика, право / научно-аналитический и информационный журнал Института проблем безопасности СНГ. 2017. № 1.
20. *Русскевич Е. А.* Неправомерный доступ к компьютерной информации: теория и судебная практика // Судья. 2018. № 10. С. 46–49.
21. *Русскевич Е. А.* Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Международное уголовное право и международная юстиция. 2018. № 3.
22. *Паламарчук А. В.* Прокурорский надзор за исполнением законодательства в сфере противодействия правонарушениям в сети Интернет // Законность. 2016. № 12. С. 3–9.
23. *Паламарчук А. В.* О реализации новых полномочий прокурора по вопросам ограничения доступа к информации, распространяемой в сети Интернет с нарушением закона // Законность. 2019. № 10 (1020). С. 3–6.
24. *Петров А. А.* Цифровизация экономики: проблемы, вызовы, риски // Торговая политика. 2018. № 3 (15).
25. *Семыкина О. И.* Компаративистские исследования уголовного права, криминологии и уголовно-исполнительного права // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6.

26. *Скориков Д. Г.*, *Коловоротный А. А.* Особенности выявления и документирования преступлений, связанных с незаконным оборотом наркотических средств // Рос. следователь. 2018. № 3. СПС «КонсультантПлюс» (дата обращения: 08.10.2020).
27. *Талимончик В. П.* Конвенция о киберпреступности и унификация законодательства // Информационное право. 2008. № 2.
28. *Тропина Т. Л.* Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3.
29. *Шматкова Л. П.* Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. 2016. № 28. С. 720–723.
30. *Якимова Е. М.*, *Нарутто С. В.* Международное сотрудничество в борьбе с киберпреступностью // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10. № 2.
31. *Яни П. С.* Мошенничество с использованием электронных средств платежа // Законность. 2019. № 5 (1015). С. 25–28.

Приложение

РЕЗУЛЬТАТЫ АНКЕТИРОВАНИЯ ПРОКУРОРОВ[1]

1. Как вы оцениваете современное состояние преступности в сфере компьютерной информации? Всего ответивших — 342.

001 Число преступлений данного вида уменьшается — 13 — 3,8% — 3,8%[2].

002 Число преступлений данного вида увеличивается — 212 — 61,8% — 62%.

003 Число преступлений данного вида остается неизменным — 35 — 10,2% — 10,2%.

004 Статистика не отражает реального состояния преступности — 82 — 23,9% — 24%.

2.* Характерные особенности преступности данного вида. Всего ответов — 674, всего ответивших — 341.

005 Расширяются ее межрегиональные связи — 155 — 23% — 45,5%.

006 Расширяются ее международные связи — 105 — 15,6% — 30,8%.

007 Принимает выраженные организованные формы — 91 — 13,5% — 26,7%.

008 Трансграничный характер таких преступлений — 77 — 11,4% — 22,6%.

009 Приобретает политический характер — 27 — 4% — 7,9%.

---

[1] Анкетирование проводилось в 2017–2019 гг. среди прокурорских работников на курсах по повышению квалификации Иркутского, Санкт-Петербуржского филиалов Университета прокуратуры Российской Федерации, в Институте повышения квалификации Университета, а также работников прокуратур Республик Саха (Якутия), Северная Осетия — Алания, Удмуртской Республики, Владимирской, Волгоградской, Кировской, Самарской, Тюменской областей. Всего в анкетировании приняли участие 347 респондентов.

[2] Первая цифра — количество ответов, вторая цифра — процент от числа анкет, третья цифра — процент от числа ответивших на данный вопрос.

* Звездочкой отмечены вопросы, позволяющие дать несколько вариантов ответа.

010 Латентность преступных деяний — 196 — 29,1% — 57,5%.
011 Совершается не в соучастии, а одним субъектом — 20 — 3% — 5,9%.
012 Иное — 3 — 0,4% — 0,9%.

3.* Причины латентности преступлений данной категории. Всего ответов — 809, всего ответивших — 340.

013 Нежелание жертв преступлений в сфере компьютерной информации обращаться в правоохранительные органы — 101 — 12,5% (от числа ответов) — 29,7%.
014 Совершение преступлений в «виртуальной среде», скрытость для большинства населения — 149 — 18,4% — 43,8%.
015 Сложность выявления преступлений в сфере компьютерной информации — 166 — 20,5% — 48,8%.
016 Создание новых IT-технологий, увеличение пользователей сети Интернет, мобильных компьютерных устройств, переход к электронному документообороту — 160 — 19,8% — 47,1%.
017 Организованный и профессиональный характер компьютерной преступности — 66 — 8,2% — 29,4%.
018 Отсутствие эффективного государственного контроля над киберпространством и средствами массовой информации — 112 — 13,8% — 32,9%
019 Возможность совершения преступлений в автоматизированном режиме — 50 — 6,2% — 14,7%.
020 Иное — 5 — 0,6% — 1,5%.

4.* Какие факторы (социальные, экономические), по Вашему мнению, влияют на преступность в сфере компьютерной информации? Всего ответов — 710, всего ответивших — 341.

021 Компьютеризация российского общества — 132 — 18,6% — 38,7%.
022 Низкая компьютерная грамотность населения — 215 — 30,3% — 63%.
023 Низкий уровень жизни — 30 — 4,2% — 8,8%.
024 Переход на безналичные расчеты — 135 — 19% — 39,6%.
025 Безработица — 11 — 1,5% — 3,2%.
026 Высокая налоговая нагрузка — 4 — 0,6% — 1,2%.
027 Недобросовестная конкуренция между производителями программного обеспечения и антивирусной защиты — 25 — 3,5% — 7,3%.
028 Этот вид преступлений рассматривается преступниками как быстрый и относительно безопасный способ незаконного обогащения — 156 — 22% — 45,7%.
029 Иное — 2 — 0,3% — 0,6%.

5. Как Вы оцениваете эффективность действующего законодательства, регулирующего правоотношения в сфере компьютерной информации? Всего ответивших — 341.

030 На высоком уровне — 15 — 4,4% — 4,4%.
031 На среднем уровне — 185 — 53,9% — 54,3%.
032 На низком уровне — 141 — 41,1% — 41,3%.

6.* Предложения по совершенствованию законодательства, регулирующего правоотношения в сфере компьютерной информации. Всего ответов — 455, всего ответивших — 329.

033 Ужесточение санкций за совершение преступлений данной категории — 173 — 38% — 52,6%.
034 Разработка региональных программ по борьбе с преступностью в сфере компьютерной информации — 178 — 39,1% — 54,1%.
035 Внесение изменений в УК РФ (каких именно) — 10 — 2,2% — 3%.
036 Внесение изменений в УПК РФ (каких именно) — 8 — 1,8% — 2,4%.
037 Изменение системы учета таких преступлений — 24 — 5,3% — 7,3%.
038 Выработка критериев оценки ущерба, причиненного преступлениями в сфере компьютерной информации, при определении его размера судами и возмещения виновными — 50 — 11% — 15,2%.
039 Иное — 12 — 2,6% — 3,6%.

7. Каков, по Вашему мнению, в среднем уровень латентности преступлений в сфере компьютерной информации? Всего ответивших — 341.

040 До 25% — 65 — 19% — 19,1%.
041 От 26% до 50% — 139 — 40,5% — 40,8%.
042 От 51% до 75% — 98 — 28,6% — 28,7%.
043 От 76% до 100% — 39 — 11,4% — 11,4%.

8. Как Вы оцениваете эффективность деятельности правоохранительных органов по борьбе с преступностью в сфере компьютерной информации? Всего ответивших — 341.

044 Высокая эффективность — 7 — 2% (от числа анкет) — 2,1% (от числа ответивших).
045 Средняя эффективность — 86 — 25,1% — 25,2%.
046 Низкая эффективность — 248 — 72,3% — 72,7%.

9.* Какие меры, на Ваш взгляд, необходимы для повышения эффективности противодействия преступлениям в сфере компьютерной информации? Всего ответов — 1052, всего ответивших — 340.

047 Привлечение на стадиях выявления преступлений и расследования уголовных дел специалистов в области IT-технологий — 296 — 28,1% (от числа ответов) — 87% (от числа ответивших).
048 Внесение изменений в законодательство — 90 — 8,6% — 26,5%.
049 Своевременное выявление жертв преступлений — 55 — 5,2% — 16,2%.
050 Улучшение взаимодействия правоохранительных и контролирующих органов — 96 — 9,1% — 28,2%.
051 Налаживание международного сотрудничества правоохранительных органов в борьбе с преступлениями в указанной сфере — 76 — 7,2% — 22,4%.
052 Улучшение координации деятельности правоохранительных органов в борьбе с преступлениями в сфере компьютерной информации — 57 — 5,4% — 16,8%.
053 Обеспечение неотвратимости наказания — 45 — 4,3% — 13,2%.
054 Ужесточение санкций за совершение преступлений данной категории — 72 — 6,8% — 21,2%.
055 Улучшение специальной подготовки кадрового состава — 118 — 11,2% — 34,7%.
056 Улучшение материально-технического обеспечения подразделений, занимающихся борьбой с преступностью данного вида — 145 — 13,8% — 42,6%.
057 Иные меры — 2 — 0,2% — 0,6%.

10. Какие мероприятия, на Ваш взгляд, могли бы способствовать устранению причин и условий, способствующих совершению данного вида преступлений?

Нет ответов.

11.* Укажите, какие недостатки существуют в деятельности правоохранительных органов. Всего ответов — 592, всего ответивших — 336.

058 Несовершенство судебной практики по уголовным делам о преступлениях в сфере компьютерной информации — отсутствие разъяснений по квалификации и определению наказаний за преступления в сфере компьютерной информации (назначение наказаний, не связанных с лишением свободы, прекращение уголовных дел по нереабилитирующим основаниям) — 66 — 11,1% — 19,6%.
059 Недостатки при расследовании уголовных дел данной категории — 91 — 15,4% — 27,1%.

060 Недостатки при осуществлении оперативно-разыскной деятельности по компьютерным преступлениям — 207 — 35% — 61,6%.

061 Несовершенство технологий выявления и борьбы с этими преступлениями — 228 — 38,5% — 67,9%.

12. Возникали ли сложности при определении территориальной подследственности сообщений о преступлениях в сфере компьютерной информации? Всего ответивших — 332.

062 Да (каким образом разрешены) — 54 — 15,7% — 16,3%.

063 Нет — 278 — 81% — 83,7%.

13. Имела ли место практика привлечения представителей коммерческих организаций, специализирующихся на информационной безопасности, к участию в производстве процессуальных действий либо в составе межведомственной группы по противодействию преступлениям в сфере компьютерной информации? Всего ответивших — 334.

064 Да (приведите примеры организаций) — 10 — 2,9% — 3%.

065 Нет — 224 — 94,5% — 97%.

14. Возникали ли сложности при осуществлении прокурорского надзора за процессуальной деятельностью органов предварительного следствия при рассмотрении сообщений о преступлениях в сфере компьютерной информации и (или) расследовании таких уголовных дел? Всего ответивших — 335.

066 Да (какие) — 19 — 5,5% — 5,7%.

067 Нет — 316 — 92,1% — 94,3%.

15. Возникали ли сложности при изъятии электронных носителей информации при проведении осмотра места происшествия, личного обыска, обыска или выемки? Всего ответивших — 330.

068 Да (какие) — 18 — 5,2% — 5,5%.

069 Нет — 312 — 91% — 94,5%.

16. Что в основном служило поводом для обжалования прокурору в порядке, предусмотренном ст. 124 УПК РФ, действий (бездействия), решений следователя, руководителя следственного органа? Всего ответивших — 335.

070 Не обжаловались — 288 — 84% — 86%.

071 Постановление о возбуждении уголовного дела — 7 — 2% — 2,1%.

072 Постановление об отказе в возбуждении уголовного дела — 29 — 8,5% — 8,7%.

073 Проведение выемки, обыска — 9 — 2,6% — 2,7%.
074 Иное — 2 — 0,6% — 0,6%.

17. Каковы результаты рассмотрения прокурором таких жалоб? Всего ответивших — 84.

075 Жалоба удовлетворена — 11 — 3,2% — 13,1%.
076 Жалоба удовлетворена частично — 12 — 3,5% — 14,3% — в сумме с первым ответом — 27,4%.
077 Жалоба отклонена — 61 — 17,8% — 72,6%.

18. Что в основном служило поводом для обжалования в суд в порядке, предусмотренном ст. 125 УПК РФ, действий (бездействия), решений следователя, руководителя следственного органа? Всего ответивших — 321.

078 Не обжаловались — 285 — 83,1% — 88,8%.
079 Постановление о возбуждении уголовного дела — 9 — 2,6% — 2,8%.
080 Постановление об отказе в возбуждении уголовного дела — 14 — 4,1% — 4,4%.
081 Проведение выемки, обыска — 8 — 2,3% — 2,5%.
082 Иное — 5 — 1,5% — 1,6%.

19. Каковы результаты рассмотрения судом таких жалоб? Всего ответивших — 71.

083 Жалоба удовлетворена — 4 — 1,2% — 5,6%.
084 Жалоба удовлетворена частично — 5 — 1,5% — 7%.
085 Жалоба отклонена — 62 — 18,1% — 87,3%.

20. Кем из участников уголовного судопроизводства, как правило, подавалась жалоба в порядке, предусмотренном ст. 124, 125 УПК РФ? Всего ответивших — 85.

086 Потерпевший — 40 — 11,7% — 47,1%.
087 Подозреваемый, обвиняемый — 20 — 5,8% — 23,5%.
088 Адвокат — 13 — 3,8% — 15,3%.
089 Иные лица (какие) — 12 — 3,5% — 14,1%.

21. Имелись ли случаи постановления судами оправдательных приговоров по уголовным делам о преступлениях в сфере компьютерной информации? Всего ответивших — 329.

090 Нет — 324 — 94,5% — 98,5%.
091 Да (по каким причинам) — 5 — 1,5% — 1,5%.

22. Приносились ли прокурором представления на оправдательные приговоры? Всего ответивших — 189.

092 Да (каковы результаты их рассмотрения) — 11 — 3,2% — 5,8%.
093 Нет (почему) — 178 — 51,9% — 94,2%.

23. Необходима ли, по Вашему мнению, более детальная регламентация организации и осуществления прокурорского надзора за процессуальной деятельностью органов предварительного следствия при расследовании преступлений в сфере компьютерной информации путем издания соответствующего приказа Генерального прокурора Российской Федерации? Всего ответивших — 335.

094 Да — 188 — 54,8% — 56,1%.
095 Нет — 147 — 42,9% — 43,9%.

ОГЛАВЛЕНИЕ

Глава 3
ДЕЯТЕЛЬНОСТЬ ПРОКУРОРА ПО ОБЕСПЕЧЕНИЮ ИСПОЛНЕНИЯ ЗАКОНОВ ПРИ ВЫЯВЛЕНИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ