**Федеральное государственное казенное
образовательное учреждение высшего образования
«Уральский юридический институт
Министерства внутренних дел Российской Федерации»**

Кафедра уголовного процесса

Использование результатов оперативно-розыскной деятельности при расследовании хищений денежных средств граждан с использованием сети «Интернет», сотовой связи

Учебное пособие

**Екатеринбург
2022**

ББК 67.410.212
И883

И883 **Использование результатов оперативно-розыскной деятельности при расследовании хищений денежных средств граждан с использованием сети «Интернет», сотовой связи:** *учебное пособие.* – Екатеринбург: Уральский юридический институт МВД Российской Федерации, 2022. – 80 с.

ISBN 978-5-88437-891-9

Коллектив авторов **В. С. Балакшин,** доктор юридических наук, профессор (Уральский юридический институт МВД России) – введение (в соавт.), § 2–3 гл. 1 (в соавт.), § 1–2 гл. 2 (в соавт.); **М. В. Назаров** (Уральский юридический институт МВД России) – введение (в соавт.), § 2–3 гл. 1 (в соавт.), § 1–2 гл. 2 (в соавт.), заключение; **Д. И. Шнейдерова** (Могилевский институт МВД Республики Беларусь) – § 2–3 гл. 1 (в соавт.), § 1 гл. 2 (в соавт.); **К. Б. Манапов,** кандидат юридических наук, ассоциированный профессор (Карагандинская академия МВД Республики Казахстан имени Баримбека Бейсенова) – § 1 гл. 1 (в соавт.), § 1 гл. 2 (в соавт.); **Т. А. Косжанов,** кандидат юридических наук (Карагандинская академия МВД Республики Казахстан имени Баримбека Бейсенова) – § 1 гл. 1 (в соавт.), § 1 гл. 2 (в соавт.)

Рецензенты: **В. Н. Чаплыгина,** начальник кафедры криминалистики и предварительного расследования в ОВД Орловского юридического института МВД России имени В. В. Лукьянова, кандидат юридических наук, доцент;

Д. Н. Рудов, заместитель начальника кафедры уголовного процесса Белгородского юридического института МВД России имени И. Д. Путилина, кандидат юридических наук, доцент

Учебное пособие содержит комплексный анализ законодательной регламентации, а также практики использования результатов оперативно-разыскной деятельности при расследовании хищений денежных средств граждан с использованием сети Интернет, сотовой связи. Рассмотрены источники регулирования уголовно-процессуальной деятельности, смежной с ней оперативно-розыскной, банковской и финансовых сфер на территории крупнейших государств – участников Союза Независимых Государств.

Издание предназначено для курсантов и слушателей образовательных организаций системы МВД России, подготовлено в целях реализации приоритетного профиля подготовки «Деятельность подразделений дознания».

Обсуждено на заседании кафедры уголовного процесса УрЮИ МВД России (протокол № 13 от 22 июня 2022 г.).

Рекомендовано к использованию в учебном процессе методическим советом УрЮИ МВД России (протокол № 12 от 18 июля 2022 г.).

ISBN 978-5-88437-891-9 ББК 67.410.212

Введение

Планомерно и непрерывно развивающаяся индустрия информационных технологий не только способствует упрощению определенных процессов жизнедеятельности современного техногенного общества (коммуникативных, экономических, социокультурных, трудовых, финансовых и т. д.), но и нередко используется для совершения преступлений в сфере компьютерной информации. Согласно статистическим данным МВД России, за 10 месяцев 2020 года больше половины всех зарегистрированных преступлений (54,9 %) составляют хищения чужого имущества, совершенные путем: кражи – 635,1 тысяч, мошенничества – 283,1 тысяч, грабежа – 33,2 тысяч, разбоя – 4,4 тысяч[1].Чаще других предметами преступных посягательств становятся денежные средства. Центральный банк России указывает, что, по состоянию на 1 декабря 2020 г., общее количество денежной массы, находящейся в обращении на территории нашей страны, составляет 56 122,6 миллиарда рублей, из которых 43 988 миллиарда – в безналичной форме[2]. Не удивительно, что актуальные виды хищений направлены именно на неправомерные изъятия денежных средств с банковских счетов. В последние годы расследование преступлений, предусмотренных статьей 159 (Мошенничество), пунктом «г» части 3 статьи 158 (Кража с банковского счета электронных денежных средств) Уголовного кодекса Российской Федерации[3], стало своеобразным «лейтмотивом» деятельности подразделений органов внутренних дел России, занимающихся противодействием имущественным преступлениям.

Одной из причин является то, что двадцатое и двадцать первое столетия ознаменовали расцвет эпохи электронно-вычислительной техники, повсеместную цифровизацию, внедрение новых технологий во все сферы жизнедеятельности. В глобальном смысле текущий период можно охарактеризовать как начало очередной, четвертой промышленной революции, в ходе которой осуществляется повсеместная цифровизация. Происходит развитие таких перспективных отраслей, как «онлайн-торговля», мобильный «банкинг», различные цифровые сервисы, кото-

[1] См.: Краткая характеристика состояния преступности в Российской Федерации за январь – октябрь 2020 г. [Электронный ресурс] // Официальный сайт МВД России. URL: https://мвд.рф/reports/ item/21933965

[2] См.: Денежная масса (национальное определение) [Электронный ресурс] // Официальный сайт Центрального Банка России. URL: https://cbr.ru/statistics/ms/

[3] Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_ 10699/

рые уже существенно поменяли структуру экономик развитых стран и придали новое качество традиционным отраслям за счет таких направлений, как роботизация, искусственный интеллект, обмен «большими данными» и других[1]. Становится очевидным, что названная тенденция одной из первых охватила финансово-экономические отношения. Слова из разряда «цифровой», «электронный», «крипто», а также их производные, в изобилии представлены в рамках банковских продуктов, средствах платежа, обмена информацией и многого другого. Действительно, обилие национальных валют, политических проблем, разнородность законодательного регулирования финансового сектора привело к таким явлениям, как «надгосударственные» средства оборота и платежа, заявляющие себя в качестве существующих обособленно от традиционных институтов, подконтрольных политико-правовым образованиям. Так называемая «криптовалюта» помимо положительных, имеет отрицательные аспекты, в их числе и то, что она активно используется криминальными элементами для легализации денежных средств, полученных преступным путем, расчетов при незаконном обороте наркотических средств, иных предметов, изъятых из гражданского оборота. Также имеют место случаи, когда данная категория, позиционируемая как новое средство платежа, сама становится предметом хищений, совершаемых посредством неправомерного доступа к учетным записям в рамках соответствующих интернет-ресурсов. Мировая пандемия коронавирусной инфекции, вследствие которой использование ресурсов сети «Интернет» стало условием сохранения жизни, здоровья населения всей планеты, обострила существующие проблемы, связанные с совершением преступлений в глобальной сети.

Темы, связанные с хищениями безналичных денежных средств, криптовалют, все чаще оказываются в фокусе внимания общественности и высших государственных органов, что объясняется набирающей обороты «киберпреступности», по сути своей являющейся формой реализации 2 видов преступлений:

1) хищений, имеющих главной целью неправомерное завладение финансами,

2) получения, модификации, уничтожения, копирования содержащейся на электронно-вычислительной технике информации, оказания влияния на инфраструктуру, обеспечивающую ее хранение.

[1] См.: Послание Президента Республики Казахстан от 31 февраля 2017 г. «Третья модернизация Казахстана: глобальная конкурентоспособность» [Электронный ресурс] // Официальный сайт Информационно-правовой системы нормативных правовых актов Республики Казахстан. URL: http://adilet.zan.kz/rus/docs/K1700002017

Не секрет, что указанные преступления совершаются посредством использования ресурсов сети «Интернет» и сотовой связи. При этом меры нормативного и организационного порядка, принимаемые с целью противодействия данным деяниям, не дают должного эффекта. Об этом свидетельствуют статистические данные, приведенные министром внутренних дел России на состоявшемся 7 октября 2020 г. заседании Совета Федерации. Так, с начала 2020 года в России было зафиксировано 363 000 «киберпреступлений» – это на 77 % больше, в каждом пятом регионе их число увеличилось в два и более раза[1]. Только эти цифры свидетельствуют о необходимости усиления действий по предупреждению, раскрытию и качественному расследованию данных преступлений. Между тем их успешное раскрытие и расследование, выявление и изобличение всех лиц, причастных к совершению, невозможно без дальнейшего совершенствования уголовно-процессуального, оперативно-розыскного законодательства, правоприменительной практики. Требуются новые подходы к способам и средствам применения оперативно-розыскных действий, оснований и порядка производства тех оперативно-розыскных мероприятий (далее – ОРМ), которые позволяют оперативно выявлять, закреплять и предоставлять органам расследования и суду соответствующие материалы.

К сожалению, действующая редакция статьи 89 Уголовно-процессуального кодекса Российской Федерации[2] (далее – УПК РФ), соответствующие нормы Федерального закона «Об оперативно-розыскной деятельности»[3] не всегда позволяют эффективно, в короткие сроки реализовывать имеющиеся возможности органов дознания. Нередко эти возможности не реализуются вследствие слабой профессиональной подготовки сотрудников соответствующих подразделений, отсутствия единообразия в практике производства конкретных ОРМ, документирования их результатов и предоставления в органы предварительного расследования, несмотря на изменение в лучшую сторону законодательства, регламентирующего оперативно-розыскную деятель-

[1] См.: Репортаж по итогам заседания Совета Федерации Федерального собрания Российской Федерации [Электронный ресурс] // Официальный сайт информационного агентства «Тасс». URL: https://tass.ru/obschestvo/9650951

[2] Уголовно-процессуальный кодекс: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34481/

[3] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_ LAW_7519/

ность (далее – ОРД). Имеется в виду изменение перечня ОРМ и более дельное их регулирование.

В настоящем пособии предпринята попытка, опираясь на результаты обобщения имеющейся практики выявления и раскрытия названных преступлений, выявить основные способы совершения хищений с использованием сети «Интернет» и сотовой связи. Ибо их знание уже есть шаг к тому, чтобы, реализуя конкретные ОРМ, выявить, задокументировать факт преступления, изобличить преступников и дать возможность органам расследования и суду реализовать уголовный закон. В пособии обозначены проблемы имплементации и использования результатов ОРМ при расследовании хищений денежных средств, криптовалют посредством сети «Интернет», сотовой связи, сформулированы перспективы этой деятельности. Как известно, передача материалов, полученных оперативными подразделениями органов дознания в рамках реализации розыскных функций, происходит посредством направления результатов ОРД в строгом соответствии с требованиями статьи 89 УПК РФ иными нормами, развивающими ее положения, а также в порядке, предусмотренном ведомственными подзаконными актами. Однако таковые не являются самостоятельным видом доказательств.

Заложенная плеядой ученых советской школы уголовного процесса парадигма теории доказательств, согласно которой результаты ОРД рассматриваются в качестве вспомогательного института, не вызывающего доверие и не способного служить цели получения доказательств по уголовному делу, оказала огромное влияние на современную науку, законодательную и правоприменительную практику[1]. Стоит отметить, что сегодня сложились объективные факторы к изменению существующего положения дел. Изменился перечень оперативно-розыскных мероприятий, их правовое регулирование стало более доскональным. Сегодня принцип законности является ключевым и в оперативно-розыскном праве. Судебный контроль за проведением ОРМ, ограничивающих конституционные права граждан, а также прокурорский надзор за оперативным делопроизводством развиты, как некогда ранее. До введения в уголовно-процессуальную плоскость ОРД находится в поле зрения достаточного количества должностным лиц независимых ветвей власти,

[1] Ссылки на труды И. М. Лузина, Р. С. Белкина, М. С. Строговича и ряда иных авторов традиционно в изобилии представлены в научных изысканиях, имеющих предметом исследования вопросы использования результатов ОРД в доказывании по уголовным делам. Однако не стоит забывать, что их авторские позиции складывались в период существования общественных отношений, сформированных социалистическим строем, плановой экономикой и, само собой, действия УПК РСФСР 1922, 1923, 1960 гг.

при том самых подготовленных и компетентных, имеющих допуск к сведениям, составляющим государственную тайну.

Схожие с изложенными выше тенденции имеют место на территории всех государств Евро-Азиатского региона, в особенности, постсоветского пространства.

Актуальность настоящего учебного пособия несомненна, поскольку подавляющее большинство совершаемых преступлений, не обходится без использования информационно-телекоммуникационных технологий, финансовой составляющей. Также имеет место тенденция к тому, что противоправные деяния приобретает межрегиональный и межгосударственных характер, высокую степень организованности. Своевременное документирование и закрепление следовой картины выступает неотъемлемым элементом последующего раскрытия и расследования. Реализовать обозначенное возможно лишь посредством проведения ОРМ, которые нередко проводятся в период приготовления и совершения объективной стороны преступлений. Хищения денежных средств в их безналичной и электронной форме в последние годы и обозримый период будущего выступают одним из самых совершаемых видов преступлений, «конкурируя» с хранением и сбытом наркотических веществ. Использование так называемых криптовалют для сокрытия преступной деятельности, а также их распространённость в качестве средства платежа у отдельных категорий лиц, обуславливает вовлечение таковых в уголовно-правовые и процессуальные правоотношения.

Практическая и теоретическая значимость издания состоит в том, что в нем проанализированы и разъяснены правовые, а также фактические основы использования концептуально важных категорий, таких как «криптовалюта», «электронные денежные средства», обозначены проблемные аспекты и рекомендации по вопросам использования результатов ОРД при расследовании хищений перечисленного. Данное пособие подготавливалось коллективом авторов из числа представителей научных школ России, Беларуси, Казахстана, а также действующих сотрудники правоохранительных органов.

Учебное пособие предназначено для обучающихся по специальности 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, направлениям подготовки 40.03.01 Юриспруденция, 40.03.02 Обеспечение законности и правопорядка при изучении учебных дисциплин «Уголовно-процессуальное право (уголовный процесс)», «Предварительное следствие в органах внутренних дел», «Дознание в органах внутренних дел», «Расследование преступле-

ний в сфере компьютерной информации» и других и будет способствовать формированию следующих профессиональных компетенций:

общепрофессиональные компетенции:

– способность реализовывать нормы материального и процессуального права, законодательство Российской Федерации, в том числе Конституцию Российской Федерации, федеральные конституционные законы и федеральные законы, а также общепризнанные принципы, нормы международного права и международные договоры Российской Федерации;

– способность использовать знания основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений применительно к отдельным отраслям юридической науки;

– способность сохранять и укреплять доверие общества к юридическому сообществу;

– способность логически верно, аргументированно и ясно строить устную и письменную речь;

профессиональные компетенции:

– способность юридически правильно квалифицировать факты, события и обстоятельства;

– способность обеспечивать соблюдение законодательства Российской Федерации субъектами права;

– способность принимать решения и совершать юридические действия в точном соответствии с законодательством Российской Федерации;

– готовность к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства,

– способность уважать честь и достоинство личности, соблюдать и защищать права и свободы человека и гражданина;

– способность выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения;

– способность осуществлять профилактику, предупреждение правонарушений, коррупционных проявлений, выявлять и устранять причины и условия, способствующие их совершению;

– способность толковать нормативно-правовые акты.

Пособие отвечает задачам овладения обучающимися качественными теоретическими знаниями, роли, значению и правовому обеспечению профессии следователя в деятельности современных правоохранительных органов.

Глава 1. Уголовно-процессуальные и криминалистические особенности использования результатов оперативно-розыскной деятельности при расследовании хищений денежных средств, криптовалют посредством сети «Интернет», сотовой связи

§ 1. История развития международного законодательства по противодействию преступлениям, совершаемым с использованием Интернета, сотовой связи

Состояние правового регулирования противодействия совершению преступлений с использованием электронно-вычислительной техники («кибер», «АйТи»-преступлений) требует изучения его динамики, как в России, так и в международной области, которая является одним из важных источников для формирования национального законодательства. Большинство международных нормативных правовых актов основываются на фундаментальных международных документах в области защиты прав человека, таких как Конвенция Совета Европы о защите прав человека и основных свобод от 1950 года, Международный пакт ООН о гражданских и политических правах от 1966 года. В них в качестве одного из основных прав человека провозглашается право на свободу поиска, получение и распространение всякого рода информации и идей, независимо от государственных границ, основываясь на праве невмешательства в личную жизнь[1].

Между тем нередко такие широкие возможности используются преступными элементами, включая преступные организации. С появлением компьютерной и иной высокотехнологичной преступности международное сообщество начало вырабатывать правовые инструменты противодействия ей. Первое всестороннее исследование проблемы киберпреступности и уголовно-правовых мер по борьбе с ней в международном масштабе было предпринято Организацией экономического сотрудничества и развития (далее – ОЭСР), которая с 1983 по 1985 гг. изучала возможности гармонизации норм, предусматривающих уголовную ответственность за компьютерные преступления. Выводы ОЭСР были изложены в докладе «Преступления, связанные с компьютером: анализ правовой политики», где анализировалось существующее законодательство и делались предложения по его реформированию, а также был рекомендован минимальный список деяний, подлежащих криминализа-

[1] Европейская Конвенция о киберпреступности, преамбула [Электронный ресурс]. URL: http://pravo.ru/interpravo/ legislative/view/27

ции[1]. С 1985 по 1989 гг. Специальный Комитет экспертов Совета Европы по вопросам преступности, связанной с компьютерами, выработал Рекомендацию № 89 от 13 сентября 1989 г. утвержденную комитетом министров Европейского Союза. Она содержит список правонарушений, рекомендованный странам-участницам ЕС для разработки единой уголовной стратегии, связанной с компьютерными преступлениями. Также в документе была отмечена необходимость достижения международного консенсуса по вопросам криминализации некоторых преступлений, связанных с компьютерами. Рекомендация содержит два списка преступлений – «минимальный» и «факультативный (дополнительный)». «Минимальный» список включает деяния, которые обязательно должны быть запрещены международным законодательством и подлежат преследованию в судебном порядке. «Дополнительный» список содержит те правонарушения, по которым достижение международного согласия представляется затруднительным[2].

В 1990 году восьмой Конгресс ООН по предупреждению преступности и обращению с правонарушителями принял резолюцию, призывающую государства – члены ООН увеличить усилия по борьбе с компьютерной преступностью, модернизируя национальное уголовное законодательство, содействовать развитию в будущем структуры международных принципов стандартов предотвращения, судебного преследования и наказания в области компьютерной преступности. 14 декабря 1990 г. Генеральной Ассамблеей ООН была принята резолюция, призывающая правительства государств-членов руководствоваться решениями, принятыми на 8 (восьмом) Конгрессе ООН. В 1995 году опубликован «Справочник ООН по предотвращению и контролю преступности, связанной с компьютерами», который исследует явление компьютерной преступности, анализирует существующее уголовное право о защите данных и информации, процессуальное право в этой области, а также вопросы предотвращения преступлений в киберпространстве, возможности международного сотрудничества в данной сфере[3]. В том же году была проведена первая международная конференция Международной полицейской организации (Интерпола) по компьютерной преступности, под-

[1] См.: *Повышев В.* Борьба с киберпреступностью и кибертерроризмом [Электронный ресурс]. URL: http://www.crime.vl.ru/index.php?p=4149&more=1&c=1&tb= 1&pb=1#more4149

[2] Рекомендация № 89, утвержденная комитетом Министров ЕС 13 сентября 1989 г. [Электронный ресурс]. URL: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2

[3] См.: Справочник ООН по предотвращению и контролю преступности, связанной с компьютерами [Электронный ресурс]. URL: http://www.uncjin.org/Documents/congr10/10r.pdf

твердившая обеспокоенность международного сообщества распространением киберпреступности. Участники конференции подчеркнули, что вызывает тревогу отсутствие международного механизма для рационального и эффективного противостояния этому виду преступности. В последующем подобные конференции были проведены Интерполом в 1996, 1998 и 2000 гг.

В мае 2000 года «Большая восьмерка» провела конференцию по киберпреступности, главной темой которой была координация усилий по борьбе с преступностью в сети «Интернет». Конференция составила повестку дня для последующей встречи на высшем уровне, проведенной 22 июля 2000 г. в Японии, на о. Окинава[1]. По ее результатам была принята Окинавская хартия глобального информационного общества, в которой заявлено, что усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства[2].

На этой встрече было также выпущено коммюнике, декларирующее, что страны будут принимать соответствующие усилия для выработки совместного похода к высокотехнологичным преступлениям типа киберпреступлений, способных серьезно угрожать безопасности глобального информационного сообщества. Нарастающая актуальность данной проблемы инициировала ее специальное рассмотрение на Генеральной Ассамблее ООН в январе 2001 года, по результатам которого была принята резолюция «Борьба с преступным использованием информационных технологий». В ней Генеральная Ассамблея выражает обеспокоенность в связи с тем, что технический прогресс создал новые возможности для преступной деятельности, и в частности, для преступного использования информационных технологий. Также отмечено, что повсеместное распространение информационных технологий, масштабы использования которых в разных государствах могут быть различными, привело к значительному росту глобального сотрудничества и координации, в результате чего преступное использование информационных технологий может иметь серьезные последствия для всех государств. В связи с этим был намечен ряд мер:

---

[1] См.: *Повышев В.* Указ. соч.

[2] См.: Окинавская хартия Глобального информационного общества [Электронный ресурс]. Принята главами государств и правительств «Группы восьми» 22 июля 2000 г. URL: http://www.kremlin.ru/ supplement/3170

– государства должны обеспечить, чтобы их законодательство и практика не оставляли возможности тем, кто злоупотребляет информационными технологиями, укрываться где бы то ни было;

– сотрудники правоохранительных органов должны быть обучены и оснащены для борьбы с преступным использованием информационных технологий;

– правовые системы должны защищать конфиденциальность, целостность и доступность данных и компьютерных систем от несанкционированного вмешательства и предусматривать наказания за злоупотребления, совершаемые в преступных целях;

– правовые системы должны обеспечивать сохранность электронных данных, имеющих отношение к расследованию конкретных преступлений, и быстрый доступ к ним;

– общественность должна быть осведомлена о необходимости предупреждения преступного использования информационных технологий и борьбы с ним;

– насколько это практически осуществимо, информационные технологии должны разрабатываться таким образом, чтобы содействовать предупреждению и обнаружению случаев преступного использования, отслеживанию преступников и сбору доказательств;

– борьба с преступным использованием информационных технологий требует выработки решений, учитывающих как необходимость защиты личных свобод и частной жизни, так и сохранения у правительств возможности бороться с подобным явлением[1].

Логическим продолжением данной резолюции ООН и плодом многолетних усилий международного сообщества стала принятая 23 ноября 2001 г. в Будапеште Конвенция Совета Европы о киберпреступности. Это один из важнейших документов, регулирующих правоотношения в сфере глобальной компьютерной сети и пока единственный документ такого уровня. По мнению экспертов, его принятие – это своеобразная веха в истории борьбы с киберпреступностью. Подготовка Конвенции стала длительным процессом – за четыре года было составлено 27 проектов. Заключительная версия, содержащая преамбулу и 4 главы, датируемая 25 мая 2001 г., была представлена Европейской комиссии по борьбе с киберпреступностью на 50-м Пленарном заседании 18–22 июня 2001 г. Ее значение состоит в том, что впервые на международном

[1] Резолюция, принятая 22 января 2001 г. Генеральной Ассамблеей ООН [по докладу Третьего комитета (A/55/593)] 55/63. Борьба с преступным использованием информационных технологий [Электронный ресурс]. URL: https://undocs.org/ru/A/RES/55/63

уровне были обозначены правовые рамки некоторых важных понятий. Так, согласно Конвенции, «компьютерная система» означает любое устройство или группу взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных. Аналогичным образом «компьютерные данные» означают любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию. Она также определяет процедурную сторону производства по уголовным делам по преступлениям в сфере высоких технологий. Прежде всего это касается полномочий правоохранительных органов по выемке компьютерных данных:

а) производить выемку компьютерной системы, ее части или носителей, используемых для хранения компьютерных данных, либо иным аналогичным образом обеспечивать их сохранность;

б) изготавливать и оставлять у себя копии соответствующих компьютерных данных;

в) обеспечивать целостность относящихся к делу хранимых компьютерных данных;

г) делать компьютерные данные, находящиеся в компьютерной системе, доступ в которую был получен, недоступными или изымать их из нее[1].

Кроме того, ряд статей Конвенции посвящен процессу получения фактических данных. Так, статья 20 «Сбор в режиме реального времени данных о потоках информации» предоставляет компетентным органам полномочия:

– собирать или записывать с применением технических средств,

– обязать поставщиков информационных услуг в пределах имеющихся у них технических возможностей собирать или записывать с применением технических средств.

Статья 32 «Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным» говорит о том, что одна страна может без согласия другой страны:

а) получать доступ к общедоступным (открытому источнику) компьютерным данным независимо от их географического местоположения,

б) получать через компьютерную систему на своей территории доступ к хранящимся на территории другой страны компьютерным данным

[1] Конвенция о компьютерных преступлениях. Будапешт, 23 ноября 2001 г. [Электронный ресурс]. URL: https://rm.coe.int/1680081580

или получать их, если эта страна имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стране через такую компьютерную систему.

По объекту посягательства Конвенция выделяет следующие группы киберпреступлений: преступления против конфиденциальности, целостности и доступности компьютерных данных и компьютерных сетей, экономические компьютерные преступления, компьютерные преступления против личных прав и неприкосновенности частной сферы, компьютерные преступления против общественных и государственных интересов. Однако многие киберпреступления посягают сразу на несколько объектов: например, незаконный перехват частных электронных коммуникаций посягает на неприкосновенность частной сферы и на конфиденциальность компьютерных данных, компьютерное мошенничество – на собственность и на целостность компьютерных данных и т. д. При этом Конвенция изначально подразделяла киберпреступления на четыре группы (потом был принят дополнительный протокол и теперь групп 5). Эта классификация в настоящее время является «эталоном», поскольку имеющиеся международные и региональные документы, а также научная практика, следуют именно этому подразделению компьютерных преступлений на пять групп.

В первую группу выделены преступления против конфиденциальности, целостности и доступности компьютерных данных и систем, такие как незаконный доступ, незаконный перехват, вмешательство в данные, вмешательство в систему. Во вторую группу входят преступления, связанные с использованием компьютера как ресурса совершения преступлений, а именно как средства манипуляций с информацией. В эту группу входят компьютерное мошенничество и компьютерный подлог. Третью группу составляют преступления, связанные с контентом, то есть с содержанием данных, размещенных в компьютерных сетях. Самый распространенный и наказуемый практически во всех государствах вид этих киберпреступлений – преступления, связанные с детской порнографией. В четвертую группу вошли преступления, связанные с нарушением авторского права и смежных прав, при этом установление таких правонарушений отнесено документом к компетенции национальных законодательств государств. Пятая группа преступлений зафиксирована в отдельном протоколе – это акты расизма и ксенофобии, совершенные посредством компьютерных сетей.

В Конвенции не выделяются в отдельные группы некоторые деяния, которые широко обсуждаются, но до сих пор являются спорными с точки зрения техники их криминализации и необходимости гармонизации

законодательства на международном уровне. Одно из них – это так называемый «кибертерроризм» и использование киберпространства в террористических целях (например, вовлечение в совершение преступлений террористического характера или иное содействие их совершению). Отсутствие согласованного определения терроризма на международном уровне в настоящее время затрудняет дебаты о кибертерроризме как о явлении, криминализация которого необходима в виде универсальной модели для всего международного сообщества. Вместе с тем это не мешает государствам и международным организациям предпринимать усилия по борьбе с использованием сети «Интернет» террористическими организациями. Например, на уровне Европейского Союза существует проект «Clean IT», целью которого является борьба с этим явлением.

Еще одна категория преступлений, не включенная отдельно в Конвенцию (но получившая распространение после ее принятия) – «identitytheft», т. е. кража, передача и использование персональных данных в целях совершения преступлений. Одни страны выделяют эти преступления в отдельную категорию, другие считают, что данные деяния подпадают под несколько статей уголовного законодательства. Поскольку данные преступления получили широкое распространение относительно недавно, в настоящее время ведутся дебаты о выделении их в отдельную группу и необходимости гармонизации законодательства в этой сфере на международном уровне[1].

В последующие годы актуальность проблемы противодействия высокотехнологичным преступлениям не утратила своей остроты и неоднократно становилась предметом рассмотрения на уровне Генеральной Ассамблеи ООН. Так, в Резолюции от 23 января 2002 г. «Борьба с преступным использованием информационных технологий» выражалась обеспокоенность в связи с тем, что технический прогресс создал новые возможности для преступной деятельности, и в частности, для преступного использования информационных технологий. Поэтому акцент необходимо делать на предупреждении таких деяний[2]. Об этом же говорится в Тунисской программе для информационного общества, которая была принята на Всемирной встрече на высшем уровне (Женева, 2003 – Тунис, 2005). В ней подчеркивается важность уголовного преследования киберпреступности, включая преступления, совершенные в рамках

[1] См.: The Economic impact of cybercrime and cyberspionage [Электронный ресурс] // Center for Strategic and International Studies July 2013 Report.

[2] Резолюция, принятая 23 января 2002 г. Генеральной Ассамблеей ООН [по докладу Третьего комитета (A/56/574)] 56/121. Борьба с преступным использованием информационных технологий [Электронный ресурс]. URL: https://undocs.org/ru/A/RES/56/121

юрисдикции одной страны, но имеющие последствия в другой, а также борьбы против терроризма во всех его формах и проявлениях в Интернете. Программа призывает правительства обеспечить безопасное, непрерывное и стабильное функционирование Интернета и необходимость защиты информационно-коммуникационных технологий (далее – ИКТ) от возможного неблагоприятного воздействия или подверженности рискам[1].

Проблемы экстерриториальности преступлений в сфере высоких технологий отражены в Глобальной программе кибербезопасности Международного союза электросвязи, который еще в 2008 году обратил внимание на то, что киберпреступники используют уязвимые места и лазейки в национальном и региональном законодательстве. Они переносят свои операции в страны, которые еще не приняли адекватные и имеющие обязательную юридическую силу законы, и поэтому могут атаковать свои жертвы почти абсолютно безнаказанно даже в тех странах, в которых действуют эффективные законы[2]. Вопросам информационной безопасности была посвящена специальная Резолюция, принятая Генеральной Ассамблеей ООН 21 декабря 2009 г. В ней отмечено, что угрозы надежному функционированию важнейших информационных инфраструктур и целостности информации, передаваемой по этим сетям, приобретают все более изощренный и серьезный характер, отрицательно сказываясь на уровне семейного, национального и международного благополучия[3].

Некоторые наиболее актуальные проблемы противодействия преступлениям в сфере высоких технологий также рассматривались на высоком уровне. Так, необходимость противодействия нелегальному наркообороту с использованием компьютерных средств определена Конгрессом ООН по предупреждению преступности и уголовному правосудию в апреле 2015 года в Дохе. В резолюции, принятой Конгрессом, говорится о взаимном сотрудничестве, реализации совместных программ, эффективном обмене информацией, сведениями и опытом эффективных механизмов противодействия преступным связям транснациональной

---

[1] Тунисская программа для информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R от 15 ноября 2005 г. [Электронный ресурс]. Всемирная встреча на высшем уровне по вопросам информационного общества (Женева, 2003 – Тунис, 2005). URL: https://www.un.org/ru/events/pastevents/pdf/ agenda_wsis.pdf

[2] Глобальная программа кибербезопасности Международного союза электросвязи [Электронный ресурс]. URL: https://www.ifap.ru/pr/2008/080908aa.pdf

[3] Резолюция, принятая Генеральной Ассамблеей ООН 21 декабря 2009 г. [по докладу Второго комитета (A/64/422/Add.3)] 64/211. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур [Электронный ресурс]. URL: https://undocs.org/ru/A/RES/64/211

организованной преступности, участвующей в незаконном наркообороте при использовании современных ИКТ. Были проанализированы вопросы использования геолокации и сетевого протокола прикладного уровня, базирующегося на протоколе TCP (порт 43), основное его применение – получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем (WHOIS), а также проблемы в способах измерения, отслеживания и сбора данных. Кроме того, предлагалось реализовать меры, направленные на создание защищенной киберсреды и противодействие криминальной деятельности, осуществляемой с помощью сети «Интернет». В ходе Конгресса проведен семинар-практикум, посвященный информационной преступности, на котором дифференцированы киберпреступления:

– правонарушения, направленные против свойств компьютерных систем;

– правонарушения, связанные с использованием компьютерных средств;

– правонарушения, связанные с содержанием компьютерных данных[1].

Следуя этим основным направлениям, изложенным в вышеперечисленных международных нормативных правовых актах, различные страны совершенствуют свою законодательную базу. Так, в Великобритании деяния, связанные с использованием Интернета («Offences of encouragement and dissemination using the Internet»), относятся к категории тяжких преступлений и подлежат наказанию в виде тюремного заключения вплоть до пожизненного. Юридические лица наказываются штрафом, размер которого определяет суд[2]. Законодатели Германии и Дании установили обособленную ответственность за компьютерное мошенничество (параграфы 263а и 279а). В Уголовном кодексе Испании в главе «Об обманном присвоении чужого имущества» статьи 255 и 256 отдельно выделяют ответственность за незаконный обман, совершенный с применением подобных методов. Аналогичные нормы содержатся в УК Швеции и многих других европейских стран. Видимо, поэтому Модельный уголовный кодекс для государств – участников СНГ рекомендовал наряду с другими хищениями предусмотреть состав хищения,

[1] См.: Доклад о работе тринадцатого Конгресса Организации Объединенных Наций по предупреждении преступности и уголовному преследованию. Доха, 12–19 апреля 2015 г. [Электронный ресурс] // Официальный сайт Организации Объединенных Наций. URL: http: www.un.org/ru/events/crimecongress

[2] См.: *Болычев Н. И.* О зарубежном опыте правового регулирования противодействия экстремизму в сети Интернет // Вестник Воронежского института МВД России. 2015. № 3. С. 211.

совершенного путем использования компьютерной техники[1]. Статья 287 УК Китайской Народной Республики признает преступным использование компьютера для финансового мошенничества, кражи, хищения, присвоения государственных средств, хищения государственной тайны и другие подобные деяния[2].

Несмотря на принимаемые международным сообществом меры, ряд актуальных вопросов противодействия преступлениям в сфере высоких технологий остается нерешенным. Так, в ходе вышеуказанного Конгресса ООН в апреле 2015 года, в Дохе участники пришли к мнению, что киберпреступность является сложным и многогранным явлением с новым «modusoperandi»[3], используемым для совершения рассматриваемых преступлений. При этом акцентировалось внимание на том, что большое количество вопросов возникает при оценке цифровых доказательств, это представляет сложность в деятельности правоохранительных ведомств. В обеспечение деятельности силовых структур предложено привлекать внешних подрядчиков либо создавать специализированные полицейские подразделения[4]. Значительную помощь в этом могут оказать 6 базовых принципов при работе с цифровыми доказательствами, которые разработаны Международной организацией по компьютерным доказательствам (IOCE).

1. При работе с цифровыми доказательствами должны быть применимы все основные процессуальные принципы и принципы компьютерной криминалистики.

2. Действия, выполняемые в процессе сбора цифровых доказательств, не должны изменять эти доказательства.

3. Допуск к оригинальным цифровым доказательствам может быть предоставлен при необходимости только лицу, прошедшему специальное обучение по работе с ними.

---

[1] Проблемы европейской интеграции: правовой и культурологический аспекты: сб. науч. статей. СПб., 2007. С. 134.

[2] См.: *Дремлюга Р. И.* Интернет как способ и средство совершения преступления // Информационное право. 2008. № 4. С. 609.

[3] Латинская фраза, которая обычно переводится как «образ действий» и обозначает привычный для человека способ выполнения определенной задачи. Данное выражение особенно часто используется в криминалистике для указания на типичный способ совершения преступлений данным преступником или преступной группой, служит основой для составления психологического профиля преступника.

[4] См.: Доклад о работе тринадцатого Конгресса Организации Объединенных Наций по предупреждении преступности и уголовному преследованию. Доха, 12–19 апреля 2015 г. [Электронный ресурс] // Официальный сайт Организации Объединенных Наций. URL: http: www.un.org/ru/events/crimecongress

4. Все действия, связанные со сбором, использованием, хранением или передачей цифровых доказательств, должны быть надлежащим образом задокументированы, а документы должны быть сохранены и доступны для изучения.

5. Лицо несет ответственность за все действия в отношении цифровых доказательств, которые находятся в его распоряжении.

6. Любое учреждение, в обязанности которого входит сбор, использование, хранение или передача цифровых доказательств, несет ответственность за соблюдение этих принципов[1].

Возвращаясь к рассмотрению Конвенции Совета Европы от 2001 года, следует отметить один из ее аспектов. Специалисты обратили внимание на то, что в ней не дается понятия «компьютерное преступление» или «преступление, связанное с использованием компьютерных технологий», которые применялись в принятых ранее международных документах. В документе используется понятие «киберпреступление», содержание которого раскрывается с помощью перечня, включающего в себя:

1) деяния, направленные против компьютерной информации (как предмета преступного посягательства),

2) деяния, посягающие на иные охраняемые законом блага, при этом информация, компьютеры и т. д. являются одним из элементов их объективной стороны, выступая в качестве, к примеру, орудия их совершения либо составной части способа их совершения или сокрытия[2].

В связи с этой двойственностью у экспертов возникает вопрос о дефиниции «киберпреступности» как явления, включающего «традиционные» преступные деяния, совершенные с помощью новых технологий, и деяния, направленные на новые объекты посягательств. При этом термин «киберпреступность» часто употребляется наряду с термином «компьютерная преступность», причем нередко эти понятия используются как синонимы. Действительно, эти термины очень близки друг другу по смыслу, но не синонимичны. Понятие «киберпреступность» (cybercrime) шире, чем «компьютерная преступность» (computercrime), и более точно отражает природу такого явления, как преступность в информационном пространстве. Так, Оксфордский толковый словарь определяет приставку «cyber» как компонент сложного слова. Ее значение –

---

[1] См.: *Урденко О. Г.* Необходимость компьютерной криминалистики (forensics) как науки [Электронный ресурс]. URL: http://www.epos.ua/site/file_uploads/ cfu2012_1-4_Urdenko.pdf

[2] См.: *Аратулы К.* Преступления в сфере компьютерной информации в РК и зарубежных странах [Электронный ресурс] // Вестник КазНУ. Алматы, 2010. URL: https://articlekz.com/article/10037

«относящийся к информационным технологиям, сети «Интернет», виртуальной реальности». Практически такое же определение дает Кембриджский словарь. «Cybercrime» – это преступность, связанная как с использованием компьютеров, так и с использованием информационных технологий и глобальных сетей. В то же время термин «computercrime» в основном относится к преступлениям, совершаемым против компьютеров или компьютерных данных. Поэтому термин «компьютерная преступность» уже по своей смысловой нагрузке и сводит суть явления к преступлениям, совершенным с помощью компьютера. В настоящее время, с развитием информационных технологий, уже само понятие «компьютер» становится размытым. Например, сегодня практически все мобильные телефоны имеют доступ в сеть «Интернет». С развитием сетей (3G, 4G, 5G) мобильные телефоны способны подключаться к глобальной сети со скоростями, не уступающими возможностям подключения к сети «Интернет» с помощью обычного компьютера, а в перспективе – и превышать их[1].

По пути аналогичного разделения терминов «киберпреступность» и «компьютерная преступность» и использованию именно первого термина идет также международное право. В Конвенции Совета Европы от 2001 года употребляется именно термин «cybercrime», а не «computercrime». Киберпреступность – это преступность в так называемом киберпространстве. Авторы «модельного закона» о киберпреступности Международного Союза Электросвязи (2009) определяют киберпространство как «физическое и не физическое пространство, созданное и (или) сформированное следующим образом: компьютеры, компьютерные системы, сети, их компьютерные программы, компьютерные данные, данные контента, движение данных и пользователи». В настоящее время официальное определение киберпространства на международном уровне отсутствует, впрочем, как и определение киберпреступности. Вместе с тем понятие киберпреступности как совокупности преступлений распространяется на все виды преступлений, совершенных в информационно-телекоммуникационной сфере, где информация, информационные ресурсы, информационная техника могут выступать (являться) предметом (целью) преступных посягательств, средой, в которой совершаются правонарушения, и средством или орудием преступления[2].

[1] См.: *Тропина Т. Л.* Киберпреступность. Владивосток, 2009. С. 64.
[2] Там же. С. 65.

Таким образом, киберпреступность может быть определена как совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных[1].

§ 2. Нормативно-правовые и фактические основания использования результатов оперативно-розыскной деятельности в уголовном процессе

Сложившееся понимание об общих положениях существующей концепции доказывания по уголовным делам, в том числе в части использования результатов ОРД, есть необходимое условие для анализа вопросов правового регулирования и правоприменительной практики по отдельным видам преступлений, в числе которых и хищения денежных средств, криптовалют. Прежде чем перейти к рассмотрению оснований использования результатов ОРД в рамках уголовного процесса, необходимо остановиться на спорных вопросах терминологии, возникающих в связи с их использованием у научного сообщества, правоприменителей. Отметим, что в литературных источниках нередко встречается смешение таких терминов как «результаты ОРД», «материалы ОРД», «предметы и документы, полученные или использованные при осуществлении ОРД». Сопоставление сущностного наполнения приведенных терминов не позволяет отождествлять их между собой. К примеру, согласно статье 2 Закона Республики Беларусь «Об оперативно-розыскной деятельности» материалами оперативно-розыскной деятельности признаются оперативно-служебные документы, материальные носители информации, содержащие порядок проведения ОРМ, и сведения, полученные при их проведении, а также иные сведения и документы, полученные при осуществлении ОРД[2]. При этом к оперативно-служебным документам относятся:

- постановление о проведении оперативно-розыскного мероприятия;
- специальное задание;
- протокол проведения оперативно-розыскного мероприятия;
- справка;
- рапорт;

[1] См.: *Gercke M.* Understanding Cybercrime: A Guide for Developing Countries. ITU, 2011. P. 43.

[2] Об оперативно-розыскной деятельности: Закон Республики Беларусь от 15 июля 2015 г. № 307-З [Электронный ресурс] // Национальный правовой интернет-портал Республики Беларусь. URL: https://pravo.by/upload/docs/op/H11500307_1437685200.pdf

– акт;
– письменный запрос и (или) запрос в электронном виде;
– письменное уведомление прокурора или его заместителя
– и иные документы, образующиеся при осуществлении ОРД.

Материальными носителями информации признаются объекты, способные любым путем (магнитным, электронным, оптическим, фотографическим, механическим и т. д.) записывать и хранить сведения графического, текстового, звукового, цифрового, фото-, видео-, речевого и иного характера (CD, DVD-диски, флеш-карты, винчестеры, фото- и видеопленки, бумага и др.). Также статьей 2 этого же нормативного правового акта приводится и понятие «предметы и документы», под которыми понимаются вещества, вещи, иные объекты, имущественные права, программные продукты, в том числе изъятые из оборота и ограниченно оборотоспособные, полученные или использованные при осуществлении ОРД. В свою очередь, дефиниция «результаты ОРД» законодательного закрепления в Республике Беларусь не получила, несмотря на довольно широкое распространение среди белорусских правоведов и правоохранителей. Соглашаясь с мнением А. Н. Тукало отметим, что под результатами ОРД следует признавать фактические данные, полученные гласно и негласно при проведении ОРМ, зафиксированные в установленном порядке в материалах, полученных в ходе ОРД, имеющих значение для решения задач ОРД[1]. В российском правовом поле статьей 5 УПК РФ результаты ОРД определяются как «…сведения, полученные в соответствии с Федеральным законом об оперативно-розыскной деятельности, о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия или суда». Однако Федеральный закон «Об оперативно-розыскной деятельности» содержит положения, согласно которым результаты ОРД рассматриваются в качестве материалов, а также оперативно-служебных документов, полученных в результате проведения ОРМ. Так, ст. 5, гласящая о соблюдении прав и свобод человека и гражданина при осуществлении ОРД, имеет настоящие строки: «Полученные в результате проведения ОРМ материалы в отношении лиц, виновность которых в совершении преступления не доказана в установленном законом порядке, хранятся один год, а затем уничтожаются, если служебные

[1] См.: *Тукало А. Н.* Использование результатов оперативно-розыскной деятельности в работе оперативных и следственных подразделений органов внутренних дел: автореф. дис. … канд. юрид. наук. Минск: Академия Министерства внутренних дел Республики Беларусь. 2011. С. 18.

интересы или правосудие не требуют иного». Добавим, что ст. 21, содержащая положения о прокурорском надзоре за ОРД, закрепляет следующие положения: «По требованию указанных прокуроров руководители органов, осуществляющих ОРД, представляют им оперативно-служебные документы, включающие в себя дела оперативного учета, материалы о проведении ОРМ с использованием оперативно-технических средств…». Вдобавок высшие судебные инстанции, в частности Конституционный Суд, в своих решениях также смешивают понятия «результаты ОРД», «сведения», «материалы», «оперативно-служебные документы», де факто подразумевая под ними одно и то же. Таким образом, анализ содержания приведенных выше понятий позволяет говорить о невозможности их отождествления и необходимости выработки научно обоснованных позиций в части соотношения друг с другом, а также о дополнении на основе этого соответствующими нормами отраслевого законодательства. Ведь по существу перечисленные выше категории соотносятся друг с другом как материальный носитель, отражающий ход и результаты ОРМ (материалы ОРД), фактические данные (сведения) – информация (результаты ОРД) и объекты, полученные либо использованные при осуществлении ОРД (предметы и документы).

Переходя непосредственно к рассмотрению нормативно-правовых оснований использования результатов ОРД в уголовном судопроизводстве, отметим, что их стоит рассматривать в широком и узком смыслах. К первому следует отнести положения нормативно-правовых и подзаконных актов, регулирующих деятельность компетентных должностных лиц по возбуждению, расследованию и рассмотрению уголовных дел, содержащих результаты ОРД, предоставленные оперативными подразделениями органов дознания. В российском правовом поле таковыми выступают:

– Конституция Российской Федерации[1];

– УПК РФ[2];

– Кодекс Российской Федерации об административных правонарушениях[1];

[1] Конституция Российской Федерации: принята всенарод. голосованием 12 декабря 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 5 февраля 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ) [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/ cons_doc_LAW_2839

[2] Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Российская газета. 2020. 7 апр.

– Федеральный закон «Об оперативно-розыскной деятельности»[2];

– Федеральный закон «О полиции»[3];

– Федеральный закон «О федеральной службе безопасности»[4];

– Федеральный закон «О государственной охране»[5];

– Федеральный закон «О внешней разведке»[6];

– Постановление Правительства России «О Федеральной таможенной службе» (вместе с «Положением о Федеральной таможенной службе»)[7];

– Федеральный закон «О прокуратуре Российской Федерации»[8];

– Инструкция о порядке предоставления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд[9];

– иные подзаконные акты, правовые позиции высших судебных инстанций[10].

---

[1] Кодекс Российской Федерации об административных правонарушениях: Федеральный закон Российской Федерации от 30 декабря 2001 № 195-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34661

[2] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_ LAW_7519/

[3] О полиции: Федеральный закон от 7 февраля 2011 г. № 3-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_110165/

[4] О федеральной службе безопасности: Федеральный закон от 3 апреля 1995 г. № 40-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_6300/

[5] О государственной охране: Федеральный закон от 27 мая 1996 г. № 57-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_ LAW_10511/

[6] О внешней разведке: Федеральный закон от 10 января 1996 г. № 5-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_ LAW_8842/

[7] О Федеральной таможенной службе (вместе с Положением о Федеральной таможенной службе): постановление Правительства России от 16 сентября 2013 г. № 809 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_ doc_LAW_152009/

[8] О прокуратуре Российской Федерации: Федеральный закон от 17 января 1992 г. № 2202-1 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_262/

[9] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: 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 № 68 от 27 сентября 2013 г. [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_155629/

[10] После принятия Конституционным судом Определения от 14 июля 1998 г. № 86-0 по о проверке конституционности отдельных положений Федерального закона «Об оперативно-розыскной деятельности» по жалобе гражданки И. Г. Черновой в число нормативно-правовых актов включают и определения Конституционного Суда, немаловажное значение

Аналогичные по своей сути и схожие по названиям, нормативно-правовые акты, решения высших судебных инстанций, регулируют общественные отношения и на территории стран СНГ. Причин к тому несколько: общность правовых систем (романо-германская), исторические, социокультурные и сопутствующие связи. К примеру, на территории Республики Беларусь действует ранее упомянутый Закон Республики от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности». Не стоит забывать, что на объединяющем наши территории пространстве приняты и межгосударственные нормативно-правовые акты, в том числе регулирующие вопросы уголовно-процессуального и оперативно-розыскного противодействия преступлениям, совершаемым с использованием сети «Интернет». Так, статья 6 Модельного информационного кодекса для государств – участников СНГ предусматривает ограничение законом прав и свобод в информационной сфере в интересах защиты основ конституционного строя, обеспечения национальной безопасности, защиты территориальной целостности и общественного порядка с целью предотвращения беспорядков, преступлений, разжигания социальной, расовой, межнациональной, межэтнической и религиозной вражды, и др.[1] Эту норму дополняет статья 177.1. «Склонение, вербовка или иное вовлечение в совершение преступлений террористического характера либо иное содействие осуществлению террористической деятельности» Модельного Уголовного кодекса для государств – участников СНГ, где часть третья относит деяния, совершенные с использованием компьютерных устройств, системы или их сети, к особо тяжким преступлениям[2].

Очевидно, что источники регулирования проведения ОРМ и последующего предоставления их результатов в органы предварительного расследования не ограничены лишь профильным Федеральным законом. Это лишний раз подчеркивает, что ОРД сродни уголовно-процессуальной деятельности должностных лиц органов предварительного расследования, надзора, судебной системы и достаточно детально регламенти-

---

имеют и решения Верховного Суда, в частности, выраженные в Постановлении Пленума от 29 ноября 2016 г. № 55 «О Судебном приговоре».

[1] Модельный информационный кодекс для государств – участников СНГ [Электронный ресурс]. Принят в г. Санкт-Петербурге 23 ноября 2012 г. Постановлением № 38-6 на 38-м Пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ. URL: https://docs.cntd.ru/document/902124603

[2] Модельный Уголовный кодекс для государств – участников СНГ [Электронный ресурс]. Принят в г. Санкт-Петербурге 27 ноября 2015 г. Постановлением № 43-16 на 43-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ. URL: https://docs.cntd.ru/document/901781490

рована. В научном сообществе существует расхожее мнение о том, что это не так. К примеру, Т. Г. Николаева, Е. Л. Никитин, А. А. Ларинков, в своей статье, посвященной правовой природе использования результатов ОРД и процедуре их использования в уголовном процессе, указывают: «Оперативно-розыскные действия, в отличие от уголовно-процессуальных, в меньшей мере обеспечены различными ограничениями и запретами. Для оперативно-розыскных мероприятий процедурные гарантии не характерны еще и в силу того, что они ограничивают суть разведывательно-поисковых действий, которые осуществляются преимущественно негласно»[1]. Взгляды С. А. Бочинина о доказательственном значении результатов ОРД также символизируют общую тенденцию скептического отношения к данному институту в уголовном процессе: «…в ходе ОРД не могут быть созданы условия, при которых ее результаты отвечали бы требованиям, предъявляемым к доказательствам УПК РФ. Таким требованиям могут отвечать только доказательства, полученные в рамках возбужденного уголовного дела способами, предусмотренными этим Законом»[2].

Распространенность взглядов относительно «неполноценности» ОРД в уголовно-процессуальном праве подтверждают и мнения белорусских исследователей. Приверженцами указанных взглядов выступают такие авторы, как В. Ч. Родевич, А. Н. Тукало, Р. Г. Зорин и О. Т. Супытко, по мнению которых материалы ОРД не следует признавать доказательствами по уголовным делам. Этому, на наш взгляд, способствуют следующие причины:

1) источники получения доказательственной информации в рамках ОРД, в отличие от уголовного процесса, непроцессуальные. Кроме того, не всегда существует возможность проверки таких источников с целью установления достоверности и допустимости полученных данных, предметов и документов, поскольку указание на них может отсутствовать в материалах ОРД, что связано со спецификой осуществления ОРД как гласно, так и негласно (например, согласно ст. 14 Закона Республики Беларусь «Об оперативно-розыскной деятельности», подлежат сохранению в тайне сведения о гражданах, оказывающих или оказывавших содействие на конфиденциальной основе (конфидентах), что, в

[1] *Николаева Т. Г., Никитин Е. Л., Ларинков А. А.* Правовая основа использования результатов оперативно-розыскной деятельности и процедура их использования в уголовно-процессуальном доказывании // Вестник Санкт-Петербургского университета МВД России. 2006. № 2 (30). С. 301–307.

[2] *Бочинин С. А.* Следственные действия и их соотношение с оперативно-розыскными мероприятиями // Вестник ПАГС. 2010. С. 100–105.

свою очередь, затрудняет возможность проверки достоверности и законности предоставленной такими лицами информации в процессе расследования по уголовному делу);

2) различным представляется правовое значение фактических данных, полученных в процессе ОРД, и уголовно-процессуальной деятельности в связи с чем результаты ОРД не могут быть положены в основу принятия достоверного решения по уголовному делу;

3) материалы ОРД могут быть полностью или частично опровергнуты в процессе расследования уголовного дела или на судебных стадиях уголовного процесса;

4) доказывание в уголовном процессе и в рамках ОРД отличаются друг от друга, поскольку обладают собственными методами и реализуются в разных правовых режимах;

5) по материалам ОРД выявлению подлежат не сами доказательства, а лишь их источники (например, свидетели), которые уже в рамках уголовного процесса предоставляют доказательственную информацию, облачаемую в соответствующую процессуальную форму[1].

Таким образом, вышеуказанные авторы полагают, что признание материалов ОРД доказательствами по уголовным делам является преждевременным, поскольку проблемы их имплементации в уголовный процесс возникают еще на стадии оценки согласно требованиям, предусмотренным ст. 88, 101, 104 и 105 Уголовно-процессуального кодекса Республики Беларусь от 16 июля 1999 г. № 295-З[2]. В свою очередь, фактические данные, закрепленные в материалах ОРД, имеют ориентирующий характер и могут быть использованы органами предварительного расследования при планировании расследования, выборе необходимых к реализации следственных и процессуальных действий.

Г. В. Гудачевская считает, что материалы ОРД должны позволять сформировать на их основе доказательства, удовлетворяющие требованиям УПК, предъявляемым как к доказательствам в целом, так и к их соответствующим видам. В представляемых результатах ОРД должны содержаться сведения, имеющие значение для установления обстоятельств, подлежащих доказыванию по уголовному делу, указания на источник получения предполагаемого доказательства или предмета, ко-

[1] См.: *Родевич В. Ч.* Развитие теоретических взглядов на проблему использования результатов оперативно-розыскной деятельности в уголовном процессе / В. Ч. Родевич, А. Н. Тукало // Вестник Академии МВД Республики Беларусь. 2009. № 2. С. 60–64.

[2] Уголовно-процессуальный кодекс Республики Беларусь от 16 июля 1999 г. № 295-З [Электронный ресурс] // ЭТАЛОН. Законодательство Республики Беларусь // Национальный центр правовой информации Республики Беларусь. Минск, 2021.

торый может стать доказательством, а также данные, позволяющие надлежащим образом проверить и оценить в условиях судопроизводства доказательства, сформированные на их основе[1].

Исходя из этого, раскрывая тему нормативно-правовых основ использования результатов ОРД в уголовном процессе, стоит иметь в виду, что существующие в науке тенденции весьма однобоки, связаны с отсутствием практического опыта и объективных взглядов об указанном институте. Немногочисленные исключения представлены отдельными учеными, среди которых М. П. Поляков[2]. Строгая регламентация порядка организации и проведения ОРМ берет свое начало с концептуальных положений Конституции Российской Федерации и иных государств. ОРМ, ограничивающие права на тайну переписки, неприкосновенность жилища, а также смежные с ними, являются наиболее результативными и действительно способными стать основой изобличения лиц в совершении преступлений. Согласно статьям 23, 25 ограничение ключевых конституционных прав допускается только на основании судебного решения, что находит отражение в порядке проведения таких мероприятий, как «обследование помещений, зданий, сооружений, участков местности и транспортных средств», «контроль почтовых отправлений, телеграфных и иных сообщений», «прослушивание телефонных переговоров», «снятие информации с технических каналов связи», «получение компьютерной информации».

Иные, перечисленные выше нормативные источники закрепляют право на осуществление ОРД отдельными федеральными органами исполнительной власти, очерчивая круг субъектов ОРД и закрепляя правомочия на их проведение. Из всей их совокупности особого внимания заслуживает Кодекс Российской Федерации об административных правонарушениях. Сам собой напрашивается вопрос о том, как данный кодифицированный Федеральный закон может отождествляться с нормативно-правовыми основаниями использования результатов ОРД при расследовании уголовных дел. Однако без закрепленных в рамках него норм-гарантий, устанавливающих меры ответственности за неисполне-

---

[1] См.: *Гудачевская Г. В.* Допустимость результатов оперативно-розыскной деятельности в доказывании по уголовному делу / Г. В. Гудачевская // 68-я научная конференция студентов и аспирантов БГУ: сб. раб.: в 3 ч. / ред. кол.: А. Г. Захаров [и др.]. Минск: БГУ, 2011. Ч. 2. С. 216–219.

[2] М. П. Поляков – доктор юридических наук, профессор, профессор кафедры уголовного процесса Нижегородской академии МВД России. Один их немногих ученых-процессуалистов, признающих важность ОРД для целей уголовного процесса, рассматривает вопросы их интерпретации, порядок ввода в процесс расследования и т. д.

ние законных требований должностных лиц, осуществляющих ОРД, проблематично представить реализацию ими собственных полномочий при условии необходимости истребования информации у широкого круга имеющихся сегодня хозяйствующих субъектов[1]. Ярким примером тому служит практика направления мотивированных запросов со стороны должностных лиц оперативных подразделений органов дознания.

Нормативно-правовые основания использования результатов ОРД в уголовном процессе также представляется возможным рассмотреть и с более узкой позиции. А именно как связанные друг с другом отдельными положениями Федерального закона «Об оперативно-розыскной деятельности», УПК РФ и Инструкции о порядке предоставления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд и закрепляющие материальные и процессуальные механизмы использования результатов ОРД в уголовном судопроизводстве. В этом смысле выстраивается логическая, последовательная «цепочка», берущая начало с концептуальных положений ст. 73–74 УПК РФ, в которых очерчиваются контуры обстоятельств, подлежащих доказыванию, и средства (доказательства) их установления. При этом научный и практический интерес представляют две составляющие диспозиции ст. 74 УПК РФ. Согласно первой, доказательствами по уголовному делу являются **любые сведения**, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном настоящим Кодексом, устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела. Во второй составляющей, весьма интересны и содержательны положения о том, что в качестве доказательства, помимо прочих, допускается один из видов, который законодатель сформулировал как **«иные документы».**

Как буквальное, так и расширительное толкование данных норм вполне допускает распространение перечисленных положений на полученные в установленном законом порядке материалы, отражающие результаты ОРД. Кроме того, ст. 89 УПК РФ изложена в следующей редакции: «В процессе доказывания запрещается использование результатов ОРД, если они не отвечают требованиям, предъявляемым к доказательствам настоящим Кодексом». Очевидно, что не введенные в ранг

[1] Ст. 17.7, 19.3, 19.7 КоАП России предусматривают меры административной ответственности за невыполнение законных требований, неповиновение законному распоряжению, а также непредставление информации сотрудникам правоохранительных органов. Вопросы их применения, конкуренции норм при каждой конкретной ситуации рассматриваются в рамках самостоятельной отрасли права.

самостоятельного вида доказательств результаты ОРД, тем не менее, оцениваются аналогичным с ними образом. Данный факт, с одной стороны приводящий в замешательство, вместе с тем указывает на то, что рассматриваемый нами институт имеет самостоятельное и важное значение для уголовно-процессуальной деятельности и всей отрасли права. Ст. 140 УПК РФ, закрепляющая поводы для возбуждения уголовного дела, одним из таковых именует «сообщение о совершенном или готовящемся преступлении, полученное из иных источников». Названная статья выступает «связующим звеном» со смежными, но более конкретизированными положениями ст. 11 Федерального закона «Об оперативно-розыскной деятельности». Напомним, что результаты ОРД могут быть использованы в следующих процессуальных аспектах: 1) для подготовки и осуществления следственных и судебных действий; 2) для розыска лиц, скрывшихся от органов дознания, следствия и суда, уклоняющихся от исполнения наказания и без вести пропавших; 3) для розыска имущества, подлежащего конфискации; 4) могут служить поводом и основанием для возбуждения уголовного дела; 5) могут использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства Российской Федерации.

Примечательно, что источником уголовно-процессуальных отношений, притом детально урегулированных, выступает вовсе не УПК РФ, являющийся кодифицированным Федеральным законом, а иной нормативно-правовой акт. Нельзя придавать забвению и тот факт, что негласные подзаконные акты, хоть и в меньшей степени, но все же регулируют отдельные внутриструктурные элементы предоставления оперативно-розыскных документов оперативных подразделений органов дознания следователю (дознавателю).

Фактические основания использования результатов ОРД имеют прямую связь с нормативно-правовыми по двум причинам. Первая состоит в том, что они также строго ими закреплены, т. е. оперативный уполномоченный не может провести ОРМ того или иного характера, не имея на то фактических оснований, предусмотренных источниками регулирования его служебной деятельности. В частности, ч. 2 ст. 7 Федерального закона «Об оперативно-розыскной деятельности» в качестве таковых закрепляет сведения: 1) о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах, его подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела; 2) событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопас-

ности Российской Федерации; 3) лицах, скрывающихся от органов дознания, следствия и суда или уклоняющихся от уголовного наказания; 4) лицах, без вести пропавших, и об обнаружении неопознанных трупов.

Второй причиной является возможность определить направленность поиска, получения, проверки фактических оснований использования результатов ОРД для достижения исключительно правового результата. Ведь конечным итогом работы оперативных подразделений органов дознания выступает привлечение к уголовной либо иной, предусмотренной законом ответственности физического лица, виновного в совершении деяния, за которое уголовным законом предусмотрено наказание. Однако проблемы соотношения вопроса «права» и «факта» в плоскости ОРД как вида деятельности и отрасли законодательства имеют свои особенности. Осью, вокруг которой вращается вся совокупность фактических оснований использования результатов ОРД в уголовном процессе, выступает осведомленность оперативного сотрудника о фактах, лицах криминального характера, а также реальная возможность обратить указанную информацию в юридическую плоскость путем сбора и подготовки необходимых материалов. Это выступает ключевым фактическим основанием дальнейшего использования результатов ОРД в уголовном судопроизводстве. П. В. Волосюк в своей статье на тему использования в доказывании результатов ОРД подчеркивает, что в ч. 1 ст. 86 УПК РФ изложен исчерпывающий перечень субъектов, наделенных правом собирать доказательства. К ним относятся: суд (судья), прокурор, следователь и дознаватель. Иные лица, в том числе сотрудники правоохранительных органов, уполномоченные на производство оперативно-розыскных мероприятий, а также руководители органов, осуществляющих ОРД, могут лишь представлять предметы и документы для приобщения их к уголовному делу в качестве доказательств[1]. Дополняя изложенное, обратимся к мнению, высказанному И. Н. Сорокиным, о том, что собранные оперативно-розыскным путем фактические данные сами по себе без их получения и подтверждения в уголовно-процессуальном порядке доказательствами не являются[2]. Собственно, приведенные позиции этих и других авторов ничего нового не содержат, кроме того, что сформулировал Конституционный Суд в своем определении от 4 февраля 1999 г. «По жалобе гражданина М. Б. Никольской и

[1] См.: Волосюк П. В. Проблемы использования результатов оперативно-розыскной деятельности в уголовном судопроизводстве // Юридическая наука. 2013. № 1. С. 38–41;

[2] См.: Сорокин И. Н. Использование результатов оперативно-розыскной деятельности в уголовном судопроизводстве [Электронный ресурс] // Научно-методический электронный журнал «Концепт». 2014. № 12 (декабрь). URL: http://e-koncept.ru/2014/14362.htm.

М. Н. Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона "Об оперативно-розыскной деятельности"»[1]. Изложенное свидетельствует о необходимости заблаговременной оценки полученной оперативным путем фактической информации на ее пригодность к использованию в уголовном процессе с целью дальнейшей проверки посредством производства следственных и иных процессуальных действий. Стоит обратить внимание на тот факт, что итог оперативной работы предстает перед вниманием достаточно широкого круга иных лиц, правомочных на принятие процессуальных решений. Поэтому «фильтрация» фактических сведений, способных выступать в качестве оснований, являет собой одну из важнейших функций, выполняемых сотрудниками оперативных подразделений органов дознания.

Таким образом, нормативно-правовые и фактические основания использования результатов ОРД имеют тесную связь, обуславливают взаимное существование и лишь в идеальной совокупности друг с другом обеспечивают использование анализируемого нами института в уголовном процессе. Именно с установления их наличия берет начало «предпроцессуальная», а затем и исключительно уголовно-процессуальная деятельность компетентных должностных лиц по проверке сообщения о преступлении, возбуждению, расследованию и рассмотрению в суде уголовных дел.

§ 3. Способы хищений денежных средств граждан с помощью сети «Интернет», сотовой связи и возможности для их выявления и дальнейшего расследования посредством использования результатов ОРД

Анализ специфики использования результатов ОРД при расследовании хищений денежных средств, криптовалют стоит начать с определения наиболее актуальных видов их совершения. Рассматриваемые нами преступления, совершаемые с использованием сети «Интернет», сотовой связи, регистрируемые на территории стран СНГ, представляется возможным дифференцировать на несколько групп в зависимости от способа и средств их совершения: «вишинг», «фишинг», «хищения в

[1] «По жалобе гражданина М. Б. Никольской и М. И. Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона «Об оперативно-розыскной деятельности»: Определение Конституционного Суда РФ от 4 февраля 1999 г. № 18-О [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/docu-ment//cons/cgi/online.cgi?req= doc&base=ARB&n=8328#FEGvO1TeGUyaeeUu/

социальных сетях», «хищения в сфере онлайн-кредитования», «SMS-мошенничество», мошенничество в сфере сделок купли-продажи, вымогательство через интернет-ресурсы, «онлайн» или «e-mail» хищения в отношении юридических лиц и индивидуальных предпринимателей. Рассмотрим каждый из представленных видов.

Вишинг – группа киберпреступлений, занимающая лидирующую позицию среди остальных зарегистрированных киберхищений на протяжении 2019–2021 гг. Его сущность заключается в контакте между преступником и потерпевшим, реализуемом посредством звонков на абонентский номер или вызовов в программах по мгновенному обмену сообщениями («мессенджерах»: «Вайбер» (Viber), «Телеграм» (Telegram)), в ходе которого преступник, представляясь от имени сотрудника банка (например, работника службы безопасности) или сотрудника правоохранительных органов (МВД, Следственного комитета), под различными предлогами либо получает от потерпевшего реквизиты его банковской карты либо склоняет последнего к совершению необходимых для себя в корыстных целях действий. Как итог – злоумышленник получает доступ к банковской карте или счету потерпевшего, откуда переводит имеющиеся денежные средства на контролируемые им счета или электронные кошельки.

Предлоги совершения таких звонков различны и весьма многообразны: 1. Преступник совершает звонок в адрес потерпевшего через мессенджер, представляясь сотрудником службы безопасности банка, и сообщает последнему о «подозрительном» списании с его банковской карты большой суммы денежных средств (или предстоящем совершении транзакции), для отмены которого необходимо срочно предоставить реквизиты банковской карты. Доверчивый клиент, находясь в стрессовой ситуации и убедившись, что звонок совершается сотрудником банка (о чем свидетельствуют логотип и «никнейм» звонящего), предоставляет преступнику необходимую информацию, которой он в последующем воспользуется для хищения денежных средств.

2. Преступник совершает звонок на «Вайбер» (Viber) и сообщает потерпевшему, что на его имя пытаются оформить банковский кредит. С целью предотвращения оформления кредита и установления безопасности карт (счетов) потерпевшему необходимо предоставить звонившему сотруднику реквизиты банковской карты, личные данные, логин и пароль от интернет-банкинга, назвать код подтверждения операции, поступивший в виде СМС-сообщения, и т. д. Однако в некоторых случаях сведениями от одной банковской карты преступники не ограничивают-

ся, предлагая потерпевшему предоставить реквизиты всех карт, которые он имеет, с целью установления должной защиты от хищений.

3. С потерпевшим связывается сотрудник банка и уточняет, не оформлял ли он в последнее время на свое имя заявку на кредит. Потерпевший, конечно же, сообщает, что ничего подобного не совершал, в ответ на что сотрудник банка информирует последнего, что, вероятно, в отношении него пытаются совершить преступление, о чем банк сообщит в правоохранительные органы, которые и свяжутся с потерпевшим для дальнейшего разбирательства. Через некоторое время потерпевшему вновь поступает звонок через мессенджер от сотрудника правоохранительных органов, который предлагает ему поучаствовать в установлении и задержании преступника, для чего потерпевшему необходимо взять кредиты в других банках, возвращать которые не потребуется, так как все происходит в рамках специальной операции, и перечислить средства на указанные звонящим счета. В последующем потерпевший узнает о наличии задолженности по кредитам и, как следствие, о совершении в отношении него преступления. При «вишинговых» атаках по описанной выше схеме преступники, желая убедиться, что их план реализуется в направлении намеченного результата, могут не просто давать потерпевшему указания, но осуществлять его сопровождение при получении кредитов в других банках и даже оказывать содействие в сборе необходимых документов.

4. Преступник совершает звонок в мессенджере, в ходе которого сообщает потерпевшему, что на его имя мошенники пытаются оформить кредит (либо происходит списание большой суммы средств). Для предотвращения произошедшего и сохранности средств потерпевшему предлагается установить специальное приложение и сообщить необходимую преступнику информацию для его корректной работы. В результате функционирования такого приложения преступникам удается отслеживать действия потерпевшего на мобильном телефоне и получать необходимую информацию для доступа к денежным средствам на его банковских картах, откуда в последующем они и похищаются. Еще одна из довольно востребованных среди преступников «вишинговых схем» – вовлечение потерпевшего в «оперативную игру», в результате которой последний совершает ряд транзакций со своими денежными средствами по указанию злоумышленников, полагая, что участвует в поимке опасных мошенников, хотя на самом деле собственноручно передает свои сбережения преступникам. При этом предлогом для вовлечения в «игру» может служить не только заявка на кредит от сторонних лиц или подозрительное списание денежных средств, но и потеря личных данных.

5. Резервная карта как способ сберечь похищаемые денежные средства – еще одна уловка, которой пользуются «вишеры». Так, преступник сообщает потерпевшему о подозрительных переводах или случайном зачислении на его счет чужих денежных средств и просит перевести определенную сумму на указанную карту – страховую ячейку, где денежные средства будут в сохранности до выяснения обстоятельств.

Представленные выше схемы вишинга не единичны, с каждым днем преступники совершенствуют механизм совершения хищения, усложняя его многоступенчатостью действий и новыми действующими лицами. При этом для придания реализуемым схемам убедительности преступники используют логотипы банков и геральдику правоохранительных органов (помещают на «аватар» в мессенджерах), а также IP, VoIP, SIP-телефонию с виртуальными номерами, позволяющую совершать звонки с измененных номеров (в том числе коротких – трех- или четырехзначного формата) и оставаться неидентифицируемыми. Напомним, что IP, VoIP, SIP-телефонии – сервисы, позволяющие совершать вызовы, в том числе международные, через сеть «Интернет» (базовые станции операторов сотовой связи используются во вспомогательном значении) в режиме реального времени с использованием виртуального номера (т. е. номер не имеет традиционного материального носителя и может быть идентичен любой «классической» номерной емкости). При этом виртуальные мобильные номера могут иметь различный формат и вид, что делает их максимально схожими с номерами действующих мобильных операторов, а также официальными или короткими номерами банков, предоставляя широкий спектр возможностей для киберпреступников совершать звонки с желаемых абонентских номеров, находясь в любой точке мира и по низким тарифам.

Так, например, в России, Беларуси, Казахстане с 2019 г. по настоящее время фиксируются факты совершения «вишинговых» звонков в мессенджерах от имени сотрудников центральных банков с использованием официального логотипа и номеров, идентичных действительно выделенных им со стороны операторов связи. Однако в ряде случаев, например, для белорусского вишинга, характерно использование мобильных номеров, имеющих коды других государств: +797 (Россия), +373 (Молдавия), +370 (Литва), +380 (Украина), +40 (Румыния). Несмотря на явное различие белорусских номеров с номерами, используемыми преступниками, последним удается «втереться в доверие» к потерпевшему, размещая мобильный номер нужной организации, от лица которой осуществляется звонок, в «никнейм» профиля мессенджера (например, милиция – 102, Беларусбанк – 147 и т. д.). Таким образом,

принимая входящий вызов в мессенджере, потерпевший в первую очередь видит логотип организации и в области «никнейма» ее название с официальным номером крупным шрифтом, а уже при должной осмотрительности обращает внимание и на абонентский номер, указываемый меньшим шрифтом, чем «никнейм». Отметим, что ресурсы IP, VoIP, SIP-телефонии предоставляют возможность одному пользователю иметь от одного до нескольких десятков виртуальных абонентских номеров, зарегистрированных на одну учетную запись, что позволяет преступникам реализовывать многоступенчатые схемы «вишинга» в отношении одного и того же потерпевшего. Кроме того, отличительной чертой «вишинговых» схем является обладание преступниками некоторой информацией о потенциальном потерпевшем, что помогает им предрасположить к себе собеседника. Такая информация становится доступной благодаря приобретению от недобросовестных сотрудников коммерческих организаций и банков систематизированных данных в теневом сегменте «Интернета» (DarkNet), а также взломанных виртуальных («облачных») серверов и социальных сетей. Для сотрудников правоохранительных органов используемая в «вишинговых» схемах IP, VoIP, SIP-телефония становится серьезным препятствием в расследовании и раскрытии преступлений, поскольку не позволяет установить личность преступника, совершившего тот или иной звонок.

Фишинг – вид киберпреступлений, сущность которого заключается в получении преступником путем использования поддельных веб-страниц доступа к личным данным пользователей (банковские реквизиты карты, логины и пароли для входа в Интернет или мобильный банкинг для доступа к электронным кошелькам, в том числе криптовалютным) для использования их в целях хищения денежных средств, электронных денег и криптовалют. Основная отличительная черта фишинга – рассылка различными способами (по электронной почте, в сообщении в социальных сетях или мессенджерах, в рекламных объявлениях, в чатах на торговых площадках, через СМС-сообщения и т. д.) ссылок на поддельные сайты, которые как внешне схожи с оригинальными, так и по адресу ресурса – доменному имени. Например, поддельные сайты системы ЕРИП (*raschet.by*): erip-online.com, ERIP.lact.ru, erip-service.umi.ru; поддельные сайты торговой площадки Kufar (*kufar.by*): kufar-dostavka.by, kufar24.space; фишинговые веб-страницы Белпочты (*belpost.by*): belpost.by, bellpost.be, belpost.getpay.by, поддельные сайты Беларусбанка (belarusbank.by): belarusbank24.xyz и т. д. Потерпевший, попавший на поддельный сайт под любыми предлогами, использованными «фишерами», вводит необходимые преступникам данные в соответствующие

поля на веб-странице, после чего она либо обновляется либо выдает ошибку операции. В этот момент преступник получил необходимую для совершения хищения информацию и приступил к ее реализации, о чем вскоре становится известно потерпевшему. В настоящее время характерны следующие способы совершения «фишинговых» атак:

1. «Фишинговые» атаки, осуществляемые посредством торговых интернет-площадок. Преступник подбирает объявления о продаже различных товаров бытового назначения или электротехники (обычно новые), связывается с продавцом либо через чат самой торговой площадки, либо, если продавец указывает номер мобильного телефона для связи, через мессенджеры. В ходе общения «фишер» предлагает продавцу приобрести товар с внесением предоплаты на банковскую карту, и если последний соглашается, направляет ему ссылку для перехода на сайт системы оплаты через Интернет. Продавец, перейдя по ссылке, попадает на сайт либо хорошо известных банков, либо платежно-расчетной системы для безналичных платежей. На сайте для осуществления покупателем предоплаты продавцу необходимо указать реквизиты своей банковской карты, получив которые преступники списывают имеющиеся денежные средства и на связь с продавцом уже не выходят. Описанная схема может осуществляться и повторно, когда преступник вновь связывается с продавцом либо от имени все того же покупателя, либо от службы поддержки торговой площадки, и сообщает, что с денежным переводом произошла ошибка и продавцу необходимо перейти по ссылке на другой сайт и заново ввести реквизиты банковской карты. Так осуществляется повторное списание средств с карт (счетов) потерпевшего. Еще одна преступная «фишинговая» схема, действующая через торговые площадки, реализуется под предлогом осуществления доставки товара с холдированием средств (отложенная оплата). Так, преступник публикует объявление о продаже товара по относительно низкой цене, когда покупатель откликается на объявление, «фишер» предлагает для дальнейшего общения перейти в социальные сети или мессенджер, где уже в ходе переписки под различными предлогами уговаривает покупателя на осуществление доставки товара с отложенным платежом. Услуга холдирования представляет собой «заморозку» необходимой для оплаты товара суммы на счете покупателя, которая будет переведена продавцу после подтверждения состоявшейся доставки товара. Преступник отправляет покупателю ссылку на поддельный сайт банка или платежной системы, где последнему необходимо ввести реквизиты для предоплаты по системе отложенного платежа. Далее «фишер» действует по стандартной схеме. В данном случае, как и в ситуации с предоплатой, воз-

можна повторная связь преступника с покупателем, где ему сообщается либо о невозможности доставки товара и желании вернуть средства, либо об ошибке операции по переводу платежа, после чего предоставляется ссылка для ввода реквизитов карты, в некоторых случаях «фишер» также может затребовать проверочный код, отправляемый покупателю банком посредством СМС-сообщения. Самыми популярными торговыми интернет-площадками в России, Республике Беларусь являются «Авито» (avito.ru), «Куфар» (Kufar.by), которые активно используются не только добросовестными покупателями и продавцами, но и киберпреступниками. При этом подделке подвергаются сайты не только банков и платежных систем, но и самих торговых площадок, где преступниками размещаются поддельные объявления о продаже товаров. Доступ к поддельному сайту, внешне схожему с оригинальным, может осуществляться через всплывающие рекламные объявления, ссылки, размещенные в социальных сетях и мессенджерах, а также через поисковой запрос в браузере.

2. «Фишинговые» сайты, распространяемые через поисковые запросы в браузерах. При формировании в браузере запроса на поиск банкинга, личного кабинета банкинга, сайтов банков, торговых площадок, платежных систем и т. д. пользователи в большинстве случаев выбирают первый сайт, предложенный поисковой системой, не обращая внимание на доменное имя ресурса. Перейдя по предложенной ссылке, пользователь попадает на поддельный сайт мошенников, где, без сомнения, вводит данные либо банковской карты, либо логин и пароль от входа в кабинет интернет-банкинга со специальными сеансовыми ключами, поскольку визуально сайт-дублер отличить от оригинала затруднительно, после чего ожидает нормальной работы сервиса, чего, однако, не происходит. «Фишинговый» сайт либо бесконечно обновляется, либо выдает ошибку доступа, получив необходимые сведения от пользователя. После чего преступниками за короткий временной период осуществляется безвозвратное списание средств с банковского счета или карты потерпевшего. Использование возможностей поисковых сервисов в преступных целях стало доступным благодаря покупке у них слов, формирующих приоритетные запросы. Например, пользующийся популярностью сервис «Гугл» (Google) предлагает своим клиентам приобретение определенного набора слов, поиск которых приведет пользователей в первую очередь к тем веб-страницам, владельцы которых заплатили за первое место в подборке однородных интернет-ресурсов.

3. «Фишинг», осуществляемый посредством взлома учетных записей в социальных сетях и мессенджерах. Преступники либо путем взлома,

либо путем «фишинга», получают доступ к личным страницам пользователей в социальных сетях, от имени которых вступают в контакт с их «друзьями» и «подписчиками», в ходе которого под различными предлогами провоцируют последних перейти на определенный сайт и ввести реквизиты банковской карты. Предлоги разнообразны: благотворительность, помощь в трудной жизненной ситуации, необходимость срочно перевести деньги с карты на карту, когда своя карта заблокирована или недействительна, небольшой взнос для получения крупного дорогостоящего приза (мобильные телефоны, бытовая техника, автомобили, крупная сумма денег и т. д.), участие в голосовании в рамках какого-либо конкурса, где необходимо также сделать взнос для зачета голоса и другие. Полученные реквизиты в дальнейшем используются преступниками для хищения денежных средств. Анализ киберхищений, совершаемых посредством «фишинга», показал, что предметом преступного посягательства могут становиться не только безналичные денежные средства граждан, но и цифровые валюты (криптовалюты).

Хищения, осуществляемые посредством взлома социальных сетей, в некоторой степени схожи с вышеописанным способом «фишинга» через социальные сети. Однако если для «фишинга» характерен переход на поддельный сайт, где пользователь оставляет свои личные данные, то для рассматриваемого вида киберпреступлений свойственно получение данных в порядке виртуального общения преступника с потерпевшими.

Хищения через социальные сети могут осуществляться двумя способами: 1) либо путем предоставления преступником потерпевшему реквизитов счета, электронного кошелька или номера мобильного телефона, куда обманутый пользователь переводит свои денежные средства, думая, что помогает другу или совершает доброе дело в рамках благотворительности, 2) либо посредством получения от потерпевшего обманным путем реквизитов его банковской карты и счета, которыми в последующем воспользуется злоумышленник. В обоих случаях преступник вступает в переписку с друзьями и знакомыми лица, чью учетную запись в социальной сети ему удалось взломать, убеждает их оказать ему денежную помощь или предоставить банковскую карту для временного перевода средств. Злоумышленники используют во время общения информацию о взаимоотношениях лица, от чьего имени выступает, с потерпевшим, которые могут стать ему известны благодаря анализу историй сообщений, совместных фотографий и т. д.

С хищениями в сфере онлайн-кредитования можно встретиться не только при исследовании способов осуществления «вишинга», где кредит выступает лишь предлогом для получения реквизитов банковских

карт, но и в рамках реализации преступных схем, направленных непосредственно на получение кредитных средств и их последующее незаконное списание с карт владельцев. Распространены три способа хищения денежных средств через онлайн-кредитование:

1) получение кредитов через мобильный или интернет-банкинг: преступники по результатам «вишинга» или «фишинга», получив доступ к банкингу и, соответственно, банковскому счету пользователя, обнаруживают, что денежные средства на нем отсутствуют или имеются в небольшом количестве, что не соответствует запланированному результату. Для исправления данной ситуации злоумышленники через мобильное приложение, личный кабинет интернет-банкинга подают заявку на получение максимально возможной суммы в кредит. Если потерпевший обладает хорошей кредитной историей, то банк спустя непродолжительное время одобряет заявку и переводит денежные средства на карту, которые преступники переводят в свою пользу на другой счет, зарегистрированный в зарубежном банке, или на электронный / криптовалютный «кошелек». Если для подтверждения заявки на кредит банк требует от потерпевшего ввести код из СМС-сообщения, предоставить паспортные данные, то преступники по уже отработанной ранее схеме получают от потерпевшего необходимые сведения обманным путем. Еще один способ хищения путем получения онлайн-кредита через банкинг связан с желанием пользователей заработать быстрые деньги без особого труда, предоставив лишь свои банковские карты на время сторонним гражданам. Об этом свидетельствует следующий пример: 28-летний житель областного центра Л. подыскивал на территории города Гродно и Гродненского района держателей банковских платежных карт или тех, кто мог оформить такие карты на свое имя. После чего предлагал за вознаграждение помочь ему перевести на эти карт-счета деньги его фирмы для обналичивания. Как оказалось, Л. таким образом вводил в заблуждение доверчивых граждан. Используя чужие мобильные телефоны, он через специальное приложение оформлял заявки в одном из коммерческих банков города на выдачу онлайн-кредитов. После принятия решения банком и зачисления кредитных средств на карт-счета клиентов им приходили СМС-сообщения о поступлении заявленной суммы. В них, однако, ничего не говорилось об оформлении онлайн-кредита. Это убеждало держателей платежных карт в том, что перевод денег произвел именно Л. с расчетного счета его фирмы. Потерпевшие снимали наличные с «карточек» и передавали их обвиняемому, за что получали обещанное вознаграждение. Когда же обманутые клиенты узнали о заключенных с ними кредитных договорах, Л. объяснил им такие манипуля-

ции сложным финансовым положением фирмы, обещал самостоятельно уплачивать банку ежемесячные платежи. В действительности Л. никогда не работал, и никакой фирмы у него не было. Все наличные деньги, полученные от граждан, он проиграл в казино[1]; 2) оказание посреднических услуг в получении онлайн-кредита лицам, обладающим плохой кредитной историей. Преступное посредничество может осуществляться несколькими путями: либо потерпевший сам отыскивает в социальных сетях или на различных тематических форумах объявление о помощи в получении кредита, либо сам размещает объявление с аналогичными просьбами, различными советами и уловками, на которые откликаются мошенники. В первом случае преступники, имитируя активное сотрудничество с клиентом, получают необходимые личные данные от пользователя, осуществляют деятельность по подбору банка и подходящего кредита, занимаются оформлением, при этом используя ложную информацию о клиенте (завышенный доход, указание на отсутствие задолженности, запрос на большую сумму кредита, о чем просил клиент и т. д.), и, если банк одобряет кредит, получают денежные средства, с которыми в последующем и скрываются. Если оформить кредит все же не представляется возможным, преступники выманивают у клиента предоплату за свои услуги, не сообщая об отрицательном результате, после чего на связь уже не выходят. Во втором случае потерпевший сам привлекает внимание злоумышленников, делясь своей проблемой в социальных сетях или на форумах. Преступник вступает в контакт с пользователем, сообщает ему, что является представителем банка и имеет возможность за вознаграждение «поправить» в базах кредитную историю последнего, чтобы возможность взять кредит стала реальной. Соглашаясь на предложение, потерпевший сообщает паспортные данные, номер мобильного телефона и проверочный код, отправленный банком по СМС. Преступник оформляет кредит на потерпевшего, распорядившись денежными средствами по своему усмотрению;

3) хищение денежных средств, получаемых посредством мобильных кредитов. С недавнего времени операторы мобильной связи ввели новую услугу для своих клиентов, позволяющую получать денежные средства в кредит посредством специального мобильного приложения на любую банковскую карту, синхронизированную с абонентским но-

[1] См.: Похитил и проиграл в казино 420 тыс. рублей. Прокуратура Гродненской области направила уголовное дело в суд [Электронный ресурс] // Официальный сайт Генеральной прокуратуры Республики Беларусь. URL: http://www.prokuratura.gov.by/ru/info/novosti/ nadzor-za-resheniyami-po-ugolovnym-i-grazhdanskim-delam/pokhitil-i-proigral-v-kazino-420-tys-rubley-prokuratura-grodnenskoy-oblasti-napravila-ugolovnoe-delo/

мером, или на виртуальную карту мобильного оператора (например, «МТС Деньги»). Простым способом хищения мобильных кредитных средств является просьба преступника к владельцу мобильного телефона позвонить или воспользоваться Интернетом. Соглашаясь на данную просьбу, потерпевший передает свой мобильный телефон мошеннику, который за короткий период времени проводит необходимые операции по получению кредита и переводу средств в свою пользу. Более сложный механизм требует от преступника составления легенды, позволяющей ему получить чужие СИМ-карты для последующего использования в преступных целях.

Реже встречающимися, но все еще практикуемыми являются СМС-мошенничество и мошенничество в сфере сделок купли-продажи товаров через Интернет. Механизм СМС-мошенничества заключается в рассылке текстовых сообщений случайным гражданам от лица родственников или знакомых людей (чаще от имени сына или дочери, брата или сестры, либо родителей) с просьбой о денежной помощи, которую необходимо оказать немедленно, в противном случае отправителя «ждут проблемы». Мошенники просят перевести небольшую сумму денежных средств на платежные реквизиты, нередко иностранного государства, что поможет им благоприятно решить возникшую проблему и не попасть в беду (например, расплатиться за долги, откупиться от правоохранительных органов и т. д.). Итог подобных действий – обогатившиеся преступники и обманутые потерпевшие. Поводы для получения денежных средств посредством СМС различны: помощь человеку, попавшему в беду, благотворительность, участие в розыгрыше призов, оплата штрафов и т. д.

Мошенничество в сфере сделок купли-продажи товаров через торговые сервисы, «мессенджеры» или социальные сети отличается от хищений путем «фишинга» тем, что покупатели добровольно переводят денежные средства на карты или электронные кошельки продавцам, обнаруживая в последующем, что ни возврата денег, ни товар они не получат, т. е. хищение осуществляется не посредством получения конфиденциальных данных пользователя о реквизитах банковской карты и их последующего использования в корыстных целях, а путем обмана покупателя, который отличается от бытового мошенничества лишь виртуальным характером контакта.

Вымогательство, осуществляемое через интернет-ресурсы, по способу его совершения можно разделить на несколько видов: вымогательство посредством распространения вирусных программ и вымогательство в социальных сетях. Если говорить о первом способе, то стоит отметить,

что преступники распространяли вирусные программы через активные ссылки или «зараженные» документы, которые доходили до пользователей либо через электронную почту (чаще различным организациям, чем одиночным пользователям), либо через рекламные объявления, поддельные сайты, сообщения в социальных сетях и на форумах. Переход по ссылке или скачивание документа активировали установку вируса на устройство пользователя, который блокировал доступ к файлам, доступ к которым осуществляется с помощью определенных программных продуктов («Майкрософт Ворд, Эксель», Word, Excel и т. д.), выводя пользователю текстовое сообщением с требованием перевести денежную сумму на указанный электронный счет (криптовалютный кошелек). Если требование об оплате не выполнялось, то файлы уничтожались, что, к слову, происходило и в случае, если вымогатель все же получил желаемое. Такой способ хищения был распространен в 2018–2019 гг., сегодня встречается реже, в отличие от вымогательства через социальные сети, которое осуществляется следующим образом: преступник получает доступ к личной информации пользователя, которую он желает сохранить втайне (компрометирующие фотографии, переписки, видеозаписи, голосовые сообщения), посредством неправомерного доступа к учетной записи социальной сети, электронной почты или «облачного» хранилища. После чего вступает с пользователем в переписку, в рамках которой сообщает, какими сведениями обладает, и требует от собеседника денежное вознаграждение, угрожая их распространить. Пользователи, не желая раскрывать свои тайны, часто соглашаются на условия вымогателей и передают им свои сбережения.

Хищения путем использования компьютерной информации могут не только осуществляться в отношении одиночных пользователей, но и причинять существенный имущественный ущерб юридическим лицам (государственной и частной форм собственности), индивидуальным предпринимателям. Так, на постсоветском пространстве распространена преступная схема хищений с использованием электронных почтовых ящиков («BEC-атаки» – компрометация бизнес-переписки), где злоумышленники, путем взлома почтового ящика одного из партнеров сделки, изучив переписку и прикрепленные к ней документы, внедрялись в диалог на стороне одного из партнеров, изменяли банковские реквизиты в документах (если они отсканированы, то подделка осуществлялась посредством наложения новых данных на готовый документ), куда вторая сторона должна была перечислить средства для совершения сделки, и сроки выплаты. Ничего не подозревающий контрагент выполнял поставленные условия, однако исполнения договора от второй сто-

роны не получал, благодаря чему и вскрывался обман. Также имела место ситуация, когда «киберпреступники» вступали в переписку с одним из партнеров от лица обслуживающего банка и сообщали об изменении реквизитов и необходимостью перечисления средств по сделке на новый счет.

Хищение путем использования компьютерной информации возможно и в случаях свободного доступа к реквизитам банковской карты. Например, имеют место случаи, когда карта попадает в руки преступника во время совместного распития спиртных напитков, либо потерпевший сам оставил карту в зоне доступа злоумышленника, чем последний и воспользовался, либо забыл ее в банкомате или инфокиоске, либо единожды предоставлял свою карту знакомому для оплаты товаров или услуги, а последний сохранил ее реквизиты и воспользовался этой картой вновь в корыстных целях и т. д.

Не менее значимым для целей настоящей работы имеет и характеристика предмета преступления. Термин «криптовалюта», с одной стороны, вошел в повседневный обиход, а с другой – до настоящего времени остается загадкой для многих людей, ассоциирующих данный актив с безналичными денежными средствами, их электронными аналогами, схожими институтами. На территории России ключевым нормативно-правовым актом, регулирующим общественные отношения в названной сфере, является Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[1]. Законодатель представляет, на наш взгляд, довольно содержательную дефиницию такого явления, как «криптовалюта», именуя таковую в качестве «цифровой», а именно: «Цифровой валютой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электрон-

[1] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 30 декабря 2001 г. № 195-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_ LAW_358753 /

ных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам». Стоит акцентировать внимание на следующих составляющих термина:

1) информационная система;

2) средство платежа, не являющееся денежной единицей;

3) лицо, обязанное перед каждым обладателем электронных данных;

4) действия по внесению записей.

При многократном прочтении вышеуказанного, напрашивается однозначный вывод: цифровая («криптовалюта») есть не что иное, как созданный специальным оборудованием и программным обеспечением свод упорядоченных данных, внешне выраженных как самостоятельная информационная система, не являющихся денежной единицей, меновая стоимость которых складывается из интереса ограниченного круга лиц, приобретающих ее для собственных нужд. При этом цифровая валюта связана с обыкновенными денежными единицами, имеющими оборот в рамках конкретного государства либо международное хождение. Ведь в конечном итоге происходит ее обмен именно на общепризнанные финансовые продукты. Создание «кошельков» (де-факто учетных записей в рамках сайтов, позиционирующих себя как организации-эмитенты «криптовалюты»), прием и перевод средств есть не что иное, как модификация компьютерной информации на серверном оборудовании или, как гласит закон, действия по внесению записей.

На наш взгляд, ажиотаж вокруг цифровой валюты есть искусственно созданное явление, обеспечиваемое интересами владельцев конкретных интернет-ресурсов, на которых и размещены внешние формы проявления рассматриваемых информационных систем. Также спекулятивные действия осуществляют и отдельные граждане, пользующиеся интересом более доверчивых лиц, стремящихся вложить собственные деньги с целью получения прибыли от разницы курса и т. д. Привлекательность института цифровой валюты также неоднозначна и находится в авангарде интересов лиц, желающих скрыть движения денежных средств по обыкновенным банковским счетам, а также «спекулянтов», занимающихся куплей-перепродажей в зависимости от сугубо коммерческого интереса.

Схожей позиции придерживаются и должностные лица Центрального банка России, которые от заявления к заявлению указывают на суррогатный и «псевдо» характер «криптовалют», подчеркивая их зависимость от имеющих обращение денежных средств. Как заявил директор Юридического департамента Банка России А. А. Гузнов, «позиция Центрального банка остается неизменной. Мы считаем, что существуют

большие риски при легализации обращения «криптовалюты», как с точки зрения финансовой стабильности и системы противодействия отмывания доходов, так и с точки зрения защиты прав потребителей. Поэтому в ходе дискуссии по законопроекту мы возражали против того, чтобы этот, так сказать, «инструмент» был легализован как объект обращения»[1].

Выходит, что цифровая или «криптовалюта» есть не что иное, как совокупность компьютерной информации, размещенной в рамках интернет-ресурсов, обеспеченной лишь активностью пользователей. Реакцию органов публичной власти в различных государствах по всему миру, в том числе и в России, на общественный интерес к цифровой валюте, допустимо назвать сдержанной. Повсеместно принимаются нормативно-правовые акты, регулирующие общественные отношения, возникающие в связи с ее использованием. Однако ввод подобного ничем не обеспеченного средства платежа в свободный гражданский оборот, например для оплаты товаров или услуг, невозможен. На территории России, в соответствии с профильным федеральным законом, цифровая валюта имеет правовой статус имущества, в связи с чем уголовно-правовые отношения, возникающие в связи с ее хищениями либо использованием как средства совершения преступления, стоит рассматривать именно в такой плоскости. Рассматривая вопросы цифровой валюты, мы не подвергаем глубокому анализу созвучную, но совершенно иную по существу категорию «цифровых финансовых активов», являющихся цифровыми правами по эмиссионным ценным бумагам, долевому вложению в непубличное АО, денежными требованиями.

Для усвоения затронутых вопросов следует кратко раскрыть особенности категории «электронные денежные средства». Источником, закрепляющим данное понятие, является Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»[2]. Аутентичное понятие представлено в следующем виде: «электронные денежные средства – денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средст-

[1] Интервью Гузнова А. А. независимому информационному агентству «Интерфакс» от 16 марта 2020 г. [Электронный ресурс] // Официальный сайт Банка России. URL: https://cbr.ru/press/event/?id=6512

[2] О национальной платежной системе: Федеральный закон Российской Федерации от 27 июня 2011 г. № 161-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_115625/

ва, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа». Ключевыми характеристиками электронных денежных средств являются:

1) относимость к обыкновенным денежным средствам;

2) отсутствие открытого банковского счета;

3) передача распоряжений посредством специальной инфраструктуры – электронных средств платежа (терминалы и внутреннее программное обеспечение платежных систем, торговых площадок в сети «Интернет», иных организаций). Электронные денежные средства не имеют собственного условного курса, который задают эмитенты цифровой валюты, их расчет происходит один к одному с национальной валютой.

Возвращаясь к вопросам использования результатов оперативно-розыскной деятельности при расследовании хищений денежных средств, криптовалют с помощью сети «Интернет», сотовой связи, стоит отметить, что время и место – одни из важнейших составляющих события преступления. Их своевременное определение позволяет приблизить установление виновного в совершении лица (лиц). Поскольку процесс раскрытия и расследования преступлений является ретроспективным, то действия по обнаружению следов, их фиксации производится в момент приготовления, покушения или после совершения деяния. Данное обстоятельство необходимо учитывать и по рассматриваемым категориям преступлений. Как правило, указанные виды хищений выявляются посредством производства ОРД с последующим предоставлением их результатов с целью возбуждения уголовного дела либо использования в установленном законом порядке в процессе производства предварительного расследования. Уместно говорить о том, что противодействие хищениям денежных средств (преимущественно в форме мошенничества, краж с банковских счетов) сегодня имеет крайне низкую эффективность. Согласно статистическим сведениям МВД России, за январь – август 2021 г. зарегистрировано 358 773 преступления подобного рода. Их раскрываемость за отчетный период варьируется от 12,6 до 53,6 % в зависимости от конкретного региона[1]. При этом достоверность цифры верхнего потолка раскрываемости вызывает объективное сомнение. Причинами столь большого количества преступлений подобного рода выступают:

[1] См.: Краткая характеристика состояния преступности в Российской Федерации за январь – август 2021 г. [Электронный ресурс] // Официальный сайт МВД России. URL: https://мвд.рф/reports /item/26023627/

– использование виртуальных частных сетей (VPN), скрывающих точку подключения к сети «Интернет» злоумышленниками, не поддающимся подсчету количеством организаций, оказывающих услуги связи, провайдеров, многие из которых реализуют свою деятельность без лицензии;

– широкий круг банковских организаций, НКО, предоставляющих услуги финансового характера, а также существование интернет-ресурсов, оказывающих услуги по купле-продаже вышеупомянутой цифровой валюты. Нередко так называемые «криптообменники» юридически зарегистрированы на территории иностранных государств. Как следствие, затрачивается продолжительное время на получение от них необходимой информации;

– тесно связанная с предыдущей причина, заключающаяся в свободном распространении неограниченного количества средств платежа (банковских карт, в том числе виртуальных) из расчета на одно физическое или юридическое лицо, что позволяет в кратчайшие сроки «вывести» похищенные денежные средства;

– межрегиональный и межнациональный характер совершения хищений, отсутствие эффективных форм и методов взаимодействия между структурными подразделениями правоохранительных органов.

Перечисленное выше не является исчерпывающим. Очевидно, что проведение ОРМ является необходимым и обязательным условием сбора и фиксации информации, имеющей перспективно-доказательственное значение. Наиболее актуальными из 15 (пятнадцати) предусмотренных действующим законодательством ОРМ выступают те, что связаны с истребованием информации финансового (банковского) характера, а также о соединениях между абонентами и устройствами связи.

Подчеркнем, что подавляющее большинство бесконтактных хищений сопряжены со звонками на сотовые телефоны пострадавших. При этом участники преступных групп, ответственные за выполнение ключевой части объективной стороны хищений, непосредственное введение граждан в заблуждение путем предоставления ложной информации о работе службы безопасности банка, правоохранительных органов и т. д., используют бесконтрольно предоставляемые ресурсы IP, VoIP, SIP-телефонии российских и зарубежных организаций, позволяющие на уровне биллингового оборудования осуществлять подмену собственных абонентских номеров на любой из уже существующих. Как правило, подбираются абонентские номера, идентичные номерам кредитно-финансовых организаций, территориальных подразделений правоохранительных органов, имеющие номерную емкость «+7495», т. е. отожде-

ствляемые у обывателей с теми, что используются на территории г. Москвы и Московской области. Таким образом, целесообразно выделить 2 (два) направления ОРМ:

1) направленные на истребование информации о движении похищенных денежных средств из кредитно-финансовых организаций,

2) предназначенные для получения и фиксации информации о ресурсах связи, используемых для совершения хищений, как следствие о лицах, совершивших звонки.

Первое из обозначенных подразумевает собой единственное в своем роде ОРМ, именуемое «наведение справок». Реализуется оно на основании судебного решения, которому предшествует ходатайство руководителя органа, осуществляющего ОРД, об истребовании сведений о движении денежных средств по счету. Ныне существующая правоприменительная практика, направленная на превентивную и расширительно толкуемую защиту прав граждан, выработала аналогичный подход (т. е. необходимость вынесения судебного решения) не только для банков, но и любых юридических лиц, деятельность которых связана с приемом/перечислением финансов (платежные системы, некоммерческие организации).

Второе направление предусматривает, помимо получения информации посредством организации и проведения «наведение справок», иные ОРМ: «снятие информации с технических каналов связи», «получение компьютерной информации». Последнее в настоящее время только проходит свое становление, редко реализуется в практической деятельности, в связи с чем предложить научно обоснованные доводы не представляется возможным. Снятие информации с технических каналов связи представляет собой многосоставное мероприятие, включающее получение как детализированных отчетов о входящих/исходящих вызовах, так и иной сопутствующей информации. Именно в рамках данного мероприятия подтверждаются либо опровергаются факты, указывающие на хищения денежных средств в той или иной безналичной форме. Обе организационно-правовые формы подразумевают направление запросов, адресованных операторам связи, интернет-провайдерам, фирмам, предоставляющим услуги IP, VoIP, SIP-телефонии, с целью установления лиц, которым присваивался тот или иной абонентский номер.

По получении совокупности сведений, необходимых для установления признаков состава преступления и (или) лиц, причастных к его совершению, сотрудники оперативных подразделений органов дознания приступают к формированию и передаче в органы предварительного расследования результатов ОРД. Специфика использования результатов

ОРД при расследовании хищений денежных средств, криптовалют с помощью сети «Интернет», сотовой связи заключается в том, что их наличие и обуславливает инициирование факта регистрации сообщения о преступлении, начала процессуальной проверки и, как следствие, возбуждения уголовного дела.

Признаки рассматриваемых нами хищений, в отличие от иных составов преступлений, не подвергаются исчерпывающему установлению в рамках зарегистрированного материала. Максимально установленного уголовно-процессуальным законом срока проверки сообщения о преступлении в 30 суток объективно недостаточно по вышеуказанным причинам. Кроме того, информационный обмен между правоохранительными органами и различными «контрагентами» в лице кредитно-финансовых организаций, операторов связи и т. д. на сегодняшний день остается «растянутым» во времени. Электронный документооборот организован не с каждым из хозяйствующих субъектов. Все это «укрепляет» правовые позиции результатов ОРД, которые содержат заблаговременно собранные и систематизированные сведения. Их наличие позволяет принять итоговое процессуальное решение в максимально короткий срок (вплоть до 3 (трех) суток). При этом результаты ОРД могут содержать оформленную в рамках ОРМ «Опрос» информацию от перспективного участника проверки по сообщению о преступлении, уголовному делу (заявителя, пострадавшего, потерпевшего, свидетеля). Научный интерес рассматриваемого вопроса заключается еще и в том, что де-факто результаты ОРД могут выступать совокупностью юридических материалов, заменяющих проверочные действия по сообщению о преступлении и выступающих основанием для возбуждения уголовного дела. Полнота и достоверность истребованных и собранных таким образом материалов не подвергается сомнению ни со стороны практических сотрудников следственных органов, прокуроров, судей, ни со стороны ученых. Специфика использования предоставленных результатов ОРД напрямую связана с предметом рассматриваемых нами хищений как относящаяся к хищениям денежных средств:

– в безналичной форме;

– электронных;

– цифровой валюты.

Особенности использования предоставленных результатов ОРД заключаются в источниках сбора первоначальной информации и последующего формирования материалов (путем проведения следственных действий) с целью перепроверки сведений, изложенных в результатах ОРД. При хищениях, направленных на обращение в собственную пользу

безналичных денежных средств, таковыми выступают банки (ПАО «Сбербанк», АО «Тинькофф банк», ПАО «ВТБ» и т. д.). В случае хищений электронных денежных средств, сотрудники оперативных подразделений органов дознания обращаются к организациям, специализирующимся на работе с данными активами, таким как ООО НКО «Яндекс Деньги», АО «Киви банк», операторам связи, предоставляющим балансовые счета абонентских номеров для использования в качестве «хранилища» электронных денежных средств[1].

Не стоит забывать о прогрессирующей сфере интернет-торговли. Крупные онлайн-площадки предлагают владельцам учетных записей на собственных сайтах не только подключить банковскую карту для мгновенных расчетов, но и открыть пользовательский счет, на который также возможно зачисление финансов. Следственно-судебная практика идет по пути признания таковых активов в качестве электронных денежных средств.

Так, 15 февраля 2021 г. Чкаловским районный судом г. Екатеринбурга в отношении гражданки Е. вынесен обвинительный приговор по делу № 1-23/2021 (1-658/2020). Уголовно преследуемое лицо, неправомерно используя доступ к учетной записи администрирования интернет-магазина «ozon.ru», под предлогом возврата товаров (в действительности не происходившего) осуществляла начисление электронных денежных средств на созданные и подконтрольные ей же пользовательские личные кабинеты. По результатам ОРД, проводимой сотрудниками ГУ МВД России по Свердловской области, возбуждено и рассмотрено в суде уголовное дело по признакам преступлений, предусмотренных п. «г» ч. 3 ст. 158, ч. 2 ст. 272 УК РФ[2]. Ключевым мероприятием, заложенным в основу подготовленных сотрудниками органа дознания результатов ОРД, являлось наведение справок в ООО «Интернет Решения»

[1] В настоящее время подобная практика распространена у широкого круга операторов связи, среди наиболее известных ПАО «Мегафон», ООО «Т2 Мобайл». При подключении дополнительных опций баланс абонентского номера соответствует электронному «кошельку» (т. е. прием/перевод средств возможен без открытия банковского счета). В 2021 году сотрудниками ГУ МВД России по Свердловской области установлены не менее 20 фактов совершения дистанционных мошеннических действий, при которых вывод похищенного происходил посредством зачисления денежных средств с банковских карт на балансовые счета абонентских номеров.

[2] Дело № 1-23/2021 (1-658/2020) [Электронный ресурс] // Официальный сайт Чкаловского районного суда г. Екатеринбурга Свердловской области. URL: https://chkalovsky--svd.sudrf.ru/modules.php? name=sud_delo& name_op=r&vnkod=66RS0007&srv_num=1&delo_id=1540006&delo_table= u1_case&case_type=0&u1_case__JUDICIAL_UIDSS=66RS0007-01-2020-005961-47

(«ozon.ru»). В дальнейшем должностные лица следственных органов для принятия решения о возбуждении уголовного дела, выдвижения версий, проведения следственных действий обращались именно к информации, истребованной в ходе этого ОРМ.

Ключевой особенностью использования предоставленных результатов ОРД по фактам хищений криптовалют является не только взаимодействие с организацией, ее выпускающей, но и достоверное установление заданного ей же курса условных обменных единиц к национальной валюте на момент совершения преступления. К тому же хищения цифровых активов сопряжены с доступом к учетным записям ресурсов, в рамках которых они используются. Выявление факта получения законного либо неправомерного доступа к ним служит цели установления объективной стороны совершенного деяния, так как без входа в раздел использования сайта (приложения) не представляется возможным осуществить перечисление предмета преступления на подконтрольные счета.

Подводя итог, отметим, что специфика использования результатов ОРД при расследовании хищений денежных средств, криптовалют с помощью сети «Интернет», сотовой связи состоит в многообразии способов их совершения («вишинг», «фишинг», мошенничества в сфере купли-продажи и т. д.), а также в верном установлении предмета преступления. Это становится возможным при обращении к источникам, регулирующим соответствующие общественные отношения: профильным федеральным законам, регламентирующим использование и оборот безналичных, электронных денежных средств, цифровой валюты, а также работу банков и банковских организаций, а именно:

– Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»;

– Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»;

– Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»[1].

Иные особенности использования в уголовном судопроизводстве результатов ОРД состоят в организации взаимодействия с источниками сбора информации о противоправных деяниях, а также в правовых формах фиксации, имеющих значение для расследования преступления, т. е.

[1] О банках и банковской деятельности: Федеральный закон от 2 декабря 1990 г. № 395-1 [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5842/

конкретных ОРМ (наведение справок, снятие информации с технических каналов связи, получение компьютерной информации).

Вопросы для самоконтроля

1. Перечислите международные нормативные правовые акты, регламентирующие противодействие преступлениям в сфере информационно-телекоммуникационных технологий.
2. Существует ли в настоящее время на международном уровне определение, характеризующее «киберпреступность»?
3. По какой причине в настоящее время результаты оперативно-розыскной деятельности, переданные в установленном порядке следователю (дознавателю), в суд, не являются самостоятельным видом доказательств?
4. Раскройте значение понятий «безналичные денежные средства», «электронные денежные средства», «цифровая валюта».
5. Раскройте актуальные виды хищений с использованием информационно-телекоммуникационных технологий.

Глава 2. Проблемы и перспективы использования результатов оперативно-розыскной деятельности при расследовании хищений денежных средств, криптовалют с использованием сети «Интернет», сотовой связи

§ 1. Проблемы имплементации и использования результатов оперативно-розыскной деятельности при расследовании хищений денежных средств, криптовалют с использованием сети «Интернет»

Любой вид человеческой деятельности не обходится без проблемных аспектов. Использование результатов ОРД в производстве по уголовным делам, в том числе при расследовании хищений денежных средств, криптовалют, не является исключением. Изучение точек зрения ученых по данной проблеме позволяет сделать вывод, что к числу проблемных отнесены чересчур абстрактные и не связанные с текущей деятельностью органов дознания, предварительного следствия, вопросы. Ряд исследователей требует доскональной регламентации процедуры введения в уголовно-процессуальную сферу документов оперативно-розыскного характера. Другие твердят о необходимости дополнения уголовно-процессуальных законов так называемыми «негласными» следственными действиями, т. е., по сути, наделения следователей (дознавателей) полномочиями производить ОРМ. Скажем, С. Б. Россинский утверждает: «УПК РФ не имеет какого-либо механизма, позволяющего сделать результаты ОРД равными результатам следственных действий. Законодатель не запрещает правоприменителю получать определенные материалы, которые отражают ход и результаты ОРМ, но они не уполномочены вводить такие материалы в уголовное разбирательство посредством проведения следственных или других процессуальных действий; Уголовно-процессуальный кодекс не предусматривает такие действия»[1]. Я. М. Мазунин в своей статье, посвященной необходимости наделения следователя правом на проведение «негласных» следственных действий, пришел к следующему выводу: «…полагаем целесообразным предусмотреть данную форму расследования и российским законодательством. Одним из условий данного предложения является расширение полномочий следователя, которому необходимо предоставить право проведения как гласных, так и негласных следственных (розыскных) дейст-

[1] *Россинский С. Б.* Результаты оперативно-розыскной деятельности нужно признать доказательствами по уголовному делу [Электронный ресурс] // Судебная власть и уголовный процесс. 2018. № 2. URL: https://cyberleninka.ru/article/n/rezultatyoperativno-rozysknoy-deyatelnosti-nuzhnopriznat-doka-zatelstvami-po-ugolovnomu-delu

вий, что уже частично нашло отражение в уголовно-процессуальном законодательстве. Анализ действующего российского законодательства свидетельствует о том, что современное российское досудебное производство воспринимается как гласная деятельность следователя и негласная деятельность органов, осуществляющих ОРД. Однако так ли это на самом деле?»[1].

Не умаляя значимость плюрализма мнений в области юридических наук, считаем, что приведенные в качестве примеров, а также иные существующие в настоящее время подходы есть субъективное мнение конкретного автора. Их практическая полезность, а также объективная ценность, требуют изучения. Источники уголовного судопроизводства не ограничиваются самим кодексом, поскольку излишняя перегрузка УПК сугубо технико-процедурными положениями, требующими непрерывного совершенствования в рамках ведомственных приказов, усложнит его адаптацию к требованиям времени, равно как и выдвигаемые предложения об объединении. Что касается смешения гласной уголовно-процессуальной деятельности с оперативно-розыскной, имеющей иную правовую сущность, предназначение, круг участников, то это вызывает недоумение.

В то же время представляется справедливым мнение специалистов из Казахстана, пришедших к выводу, что отрасль телекоммуникаций достаточно специфична, поскольку ее регулирование осуществляется на стыке сложных технических моментов, устаревшей конструкции правовых норм и стремительного развития рынка. При этом темпы развития технологий значительно опережают темпы изменения и гармонизации законодательства, которое можно охарактеризовать как непоследовательное и противоречивое. Основные нормативные правовые акты приняты и вступили в силу в разное время и построены на основе различных юридических концепций. В целом, текущее отраслевое регулирование не отвечает современному развитию рынка услуг телекоммуникаций[2].

Совершенствование текущего правоприменения, обогащение науки уголовного судопроизводства объективно необходимыми, обусловленными целями ее существования позициями – это то, что от нас требует время и общество. Как ни странно, основу проблемных вопросов, свя-

---

[1] *Мазунин Я. М.* Негласная деятельность следователя: пора признать данность [Электронный ресурс] // Юридическая наука и правоохранительная практика. 2015. № 1 (31). URL: https://cyberleninka.ru/article/n/ neglasnaya-deyatelnost-sledovatelya-pora-priznat-dannost/viewer

[2] Концепция проекта Закона Республики Казахстан «Об электронных коммуникациях» (подготовлена ОЮЛ «Национальная телекоммуникационная ассоциация Казахстана» в 2016 году) [Электронный ресурс]. URL: http://www.ntark.kz/?uin=1418145042

занных с имплементацией и использованием результатов ОРД, составляют сроки. Разумный срок уголовного судопроизводства является одним из базовых принципов, что влечет за собой существование десятков статей, ограничивающих участников уголовного процесса в принятии решений, осуществлении действий. Ни УПК (РФ, Республик Беларусь, Казахстан) ни Инструкция о порядке предоставления результатов ОРД (в России) не содержат положений, регламентирующих сроки предания оперативно-розыскной информации статуса процессуальной. Речь не идет о направлении в орган расследовании рапорта об обнаружении признаков преступления или сообщения о преступлении, т. е. сообщения о преступлении. Как известно, одной из основных целей передачи результатов ОРД следователю, дознавателю, в суд является их использование в доказывании. Производство осмотра предоставленных материалов, направление сформированных на их основании следственных запросов не всегда производится в разумный срок, что влечет нарушение законных прав пострадавших от преступлений, а также иные последствия. Для Республики Беларусь указанная проблема актуальна в связи с отсутствием установленных законодательством сроков предоставления органом, осуществляющим ОРД, оперативной информации / материалов ОРД иным органам в следующих случаях:

1) ответ на запрос органа уголовного преследования о предоставлении органом, осуществляющим ОРД, информации, предметов и документов, имеющих значение для уголовного дела (ч. 2 ст. 103 УПК), в том числе, представлении материалов ОРД для ознакомления в порядке ст. 50 Закона «Об оперативно-розыскной деятельности»;

2) информирование органа, ведущего уголовный процесс, о полученной в рамках оперативного сопровождения уголовного дела органами, осуществляющими ОРД, информации, имеющей значение для расследования уголовного дела и изобличения виновных лиц (ч. 4 ст. 186 УПК);

3) передача органом, осуществляющим ОРД, но не являющимся органом дознания, материалов надзирающему прокурору для перенаправления их органу уголовного преследования с целью регистрации последним заявления, сообщения о преступлении и принятии решения о возбуждении уголовного дела.

Отсутствие четко установленных сроков в вышеперечисленных случаях порождает ряд вопросов, связанных с процессуальным промедлением, влияющим на ход и результаты предварительного расследования. Производя оперативное сопровождение уголовного дела, органы, осуществляющие ОРД (дознание), обязаны уведомлять следователя о полу-

ченных результатах. Однако ни срок такого уведомления, ни его порядок в уголовно-процессуальном законодательстве не прописаны.

Возвращаясь к проблемным аспектам, имеющим равное значение для большинства стран содружества, отметим, что остается открытым вопрос, тесно связанный со сроками, но имеющий значение для соблюдения процессуальной формы в части передачи отдельных результатов ОРД, дополняющих ранее направленные. Так, сведения от отдельных организаций, например, платежных систем, могут быть запрошены в рамках проведения оперативной проверки, по окончании которой формируются и направляются результаты ОРД. В ряде территориальных подразделений органов дознания складывается практика передачи впоследствии поступивших документов не через формирование нового комплекта документов с вынесением постановления о предоставлении результатов ОРД с его подписанием у руководителя соответствующего уровня, а посредством составления сопроводительного письма, визируемого начальником отдела. По нашему мнению, данная практика является спорной, и с целью соблюдения принципа законности необходимо придерживаться порядка повторного вынесения постановлений о предоставлении результатов ОРД, особенно в случае передачи документов, имеющих существенное значение.

В качестве еще одного проблемного аспекта приобщения оперативно полученных данных к материалам уголовного дела, присущего исключительно нашей стране, необходимо обозначить неоднозначную позицию Верховного Суда России, выраженную в постановлениях № 29, 48, 22 от 27 декабря 2002 г.[1], 30 ноября 2017 г.[2], 29 июня 2021 г.[3] Второе, содержащее общие рекомендательные нормы, касающиеся рассмотрения уголовных дел, связанных с мошенничеством, вводило в заблуждение сотрудников правоохранительных органов и работников судебной системы формулировкой, разъясняющей момент окончания хищений денежных средств с банковских счетов. Дело в том, что неоднозначному толкованию подвергались следующие строки: «Если предметом престу-

[1] О судебной практике по делам о краже, грабеже и разбое [Электронный ресурс]: Постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_40412/

[2] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_283918/

[3] О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам [Электронный ресурс]: Постановление Пленума Верховного Суда РФ от 29 июня 2021 г. № 22 // СПС «КонсультантПлюс». URL: http://www. consultant.ru/document/cons_ doc_LAW_5842/

пления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу положений пункта 1 примечаний к статье 158 УК РФ и статьи 128 Гражданского кодекса Российской Федерации 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 практической деятельности данное положение превратно отождествляли с местом окончания преступления, а не выполнения его объективной стороны и, соответственно, предварительного расследования. С выходом в 2021 году уточняющего постановления изложенная позиция стала абсолютно законной в связи с тем, что п. 25.2 предусматривает следующее: «Местом окончания такой кражи является место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета». Данная логическая цепь, по сути, описывает ч. 2 ст. 152 УПК РФ, согласно которой если преступление было начато в одном месте, а окончено в другом, то уголовное дело расследуется по месту окончания преступления. Несмотря на то, что постановления Пленума Верховного Суда изначально являются актами толкования права и имеют рекомендательный характер, а ст. 152 УПК РФ содержит положения, допускающие производство предварительного расследования по месту нахождения потерпевшего, обвиняемого и т. д., руководство следственных органов, избегая излишней производственной нагрузки, направляет переданные в их адрес материалы по месту открытия счета потерпевшего лица. Сложившееся положение дел опасно и лишь усложнило борьбу с хищениями денежных средств, криптовалют с использованием сети «Интернет», сотовой связи.

Сегодня многие банки и банковские организации осуществляют открытие счетов дистанционно, имея лишь один офис по месту регистрации юридического лица. Например, АО «Тинькофф Банк» является онлайн-банком, не имеет представительств и расположен по адресу: г. Москва, ул. Хуторская, 2-я, д. 38а, стр. 26. Из-за этого возникают парадоксальные ситуации. Допустим, сотрудниками оперативного подразделения органа дознания установлен факт, что в отношении жителя г. Воронежа совершено хищение денежных средств со счета, открытого в вышеуказанном банке, лицом, фактически находящимся в г. Чебоксары. По направлению результатов ОРД в следственный отдел, находящийся в г. Воронеже, руководитель последнего, ссылаясь на п. 25.2 По-

становления Пленума, указывает на то, что территориальная подследственность установлена неверно и производство расследования необходимо осуществлять в г. Москве.

Схожая ситуация сегодня наблюдается и в Свердловской области. Более того, в данном регионе имел место случай направления судьей Ленинского районного суда г. Екатеринбурга уголовного дела для рассмотрения по существу в суд, на территории которого находится офис АО «Тинькофф банк» по причине совершения деяний, предусмотренных п. «г» ч. 3 ст. 158 УК РФ, жителем г. Екатеринбурга в отношении граждан, проживающих в различных субъектах России, но имеющих счета в упомянутом банке. В текущих условиях взаимодействие между оперативными подразделениями органов дознания, занимающихся борьбой с хищениями и представляющих результаты ОРД в следственные органы, находится в состоянии кризиса и неопределенности. Имеют место необоснованные перенаправления материалов из органа в орган, затягиваются сроки принятия процессуальных решений.

Наряду с вышеперечисленным, проблемным аспектом предоставления и использования результатов ОРД в уголовном процессе при расследовании хищений денежных средств, криптовалют является неоднозначная позиция потерпевших по данной категории дел. Недоверие значительного количества граждан к сотрудникам правоохранительных органов – факт, который невозможно отрицать. По официальным данным МВД России в 2020 году в результате выборочного опроса населения в 85 субъектах получены сведения об общей удовлетворенности деятельностью полиции 51,6 % населения[1].

Исходя из статистики, можно сделать вывод, что реальная картина взаимоотношений органов правопорядка и населения оставляет желать лучшего. Усугубляет данную проблему и тот факт, что в настоящее время лица, совершающие мошеннические действия, кражи в отношении держателей банковских карт, действуют от имени сотрудников полиции, иных правоохранительных органов, для звонков гражданам используют номера IP, VoIP, SIP-телефонии, идентичные действительно существующим и выделенным территориальным органам МВД России. Такое положение дел вводит в недоумение граждан, осложняет коммуникацию с ними в случае объективной необходимости связаться по вопросам, касающимся исполнения служебных обязанностей. Как извест-

[1] См.: Оценка деятельности полиции Российской Федерации в 2020 году. По данным ФГКУ «ВНИИ МВД России» [Электронный ресурс] // Официальный сайт МВД России. URL: https://мвд.рф/publicopinion

но, деяния уголовно преследуемых лиц, совершающих хищения денежных средств, в том числе электронных, а также криптовалют, подпадают под признаки составов преступлений, предусмотренных ст. 158, 159 УК РФ, которые относятся к категории публичного обвинения. Оперативный уполномоченный, выявивший факт совершения рассматриваемых преступлений, обязан принять меры к установлению лиц, их совершивших, документированию имеющейся информации, формированию и предоставлению результатов ОРД для решения вопроса о возбуждении уголовного дела. Трудности возникают с установлением места жительства, коммуникацией, а также проведением оперативно-розыскных и процессуальных действий с пострадавшими от преступлений. Учащаются случаи, при которых последние вовсе категорически отказываются от явки в отделы полиции в связи с несущественностью причиненного им вреда, лояльного отношения к преступному миру и т. д.

Действующий закон «Об оперативно-розыскной деятельности», УПК РФ (в части регламентации стадии проверки по сообщению о преступлении, применения мер процессуального принуждения), КоАП РФ[1] не предусматривают механизмов воздействия и ответственности за неявку гражданина к должностному лицу, осуществляющему оперативную или процессуальную проверку по сообщению о преступлении. В то же время, установление обстоятельств совершенного деяния, размеров причиненного имущественного вреда, реквизитов, с которых произошло хищение, объективно невозможно без участия пострадавшего лица. Неоднократно предоставляемые в органы предварительного расследования материалы, отражающие результаты ОРД, даже содержащие сведения о причастном к совершению хищений лице, но не включающие оперативных материалов (протоколов проведения ОРМ «опрос», объяснения лица, полученного в рамках ст. 144 УПК РФ, по факту совершения в отношении него хищений), оставались без принятия итогового процессуального решения. Практикой фактически выработан иной вид уголовного преследования, схожий с уже существующим в науке публично-частным, т. е. возбуждение уголовного дела по фактам хищений денежных средств, криптовалют только при наличии заявления или объяснения пострадавшего.

Предыдущий проблемный аспект актуален не только в случаях, когда хищение совершено в отношении физического лица. Схожая ситуа-

[1] Кодекс Российской Федерации об административных правонарушениях: Федеральный закон Российской Федерации от 30 декабря 2001 г. № 195-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34661/

ция имеет место и с организациями. Отдельные торговые площадки на сегодняшний день, зарегистрированы за рубежом и не имеют юридических представительств в России. Кроме того, даже при их наличии (как правило, офисы крупных организаций расположены в г. Москва) имеют место случаи фактического отказа от предоставления информации, имеющей значение для раскрытия и расследования преступления, со стороны некомпетентных работников. С одной стороны, мы имеем дело с нарушением устоявшихся общественных отношений, с другой – с нежеланием представителей юридического лица участвовать в сугубо формальных процедурных мероприятиях. Разумеется, о применении каких-либо мер административной и иной ответственности в указанной плоскости говорить не приходится, текущее правоприменение оставляет открытым вопрос относительно верных действий сотрудников органов дознания в подобных ситуациях.

Как мы полагаем, с целью избежать негативных дисциплинарных и вытекающих из них последствий необходимо нарабатывать практику не укрытия осведомленности о фактах преступной деятельности, а предоставления имеющихся результатов ОРД в орган предварительного расследования для принятия процессуального решения. В случае наличия достаточного количества материалов, указывающих на признаки преступления, отказ в возбуждении уголовного дела либо направление материалов по подследственности станет действием, ответственность за которое возлагается на следователя (дознавателя). Если же уголовное дело будет возбуждено, то в случае уклонения от явки, неисполнения иных обязанностей возможно применение мер процессуального принуждения, привлечение к административной ответственности.

Препятствием в сборе и формировании результатов ОРД по преступлениям, связанным с хищениями денежных средств, криптовалют, выступает отсутствие налаженного международного взаимодействия по вопросам истребования необходимых сведений до возбуждения уголовного дела. В МВД России ключевым источником взаимодействия оперативных подразделений с НЦБ Интерпола выступает Приказ[1]. Несмотря на содержащиеся в нем расплывчатые формулировки, приходится им руководствоваться, ибо в настоящее время отсутствует реальная возможность других способов истребования сведений от зарубежных банков, платежных систем, игровых платформ, эмитентов цифровой валю-

[1] Об утверждении Инструкции об организации информационного обеспечения сотрудничества по линии Интерпола: приказ МВД России № 786, Минюста № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКН РФ № 333, ФТС РФ № 971 от 6 октября 2006 г. // Бюллетень нормативных актов федеральных органов исполнительной власти. 2006. № 47.

ты до возбуждения уголовного дела. Скажем, ближайшее представительство наиболее популярной платформы в среде любителей компьютерных игр «Стим» (Steam) находится на территории Эстонской Республики. В результате должностные лица следственных органов, требующие для решения вопроса о возбуждении уголовного дела сведений, собранных в исчерпывающем объеме, предпочитают не обременять себя расследованием. К тому же, отсутствует устоявшаяся практика и методики расследования преступлений подобного рода. Даже хищения денежных средств держателей счетов зарубежных банков, равно как и цифровой валюты, на территории России не имеют позитивных примеров расследования и направления уголовного дела для рассмотрения по существу в судебные инстанции. Вместе с тем раздел 8 УПК РФ предусматривает достаточно детально упорядоченный порядок взаимодействия следственных органов, прокуроров, судей с компетентными должностными лицам иностранных государств. Полагаем необходимым введение схожих норм в Федеральный закон «Об оперативно-розыскной деятельности», дополнение ведомственных приказов действительно работающими процессуальными нормами, позволяющими в необходимом объеме получать интересующие оперативные подразделения сведения в ходе взаимодействия с зарубежными коллегами.

Словом, в настоящее время продолжает оставаться открытым ряд теоретико-правовых и практических вопросов, связанных с введением и использованием результатов ОРД при расследовании хищений денежных средств, криптовалют с использованием сети «Интернет». К ключевым из них относятся:

– неосведомленность научного сообщества об актуальных вопросах, решение которых не представляется возможным без комплексного осмысления и выработки методологически обоснованных подходов. Причина тому – разнородность целей, задач, отсутствие взаимодействия между исследователями, педагогическими кадрами и сотрудниками территориальных подразделений правоохранительных органов;

– отсутствие нормативно урегулированных сроков, в рамках которых сотрудники органов предварительного расследования обязаны принять к сведению и организовать производство необходимых процессуальных действий по предоставленным в их адрес результатам ОРД;

– неурегулированные положения относительно предоставления в органы предварительного расследования дополнительно поступивших сведений по ранее направленным результатам ОРД;

– отсутствие мер административного и процессуального воздействия на лиц, в отношении которых совершено преступление публичного ха-

рактера, уклоняющихся от явки к сотрудникам органов дознания для проведения оперативно-розыскных, следственных мероприятий. Как следствие, невозможность формирования и направления комплексных результатов ОРД оперативными уполномоченными, а также принятия однозначных процессуальных решений следователями (дознавателями). Данный вопрос актуален как для физических лиц, так и представителей юридических лиц;

– спорная позиция Верховного Суда РФ, выраженная в постановлениях Пленумов: «О судебной практике по делам о краже, грабеже и разбое», «О судебной практике по делам о мошенничестве, присвоении и растрате», «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам». Положения, определяющие местом производства расследования территорию, на которой располагается подразделение банка, иной организации, где открыт счет, вызвало кризисную ситуацию во взаимодействии подразделений органов дознания и следственных органов, специализирующихся на борьбе с хищениями денежных средств, криптовалют. Вопреки здравому смыслу, нередко результаты ОРМ, предоставленные следователю (дознавателю) для решения вопроса о возбуждения уголовного дела, направляются в следственные органы, судебные инстанции, на территории обслуживания которых находятся счета потерпевших. При этом последние, как и уголовно изобличаемое лицо, зачастую не проживают и никак не связаны с местом нахождения кредитно-финансовых и иных организаций;

– реально не выполняемые в действительности положения нормативно-правовых актов, регламентирующих порядок международного взаимодействия оперативных подразделений органов дознания с компетентными органами иностранных государств. Результатом имеющего место положения дел является отсутствие возможности направления собранных в полном объеме результатов ОРД по преступлениям, в рамках которых тем или иным участником является физическое, юридическое лицо, находящееся на территории иностранного государства.

§ 2. Перспективы использования результатов оперативно-розыскной деятельности при расследовании хищений денежных средств, криптовалют с помощью сети «Интернет»

Одной из самых существенных и социально полезных функций науки является прогностическая. Ее значимость велика и для уголовного судопроизводства. Интересной в данном ключе является позиция, представленная Д. А. Керимовым, который прогностическую функцию име-

новал не иначе, как «функцией опережающего отражения, «забегания вперед». По его мнению, она достигается через опережающее видение регулируемых общественных отношений, в котором опыт прошлого и настоящего проецируется на будущее и открывает возможность предвидения и оценок предлагаемого в концепции будущего правового воздействия[1].

Рассматриваемая нами тема сама по себе представляет научный интерес, поскольку не в достаточной степени подвергнута анализу современных исследователей, слепо следующим доктринам, предложенным «классиками» науки уголовного процесса 20 (двадцатого) столетия[2]. В то же время практическое значение оценки перспектив использования результатов ОРД при расследовании хищений денежных средств, криптовалют с использованием сети «Интернет» трудно переоценить с учетом существующей динамики роста преступлений данной категории. Необходимость оценки перспектив использования результатов ОРД в уголовном процессе – это не возможность или право исследователей и методологов-правоприменителей, а, скорее, их обязанность, с учетом перспективности этого направления для достижения целей уголовного судопроизводства. Как отмечал И. Н. Глебов, «часто без внимания теоретиков и практиков остаются новые перспективные направления правосознания и правоприменения. Так уже получилось с «Интернет правом», электронной демократией, электронным правосудием, биотехнологиями и другими направлениями, в которых мы отстали, вместо того, чтобы сработать на опережение»[3]. И. Н. Глебов призывает к тому, чтобы аналогичное не произошло с искусственным интеллектом, а также в других сферах государственности, в экономике, в инфо-коммуникации и массовой информации. На наш взгляд, определить вероятные пути развития того или иного института возможно на период не более 5–7 грядущих лет. В дальнейшем не исключена деформация общественных отношений, правовой основы, обуславливающих их существование, а

[1] *Керимов Д. А.* Методология права (предмет, функции, проблемы философии права). М.: Аванта+, 2001;

[2] Ссылки на работы И. М. Лузина, Р. С. Белкина, М. С. Строговича и ряда иных авторов, традиционно в изобилии представлены в научных изысканиях, имеющих предметом исследования вопросы использования результатов ОРД в уголовном процессе. Однако подавляющее большинство современных исследователей не принимает во внимание, что авторские позиции указанных ученых складывались в период существования общественных отношений, сформированных социалистическим строем, плановой экономикой и, само собой, действия УПК РСФСР 1922, 1923, 1960 гг.

[3] *Глебов И. Н.* Правовая футурология: постановка проблемы искусственного юридического разума // Российское государствоведение. 2018. № 1. С. 12–29.

также внедрение технических решений, упрощающих воплощение в жизнь действий, операций.

Перспективы использования результатов ОРД при расследовании хищений денежных средств, криптовалют необходимо разделить на следующие виды,

– связанные с процессуальным порядком предоставления и использования в ходе проверки по сообщению о преступлении, расследования уголовного дела,

– относящиеся к организации и характеру проведения самих ОРМ, а также получаемой в рамках них информации.

Как ни странно, но второе выделенное нами направление имеет не меньшее отношение к уголовному судопроизводству, чем первое. Дело в том, что в последние годы намечается слабая, но, тем не менее, позитивная тенденция на адаптирование процесса расследования к решению общественно значимых задач. Шаблонное использование и отношение к процессуальным и следственным действиям имеет место со стороны отдельных некомпетентных сотрудников органов предварительного расследования, надзора, судебной системы. В то же время подавляющее большинство сотрудников применяют имеющийся «инструментарий» процессуальных и следственных действий, который закладывался законодателем задолго до появления обширного количества актуальных видов преступлений. К примеру, организация взаимодействия с многократно упомянутыми нами организациями, предоставляющими услуги IP, VoIP, SIP-телефонии, сегодня проводится как оперативными сотрудниками посредством организации проведения ОРМ «наведение справок», так и сотрудниками следственных органов путем проведения следственного действия «получение информации между абонентами и (или) абонентскими устройствами». В ходе описанных нами ОРМ, следственных действий осуществляется истребованием технической информации с коммутационного устройства операторов сотовой связи, к которым через интернет-трафик поступило соединение. В связи с этим ОРМ, которые при правильной организации работы территориальных подразделений органов дознания должны опережать проведение следственных действий, наиболее пластичны к условиям и требованиям, выдвигаемым действительностью. Результаты их проведения оказывают прямое влияние на производство по уголовному делу, перспективу его направления в суд.

Первый предложенный к рассмотрению вид, а именно перспективы, связанные с процессуальным порядком предоставления и использования в ходе проверки по сообщению о преступлении, расследования уголов-

ного дела, связан с исключительно формальными процедурами, выраженными в вынесении оперативно-розыскных и процессуальных актов. Как известно, в настоящее время «звенья» юридических документов и решений, ведущих от события преступления к решению суда по существу, расположены в следующей последовательности:

1) первоначальные документы оперативного толка, имеющие негласный характер и указывающие на факты либо лиц, совершивших, совершающих преступления;

2) оперативно-служебные документы, выносимые с целью организации и проведения ОРМ;

3) сбор, обобщение, оценка, анализ проведенных мероприятий;

4) вынесение полномочным руководителем постановления о рассекречивании сведений, составляющих государственную тайну (при необходимости);

5) вынесение полномочным руководителем постановления о предоставлении результатов ОРД следователю, дознавателю, в суд;

6) составление рапорта об обнаружении признаков преступления либо сообщения о преступлении, визируемого тем же руководителем органа, уполномоченного на осуществление ОРД;

7) регистрация рапорта об обнаружении признаков преступления либо сообщения о преступлении в книге учета сообщений о преступлениях, правонарушениях, происшествиях (КУСП, КРСП);

8) фактическая передача материалов, содержащих оперативно-служебные документы, отражающие ход и результаты ОРД, с их одновременной регистрацией в учетной документации принимающего органа предварительного расследования;

9) оценка поступивших результатов ОРД со стороны должностных лиц органов предварительного расследования, принятие процессуального решения;

10) предоставление результатов ОРД, минуя предыдущие пункты или вдобавок к ним, с целью использования для подготовки и проведения следственных действий, для использования в доказывании по уголовным делам;

11) производство процессуальных действий, в том числе следственных, таких как допросы необходимых участников, обыски, осмотры предоставленных детализированных отчетов по абонентским и иным номерам, фонограмм, полученных в ходе отдельных ОРМ;

12) вынесение постановления о признании вещественным доказательством материальных носителей, на которых содержатся зафиксированные результаты проведенных ОРМ.

Не поддается сомнению тот факт, что следователем (дознавателем) производятся и иные необходимые действия с поступившими в их адрес результатами ОРД. Среди прочего, на их основании формируются границы обвинения, складывается вывод о наличии в действиях изобличаемого лица признаков состава преступления, подготавливается постановление о привлечении в качестве обвиняемого, обвинительное заключение и т. д. Очевидные среднесрочные перспективы развития института использования результатов ОРД в уголовном судопроизводстве не коснутся порядка вынесения ныне существующих оперативно-розыскных документов (постановлений о рассекречивании сведений, составляющих государственную тайну, предоставлении результатов ОРД).

Существующий порядок ввода оперативных документов в уголовный процесс, предусмотренный межведомственной Инструкцией, отвечает требованиям времени и законности, вполне емок и понятен. На наш взгляд, изменится доказательственное значение предоставленных материалов. Сегодня результаты ОРД сами по себе не включены в перечень доказательств, предусмотренных ст. 74 УПК РФ. Доказательственное значение им придается посредством проверки следственным путем. Каким именно, в каждом конкретном случае решает следователь (дознаватель). Нередко не обходится и без формальностей, когда следователь механически дублирует документы, предоставленные органами дознания. Поэтому требуется упрощение процессуальной формы и придание ей большей жизнеспособности, что неуверенно, но все-таки внедряется в современное правоприменение. Законодатель уже апробирует подобное, упрощая правоотношения, находящиеся на стыке ОРД и уголовного процесса. Отметим, что с 1 июля 2021 г. ст. 8 Федерального закона «Об оперативно-розыскной деятельности» дополнена следующим содержанием: «В случае получения сообщения о без вести пропавшем лице на основании мотивированного постановления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, вынесенного в течение 24 часов с момента поступления сообщения о без вести пропавшем лице, допускается получение информации о соединениях абонентского устройства, находящегося у без вести пропавшего лица, с иными абонентами и (или) их абонентскими устройствами, иным оборудованием, а также о местоположении данного абонентского устройства путем снятия информации с технических каналов связи с обязательным уведомлением суда (судьи) в течение 24 часов. При получении сообщения о без вести пропавшем несовершеннолетнем либо лице, признанном в установленном законом порядке недееспособным или ограниченно дееспособным, получение соответствующей информации

осуществляется при наличии письменного согласия законного представителя такого без вести пропавшего лица. В течение 48 часов с момента начала проведения оперативно-розыскного мероприятия орган, его осуществляющий, обязан получить судебное решение о проведении такого оперативно-розыскного мероприятия либо прекратить его проведение»[1].

Очевидно, что само по себе сообщение о без вести пропавшем лице есть не что иное, как зарегистрированное сообщение о преступлении, т. е. уголовно-процессуальная категория. При этом законодатель не исходит из необходимости включения в перечень следственных действий, проводимых до возбуждения уголовного дела, «получения информации о соединениях между абонентами и (или) абонентскими устройствами». Но позволяет именно оперативным подразделениям органов дознания проведение ОРМ «снятие информации с технических каналов связи», при этом не имея в текущий момент санкции судьи, т. е. приравнивая пропажу несовершеннолетнего либо недееспособного лица к случаям, не терпящим отлагательства. Передача полученных по результатам проведения подобных мероприятий сведений осуществляется аналогично, также в форме предоставления результатов ОРД. При выполнении социально полезных функций процессуальное «доверие» к результатам ОРД гораздо выше. При этом в конечном итоге не имеет значения, станет ли результатом проведения ОРМ возбуждение уголовного дела и его направление в суд для привлечения виновного лица к уголовной ответственности. С уверенностью можно говорить о том, что если данная практика устоится и принесет позитивные плоды в течение ближайших нескольких лет, ресурсы ОРД чаще будут применяться для целей уголовного процесса. Вполне ожидаемой перспективой может стать дополнение ст. 74, 89 УПК РФ положениями, касающимися признания отдельных видов ОРМ в качестве самостоятельных доказательств с целью минимизации практики дублирования информации от документа к документу, объективной нецелесообразности подобных действий. Проведение таких ОРМ, как «снятие информации с технических каналов связи», «прослушивание телефонных переговоров», «получение компьютерной информации, отдельные виды таких мероприятий», как «наведение справок», «обследование помещений, зданий и сооружений» допускается исключительно на основании судебного решения. Должностные

[1] О внесении изменения в статью 8 Федерального закона «Об оперативно-розыскной деятельности»: Федеральный закон № 252-ФЗ от 1 июля 2021 г. [Электронный ресурс] // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_ LAW_388854/

лица самостоятельной ветви власти, изучившие предоставленные материалы и давшие свою правовую оценку в виде разрешения на проведение ОРМ, выступают гарантами законности, что обеспечивает большую доказательственную пригодность результатов. Примечательно, что актуальность проведения перечисленных ОРМ высока как раз при раскрытии и дальнейшем расследовании хищений денежных средств, криптовалют с использованием сети «Интернет». Представляется, что именно в рамках дел данной категории и пройдет становление и практика признания самостоятельным видом доказательств материалов, отражающих результаты ОРД.

К перспективам, относящимся к организации и характеру проведения ОРМ, получаемой в рамках них информации, для расследования хищений денежных средств, криптовалют предполагаем отнести дальнейшее расширение их организационно-тактических форм в аспекте истребования информации программного и технического характера. Истребование и надлежащая фиксация систематизированных массивов данных о пользователях интернет-ресурсов, владельцах виртуальных («облачных») серверов, подключениях с помощью виртуальных частных сетей (VPN) является прямым условием установления обстоятельств, подлежащих доказыванию по делам о хищениях денежных средств, криптовалют.

Отдельным криминальным направлением, требующим противодействия со стороны органов предварительного расследования, оперативных подразделений органов дознания, остается распространение в рамках общедоступных сайтов, а также «теневого» Интернета, деструктивных течений и культов. У всех на слуху так называемое АУЕ-движение, ключевой идеей которого выступает поощрение противоправного образа жизни, совершения преступлений, однако существует множество подобных ему. Прославление хищений денежных средств, криптовалют происходит и в рамках скам-культуры (от английского «scam» – мошенничество), которой посвящены многие сайты, группы в социальных сетях, в рамках которых подробно разъясняются порядок и способы совершения краж, мошеннических действий со средств платежа.

С сожалением отметим, что целевую аудиторию данных движений образуют подростки, молодые люди и девушки от 12 до 20 лет, воспитанные на общественных устоях рыночной экономики и желающие получить материальную выгоду любой ценой. На территории России ключевым ведомством, ответственным за контроль над происходящим в сети «Интернет», является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роском-

надзор). Однако в функции службы не входит осуществление ОРД, блокирование интернет-ресурсов в настоящее время ей не под силу по причине отсутствия специалистов надлежащего уровня и технических возможностей. В связи с этим вполне очевидно, что на органы дознания и предварительного следствия в ближайшие годы будет возлагаться задача на отыскание, установление администрирующих лиц и привлечение их к установленной законом ответственности в связи с необходимостью реакции со стороны государственных органов на подобные явления. Логично предположить, что полученные в ходе проведения ОРМ материалы после направления в качестве результатов ОРД в органы предварительного расследования выступят основанием для возбуждения уголовного дела, которое, в свою очередь, должно влечь правомочие на техническое блокирование интернет-ресурсов, разделов социальных сетей и т. д. С уверенностью можем утверждать, что право на реализацию блокировки будет возложено на оперативные подразделения органов дознания. Основанием должно служить постановление руководителя органа, осуществляющего ОРД, и наличие уголовно-процессуальных документов, указывающих на оценку действий неустановленных лиц как противоправных.

Небезосновательным представляется вышеизложенное суждение с учетом того, что в настоящее время рассматривается законопроект, регулирующий как оперативно-розыскные, так и процессуальные нормы относительно приостановления операций, связанных со списанием денежных средств с банковских счетов или с уменьшением остатка электронных денежных средств[1]. В соответствии с ним предлагается наделить руководителей федеральных органов исполнительной власти в сфере внутренних дел (из заместителей), а также руководителей органов Федеральной службы безопасности правом на вынесении постановлений о приостановлении операций по банковским и иным счетам в случае получения информации о том, что денежные средства получены преступным путем либо используются для финансирования терроризма (экстремизма). Данный нормативно-правовой акт позволит в оперативном порядке предотвращать окончание совершения многих преступлений, в том числе и хищений безналичных денежных средств, цифровой

[1] О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия финансированию терроризма и (или) иных противоправных деяний: законопроект, предложенный Росфинмониторингом [Электронный ресурс] // Официальный сайт для размещения информации о подготовке федеральными органами исполнительной власти проектов нормативных правовых актов и результатах их общественного обсуждения. URL: https://regulation.gov.ru/projects#npa=121323

валюты. Предлагается, чтобы блокировка счетов на основании постановления компетентного руководителя была возможна на срок до 10 суток. За это время имеющимися оперативно-розыскными и уголовно-процессуальными средствами вполне возможно установить источник происхождения средств, лиц, у которых таковые похищены, принять решение о возбуждении уголовного дела, производстве следственных действий в случаях, не терпящих отлагательства. При принятии данного законопроекта в ближайшие годы расширится практика производства блокировки счетов, используемых в противоправных целях, а также передачи в следственный орган результатов ОРД, отражающих итоги данного мероприятия.

Иной ожидаемой к воплощению перспективой использования результатов ОРД в уголовном судопроизводстве по фактам, связанным с хищениями денежных средств, цифровой валюты, является расширение практики привлечения специалистов к организации и проведению ОРМ. Уголовно-процессуальный закон с 2018 года предусматривает практику изъятия электронных носителей информации исключительно с участием специалиста. Предполагаем, что схожее положение дел найдет отражение и при проведении такого ОРМ, как «обследование помещений, зданий, сооружений», выступая дополнительной гарантией возможности использования их результатов в ходе дальнейшего производства по уголовному делу. Проведение иных ОРМ, так или иначе связанных со взаимодействием с электронно-вычислительной техникой, кредитно-финансовыми инструментами, таких как «проверочная закупка» и «контролируемая поставка», на наш взгляд, также будут проводиться с участием лица, обладающего специальными познаниями. При предоставлении результатов ОРД сотрудники следственных органов будут иметь возможность укрепить доказательственную базу путем допроса еще одного, при этом не имеющего собственного правового интереса, участника ОРМ.

Подводя итоги настоящего параграфа, отметим, что актуальные перспективы использования результатов ОРД при расследовании хищений денежных средств, криптовалют с использованием сети «Интернет» необходимо рассматривать в двух аспектах:

1) связанных с процессуальным порядком предоставления и использования в ходе проверки по сообщению о преступлении, расследования уголовного дела,

2) имеющих отношение к организации и характеру проведения самих ОРМ, а также получаемой в рамках них информации.

К числу первых представляется возможным отнести среднесрочную перспективу, направленную на упрощение процессуальной формы в части признания ОРМ, проводимых на основании судебного решения, в качестве самостоятельного вида доказательств при соблюдении ряда условий и вынесении следователем, дознавателем (судом) соответствующего процессуального документа. В связи с этим вероятны дополнения в ст. 74, 89 УПК РФ.

Второе направление, т. е. перспективы, относящиеся к организации и характеру проведения самих ОРМ, а также получаемой в рамках них информации, по нашим оценкам, подразумевает:

а) расширение границ проведения ОРМ технического и программного характера;

б) предоставление оперативным подразделениям органов дознания (вероятно, Бюро специальных технических мероприятий МВД) правомочий на блокировку деструктивных интернет-ресурсов, в том числе содержащих информацию о формах и методах хищений;

в) становление и совершенствование практики блокировки счетов, используемых в противоправных целях, а также передачи в следственный орган результатов ОРД по итогам данного мероприятия;

г) расширение практики привлечения специалистов к организации и проведению ОРМ технического и смежного характера, результаты которых впоследствии также направляются в следственный орган.

Вопросы для самоконтроля

1. Раскройте теоретико-правовые и практические вопросы, связанные с имплементацией и использованием результатов оперативно-розыскной деятельности в уголовное судопроизводство.

2. На какие две группы возможно разделить перспективы использования результатов оперативно-розыскной деятельности в уголовном процессе?

3. Необходимо ли, на ваш взгляд, наделить сотрудников правоохранительных органов правом на блокирование отдельных банковских операций? Какие законодательные новеллы в этом направлении приняты на территории России?

4. Для какой социально значимой цели, напрямую не связанной с раскрытием преступлений, с 2021 года на территории России предусмотрен упрощенный порядок организации оперативно-розыскного мероприятия «снятие информации с технических каналов связи»?

5. Результаты каких оперативно-розыскных мероприятий наиболее продуктивны при расследовании хищений безналичных, электронных денежных средств, криптовалют?

Заключение

Исходя из того, что хищения безналичных, в том числе электронных, денежных средств, цифровой валюты продолжат оставаться самой распространенной категорией преступлений, более того, будут совершенствоваться в своем исполнении, вопросы организационно-тактических форм их раскрытия и расследования должны находиться в поле зрения уголовно-правовых наук. Своевременное нормативное регулирование, превентивные действия работников кредитно-финансовых учреждений, качественное использование возможностей ОРД и уголовного процесса – все это не предел стремлений, а необходимые условия удержания уголовно наказуемых деяний на социально приемлемом уровне. При этом «застрельщиками» противодействия данным деяниям обязаны выступать именно исследователи, представители научных школ.

За рамками нашего исследования остались отдельные вопросы административно-правового регулирования реализации полномочий должностных лиц оперативных подразделений органов дознания, следователей (дознавателей) и судей. Административно-правовые нормы материального, процессуального характера имеют не меньшее значение, так как именно от них зависит действительное исполнение законных требований правоохранительных органов при сборе, подготовке результатов ОРД. В условиях неисчислимого количества организаций, предоставляющих разноплановые услуги, триада «оперативно-розыскные, уголовно-процессуальные, административные полномочия» становится главным условием надлежащего выполнения оперативно-служебных задач сотрудниками правоохранительных органов.

Резюмируя изложенное, напомним, что нами рассмотрены нормативно-правовые и фактические основания использования результатов ОРД в уголовном процессе, определена специфика их использования при расследовании хищений денежных средств, «цифровых» криптовалют с помощью сети «Интернет», сотовой связи, а также разъяснены ключевые категории, относящиеся к предметам преступлений. Коллективом автором установлены актуальные проблемные аспекты и перспективы использования результатов ОРД при расследовании анализируемых видов хищений, обозначена проблематика имплементации (ввода) и использования в уголовном судопроизводстве результатов ОРД, обусловленная нормами действующего законодательства, сложившейся правоприменительной практикой. Важное теоретическое и методическое значение настоящего издания состоит в определении среднесрочных перспектив использования результатов ОРД при расследовании хищений денежных средств, цифровых (криптовалют).

Список литературы

1. Международные нормативно-правовые акты. Европейская Конвенция по киберпреступлениям (преступления о киберпространстве) [Электронный ресурс] : [принята 21 ноября 2001 г.]. – URL: http://pravo.ru.

2. Международные нормативно-правовые акты. Окинавская хартия Глобального информационного общества [Электронный ресурс] : [принята 22 июля 2000 г.]. – URL: http://www.kremlin.ru.

3. Международные нормативно-правовые акты. Рекомендация, утвержденная комитетом Министров ЕС [Электронный ресурс] : [утверждена 13 сентября 1989 г. № 89]. – URL: https://wcd.coe.int/com.

4. Международные нормативно-правовые акты. Резолюция, принятая 22 января 2001 г. Генеральной Ассамблеей [по докладу Третьего комитета (A/55/593)] 55/63 «Борьба с преступным использованием информационных технологий» [Электронный ресурс]. – URL: https://undocs.org.

5. Международные нормативно-правовые акты. Резолюция, принятая 23 января 2002 г. Генеральной Ассамблеей [по докладу Третьего комитета (A/56/574)] 56/121 «Борьба с преступным использованием информационных технологий» [Электронный ресурс]. – URL: https://undocs.org.

6. Международные нормативно-правовые акты. Резолюция, принятая 21 декабря 2009 г. Генеральной Ассамблеей [по докладу Второго комитета (A/64/422/Add.3)] 64/211 «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» [Электронный ресурс]. – URL: https://undocs.org.

7. Российская Федерация. Федеральные законы Российской Федерации. Уголовный кодекс Российской Федерации. [Электронный ресурс] : [федеральный закон от 13 июня 1996 г. № 63-ФЗ]. – URL: http://www.consultant.ru.

8. Российская Федерация. Федеральные законы Российской Федерации. Уголовно-процессуальный кодекс РФ [Электронный ресурс] : [федеральный закон от 18 декабря 2001 г. № 174-ФЗ]. – URL: http://www.consultant.ru.

9. Российская Федерация. Федеральные законы Российской Федерации. Кодекс Российской Федерации об административных правонарушениях РФ. [Электронный ресурс] : [федеральный закон от 30 декабря 2001 г. № 195-ФЗ]. – URL: http://www.consultant.ru.

10. Российская Федерация. Федеральные законы Российской Федерации. О банках и банковской деятельности [Электронный ресурс] : [федеральный закон от 2 декабря 1990 г. № 395-1]. – URL: http://www.consultant.ru.

11. Российская Федерация. Федеральные законы Российской Федерации. О национальной платежной системе [Электронный ресурс] : [федеральный закон от 27 июня 2011 г. № 161-ФЗ]. – URL: http://www.consultant.ru.

12. Российская Федерация. Федеральные законы Российской Федерации. О внесении изменения в ст. 8 Федерального закона «Об оперативно-розыскной деятельности» [Электронный ресурс] : [федеральный закон от 1 июля 2021 г. № 252-ФЗ]. – URL: http://www.consultant.ru.

13. Российская Федерация. Федеральные законы Российской Федерации. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации [Электронный ресурс]: [федеральный закон от 30 декабря 2001 г. № 195-ФЗ]. – URL: http://www.consultant.ru.

14. Российская Федерация. Постановления Верховного Суда Российской Федерации. О судебной практике по делам о краже, грабеже и разбое [Электронный ресурс]: [постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29]. – URL: http://www.consultant.ru.

15. Российская Федерация. Постановления Верховного Суда Российской Федерации. О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс] : [постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48]. – URL: http://www.consultant.ru.

16. Российская Федерация. Постановления Верховного Суда Российской Федерации. О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам [Электронный ресурс] : [постановление Пленума Верховного Суда РФ от 26 июня 2021 г. № 22]. – URL: http://www.consultant.ru.

17. Послание Президента Республики Казахстан Н. Назарбаева к народу Казахстана от 31 января 2017 г. «Третья модернизация Казахстана: глобальная конкурентоспособность» [Электронный ресурс]: Официальный сайт Информационно-правовой системы нормативных правовых актов Республики Казахстан. – URL: http://adilet.zan.kz/rus/docs/K1700002017.

18. Республика Беларусь. Законы Республики Беларусь. Об оперативно-розыскной деятельности [Электронный ресурс] : [закон от 15 июля 2015 г. № 307-З]. – URL: https://www.pravo.by.

19. Тунисская программа для информационного общества (15 ноября 2005 г.) [Электронный ресурс] : Всемирная встреча на высшем уровне по вопросам информационного общества (Женева, 2003 – Тунис, 2005). – URL: https://www.un.org.

20. *Аратулы К.* Преступления в сфере компьютерной информации в РК и зарубежных странах / К. Аратулы // Вестник КазНУ. – 2010. – № 4 (56). – С. 105–109.

21. *Болычев Н. И.* О зарубежном опыте правового регулирования противодействия экстремизму в сети «Интернет» / Н. И. Болычев // Вестник Воронежского института МВД России. – 2015. – № 3. – С. 209–214.

22. *Волосюк П. В.* Проблемы использования результатов оперативно-розыскной деятельности в уголовном судопроизводстве / П. В. Волосюк // Юридическая наука. – 2013. – № 1. – С. 38–41.

23. *Глебов И. Н.* Правовая футурология: постановка проблемы искусственного юридического разума / И. Н. Глебов // Российское государствоведение. – 2018. – № 1. – С. 12–29.

24. *Гудачевская Г. В.* Допустимость результатов оперативно-розыскной деятельности в доказывании по уголовному делу / Г. В. Гудачевская // 68-я научная конференция студентов и аспирантов Белорусского государственного университета: сб. работ: в 3 ч. / ред. кол.: А. Г. Захаров [и др.]. – Минск: БГУ, 2011. – Ч. 2. – С. 216–219.

25. *Дремлюга Р. И.* Интернет как способ и средство совершения преступления / Р. И. Дремлюга // Информационное право. – 2008. – № 4. – С. 27–31.

26. *Керимов Д. А.* Методология права (предмет, функции, проблемы философии права): монография / Д. А. Керимов. – 2-е изд. – Москва: Аванта +, 2001. – 560 с.

27. *Мазунин Я. М.* Негласная деятельность следователя: пора признать данность [Электронный ресурс] / Я. М. Мазунин // Юридическая наука и правоохранительная практика. – 2015. – № 1 (31). – URL: https://cyberleninka.ru.

28. *Максимов Д. А.* Криптовалюта и блокчейн в финансовой системе России / Д. А. Максимов, В. В. Монин, И. Ю. Глазкова // Экономика и управление: проблемы, решения. – 2017. – Т. 3. – № 3. – С. 217–221.

29. О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия финансированию терроризма и (или) иных противоправных деяний: законопроект, предложенный Росфинмониторингом [Электронный ресурс]. – URL: https://regulation.gov.ru.

30. *Сорокин И. Н.* Использование результатов оперативно-розыскной деятельности в уголовном судопроизводстве [Электронный ресурс] / И. Н. Сорокин // Концепт. – 2014. – № 12 (декабрь). – URL: http://e-koncept.ru/2014/14362.htm.

31. *Повышев В.* Борьба с киберпреступностью и кибертерроризмом [Электронный ресурс] / В. Повышев. – URL: http://www.crime.vl.ru.

32. Проблемы европейской интеграции: правовой и культурологический аспекты: сб. науч. статей / под ред. С. А. Гончарова, А. А. Дорской. – Санкт-Петербург, 2007. – 360 с.

33. *Тропина Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: монография / Т. Л. Тропина. – Владивосток: Дальневосточ. ун-т, 2009. – 237 с.

34. *Тукало А. Н.* Использование результатов оперативно-розыскной деятельности в работе оперативных и следственных подразделений органов внутренних дел: автореф. дис. … канд. юрид. наук / А. Н. Тукало. – Минск, 2011.

35. *Урденко О. Г.* Необходимость компьютерной криминалистики (forensics) как науки [Электронный ресурс] / О. Г. Урденко. – URL: http://www.epos.ua.

36. Денежная масса (национальное определение) [Электронный ресурс]. – URL: https://cbr.ru.

37. Доклад о работе тринадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному преследованию. Доха, 12–19 апреля 2015 г. [Электронный ресурс]. – URL: http: www.un.org.

38. Интервью Гузнова А. А. независимому информационному агентству «Интерфакс» от 16 марта 2020 г. [Электронный ресурс]. – URL: https://cbr.ru.

39. Краткая характеристика состояния преступности в Российской Федерации за январь – октябрь 2020 г. [Электронный ресурс]. – URL: https://мвд.рф.

40. Краткая характеристика состояния преступности в Российской Федерации за январь – август 2021 г. [Электронный ресурс]. – URL: https://мвд.рф.

41. Оценка деятельности полиции Российской Федерации в 2020 году (по данным ФГКУ «ВНИИ МВД России») [Электронный ресурс]. – URL: https://мвд.рф.

42. Похитил и проиграл в казино 420 тыс. рублей. Прокуратура Гродненской области направила уголовное дело в суд [Электронный

ресурс] // Официальный сайт Генеральной прокуратуры Республики Беларусь. – URL: http://www.prokuratura.gov.by/ru.

43. Репортаж по итогам заседания Совета Федерации Федерального собрания Российской Федерации [Электронный ресурс] // Официальный сайт информационного агентства «Тасс». – URL: https://tass.ru.

44. Справочник ООН по предотвращению и контролю преступности, связанной с компьютерами [Электронный ресурс]. – URL: http://www.uncjin.org.

Содержание

Введение ……... 3
Глава 1. Уголовно-процессуальные и криминалистические особенности реализации результатов оперативно-розыскной деятельности при расследовании хищений денежных средств, криптовалют посредством сети «Интернет», сотовой связи ……... 9
§ 1. История развития международного законодательства по противодействию преступлениям, совершаемым с использованием Интернета, сотовой связи …… 9
§ 2. Нормативно-правовые и фактические основания использования результатов оперативно-розыскной деятельности в уголовном процессе …… 21
§ 3. Способы хищений денежных средств граждан с помощью сети «Интернет», сотовой связи и возможности для их выявления и дальнейшего расследования посредством использования результатов ОРД ……. 32
Глава 2. Проблемы и перспективы использования результатов оперативно-розыскной деятельности при расследовании хищений денежных средств, криптовалют с использованием сети «Интернет», сотовой связи …… 54
§ 1. Проблемы имплементации и использования результатов оперативно-розыскной деятельности при расследовании хищений денежных средств, криптовалют с использованием сети «Интернет» 54
§ 2. Перспективы использования результатов оперативно-розыскной деятельности при расследовании хищений денежных средств, криптовалют с помощью сети «Интернет» ……..... 63
Заключение ……..... 73
Список литературы ……... 74

Использование результатов оперативно-розыскной деятельности при расследовании хищений денежных средств граждан с использованием сети «Интернет», сотовой связи

Учебное пособие

Редактура *И. Б. Бебих*
Компьютерная верстка *Д. А. Звездиной*

Подписано в печать 31.10.2022. Формат 60х84 1/16
Печать трафаретная. Бумага офисная
Усл. печ. л. 6,0. Уч.-изд. л. 5,2
Тираж 96 экз. Заказ № 64

Типография научно-исследовательского
и редакционно-издательского отдела
Уральского юридического института МВД России

620057, Екатеринбург, ул. Корепина, 66