Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации
Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

ПРОБЛЕМЫ КВАЛИФИКАЦИИ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Международная научно-практическая конференция
(27 мая 2022 г.)

Сборник научных трудов

1 электронный оптический диск (CD-R)
Текстовое электронное издание

Научное электронное издание

Москва
Московский университет
МВД России имени В.Я. Кикотя

2022

© Московский университет МВД России
имени В.Я. Кикотя, 2022
ISBN 978-5-9694-1185-2

УДК 343.2/.7
ББК 67.408
П78

Рецензенты:
главный научный сотрудник ВНИИ МВД России доктор юридических наук, профессор **О. А. Зайцев**; заместитель начальника кафедры криминалистики Уфимского юридического института МВД России кандидат юридических наук, доцент **Э. Р. Хакимова**

Составитель Н. Г. Кадников

П78 **Проблемы квалификации и расследования преступлений, совершаемых с применением информационно-коммуникационных технологий**: Международная научно-практическая конференция, 27 мая 2022 г. : сборник научных трудов / [сост. Н. Г. Кадников]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2022. – 305 с. – 1 электронный оптический диск (CD-R). − Системные требования : CUP 1,5 ГГЦ ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места на жестком диске.

ISBN 978-5-9694-1185-2

Сборник включает статьи по материалам международной научно-практической конференции «Проблемы квалификации и расследования преступлений, совершаемых с применением информационно-коммуникационных технологий», состоявшейся 27 мая 2022 г. в Московском областном филиале Московского университета МВД России имени В.Я. Кикотя с участием Союза криминалистов и криминологов.

Статьи посвящены проблемам квалификации и расследования преступлений, совершаемых с применением информационно-коммуникационных технологий, включая сеть Интернет. Сборник включает анализ соответствующих составов преступлений, различных вариантов уголовно-правовой оценки совершенных деяний с использованием и применением указанных технологий, предложений по совершенствованию уголовного, уголовно-процессуального и иных отраслей законодательства Российской Федерации, а также опыт противодействия преступлениям указанной категории в зарубежных странах.

Сборник будет полезен преподавателям, аспирантам и студентам юридических вузов, курсантам и слушателям вузов МВД России, практическим работникам правоохранительных органов, адвокатам, научным сотрудникам.

Научное электронное издание

Минимальные системные требования: CPU 1,5 ГГц; RAM 512 Мб; Windows XP SP3; 1 Гб свободного места на жестком диске

© Московский университет
МВД России имени В.Я. Кикотя, 2022

Издание подготовлено
с помощью программного обеспечения Microsoft Word

Корректор *Горбунова Т. С.*
Компьютерная верстка *Горбунова Т. С.*

Подписано к изданию 22.08.2022
Объем издания: 2,88 Мб
1 электронный оптический диск (CD R)

ISBN 978-5-9694-1185-2

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
http://www.mosu.mvd.ru; e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

Дашков Г. В.
Интерес в неюридических отраслях науки, обеспечивающих расследование и предупреждение преступлений 9
Гришко А. Я.
Информационно-коммуникационные технологии: квалификация преступлений и иных правонарушений в местах лишения свободы, их предупреждение 13
Кадников Н. Г., Карпова Н. А.
К вопросу о позиции Верховного Суда Российской Федерации по противодействию преступлениям и правонарушениям экстремистской направленности 17
Русскевич Е. А., Дмитренко А. П.
Актуальные вопросы квалификации посягательств на объекты критической информационной инфраструктуры Российской Федерации..... 26
Шаталов А. С.
К вопросу использования в расследовании преступлений информационно-коммуникационных технологий 31
Яковлева Л. В.
Уголовно-правовые меры противодействия деструктивному психологическому воздействию на человека 36
Жилкин М. Г., Качалов В .В.
Проблемы квалификации взяточничества, совершаемого с использованием криптовалюты 41
Борисов С. В., Чугунов А. А.
Актуальные вопросы квалификации преступлений террористической и экстремистской направленности, совершаемых с использованием информационно-коммуникационных технологий 46
Кужиков В. Н., Габдрахманов Р. Л.
Противодействие легализации доходов, полученных преступным путем, в условиях цифровизации экономики 55
Боровиков В. Б., Боровикова В. В.
Особенности российской уголовно-правовой политики в условиях цифровизации общества 59
Дарменов А. Д.
Некоторые вопросы проведения выемки сведений о произведенных переговорах с абонентских номеров при расследовании мошенничеств, совершаемых с применением информационно-коммуникационных технологий, в Республике Казахстан 65
Бахур О. И.
Особенности уголовной ответственности за преступления против компьютерной безопасности по Уголовному кодексу Республики Беларусь 73

Камчатов К. В.
Проблемы производства процессуальных действий
в отношении криптовалют 78
Ковальчук А. В., Духовник Ю. Е.
Вопросы квалификации деяний, связанных с рассылкой сообщений
с использованием информационно-коммуникационных технологий,
содержащих информацию об угрозах взрывов, в правоприменительной
практике Республики Беларусь 83
Азаренкова Е. А., Осипов В. А.
Публичные призывы и действия как признак объективной стороны
отдельных составов преступлений против общественной безопасности
и основ конституционного строя и безопасности государства 87
Горач Н. Н., Лаврова О. Н.
О некоторых вопросах признания криптовалюты
предметом преступления по уголовным делам,
связанным с расследованием взяточничества 94
Андреев А. А., Куликова О. Н.
Трансформация уголовного законодательства
в условиях информационных процессов 98
Хакимова Э. Р., Дайшутов М. М.
Некоторые особенности расследования преступлений, совершенных
с применением информационно-телекоммуникационных технологий 103
Чуканова Е. С., Бабченко А. И.
Искусственный интеллект в уголовном праве
Российской Федерации 107
Лаврентьева М. С., Туркин М. М.
Кибермошенничество в сфере интеллектуальной собственности 111
Ларина Л. Ю.
Использование информационно-телекоммуникационных
сетей как признак состава преступления 115
Горенская Е. В.
Проблемы квалификации незаконного предпринимательства
в топливно-энергетическом комплексе при выдаче лицензий
с использованием информационных технологий 120
Нгуен Дык Фук
Правовая регламентация и противодействие преступлениям
в сфере высоких технологий в соответствии
с уголовным законодательством Вьетнама 125
Нгуен Тхи Тхань Тхуи
Проблема преступности, связанной с инвестированием
в виртуальную валюту во Вьетнаме 129

Нгуен Тхи Хай Иен
Уголовная ответственность за незаконную организацию
и проведение азартных игр в киберпространстве в соответствии
с законодательством Вьетнама 134
Хоанг Тхи Тху Нга
К вопросу о некоторых мерах предупреждения мошенничеств,
совершаемых с использованием высоких технологий 138
Байтеленова С. Г., Еспергенова Е. В.
Портрет личности жертв преступлений в сфере сетей телекоммуникации,
в том числе сети Интернет 142
Абдульманов А. А.
К вопросу об уголовной ответственности за сбыт наркотических средств,
психотропных веществ или их аналогов, совершенный с использованием
средств массовой информации либо электронных или информационно-
коммуникационных сетей 147
Черепенников Р. В.
Анализ реализации в национальном законодательстве норм Модельного
Уголовного кодекса СНГ, предусматривающих ответственность
за совершение преступлений против информационной безопасности 156
Калининская Я. С., Бойцова Ж. А.
О некоторых проблемах уголовной ответственности за преступления
против общественной безопасности, совершенные
с использованием сети Интернет 161
Нестерович С. А., Купцова Ю. И.
Фишинговые атаки на мобильные телефоны с операционной
системой Android 166
Зиберова О. С.
Пути модернизации информационных технологий
в рамках противодействия преступности 174
Посельская Л. Н.
Проблемы выявления признаков экстремизма, совершаемого
с использованием интернет-технологий 178
Никулина В. А.
Уголовно-правовая охрана цифрового образа личности 183
Реутская Е. А.
Об определении объекта преступлений, совершаемых
с использованием информационно-коммуникационных технологий,
с учетом новелл уголовного законодательства Республики Беларусь 188
Кравец Е. Г., Евлушина Д. Н.
Компетентностный инструментарий специалиста, используемый
при расследовании хищений, совершаемых с использованием
вредоносных компьютерных программ 193

Пикта В. И.
Особенности следообразования при распространении программ-вымогателей 197
Лутцева К. В.
Особенности проведения допроса потерпевшего при расследовании преступлений в сфере информационно-телекоммуникационных технологий 202
Мурадян С. В., Альховская А. В.
К вопросу о посягательствах на частную жизнь в условиях цифровизации 207
Семочкина А. А., Вильмс А. А.
К вопросу об уголовно-правовом противодействии кибербуллингу в Российской Федерации 214
Густова Э. В., Хисматова А. Р.
Толкование признака публичности в преступлениях, совершаемых с использованием информационно-телекоммуникацинных сетей 219
Шемчук С. Ю., Раненкова Е. А.
К вопросу правовой оценки деятельности лиц, вовлеченных в движение «Колумбайн (скулшутинг)» 226
Мухамеджанова А. Д.
Онлайн-кредитование как частный случай интернет-мошенничества в Республике Казахстан 231
Молбасин С. И.
К вопросу об определении территориальной подследственности при расследовании уголовных дел о мошенничествах, совершаемых с применением информационно-коммуникационных технологий, в Республике Казахстан 236
Копаева Ю. Ю.
Проблемы квалификации и доказывания истязаний несовершеннолетних с причинением психических страданий, совершенных с применением информационно-коммуникационных технологий 242
Григорьев Д. А., Басина А. С.
Об отдельных проблемах досудебного производства по преступлениям, совершаемым с применением информационно-телекоммуникационных технологий 246
Корниенкова М. Р., Дякина С. Н.
К вопросу квалификации мошенничества с использованием электронных средств платежа 251
Алференок Е. А., Бандурович А. Б.
К вопросу о социальной обусловленности уголовной ответственности за мошенничество в сфере компьютерной информации 258

Котова А. А.
К вопросу о роли современных информационных систем в противодействии незаконному обороту драгоценных металлов и камней 263
Ковригин В. С.
К вопросу об ином способе приведения в негодность объектов жизнеобеспечения (ст. 215² Уголовного кодекса Российской Федерации) 267
Юдина У. С.
К вопросу об умышленных уничтожении или повреждении чужого имущества, совершенных с использованием информационно-коммуникационных технологий 272
Карпушкин А. В.
К вопросу о границах правомерного причинения вреда при задержании лица, совершившего преступление в цифровой среде 276
Попов А. Ю.
К вопросу правового регулирования отношений в сфере оборота оружия, изготовленного посредством 3D-печати 279
Меерсон В. Р.
К вопросу о дезорганизации функционирования учреждения уголовно-исполнительной системы с использованием информационно-коммуникационных технологий 285
Виссаров В. А.
К вопросу социальной обусловленности уголовной ответственности за незаконный оборот алкогольной продукции, совершаемый с использованием информационных технологий 290
Христофорова С. А.
Принуждение к даче показаний, связанное с угрозой распространения компромитирующих сведений в сети Интернет 294
Гришин Н. С.
Оборот товаров, не отвечающих требованиям безопасности, с использованием информационно-телекоммуникационных сетей 301

Дашков Г. В.[1],
профессор Московского государственного
юридического университета
имени О.Е. Кутафина (МГЮА),
доктор юридических наук, профессор

ИНТЕРЕС В НЕЮРИДИЧЕСКИХ ОТРАСЛЯХ НАУКИ, ОБЕСПЕЧИВАЮЩИХ РАССЛЕДОВАНИЕ И ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ[2]

В числе многоплановых научных и практических задач, которые необходимо решить, выполняя предписания постановления Правительства Российской Федерации от 13 мая 2021 г. № 729 «О мерах по реализации программы стратегического академического лидерства «Приоритет-2030» [1], представляется важным выделить в качестве первоочередной, проблему интереса. Особенно актуально это в той части интереса, которая касается неюридических отраслей науки, обеспечивающих расследование и предупреждение преступлений. В общетеоретическом, да и в практическом плане, на первый взгляд, здесь спорных и нерешенных проблем нет. Более того, все тут выглядит, как правило, на уровне аксиом. В уголовном праве, в криминологии, в криминалистике, они, к примеру, никем не оспариваются. Приветствуется, например, положение о необходимости тесного сотрудничества с другими науками. Но гладко тут только на бумаге. А где овраги? Их здесь предостаточно. Названный всеми принцип активно провозглашается, но на практике, в основе своей, он игнорируется даже тогда, когда успех объединения усилий в борьбе с преступностью очевиден.

Одна иллюстрация. Когда в стране удалось резко, а главное, реально добиться снижения уровня квартирных и иных краж? После очередной криминализации или декриминализации этого самого распространенного преступления (до 700 000 преступлений в год)? Конечно нет. Даже самые суровые, резонансные законодательные акты подобного рода, в лучшем случае, давали лишь сиюминутный положительный эффект. Подтверждением тому, в частности, может быть уголовная статистика по таким знаменитым нормативным актам, как Постановление ЦИК СССР и СНК СССР от 7 августа 1932 г. «Об охране имущества государственных предприятий, колхозов и кооперации и укреплении общественной собственности» [2]. Характерно, что здесь «люди, покушающиеся на общественную собственность, должны быть рассматриваемы как враги народа». Второй пример это Указ Президиума Верховного Совета СССР от 4 июня 1947 г. «Об уголовной ответственности за хищения государственного и общественного имущества» [3]. Сверхжесткие, даже по тем временам, санкции, вплоть до смертной казни и отнюдь не либеральная судебная практика, не привели к ожидаемым положительным результатам.

---

[1] © Дашков Г. В., 2022.

[2] Настоящее исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030».

Последующая, менее жесткая система наказаний за хищения государственного имущества, в лучшую сторону состояние, структуру и динамику имущественных преступлений в стране также не изменила. Успехи, фактические и статистические, здесь были достигнуты только после практической реализации в широких масштабах комплекса организационно-управленческих, технических, экономических и правовых мер противодействия посягательствам на чужое имущество. При этом, роль правовых, в частности, уголовно-правовых мер, предупреждения имущественных преступлений, была тут не решающей. Первенствовали в данном случае, базировавшиеся на криминологических, криминалистических и уголовно-правовых разработках меры технического характера, резко повысившие реальную возможность реализации принципа Пьетро Верри и Беккариа Чезаре о неотвратимости наказания [4, с. 90–104]. Есть ли в этой части мер предупреждения преступлений неиспользованные в полной мере резервы? Оценивая отрицательный и положительный опыт в сравнительном плане на уровне стран мирового сообщества, ответим на этот вопрос только положительно. Вполне естественно мы, как юристы, будем говорить не только о технических резервах. Но резервы эти наиболее значимы.

Здесь юридическая составляющая, естественно, ограничивается. Нас в этой ситуации, интересует в основном вопрос о совершенствовании механизма сотрудничества и определении сути взаимного интереса. Кроме того, следует также обратиться к вопросу о том, кто из сотрудничающих сторон должен использовать здесь приоритетные функции. В этой связи отметим следующее обстоятельство. Ведущими должны быть вроде бы криминалисты. Именно они первыми сталкиваются со способами совершения преступлений. Но тогда мы следуем за преступником. А где же предупреждение преступлений? Нужно предвидение нежелательных последствий уже при разработке тех или иных технических устройств. Так называемый криминологический технический дизайн нашего окружения, также важен. Тут аксиом быть не может и начинать надо с теорем, с постановки задач.

Среди как бы лежащих на поверхности, а на самом деле глубинных и нерешенных проблем совместной деятельности юристов с представителями неюридических наук, способных кардинально улучшить ситуацию в области расследования и предупреждения преступлений, следует выделить проблему интереса в сотрудничестве с социологами. В некоторых странах, например, в США, в этом сотрудничестве социология даже поглощает другие науки. Здесь криминология именуется как социология преступности, а базисные работы по вопросам борьбы с преступностью принадлежат перу крупнейших социологов. Один из ярких примеров тому – мировая криминологическая классика в виде анализа беловортничковой преступности Эдвина Сатерленда, Президента американского социологического общества [5].

Перебравшись в рассуждениях по этому поводу через океан в нашу страну, заметим, что в России во взаимодействии социологов и юристов в области борьбы с преступностью практика опоры только на собственные силы стала сейчас более выраженной чем, скажем, это было 20 лет назад.

Чтобы убедиться в правоте сказанного, достаточно, к примеру, ознакомиться с несколькими нынешними диссертациями по уголовному праву и криминологии. Социология здесь, в лучшем случае, обозначена для проформы во введении. И все. Может быть, отпала потребность в оценке преступности с помощью социологических механизмов? Нет. Последние неудачи в законотворческой деятельности во многом объясняются именно тем, что разработчикам уголовно-правовых норм, как и авторам криминологических и криминалистических рекомендаций, незнакомы, в должной мере, прошлые и нынешние возможности социологической науки. Почему? И у той, и у другой стороны здесь нет надлежащего интереса изменить положением дел к лучшему. Какой тут интерес есть, каким он должен быть? Даже в теоретических разработках вопрос не определен.

И еще одно обстоятельство концептуального свойства. По ряду причин объективного и субъективного характера, опыт применения института интереса на стадии использования возможностей собственно российских неюридических наук при расследовании и предупреждении преступлений весьма мал и, следовательно, ограничен для обобщения и распространения. Вместе с тем, обширная практика на этот счет имеется в части взаимодействия отдельных российских правовых структур и ученых с зарубежными странами. Многое здесь возможно имплементировать во внутреннюю российскую практику и обратно. Назовем подобного рода обстоятельства. Даже в периоды так называемого железного занавеса, ряд высоко развитых зарубежных государств, включая США, Великобританию, Францию, Германию, проявляли повышенный интерес к советскому опыту борьбы с преступностью. Что здесь особо привлекало наших зарубежных коллег? Прежде всего, органическое сочетание «общей и особенной» части наших научных исследований, касающихся вопросов расследования и предупреждения преступлений. Второе привлекательное наше криминологическое качество прошлых лет. Ни все и не всеми продается и покупается. Морально-этическая сторона сотрудничества, осознание необходимости делать общее дело, а именно совместно бороться с преступностью – это общегосударственная задача во всех частях света и во все времена. Однажды, находясь в США, в штате Вашингтон, где делают основу всей гражданской авиации мира и производят почти все программное обеспечение, а следовательно, знают что такое моральный и материальный интерес, я убедился, что материальный интерес не является основной движущей силой в деятельности государственных и общественных организаций по борьбе с преступностью, особенно в той ее части, которая касается несовершеннолетних. Тоже самое можно сказать и о других отнюдь не бедных американских общественных и других организациях, как например о «People to people», АВА, которые во многом продвинули вперед свои национальные правовые задачи за счет сотрудничества с нашей страной и внутри США. Широко трактуя понятие интереса.

А кто нам мешает таким же образом, не только за деньги, заинтересовать российских социологов, экономистов, физиков, химиков, математиков, привлекая их в качестве субъектов выявления, расследования и предупреждения преступности? Никто.

Список литературы

1. Постановление Правительства Российской Федерации от 13 мая 2021 г. № 729 «О мерах по реализации программы стратегического академического лидерства «Приоритет-2030» // СПС «КонсультантПлюс».

2. Постановление ЦИК СССР и СНК СССР от 7 августа 1932 г. «Об охране имущества государственных предприятий, колхозов и кооперации, и укреплении общественной собственности» // СПС «КонсультантПлюс».

3. Указ Президиума Верховного Совета СССР от 4 июня 1947 г. «Об уголовной ответственности за хищения государственного и общественного имущества» // СПС «КонсультантПлюс».

4. Егоров А. А. Нравственные основания учения Чезаре Беккариа о преступлениях и наказаниях // Lex russica. 2020. Т. 73. № 3. С. 90–104.

5. Мацкевич И. М. Беловоротничковая преступность. Старая теория в современной действительности // Современные проблемы уголовно-правовой политики : сборник научных трудов. Краснодар, 2015.

Гришко А. Я.[1],
профессор кафедры уголовного права и криминологии
Рязанского государственного университета
имени С.А. Есенина,
профессор кафедры уголовного права и криминологии
Рязанского филиала Московского университета
МВД России имени В.Я. Кикотя,
доктор юридических наук, профессор

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ: КВАЛИФИКАЦИЯ ПРЕСТУПЛЕНИЙ И ИНЫХ ПРАВОНАРУШЕНИЙ В МЕСТАХ ЛИШЕНИЯ СВОБОДЫ, ИХ ПРЕДУПРЕЖДЕНИЕ

Меры, предпринимаемые в сфере уголовной и уголовно-исполнительной политики, совершенствование законодательства в ней привели к позитивным изменениям в системе исполнения наказаний. К числу наиболее значимых положительных показателей здесь следует отметить продолжающееся уменьшение количества осужденных, отбывающих наказания в виде лишения свободы, и расширение практики применения наказаний без лишения свободы. Количество первых с 2010 по 2022 год сократилось с 864 тыс. до 466581 человека. Количество осужденных на 1 марта 2022 г. составило 489403 человека.

Однако приведенная положительная динамика привела к ухудшению криминологической ситуации в местах лишения свободы. Количество зарегистрированных преступлений, совершенных в исправительных учреждениях в 2021–2022 гг. составило соответственно 1183 и 1272. При этом происходит качественное ухудшение преступности. Среди преступлений, совершенных в указанных учреждениях, значительную долю составляют деяния, отличающиеся повышенной степенью общественной опасности: убийство и умышленное причинение тяжкого вреда здоровью (3,5 %), побеги (8,0 %), дезорганизация деятельности учреждений, обеспечивающих изоляцию от общества (37,7 %), приобретение, сбыт наркотических средств (12,1 %).

Криминогенную обстановку в местах лишения свободы обостряют деяния, связанные с неправомерными действиями осужденных в отношении персонала исправительных учреждений. Так, в 2018 г. было зарегистрировано 203 таких случая. Был причинен вред здоровью 55 сотрудникам указанных учреждений в связи с исполнением ими служебных обязанностей, совершенных за пределами территории исправительных учреждений. Значительное количество таких случаев имеет место и на территории мест лишения свободы – более 200 [1, с. 4].

При совершении преступлений осужденные зачастую используют одно из основных средств, которое можно отнести к категории информационно-коммуникационных – сотовые телефоны.

---

[1] © Гришко А. Я., 2022.

Так, только в 2019 г. в учреждениях УИС изъято 54,7 тыс. телефонов мобильной связи, за шесть месяцев 2020 г. – 22 тыс., из них большинство изымается при попытке доставки и около 35 % – непосредственно из обращения содержащихся под стражей лиц и осужденных. Незаконное использование ими телефонов создавало условия для совершения мошеннических действий, доставки в места принудительного содержания запрещенных предметов, поддержания преступных связей с лицами, находящимися вне мест лишения свободы.

К примеру, один из осужденных, отбывая наказание в исправительной колонии в Рязанской области, с использованием телефона сотовой связи путем обмана и злоупотребления доверием завладел денежными средствами граждан в размере около 30 млн руб.

Два сотрудника СИЗО-1 УФСИН России по г. Москве («Матросская тишина») вступили в преступную связь с содержащимися под стражей лицами, которые с их помощью с использованием телефонов сотовой связи совершали мошеннические действия в отношении граждан, находящихся вне пределов следственного изолятора, вымогали у них денежные средства. Виновные лица привлечены к уголовной ответственности [2, с. 6].

В раскрытии таких и других деяний активно применяются технические средства контроля информационно-коммуникационного характера, основными из которых являются стационарные видеокамеры и персональные средства контроля.

С их помощью осуществляется оперативно-розыскные мероприятия для фиксации криминальных процессов, происходящих в исправительных учреждениях: фиксируется деятельность лиц, занимающих высшее положение в преступной иерархии, осуществляющих руководство криминальными явлениями в учреждениях, исполняющих наказания (вымогательство денег в ходе организации азартных игр; создание воровских касс; распространение наркотиков; посягательство на жизнь и здоровье персонала, положительно характеризующихся осужденных; организация побегов; действия по дезорганизации деятельности исправительных учреждений). С помощью технических средств контроля, в частности, фиксируются случаи: входа на территорию исправительных учреждений лиц, обладающих статусом «вора в законе», с целью проведения собраний осужденных; доставки запрещенных предметов; поддержания преступных связей с лицами, находящимися в местах лишения свободы [3, с. 18–19, с. 7].

Технические средства фиксации и контроля активно используются в деле выявления нарушений режима отбывания наказания, совершения преступлений и иных правонарушений со стороны должностных лиц исправительных учреждений. Речь идет о неправомерном применении ими физической силы к осужденным, о бесконтрольности пользования сотовыми телефонами, ноутбуками, принтерами и другими техническими средствами, о создании «льготных условий» отбывания наказания.

Здесь нельзя не упомянуть и широко освещенной в СМИ истории проживания осужденного за совершение особо тяжких преступлений члена известной

своей жестокостью банды Цапков из станицы Кущевская, в условиях повышенной комфортности, которые создали ему сотрудники колонии в Амурской области. Выехавшие на место работники прокуратуры установили, что осужденный, являвшийся одним из лидеров уголовно-преступной среды, был незаконно переведен на облегченные условия отбывания наказания, неправомерно находился и даже периодически проживал в помещении на участке, приспособленном под пасеку, где в условиях полной бесконтрольности пользовался сотовым телефоном и другими запрещенными предметами, а также беспрепятственно встречался с осужденными из числа злостных нарушителей установленного режима и лицами, не отбывающими наказание. Ему без ограничений поступали продукты питания в посылках и передачах, с его лицевого счета удержания в возмещение ущерба потерпевшим от преступлений не производились, администрацией колонии к нему необоснованно применялись меры поощрения [2, с. 6].

Приведенные показатели и примеры обусловливают необходимость совершенствования законодательства и иных нормативных правовых актов в рассматриваемой сфере, практики расследования преступлений, совершаемых с использованием средств информационно-коммуникационного характера, проведения служебных проверок по фактам их незаконного проноса на территорию исправительного учреждения и использования. К числу мер по их совершенствованию следует отнести:

1. Усиление прокурорского надзора за расследованием преступлений и иных правонарушений с использованием указанных средств для установления цели их использования, их применении при совершении преступлений с помощью соответствующих служб уголовно-исполнительной системы и органов внутренних дел.

2. Осужденными и лицами, содержащимся в следственных изоляторах, выводятся из строя видеокамеры. В 2020 г. их количество составило 1445 [4, с. 8]. Нередко это делается в целях устранения условий для совершения преступлений (побеги, дезорганизация деятельности исправительного учреждения, осуществление насилия в отношении персонала учреждения, осужденных и др.). В целях повышения превентивной роли норм ст. 167 Уголовного кодекса Российской Федерации (умышленное уничтожение или повреждение имущества) следует изменить редакцию части первой данной статьи, включив в нее совершение указанного деяния, направленное на устранение препятствий для совершения преступления [5, с. 437, 438]. Дело в том, что имеющаяся норма не всегда позволяет привлечь осужденного, уничтожившего или повредившего видеокамеру в силу отсутствия «значительного ущерба». Требуется и активизация работы администрации исправительного учреждения по возмещению осужденными ущерба в результате таких деяний. Так в 2020 г. причиненный ущерб от порчи видеокамер составил 4591,2 руб. В то время за указанный период сумма возмещенного ущерба составила только 9584 руб. (21,5 %).

Необходимость принятия указанных и иных мер обуславливается не только большим количеством указанных деяний и причиняемый ущерб, но и высокой степенью эффективности их применения в деле предупреждения преступлений

и других видов правонарушений. В 2020 г. с помощью видеокамер было зарегистрировано 2360404 нарушения правил внутреннего распорядка исправительных учреждений и следственных изоляторов, с помощью персональных видеорегистраторов их зарегистрировано 624575 [4, с. 7].

3. Улучшение качества расследования уголовных дел в отношении осужденных, совершивших преступления, устранение их причин и условий их совершения, требуется активизация судов по вынесению частных определений при установлении случаев низкого уровня применения информационно-коммуникационных технологий как средства предупреждения преступления, их использования при расследовании преступлений с участием осужденных и персонала исправительных учреждений.

Список литературы

1. О состоянии режима и надзора в исправительных учреждениях и следственных изоляторах территориальных органов ФСИН России в 2018 г. Обзор ФСИН России от 28 марта 2019 г. № 03-22260. С. 4.

2. Интервью начальника управления по надзору за законностью исполнения уголовных наказаний Владимира Макарова информационному агентству ТАСС в работе: Х-1; Х-2. URL: https://epp_genproc.gou.ru//net/gpt/mass-media/news?ite 58084862. С. 6.

3. Губин С. Противодействие распространению криминальной идеологии в местах лишения свободы // Законность. 2020. № 9. С. 18–19 ; Интервью начальника управления по надзору за законностью исполнения уголовных наказаний Владимира Макарова информационному агентству ТАСС. URL: https://epp_genproc.gou.ru//web/gpt/mass-media/news?item=58084862. С. 7.

4. Об обеспечении подразделений безопасности (режима и надзора) техническими средствами надзора в 2020 г. Обзор ФСИН России от 17 марта 2021 г. № 03-17060. С. 7, 8.

5. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) / под ред. Н. Г. Кадникова. 6-е изд., перераб. и доп. М. : ИД «Юриспруденция», 2019. С. 437, 438.

Кадников Н. Г.[1],
профессор кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
доктор юридических наук, профессор

Карпова Н. А.[2],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент

К ВОПРОСУ О ПОЗИЦИИ ВЕРХОВНОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ И ПРАВОНАРУШЕНИЯМ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

Современное состояние преступности позволяет говорить о повышенной опасности деяний экстремистской направленности. В январе–декабре 2021 г. зарегистрировано 2136 преступлений террористического характера, что на 8,8 % меньше, чем годом ранее, и 1057 преступлений экстремистской направленности, что больше на 26,9 %, чем в 2020 г. [1]. В 2021 г. в 3,5 раза увеличилось число дел по статье о реабилитации нацизма (ч. 1 ст. 354 Уголовного кодекса Российской Федерации) – с шести осужденных в 2020 г. до 21. При этом в 2018–2019 гг. осужденных по этой статье не было, а в 2017 г. их число составляло всего два человека [2].

Постоянно растет количество зарегистрированных преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных технологий. Например, в 2020 г. по ст. 280 Уголовного кодекса Российской Федерации (публичные призывы к экстремистской деятельности) таких было 340 (на 32,3 % больше, чем в 2019 г.). В 2021 г. увеличилось число осужденных за участие в экстремистском сообществе (ч. 2 ст. 282.1 Уголовного кодекса Российской Федерации): по этому составу было осуждено 13 человека, что почти на 70 % больше, чем в 2020 г. (четыре человека). По сравнению с 2020 г. больше стало осужденных и по чч. 1, 2 ст. 282² Уголовного кодекса Российской Федерации, предусматривающей наказание за организацию и участие в объединениях, ликвидированных из-за признания судом экстремистскими. Так, за участие в подобной организации было осуждено 84 человека (в 2020 г. – 49), за организацию деятельности – 36 (в 2020 г. – 19). Чуть более чем в два раза выросло количество осужденных за публичные призывы к насильственному изменению конституционного строя с использованием средств массовой информации. Так, в 2021 г. их число составило 242 человека, в 2020 г. их было 135 человека, 109 и 83 человека в 2019 и 2018 гг. соответственно [3].

---

[1] © Кадников Н. Г., 2022.
[2] © Карпова Н. А., 2022.

Рост преступлений экстремистской направленности фиксирует МВД России и в первой половине 2022 г. Согласно характеристике состояния преступности, за январь–март 2022 г. зарегистрировано 340 подобных преступлений, что на 16,8 % больше, чем в аналогичном периоде прошлого года. Отдельно было подсчитано число зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий. По ст. 280 Уголовного кодекса Российской Федерации (публичные призывы к экстремистской деятельности) таких было 455 (на 33,8 % больше, чем в 2020 г.) [4].

Чаще всего, по мнению Генеральной прокуратуры Российской Федерации, экстремистские преступления совершают в мессенджерах. 25 % террористических и 66 % экстремистских преступлений, зарегистрированных в 2021 г., совершены в сети Интернет, сообщил заместитель начальника Главного управления международно-правового сотрудничества Генеральной прокуратуры Российской Федерации Вячеслав Михеев. Такие данные он озвучил 8 июля на конференции руководителей прокуратур европейских государств в Санкт-Петербурге. При этом Михеев отметил растущий тренд на размещение экстремистских материалов на личных страницах в социальных сетях, а также в мессенджерах [5].

Показатели преступности и мнения специалистов позволяют сделать вывод об особой опасности в современный период правонарушений и преступлений экстремистской направленности, совершаемых с использованием информационно-коммуникационных сетей, в том числе сети Интернет. Это связано с тем, что росту экстремизма обычно способствуют: социально-экономические кризисы, коррупция, резкое падение жизненного уровня основной массы населения, проблемы со свободой слова. Наряду с этим, отрицательные эмоции проявлялись у граждан в связи с пандемией COVID-19, когда здравоохранение было порой бессильно перед коронавирусом. В таких ситуациях некоторые граждане проявляют радикализм, что, по их ошибочному мнению, может стать единственной возможностью реально повлиять на ситуацию [6, с. 47–50]. Наряду с этим, растет количество пользователей различными мессенджерами, особенно из числа молодых людей, которые весьма податливы всяким радикальным предложениям и лозунгам, в том числе и к поиску виноватых в их жизненных неудачах и материальной недостатке.

Следует согласиться с теми авторами, которые полагают, что поводом к усилению экстремистских настроений среди молодежи становятся попытки отдельных политических сил и общественных организаций использовать молодежь в своих целях, подстрекая и провоцируя ее на различные агрессивные действия, в том числе на массовые беспорядки [6, с.47–50]. Кроме того, важно учитывать способность представителей молодежи к организации посредством информационно-коммуникационных технологий групповых форм недовольства и протеста. При этом используются анонимные телеграмм-каналы, затрудняющиеся поиск авторов экстремистских материалов.

Можно поддержать и тех специалистов, которые говорят о киберэкстремизме как относительно новой форме экстремизма, в рамках которой для пропаганды

противоправной деятельности используются новейшие средства распространения информации, коммуникационные технологии и сеть Интернет. Посредством персональных компьютеров и мобильных телефонов проводится завуалированная и открытая интернет-пропаганда, пропаганда в социальных сетях (SMM, таргетированная реклама, «лайкеры» и т. д.), пропаганда через почтовую рассылку, мобильные приложения и прочие [7].

Нельзя сказать, что российский законодатель не успевает с нормативным обеспечением противодействия экстремистским проявлениям [8]. Но и в этой работе есть проблемы, дублирование нормативных установлений, недостаточно продуманные решения, которые затрудняют правоприменение, а иногда приводят к негативным последствиям (необоснованное привлечение к ответственности, в том числе уголовной, формирование из справедливых критиков неверных действий представителей власти псевдоэкстремистов).

Вместе с тем, обвинительный уклон в сфере противодействия экстремизму и деяниям экстремистской направленности может привести к объективному вменению и привлечению к ответственности (в том числе и уголовной) граждан за критические высказывания в отношении отдельных представителей власти и нерадивых руководителей. В этом смысле важное значение имеют позиции Верховного Суда Российской Федерации, отраженные в постановлении Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 (ред. 28.10.2021) «О судебной практике по уголовным делам о преступлениях экстремистской направленности» [9]. Во-первых, Пленум Верховного Суда Российской Федерации особо отметил и подтвердил, что в соответствии со ст. 2 Конституции Российской Федерации человек, его права и свободы обладают высшей ценностью, а государство обязано их признавать, соблюдать и защищать. Наряду с этим, отмечено, что права и свободы человека и гражданина могут быть ограничены федеральным законом только соразмерно конституционно значимым целям (ст. 55 Конституции Российской Федерации). Во-вторых, в постановлении обращено внимание на то, что согласно ст. 13 Конституции Российской Федерации, в Российской Федерации признаются идеологическое и политическое многообразие, многопартийность; никакая идеология не может устанавливаться в качестве государственной или обязательной. Запрещается создание и деятельность общественных объединений, цели или действия которых направлены на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, подрыв безопасности государства, создание вооруженных формирований, разжигание социальной, расовой, национальной и религиозной розни. При этом Пленум Верховного Суда Российской Федерации разъяснил, что ст. 29 Конституции Российской Федерации гарантируется свобода мысли и слова, запрещается пропаганда или агитация, возбуждающая социальную, расовую, национальную или религиозную ненависть и вражду, пропаганду социального, расового, национального, религиозного или языкового превосходства.

Подчеркнута значимость таких международно-правовых документов, как Всеобщая декларация прав человека от 10 декабря 1948 г., Международный пакт

о гражданских и политических правах от 16 декабря 1966 г., Международная конвенция о ликвидации всех форм расовой дискриминации от 21 декабря 1965 г., Декларация Генеральной Ассамблеи ООН от 25 ноября 1981 г. о ликвидации всех форм нетерпимости и дискриминации на основе религии или убеждений, Конвенция о защите прав человека и основных свобод от 4 ноября 1950 г. [10]. При этом совершенно справедливо указывается, что данные международно-правовые документы, провозглашая право каждого человека на свободное выражение своего мнения, вместе с тем предусматривают, что это право не должно подменяться экстремистскими проявлениями, которые категорически должны быть запрещены законом. Еще раз это было подтверждено в рамках Шанхайской конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 г., согласно положениям которой терроризм, сепаратизм и экстремизм, вне зависимости от их мотивов, не могут быть оправданы ни при каких обстоятельствах. В-третьих, Пленум Верховного Суда Российской Федерации отметил важную роль уголовного закона в противодействии экстремистским проявлениям, но, тем не менее, преступления экстремистской направленности объективно требовали более точного судебного толкования в части квалификации и отграничения от смежных деяний, особенно после частичной декриминализации ч. 1 ст. 282 Уголовного кодекса Российской Федерации. В соответствии с поправками, внесенными Федеральным законом от 27 декабря 2018 г. № 519-ФЗ, уголовная ответственность по ч. 1 ст. 282 Уголовного кодекса Российской Федерации возможна только после привлечения лица к административной ответственности за аналогичное деяние в течение одного года (если это деяние не совершено с применением насилия или с угрозой его применения или лицом с использованием своего служебного положения, либо организованной группой) [11, с. 876–879].

Важное внимание уделено Пленумом Верховного Суда Российской Федерации совершению экстремистских преступлений с использованием информационно-коммуникационных сетей, в том числе и сети Интернет. Так, в соответствии с последними поправками, обращено внимание судов, что с учетом содержания диспозиций ст.ст. 280, 280.1, 282 Уголовного кодекса Российской Федерации к данным экстремистского содержания относится, например, не только сам факт размещения в сети Интернет или иной информационно-телекоммуникационной сети текста, изображения, аудио- или видеофайла, содержащего признаки призывов к осуществлению экстремистской деятельности или действий, направленных на нарушение территориальной целостности Российской Федерации, возбуждения ненависти либо вражды, унижения достоинства человека либо группы лиц, но и иные сведения, указывающие на общественную опасность деяния, в том числе на направленность умысла, мотив совершения соответствующих действий.

Наряду с разъяснением о квалификации фактов экстремистской деятельности, в том числе и с использованием информационно-коммуникационных сетей, Пленум Верховного Суда Российской Федерации совершенно справедливо уделил значительное внимание более тщательной оценке мотивов действий виновного, публичности действий. При этом следует поддержать судебное толкование

в части того, что вопрос о публичности призывов должен разрешаться судами с учетом места, способа, обстановки и других обстоятельств дела (обращения к группе людей в общественных местах, на собраниях, митингах, демонстрациях, распространение листовок, вывешивание плакатов, распространение обращений путем массовой рассылки сообщений абонентам мобильной связи и т. п.). Привлечения к ответственности по ст. 282 Уголовного кодекса Российской Федерации возможно при действиях виновного, совершаемых публично и с использованием информационно-телекоммуникационных сетей, включая сеть Интернет (размещение соответствующей информации на сайтах, форумах или в блогах, массовая рассылка электронных сообщений и иные подобные действия, в том числе рассчитанные на последующее ознакомление с информацией других лиц).

Весьма значимыми следует признать разъяснения Пленума по поводу различной уголовно-правовой оценки публичных призывов к совершению преступлений, предусмотренных ст.ст. 280^1, 280^2, 205^2 Уголовного кодекса Российской Федерации. Тем не менее, очень важными являются разъяснения Пленума Верховного Суда Российской Федерации, касающиеся характера экстремистских действий и их отличия от критических выступлений граждан по различным проблемам развития общества и государства также деятельности представителей власти и иных должностных лиц. Пленум особо отметил, что критика политических организаций, идеологических и религиозных объединений, политических, идеологических или религиозных убеждений, национальных или религиозных обычаев сама по себе не должна рассматриваться как действие, направленное на возбуждение ненависти или вражды [12].

Необходимо обратить внимание на разъяснение Пленума, касающееся критике деятельности государственных чиновников и политиков. По мнению Пленума, судам необходимо учитывать положения ст.ст. 3, 4 Декларации о свободе политической дискуссии в средствах массовой информации, принятой Комитетом министров Совета Европы 12 февраля 2004 г., и практику Европейского Суда по правам человека, согласно которым политические деятели, стремящиеся заручиться общественным мнением, тем самым соглашаются стать объектом общественной политической дискуссии и критики в средствах массовой информации; государственные должностные лица могут быть подвергнуты критике в средствах массовой информации в отношении того, как они исполняют свои обязанности, поскольку это необходимо для обеспечения гласного и ответственного исполнения ими своих полномочий.

Критика в средствах массовой информации должностных лиц (чиновников, политиков), их действий и негативных последствий их деятельности сами по себе не должны рассматриваться во всех случаях как действие, направленное на унижение достоинства человека или группы лиц, поскольку в отношении указанных лиц пределы допустимой критики шире, чем в отношении частных лиц [13]. Особо это касается случаев коррупции, должностных злоупотреблений, недостойного поведения и сомнительных высказываний, допущенных чиновниками различного уровня. Об этом написано много, но современные

факты позволяют говорить о том, что актуальность проблемы не исчерпана. Так, Хорошевский районный суд Москвы 21 января 2022 г. отправил под стражу заместителя министра транспорта В.Т., обвиняемого в особо крупном мошенничестве. Начальнику радиотехнических войск Воздушно-космических сил России А.К. предъявлено обвинение в рамках уголовного дела о получении взятки. Ему избрана мера пресечения – содержание под стражей. По версии следствия, он получил не менее 5 млн руб. от директора одного из НИИ [14]. Обвинение в групповом хищении более 860 млн руб. предъявлено бывшему начальнику отдела закупок управления снабжения бронетанковым и автомобильным имуществом Главного автобронетанкового управления Минобороны России (ГАБТУ) Е. П. [15]. В апреле 2021 г. был арестован директор департамента металлургии и строительных материалов Министерства промышленности и торговли России П. С. По версии следствия, он в 2018 г. велел выдать бюджетную субсидию в размере 31 млн руб. частной фирме на возмещение ее затрат на научно-исследовательские работы, связанные «приоритетными направлениями промышленности, в рамках комплексных инвестиционных проектов». В действительности никаких работ не проводилось, представленные же в ведомство документы были поддельные [16]. Конечно, до обвинительного приговора суда неправомерно говорить об этих лицах, как о преступниках, но критика их действий не должна квалифицироваться как экстремистское правонарушение.

Для признания публичных высказываний в качестве экстремистских, в том числе совершенных с использований информационно-коммуникационных сетей и сети Интернета, важное значение имеет такой признак субъективной стороны как вина в форме прямого умысла. Этот признак является критерием разграничения преступлений и проступков экстремистской направленности, что влияет на противоправность и наказуемость действий. В частности, судам разъяснено, что размещение лицом в сети Интернет или иной информационно-телекоммуникационной сети, в частности, на своей странице или на страницах других пользователей материала (например, видео-, аудио-, графического или текстового), созданного им самим или другим лицом, включая информацию, ранее признанную судом экстремистским материалом, может быть квалифицировано по ст.ст. 280, 280[1], 282 Уголовного кодекса Российской Федерации только в случаях, когда установлено, что лицо, разместившее такой материал, осознавало направленность деяния на нарушение основ конституционного строя, а также имело намерение побудить других лиц к осуществлению экстремистской деятельности, совершению действий, направленных на нарушение территориальной целостности Российской Федерации, либо цель возбудить ненависть или вражду, унизить достоинство человека или группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии либо принадлежности к какой-либо социальной группе. При этом наличие умысла предполагает учет всех фактических обстоятельств в совокупности, в том числе форму и содержание размещенной информации, ее контекст, наличие и содержание комментариев данного лица или иного выражения отношения к ней, факт личного создания либо заимствования лицом соответствующих аудио-, видеофайлов, текста

или изображения, содержание всей страницы данного лица, сведения о деятельности такого лица до и после размещения информации, в частности, о совершении действий, направленных на увеличение количества просмотров и расширение пользовательской аудитории, данные о его личности (например, приверженность радикальной идеологии, участие в экстремистских объединениях, привлечение ранее лица к административной и (или) уголовной ответственности за правонарушения и преступления экстремистской направленности), объем подобной информации, частоту и продолжительность ее размещения, интенсивность обновлений.

Актуальность современного судебного толкования состоит и в том, что Пленум Верховного Суда Российской Федерации не исключил, что при правовой оценке действий, направленных на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по соответствующим признакам, действия лица могут быть признаны не представляющими общественной опасности в силу их малозначительности (ч. 2 ст. 14 Уголовного кодекса Российской Федерации), хотя формально и содержат признаки какого-либо деяния, предусмотренного уголовным законом. При решении вопроса о том, является ли деяние малозначительным, то есть не представляющим общественной опасности, судам необходимо учитывать, в частности, размер и состав аудитории, которой соответствующая информация была доступна, количество просмотров информации, влияние размещенной информации на поведение лиц, составляющих данную аудиторию [17, с. 65, 66].

Очень важно при разграничении преступлений и проступков в указанной сфере, как отметил Пленум, четко и точно соблюдать все предусмотренные уголовно-процессуальным законом процедуры сбора доказательств, и оценки их достоверности.

Важными следует признать и другие разъяснения Пленума Верховного Суда Российской Федерации об уголовно-правовой оценке деяний экстремистской направленности. Особую опасность представляют действия, направленные на создание экстремистского сообщества (ч. 1 ст. 282.1 Уголовного кодекса Российской Федерации), то есть объединения двух или более лиц в устойчивую группу в целях подготовки или совершения преступлений экстремистской направленности. Информационно-коммуникационные технологии позволяют проводить действия по созданию подобных сообществ среди многих пользователей сетей, создавая иллюзию всеобщности. Но и в этом случае Пленум Верховного Суда Российской Федерации разъяснил, что о готовности такого сообщества к совершению преступлений экстремистской направленности может свидетельствовать, например, достижение договоренности о применении насилия в общественных местах в отношении лиц по признакам принадлежности (или непринадлежности) к определенным полу, расе, национальности, языковой, социальной группе, в зависимости от происхождения, отношения к религии. Получение доказательств о совершении таких действий требует глубокой технической подготовки, вклю-

чающей постоянный мониторинг социальных сетей, проведение иных предупредительных действий, позволяющих своевременно пресекать проявления экстремизма в сетях.

Таким образом, следует поддержать Пленум Верховного Суда Российской Федерации в его стремлении более точно дифференцировать публичные действия, высказывания граждан в информационно-коммуникационных сетях и сети Интернет, чтобы своевременно предупреждать экстремистские проявления, выявлять деструктивные группы и сообщества, привлекать виновных к ответственности, но не допускать обвинительного уклона и ошибочных действий в отношении граждан, высказывающих обоснованную критику в адрес представителей власти и чиновников разных уровней, так как необходимо в полной мере соблюдать права и свободы человека и гражданина, в том числе при оценке его публичных высказываний, материалов, размещенных им в средствах массовой информации, постов и репостов в информационно-коммуникационных сетях и сетях Интернет.

Список литературы

1. МВД России сообщило о росте на 27 % за год числа преступлений экстремистской направленности // Интерфакс. 2022. 18 янв.

2. URL: https://www.rbc.ru/newspaper/2022/04/22/62614a2f9a79479125d98653.

3. URL: https://www.rbc.ru/newspaper/2022/04/22/62614a2f9a79479125d98653.

4. Состояние преступности в России за январь – декабрь 2021 г. // Сайт МВД России.

5. URL: pravo.ru›Новости›233081.

6. Панталева Н. С., Пархитько Н. П. Кибертерроризм и киберэкстремизм как современные угрозы национальной и международной безопасности // Юридическая наука. 2019. № 3. С. 47–50.

7. Могилевцева О. С., Селеня Д. А. Особенности профилактики киберэкстремизма в молодежной среде // Современные научные исследования и инновации. 2016. № 12 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2016/-12/76097.

8. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (ред. от 08.12.2020) (с изм. и доп., вступ. в силу с 14.04.2021) ; Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 30.12.2021) (с изм. и доп., вступ. в силу с 01.01.2022).

9. Пленум Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (ред. от 28.10.2021) // СПС «КонсультантПлюс».

10. СПС «КонсультантПлюс».

11. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) / под ред. Н. Г. Кадникова. 6-е изд., перераб. и доп. М. : ИД «Юриспруденция», 2019. С. 876–879.

12. Пункт 7 постановления Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (ред. от 28.10.2021) // СПС «КонсультантПлюс».

13. Как представляется, в настоящее время требуются дополнительные разъяснения данной позиции с учетом принятия законов о неисполнении решений ЕСПЧ // Федеральный закон от 11 июня 2022 г. № 183-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // СПС «КонсультантПлюс».

14. URL: ТАСС //.

15. URL: ТАСС //.

16. URL: kommersant.ru›doc/4753277 //.

17. Пункт 8.1 постановления Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (ред. от 28.10.2021) // СПС «КонсультантПлюс» ; Уголовное право России : учебник в 2 томах. Т. 1: Общая часть / под общ. ред. Н. Г. Кадникова. М. : Юриспруденция, 2018. С. 65, 66.

Русскевич Е. А.[1],
профессор кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
доктор юридических наук

Дмитренко А. П.[2],
профессор кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
доктор юридических наук, профессор

АКТУАЛЬНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ПОСЯГАТЕЛЬСТВ НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

В отличие от киберинцидентов, затрагивающих отдельных пользователей, компьютерные атаки на информационные инфраструктуры органов власти, коммерческих и иных организаций представляют особую общественную опасность. Это обусловлено рядом обстоятельств. Так, компьютерные атаки на медицинские организации при помощи шифровальщиков наглядно продемонстрировали насколько уязвима система здравоохранения перед современными киберугрозами. Согласно отчету Лаборатории Касперского за 2020 г. антивирусными решениями компании были зафиксированы атаки троянцами-шифровальщиками в отношении 123630 корпоративных пользователей и 15940 пользователей, связанных с малым и средним бизнесом [3].

В этом отношении своевременным и важным явилось принятие Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в соответствии с которым госучреждения и компании должны провести работу по оценке и категорированию своих информационных инфраструктур, обеспечить установленный стандартами уровень их программно-технической защиты, а также должны отчитываться об инцидентах уполномоченному ведомству и проходить оценку безопасности.

Федеральным законом от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и ст. 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» Уголовный кодекс Российской Федерации был дополнен ст. 274[1], предусматривающей ответственность за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации.

---

[1] © Русскевич Е. А., 2022.
[2] © Дмитренко А. П., 2022.

На настоящий момент правоприменительная практика по ст. 274[1] Уголовного кодекса Российской Федерации находится в стадии своего становления. Количество зарегистрированных случаев неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (далее по тексту – КИИ) невелико, хотя наблюдается их последовательный рост и расширение географии. По данным ФКУ «ГИАЦ МВД России» в 2018 г. было зарегистрировано лишь одно преступление, предусмотренное ст. 274[1] Уголовного кодекса Российской Федерации, в 2019 г. – 4, в 2020 г. – 22. За 2021 г. было зарегистрировано 159 преступлений.

Индивидуализирующим и по большому счету главным признаком состава преступления, предусмотренного ст. 274[1] Уголовного кодекса Российской Федерации, является предмет посягательства – объект критической информационной инфраструктуры Российской Федерации. Его легальное определение сформулировано в п. 7 ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ. Здесь сразу обращает на себя внимание то обстоятельство, что закон определяет не только объекты КИИ, но и отдельно выделяет *значимые* объекты – ресурсы, которым была в установленном порядке присвоена одна из категорий значимости и которые вследствие этого были включены в соответствующий реестр значимых объектов. Отечественный уголовный закон данную классификацию, как известно, не воспринял. С одной стороны, это позволяет сделать вывод о допустимости определения предмета ст. 274[1] Уголовного кодекса Российской Федерации в широком смысле, то есть как любой информационной системы, сети и т.п. субъектов КИИ. Однако такой подход нивелирует главную цель специального выделения ст. 274[1] Уголовного кодекса Российской Федерации – повысить ответственность за неправомерное воздействие на информационные ресурсы, обеспечивающие нормальное осуществление именно критических процессов [4, с. 853–855].

Объект критической информационной инфраструктуры как предмет преступления, предусмотренного ст. 274[1] Уголовного кодекса Российской Федерации, характеризуется двумя обязательными признаками: объективно-функциональным и формально-юридическим [2, с. 27–28]. Первый признак указывает на то, что конкретная информационная система, база данных и т. п. реально функционирует в одной из критически важных сфер государства (оборона, здравоохранение, транспорт, энергетика и т. д.). Суть формально-юридического признака заключается в том, что соответствующие автоматизированные системы управления приобретают статус объекта КИИ только после прохождения установленной законом процедуры. Понятно, что для применения ст. 274[1] Уголовного кодекса Российской Федерации вопрос о моменте получения соответствующей информационной системой статуса объекта КИИ имеет принципиальное значение.

Анализ материалов правоприменительной практики показывает, что, раскрывая признаки объекта КИИ, суды ссылаются на дату вынесения внутреннего акта организации [5]. В других случаях суды исходят из момента внесения соответствующих сведений в реестр значимых объектов КИИ: «…ПАО «ВымпелКом»

является субъектом критической информационной инфраструктуры Российской Федерации, которому на праве собственности принадлежит…в том числе база данных автоматизированной системы «Amdocs Ensemble», которая «дата» внесена Федеральной службой по техническому и экспортному контролю России в реестр значимых объектов критической информационной инфраструктуры Российской Федерации под регистрационным номером: 005491/1/4/А» [6].

Учитывая, что принятие решения комиссией субъекта КИИ имеет предварительный характер, полагаем, что объект КИИ возникает в правовом поле, в том числе как предмет преступного посягательства по смыслу ст. 274^1 Уголовного кодекса Российской Федерации, только с момента принятия решения ФСТЭК России. С учетом этого неправомерное воздействие на обеспечивающие критические процессы информационные системы, автоматизированные системы управления, базы данных и т. д., не прошедшие процедуру категорирования, необходимо квалифицировать в зависимости от обстоятельств содеянного по ст.ст. 272 или 274 Уголовного кодекса Российской Федерации.

В отдельных случаях правоприменители смешивают понятия субъекта (владельца и оператора) и объекта (информационной системы, базы данных) критической информационной инфраструктуры. По одному из дел в описании признаков субъективной стороны суд указал: «…Г., действуя умышленно, достоверно зная, что ПАО «Ростелеком» относится к объектам критической информационной инфраструктуры… осуществила неправомерный доступ к охраняемой компьютерной информации …в БД «Авалон» и хранящейся на защищенных сетевых ресурсах ПАО «Ростелеком» [7].

Определенные затруднения возникают в части толкования признаков компьютерной программы и компьютерной информации, заведомо предназначенных для совершения неправомерного воздействия на объекты КИИ, по смыслу ч. 1 ст. 274^1 Уголовного кодекса Российской Федерации. Следует сделать вывод, что предназначенность для воздействия на объект КИИ как признак ч. 1 ст. 274^1 Уголовного кодекса Российской Федерации имеет не программно-технический, а в большей мере функциональный характер, заключающийся в фактической применяемости программы в отношении объекта КИИ. Это обстоятельство и должен осознавать виновный на момент совершения соответствующих действий.

Отдельно необходимо указать, что не образует преступления, предусмотренного ч. 1 ст. 274^1 Уголовного кодекса Российской Федерации, использование и распространение вредоносной компьютерной программы для личных нужд (например, для тестирования эффективности средств программно-технической защиты), ее использование в образовательных или исследовательских целях, а равно во всех случаях, когда вредоносная компьютерная программа или информация не создают угрозы для автоматизированной обработки данных, нормального функционирования объектов КИИ.

Изучение материалов правоприменения выявляет разные подходы к квалификации неправомерного воздействия на объекты КИИ, совершаемые сотрудни-

ками организации. В отдельных случаях такие действия оцениваются как неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ, совершенный лицом с использованием своего служебного положения [8]. В других – как нарушение правил эксплуатации и (или) доступа [9].

Отграничение нарушения правил эксплуатации от неправомерного доступа к компьютерной информации, содержащейся в объекте КИИ, заключается именно в том, что, по справедливому замечанию Р. Р. Гайфутдинова, в первом случае у лица имеется доступ к соответствующим объектам информационно-коммуникационной инфраструктуры [1, с. 142]. При этом доступ правомерный, обусловленный, как правило, служебным положением лица. В тех ситуациях, когда сотрудник прекратил свои отношения с организацией-субъектом КИИ, однако потом воспользовался своими учетными данными, которые по тем или иным причинам еще не были аннулированы, для входа в личный кабинет и копирования, модификации либо уничтожения компьютерной информации, содеянное необходимо оценивать как неправомерный доступ [10].

Дискуссионным является толкование такого оценочного признака ст. 274^1 Уголовного кодекса Российской Федерации как вред, причиненный критической информационной инфраструктуре Российской Федерации. Изучение материалов правоприменительной практики выявляет следующие подходы в его определении: 1) вредом признаются последствия в виде копирования сведений, составляющих коммерческую тайну [11]; 2) вред определяется как нарушение безопасности информации, принадлежащей субъекту КИИ, а также дискредитация его деловой репутации [12]; 3) раскрывается как изменение конфигурации элементов информационной системы субъекта КИИ, нарушение процесса предоставления услуг связи абонентам [13]. Сразу следует указать, что крайне спорным является толкование вреда как ущерба, причиненного деловой репутации организации-субъекта КИИ. В ст. 274^1 Уголовного кодекса Российской Федерации говорится о причинении вреда именно объекту КИИ, а не иным правам и законным интересам организации-субъекта КИИ.

Полагаем, что при толковании вреда по смыслу ст. 274^1 Уголовного кодекса Российской Федерации следует исходить из понятия компьютерного инцидента, сформулированного п. 5 ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Руководствуясь таким подходом, под вредом следует понимать: 1) нарушение функционирования объекта критической информационной инфраструктуры; 2) прекращение функционирования объекта критической информационной инфраструктуры; 3) нарушение функционирования сети электросвязи, используемой для организации взаимодействия таких объектов; 4) прекращение функционирования сети электросвязи, используемой для организации взаимодействия таких объектов; 5) нарушение безопасности обрабатываемой таким объектом информации.

Список литературы

1. Гайфутдинов Р. Р. Понятие и квалификация преступлений против безопасности компьютерной информации : дис. … канд. юрид. наук. Казань, 2017. С. 142.

2. Русскевич Е. А., Чекунов И. Г. Квалификация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Уголовное право. 2022. № 5. С. 27–28.

3. Kaspersky Security Bulletin 2020. Статистика // URL : https://securelist.ru/-kaspersky-security-bulletin-2020-statistics/99505/.

4. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) / под ред. Н. Г. Кадникова. 6-е изд., перераб. и доп. М. : ИД «Юриспруденция», 2019. С. 853–855.

5. Приговор Ленинского районного суда г. Владивостока от 7 октября 2020 г. по делу № 1-366/2020.

6. Приговор Ленинского районного суда г. Иваново от 19 февраля 2021 г. по делу № 1-88/2021.

7. Приговор Ленинского районного суда г. Владивостока от 25 сентября 2019 г. по делу № 1-368/2019.

8. Приговор Краснооктябрьского районного суда г. Волгограда от 18 марта 2021 г. по делу № 1-108/2021.

9. Приговор Петушинского районного суда Владимирской области от 17 сентября 2021 г. по делу № 1-146/2021.

10. Приговор Советского районного суда г. Волгограда от 30 ноября 2020 г. по делу № 1-37/2021 (1-395/2020).

11. Приговор Центрального районного суда г. Волгограда от 7 декабря 2020 г. по делу № 1-339/2020.

12. Приговор Абаканского городского суда Республики Хакасия от 29 июля 2020 г. по делу № 1-805/2020.

13. Приговор Ленинского районного суда г. Владивостока от 7 октября 2020 г. по делу № 1-366/2020.

Шаталов А. С.[1]*,*
профессор кафедры уголовного процесса
Московской академии Следственного комитета
Российской Федерации,
доктор юридических наук

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Для сотрудников правоохранительных органов все большее и большее значение в деле выявления, раскрытия, расследования и предотвращения преступлений приобретают цифровые следы, предопределяя, таким образом, необходимость преумножения и применения ими комплекса компетенций, непосредственно связанных со сферой применения информационно-коммуникационных технологий. Уже сейчас в своей деятельности они активно используют передовые программно-аппаратные разработки, в целях фиксации противоправной деятельности и установления личности правонарушителей, а также фактов предоставления подложных или фальшивых документов на право доступа к информации, изменения адреса или кода технического устройства, нарушения средств или системы защиты информации, значимой для расследования конкретного уголовного дела и др. [9]. Высокий уровень криминалистической и компьютерной грамотности российских следователей, позволяет доказывать и пресекать факты использования правонарушителями анонимных сетей, зарубежных VPN-серверов и механизмов утечки и шифрования данных. Принимая во внимание особенности объектов, возникающих в сетевом информационном пространстве, криминалисты предлагают осуществлять постоянный мониторинг информационных ресурсов глобальных компьютерных сетей и разрабатывают для этого научные рекомендации [6].

Разумеется, все это вселяет определенный оптимизм в общее дело борьбы с преступностью вообще и киберпреступностью, в частности, но по разным причинам, не дает оснований для вывода о скорой победе над ней. Причиной стремительного роста киберпреступности и ее популярности как некого делинквентного бизнеса, прежде всего, является ее невероятная прибыльность, а сам процесс получения доходов, которые нередко исчисляются колоссальными суммами, обычно не отождествляется с риском разоблачения и наказания, в широком их понимании. Главная криминалистическая особенность киберпреступлений заключается в том, что их предотвращение, выявление, раскрытие и расследование невозможно без использования современных информационно-телекоммуникационных технологий. Соответственно этому возрастает необходимость подготовки специалистов для борьбы с такими преступлениями, пере-

[1] © Шаталов А. С., 2022.

подготовке действующих кадров, с тем чтобы эффективно разоблачать преступников, посредством обнаружения, фиксации, изъятия и использования разного рода «электронных» доказательств.

Сам процесс выявления, раскрытия и предварительного расследования преступлений, совершенных с использованием современных информационно-коммуникационных технологий, имеет ряд существенных особенностей. Ошибки, допускаемые при этом следователями, в большинстве своем связаны с изъянами в их профессиональной подготовке для этого сегмента криминалистической деятельности. Одной из наиболее существенных причин низкого качества предварительного расследования преступлений, совершаемых в киберпространстве, следует признать отсутствие качественных методических разработок, в реализации которых были бы задействованы самые современные информационно-коммуникационные технологии. В таких условиях объективные сложности, сопряженные с обнаружением, фиксацией и изъятием криминалистически значимой информации с целью ее дальнейшего использования в качестве доказательств по уголовному делу, нередко становятся непреодолимыми. Более того, здесь как нигде высока вероятность того, что те доказательства, которые все же были обнаружены, могут быть непреднамеренно изменены или утрачены, как в результате допущенных ошибок при их фиксации или, например, изъятии, так и в ходе их исследования и использования. Собирание в ходе досудебного производства по уголовному делу доказательств такого рода для дальнейшего представления их в суде, требует обязательного наличия не только основательной профессиональной подготовки, но и регулярного обновления имеющихся знаний не только у следователей, но и оперативных работников, специалистов и экспертов. Для решения этой задачи принимаются соответствующие решения, в том числе на государственном уровне.

Исходным документом, определившим направления развития информационного общества и подходы к его формированию в России, стала соответствующая Стратегия, рассчитанная на период 2017–2030 гг. [1]. Именно она положила начало повсеместному и интенсивному использованию органами государственной власти Российской Федерации, бизнесом и гражданами информационных и коммуникационных технологий. В ней впервые было сформулировано принципиальное положение об обеспечении государственной защиты интересов российских граждан в информационно-коммуникационной сфере. Важно отметить, что их защите, в частности, от разного рода преступных посягательств, в нашей стране всегда уделялось особое внимание. Это вполне естественно, поскольку правосудие может считаться свершившимся только тогда, когда при его отправлении удалось защитить права и законные интересы потерпевших от преступлений, на всех стадиях уголовного судопроизводства и без каких-либо исключений. С наступлением нового века все большее и большее влияние на практику защиты их прав и законных интересов стали оказывать стремительно меняющиеся способы анализа, передачи, получения и хранения данных, появившихся благодаря развитию современных информационно-коммуникационных технологий (Big Data, Blockchain и др.). Вместе с тем, с их появлением, задачи российского

уголовно-процессуального права не изменились. Как и право вообще, оно призвано «…создать такие универсальные механизмы, которые, во-первых, отражали бы общечеловеческие ценности; во-вторых, предлагали бы универсальные правовые способы разрешения социальных конфликтов (основная функция права), независимые от сугубо политических или иных соображений целесообразности; и, наконец, переходя на иной уровень обобщения, способствовали бы сохранению мира и человечности, то есть нашей *цивилизации права»* [5, с. 6].

Общий объем оцифрованных данных довольно велик и возрастает в буквальном смысле ежеминутно [8]. Целенаправленное и высокоскоростное исследование их многочисленных наборов с использованием искусственного интеллекта, позволяет обнаруживать новые корреляции вообще, а для целей полного, всестороннего, объективного предварительного расследования и справедливого судебного рассмотрения уголовных дел, в частности. Все это является не чем иным, как новым аспектом процессуальной коммуникации, цель которой состоит прежде всего в получении и передаче разнообразной криминалистически значимой информации. Особо отметим, что новизна нам видится отнюдь не в изменении сути процесса доказывания по уголовным делам, а в появившихся возможностях обогащения его содержания, вызванного принципиальным обновлением самих средств получения и передачи такой информации.

Включившись в процессы глобальной цифровизации, российское уголовно-процессуальное право должно активно и своевременно рефлексировать на происходящие изменения общественной жизни. В противном случае, регламентированные его нормами процессуальные процедуры, рано или поздно утратят свое рациональное содержание. Более того, стремительное и постоянное усиление требований к цифровым навыкам всех (в том числе потенциальных) участников уголовного судопроизводства может привести к непониманию языка, предназначенного для поддержания устойчивой социальной связи между ними.

Изменение структуры противоправных действий влечет за собой закономерные изменения в досудебном и судебном производстве по уголовным делам. Нельзя исключать, например, что когда-нибудь подготовка проектов промежуточных и итоговых решений в их рамках будет доверена именно искусственному интеллекту. Расширятся возможности аналогового и дистанционного участия в уголовном судопроизводстве неограниченного круга лиц, как следствие, действующие процессуальные процедуры будут адаптироваться к меняющимся цифровым реалиям, а взамен устаревших, появятся новые. С развитием технологий анализа материалов уголовных дел при помощи все того же искусственного интеллекта, появятся широкие возможности для мгновенного формирования криминалистических алгоритмов и программ предварительного расследования преступлений. Применяя их в практической деятельности, можно будет четко предвидеть не только оптимальный ход и реальный исход досудебного производства, но и наиболее вероятный итог судебного рассмотрения, оконченного расследованием уголовного дела. Неизбежность и осознание такой перспективы

влечет за собой обсуждение в юридическом сообществе адекватных мер по совершенствованию действующего уголовно-процессуального законодательства вообще и применения информационно-коммуникационных технологий, в частности. В активный дискурс имплементируются идеи об их использовании при производстве следственных и иных процессуальных действий [4, с. 17–23]; о внедрении в уголовном процессе наряду с бумажной, электронной формы документооборота [2, с. 155–163]; о полном изменении традиционного формата материалов уголовного дела на электронный [3, с. 728–751] и др.

Ресурс повышения качества уголовного судопроизводства, процессуалисты усматривают в налаживании более тесного взаимодействия государственных органов и населения через запуск единой защищенной онлайн-платформы, предлагая интегрировать в нее специальный оцифрованный сервис, максимально упрощающий процесс обращения граждан с сообщениями о совершенных и готовящихся преступлениях [7, с. 227–231]. Целесообразность создания и внедрения данной платформы последователи этой идеи видят не только в автоматизации процессов приема и регистрации таких сообщений, но и в определении направления их дальнейшего продвижения с использованием возможностей искусственного интеллекта, позволяющего при этом обеспечивать применение семантических нейронных сетей, компьютерного зрения, кластеризации данных и др. [10, с. 376–381].

Таким образом, использование в расследовании преступлений современных информационно-коммуникационных технологий – процесс длительный и необратимый. Он формирует дополнительные возможности для полноты, объективности и всесторонности процессуальной деятельности. В результате работа следователей сможет стать максимально эффективной и контролируемой не только руководителями соответствующих подразделений, но и заинтересованными лицами, вовлеченными в производство по уголовному делу. Ее информационная открытость позволит избежать дублирования и умышленного искажения поступивших сведений третьими лицами, неминуемо повлечет рост индекса доверия к ней со стороны гражданского общества. Как следствие, механизм доступа к правосудию станет еще более современным и в наивысшей степени безупречным.

Список литературы

1. Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. : утверждена Указом Президента Российской Федерации от 9 мая 2017 г. № 203. URL: https://base.garant.ru/71670570/.

2. Вилкова Т. Ю. Реализация конституционной обязанности государства обеспечить доступ к правосудию в условиях развития цифровых технологий // Актуальные проблемы российского права. 2020. Т. 15. № 8. С. 155–163.

3. Вилкова Т. Ю., Масленникова Л. Н. Законность и унификация в уголовном судопроизводстве: от бланков процессуальных документов – к электронному уголовному делу // Вестник Пермского университета. 2019. Вып. 46. С. 728–751.

4. Девяткин Г. С. Особенности организации допроса потерпевшего с использованием высоких технологий по уголовным делам, связанным с совершением киберпреступлений // Вестник военного права. 2021. № 1. С. 17–23.

5. Зорькин В. Д. Право будущего в эпоху цифр. Индивидуальная свобода или сильное государство? // Российская газета. Федеральный выпуск. 2020. № 83 (8137). С. 6. 16 апр.

6. Иванова А. А. Методика расследования незаконного изготовления, распространения и оборота порнографических материалов или предметов : автореф. дис. ... канд. юр. наук. Псков, 2011. 24 с.

7. Масленникова Л. Н. Электронная система взаимодействия государства с населением как фактор обеспечения доступа к правосудию в уголовном судопроизводстве // Следственный комитет Российской Федерации: второе десятилетие на службе Отечеству : сборник научных трудов / под общ. ред. А. М. Багмета. М. : Московская академия Следственного комитета Российской Федерации, 2019. С. 227–231.

8. Пржиленский В. И., Лаза В. Д. Коммуникативная теория общества: социально-технологические и правоприменительные контексты // Актуальные проблемы российского права. 2019. № 1 (98). С. 35–44.

9. Харина Э. Н. Киберпреступления: уголовно-правовой и криминалистический аспект // Вестник Университета имени О. Е. Кутафина. 2017. №5 (33). URL: http://cyberleninka.ru/article/n/kiberprestupleniya-ugolovno-pravovoy-i-kriminalisticheskiy-aspekt.

10. Tabolina K., Tabolin V. Prosecutor’s Supervision in Criminal Proceedings in the Context of the Leading Development of Digital Relations // Proceedings of the 6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019).: Atlantis Press, 2020. P. 376–381.

Яковлева Л. В.[1],
главный научный сотрудник
ФГКУ «ВНИИ МВД России»,
доктор юридических наук, доцент

УГОЛОВНО-ПРАВОВЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ ДЕСТРУКТИВНОМУ ПСИХОЛОГИЧЕСКОМУ ВОЗДЕЙСТВИЮ НА ЧЕЛОВЕКА

Меняющиеся реалии современного общества, все более широкое проникновение цифровых технологий в жизнь каждого человека несоизмеримо по сравнению даже с недавним прошлым увеличивают поток информации, которую необходимо воспринять, переработать, усвоить, т. е. сформировать свою позицию по поводу нее. Взаимодействие людей происходит путем обмена сведениями, поэтому перекрыть доступ к информации как таковой невозможно.

Каждый человек в зависимости от своих социальных установок, взглядов и интересов сам определяет, как оценить поступающую ему информацию – как полезную, нейтральную или вредоносную. К одной и той же информации подход разных людей бывает различен. Кому-то интересна история, кому-то география, а кто-то будет пытаться найти сведения о способах совершения преступлений.

В связи с тем, что часть информационного потока составляют данные негативного характера, государству, обществу, личности приходится искать способы противостояния не только огромному потоку информации, но и ограждать себя от того ее сегмента, который имеет деструктивный характер. Законодательными нормативными актами федерального уровня регулируются отношения в сфере информации, предусматривающие, в том числе, возможность ограничения или полного запрета информации определенного содержания или распространяемой с нарушением установленных предписаний [1].

В последние десятилетия все активнее разрабатывают вопросы, связанные с поиском наиболее эффективных путей противостояния информации, разрушительным образом влияющей не только на человека, но и на иные социальные институты, включая государство.

В научном обиходе появляется термин «деструктивное информационно-психологическое воздействие», под которым понимается «негативное влияние на личность, социальные группы и общество деструктивного контента или коммуникации, а также сигналов от технических устройств, дистанционно воздействующих на психику человека через зрительные и слуховые сенсорные системы, создающее опасность причинения вреда интересам личности, общества и государства» [2, с. 17]. Другие авторы именуют такого рода влияние «негативным информационно-психологическим воздействием», определяя его как «воздействие на психику и сознание человека, ведущие к неадекватному отражению окружающей действительности и, как следствие, изменению поведения» [3, с. 88], либо даже к деформации личности [4, с. 82].

---

[1] © Яковлева Л. В., 2022.

Несмотря на различные подходы в описании такого явления, как негативное (деструктивное) информационно-психологическое воздействий, в приведенных выше определениях прослеживаются общие черты. Главное, на что обращается внимание, это цель создания информации определенного содержания и доведения ее до человека любым способом. Для достижения этой цели используются различные ухищрения и технологии, позволяющие преподнести человеку нежелательную информацию в таком виде, который позволил бы поверить в ее правильность и объективность, вопреки собственной структуре и особенностям его потребностей, и принять навязываемые варианты поведения, рассматривая их как осознанный выбор. Посредством такого воздействия устанавливается контроль над сознанием человека.

Манипуляции с сознанием особенно опасны, если они осуществляются с применением информационно-телекоммуникационных технологий, позволяющих контролировать и направлять поведение значительных масс населения. «Отличаясь широкими возможностями воздействия на массовую аудиторию, они изменяют ее мнения, идеалы, картины мира, потребности и т. д. в необходимом для организатора (или организаторов) направлении. Именно так агрессивный коммуникатор, находясь на расстоянии от управляемой массовой аудитории (в том числе и за пределами национальных границ государства), обладает широким возможностями управления ее сознанием, а, следовательно, в значительной мере – и ее поведением» [5, с. 158].

Позитивному праву в противостоянии такого рода информации отводится первостепенная роль. За нарушение его норм устанавливается ответственность, вплоть до уголовной. С точки зрения предлагаемых в некоторых научных исследованиях классификаций подходов к обеспечению информационно-психологической безопасности личности положения Уголовного кодекса Российской Федерации (далее – УК РФ) следует относить к запрещающим подходам, предполагающим «введение более или менее масштабных императивных ограничений в отношении потребления субъектом или некоторым сообществом информации определенного типа» [6, с. 214], с определенными оговорками. Уголовный закон содержит ограничения и запреты не только и не столько в отношении стороны, получающей информацию. Прежде всего его цель заключается в ограждении человека от негативной информации и в привлечении к ответственности лиц, виновных в ее создании и распространении.

Негативное влияние на человека оказывают разного рода угрозы, представляющие собой психическое насилие над личностью. Обращая внимание на дискуссионность термина «психическое насилие», некоторые авторы приходят к выводу, что он наиболее полно отражает описываемый им феномен: «Из всех существующих терминов, для характеристики объективного криминального воздействия, наиболее приемлемым следует рассматривать понятие «психическое насилие», суть которого заключается в применении к потерпевшему насилия, имеющего признаки объективно демонстративного свойства, в самых разнообразных его формах: понуждение, шантаж, угроза и т. п.» [7, с. 78].

Сторонники иной точки зрения предлагают для обозначения такого рода манипуляций с человеком термин «нефизическое насилие» как вид воздействия, противоположный насилию, совершаемому путем применения к лицу насилия физического [8, с. 103–104]. По сути, оба термины равнозначны, поскольку служат для описания одних и тех же способов, и видов воздействия на психику человека.

В настоящее время в УК РФ включено около 100 преступлений, совершаемых путем психического насилия. Ряд авторов к ним справедливо относятся деяния, содержащие собственно угрозу (ст. 119 УК РФ и др.), а также принуждение (ст. 120 УК РФ и др.), шантаж (ст. 133 УК РФ и др.), издевательство (ст. 111 УК РФ и др.), оскорбление (ст. 297 УК Р Ф с др.), жестокое обращение (ст. 110 УК РФ и др.), унижение (ст. 282 УК РФ и др.), клевету (ст. 128.1 УК РФ и др.), причинение психических страданий (ст. 117 УК РФ) [9, с. 168–169]. Вместе с тем представляется, что этот перечень неполон, его необходимо дополнить деяниями, способом совершения которых выступает создание угрозы (ст. 267 УК РФ и др.).

По мнению других авторов, преступления, связанные с негативным информационным воздействием на человека, позволяют выявить угрозы информационно-психологической безопасности, которые предлагается делить на угрозы «а) контентные, связанные с распространением негативных (вредных) сведений в средствах массовой информации и иных источниках; б) коммуникационные, включающие деструктивное межличностное или групповое общение» [2, с. 17–18].

С приведенной типологизацией трудно согласиться. Выделение второго вида угроз, «коммуникационных», представляется надуманным. Автор искусственно разделяет форму и содержание. Между тем главным в информации является ее содержание, а не форма преподнесения воспринимающим ее лицам. Не случайно автору не удалось в основу предлагаемого им структурирования информационных угроз положить критерии, позволяющие избежать дублирования. В результате одни и те же сведения оказались включенными в обе группы. Это сведения, фальсифицирующие историю или оскверняющие историческую память; унижающие человеческое достоинство и др.

Очевидно, классифицировать запрещенную уголовным законом информацию достаточно по содержательной стороне.

Распространяется негативная информации в настоящее время в большинстве случаев путем использования информационно-телекоммуникационных технологий, включая различные мессенджеры и сеть Интернет. В связи с этим постоянно криминализируются деяния, совершаемые таким способом. Последние подобные изменения были внесены в ст.ст. 133, 242, 242.1 УК РФ.

Приоритет в этой сфере отдается уголовно-правовой охране интересов несовершеннолетних, которых справедливо рассматривают как наиболее сильно подверженную постороннему влиянию часть общества. «В силу особенностей развития психики, молодые люди являются наиболее уязвимой аудиторией для манипулирования, поскольку им свойственны повышенная внушаемость, некри-

тичность восприятия, склонность безусловно принимать установки и мнения, доминирующие в значимых для них группах, и в то же время отрицание традиционных ценностей и авторитетов, противоречивость и бунтарство» [10, с. 79].

Оценивая в целом степень защищенности человека от негативного информационно-психологического воздействия, следует признать ее достаточно высокой, хотя вряд ли существующие меры можно признать исчерпывающими.

Однако не вся деструктивно влияющая на психику человека информация, распространяемая в сети Интернет, рассматривается как требующая принятия уголовно-правовых мер. Так, в начале прошлого года активно обсуждалась необходимость дополнения УК РФ статьей, устанавливающей ответственность за демонстрацию сцен насилия в сети Интернет (за так называемые «треш-стримы») [11]. Постепенно дискуссия по данному вопросу прекратилась, а вопрос удалось решить путем мониторинга интернет-контента и своевременной блокировки тех сайтов, которые распространяют негативную информацию.

Вместе с тем поступательное развитие цифровых технологий неизбежно приводит к совершению новых видов общественно опасных деяний, которые необходимо криминализировать. В связи с этим УК РФ будет и впредь неизбежно дополняться нормами, в которых будет регламентироваться ответственность за совершение преступлений с использованием информационно-телекоммуникационных технологий.

Список литературы

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 30.12.2021) // Собрание законодательства Российской Федерации. 2006. № 31 (1 ч.). Ст. 3448.

2. Смирнов А. А. Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации : дис. … докт. юрид. наук. М., 2022.

3. Ежевская Т. И. Психологическое воздействие информационной среды на современного человека // Психопедагогика в правоохранительных органах. 2009. № 2 (37). С. 38–41.

4. Емелин В. А., Рассказова Е. И., Тхостов А. Ш. Психологические последствия развития информационных технологий // Национальный психологический журнал. 2012. № 1 (7). С. 81–87.

5. Карнаушенко Л. В. Деструктивное информационно-психологическое воздействие на массовую аудиторию: правовые аспекты противодействия // Вестник Краснодарского университета МВД России. 2017. № 2 (36). С. 157–161.

6. Краснянская Т. М., Тылец В. Г. Классификация угроз информационно-психологической безопасности личности и основные подходы к их преодолению // Вестник Дагестанского государственного университета. 2015. Т. 30. Вып. 4. С. 210–216.

7. Дайшутов М. М., Динека В. И., Денисенко М. В. Психическое насилие в уголовном праве // Вестник Московского университета МВД России. 2019. № 3. С. 77–81.

8. Круковский В. Е., Мосечкин И. Н. Нефизическое насилие в уголовном праве: понятие и признаки // Право. 2017. № 3. С. 89–104.

9. Круковский В. Е., Мосечкин И. Н. О формах нефизического (психологического) насилия в уголовном законодательстве России // Психология и право. 2020. Т. 10. № 1. С. 165–176.

10. Столяренко А. М., Сердюк Н. В., Вахнина В. В. и др. Психологические аспекты деструктивного информационно-психологического воздействия // Психология и право. 2019. Т. 9. № 4. С. 75–89.

11. Роскомнадзор поддержал введение уголовной ответственности для организаторов треш-стримов // ТАСС. 2021. URL: https://tass.ru/obschestvo/10513357.

Жилкин М. Г.[1],
начальник кафедры уголовного права и криминологии
Московского областного филиала
Московского университета МВД России
имени В.Я. Кикотя,
доктор юридических наук, доцент

Качалов В. В.[2],
заместитель начальника
Московского областного филиала
Московского университета МВД России
имени В.Я. Кикотя по учебной и научной работе,
кандидат юридических наук, доцент

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ВЗЯТОЧНИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

В современный период с развитием цифровых технологий преступность переходит на инновационные рельсы, используя для совершения запрещенных уголовным законом деяний высокотехнологичные инструменты, в частности криптовалюту. Последняя, являясь по выражению отдельных экспертов незаконным «денежным суррогатом» [1, с. 7–29], выступает как в качестве средства отдельных преступлений, так их предмета [2, с. 51–55]. Наиболее распространено применение криптовалюты при совершении криминальных сделок с наркотиками, незаконный оборот которых сегодня преимущественно осуществляется в онлайн формате. Вместе с тем, в последнее время в уголовно-правовой науке активно обсуждается вопрос о возможности признания криптовалюты предметом имущественных преступлений, и по мнению К. В. Ображиева «нет никаких препятствий для признания криптовалюты предметом хищения» [3, с. 71–87].

Таким образом, можно с уверенностью утверждать, что сегодня сформировалась определенная криминальная ниша из разных видов преступлений, где криптовалюта активно отвоевывает место, замещая собой привычные денежные средства или иное имущество.

К подобным преступлениям, с точки зрения механизма его совершения, может быть отнесено взяточничество криптовалютой. Здесь криптовалюта выступает своеобразным платежным средством за оказанные или подлежащие оказанию взяткополучателем услуги. Вместе с тем в отличие от группы преступлений, где криптовалюта находится, по сути, за пределами признаков состава преступления (наркооборот, торговля оружием и др.), при взяточничестве, для правильной и обоснованной квалификации, криптовалюта должна получить юридическую оценку в качестве предмета соответствующего преступления. И если, например, с момента установления самых первых фактов торговли наркотическими средствами за криптовалюту никому и в голову не могло прийти назвать

[1] © Жилкин М. Г., 2022.
[2] © Качалов В. В., 2022.

это непреступными действиями (из-за неопределенности статуса криптовалюты), то применительно к взяточничеству, напротив, часто отдельные представители науки и практические работники говорили (и все еще говорят) о не преступности таких действий именно из-за того, что российское законодательство криптовалюты непосредственно не регулирует, а Уголовный кодекс Российской Федерации соответствующие признаки прямо не предусматривает [4–5].

Это напоминает ситуацию с дискуссией о признании криптовалюты предметом имущественных преступлений. Однако, в отличие от преступлений против собственности, где есть конкретный потерпевший, который заинтересован в возбуждении и расследовании уголовного дела, взяточничество – это преступление без «потерпевших», в том смысле, что его участники заинтересованы в этом преступлении. Они скрывают факт его совершения, противодействуют расследованию, если о преступлении самостоятельно узнали правоохранительные органы и пр. В результате, с учетом дополнительных юридических и технических проблем выявление, раскрытие и расследование таких преступлений очень затруднено. Также отметим, что латентность криптовалютного взяточничества максимальна.

Уголовный кодекс Российской Федерации относит к задачам уголовного законодательства охрану от преступных посягательств и предупреждение преступлений. В связи с этим справедливым представляется замечание В. А. Петрова, что «если принять точку зрения о том, что криптовалюта не является имуществом и не может быть предметом преступного посягательства, в том числе и предметом взятки, то противодействие совершению такого рода преступлений будет приближаться к нулю» [6, с. 54–57].

Относительная анонимность финансовых транзакций с использованием криптовалют, трудность доказывания фактической принадлежности криптокошелька конкретному человеку, позволяют эффективно использовать их для дачи или получения взяток. При этом уже разработаны и продолжают разрабатываться криптовалюты, анонимность которых намного превосходит таковую у биткоинов, которые практические работники даже называют «прозрачной криптовалютой» [7, с. 45–49]. Более анонимными криптовалютами, например, являются: Monero, ZCash, PIVX, Komodo, Zcoin, NAV coin, ZenCash, Verge, DASH, SmartCash, BlackCoin и пр.

Преступники не ждут, пока законодатель урегулирует оборот криптовалют, а научные работники определятся с правилами квалификации. Криптовалюты уже сейчас активно используются для подкупа должностных лиц. Не случайно в российском сегменте интернета можно встретить «просветительские» статьи типа «Как брать взятку в Bitcoin. Краткое пособие» или «Безопасная взятка. Как правильно дать и взять взятку», в которых содержится информация, пропагандирующая и поощряющая взяточничество, раскрываются принципы предложения взяток, получения взяток, способы передачи денег или какого-либо имущества, рекомендации, как избежать уголовной ответственности, а также преимущества получения взяток в биткоинах для «правоохранителей и чиновников» [8].

Но, как было отмечено выше, факты использования криптовалюты для подкупа должностных лиц уже существуют, и уголовно-правовую оценку им надо давать сейчас, а не откладывать ее до 2024 г.

В настоящее время, с учетом системного толкования российского законодательства, криптовалюты следует признавать предметом получения взятки по признаку «иное имущество». Такой подход в целом отвечает и судебной практике отнесения криптовалют к предмету преступлений против собственности и нашим представлениям о месте криптовалюты в системе объектов гражданского права. Даже если криптовалюты будут как-то регулироваться российским законодательством (причем не важно, как именно: признают ли их деньгами, иным имуществом или полностью запретят), а такие призывы регулярно звучат и соответствующие законопроекты периодически разрабатываются и представляются общественности, это не повлияет на фактическую возможность криптовалют выступать эквивалентом стоимости товаров и услуг, не будет препятствием для незаконного оборота криптовалют (в том числе и в коррупционных отношениях), и не повлияет на возможность их квалификации в качестве предмета взятки.

Между тем, правоохранительные органы не ждут решения проблем признания криптовалюты предметом преступления в научной или законодательной плоскости и принимают решения, исходя из фактически складывающихся отношений.

Так, за вымогательство взятки в размере 4,8 биткоина эквивалентных сумме 1 млн долл. Вторым Западным окружным военным судом 26 февраля 2021 г. были осуждены по ч. 6 ст. 290 Уголовного кодекса Российской Федерации бывшие следователи ФСБ России Б. и К. к 9 и 12 годам колонии строгого режима. Полученные преступниками биткоины были конфискованы в доход государства [9]. Дело направлено 15 марта 2022 г. в вышестоящий суд для рассмотрения в апелляционном порядке [10].

Первый из известных нам приговоров по делу, связанному с получением взятки криптовалютой, утвержденный в апелляционной инстанции вынесен Верховным Судом Республики Хакасия 22 сентября 2020 г. в отношении бывшего начальника отдела Управления по контролю за оборотом наркотиков по обвинению в получении взятки в значительном размере за совершение незаконных действий в интересах взяткодателя путем перечисления на его биткоин-кошелек двумя транзакциями криптовалюты в качестве взятки в размере 0,10434405 биткоина и 0,08979916 биткоина, эквивалентном сумме 50 тыс. руб. [11].

О том, что «судебная практика по уголовным делам идет по пути признания криптовалюты имуществом, т. е. предметом взятки», говорит и Генеральный прокурор Российской Федерации И. Краснов. Вместе с тем далее он отмечает, что «все-таки нельзя признать это достаточным обстоятельством для формирования единого и устойчивого правоприменения. Как полагаю, этому должно способствовать введение понятия криптовалют и иных виртуальных активов в уголовно-правовое пространство посредством закрепления соответствующих норм

в законодательстве. Тем более, что применительно к его отдельным отраслям такие решения уже реализованы» [12].

В соответствии с п. 10 Постановления по делам о взяточничестве «получение и дача взятки… считаются оконченными с момента принятия должностным лицом… хотя бы части передаваемых ему ценностей (например, с момента передачи их лично должностному лицу, зачисления с согласия должностного лица на указанный им счет, «электронный кошелек»). При этом не имеет значения, получили ли указанные лица реальную возможность пользоваться или распоряжаться переданными им ценностями по своему усмотрению. Как оконченное преступление следует квалифицировать получение и дачу взятки в случае, когда, согласно предварительной договоренности, взяткодатель помещает ценности в условленное место, к которому у взяткополучателя имеется доступ либо доступ обеспечивается взяткодателем или иным лицом после помещения ценностей».

Таким образом, получение в качестве взятки криптовалюты следует признавать оконченным преступлением с момента, когда у должностного лица появилась реальная возможность этой криптовалютой воспользоваться или распорядиться по своему усмотрению: поступление криптовалюты в кошелек должностного лица, передача должностному лицу физического носителя с холодным криптокошельком, передача в любой форме (на носителях, посредством QR-кода, NFC-метки и пр.) реквизитов доступа к горячему криптокошельку и т. п. Соответственно, нет необходимости ждать, когда должностное лицо конвертирует криптовалюту в фиатные деньги или приобретет на нее какие-либо товары, оплатит работы или услуги.

В соответствии с п. 9 Постановления по делам о взяточничестве «переданное в качестве взятки… имущество, оказанные услуги имущественного характера или предоставленные имущественные права должны получить денежную оценку на основании представленных сторонами доказательств, в том числе, при необходимости, с учетом заключения специалиста или эксперта». У криптовалют нет какого-либо официального курса, и они отличаются большой волатильностью. Представляется, что именно заключение специалиста или эксперта будет играть основную роль при определении конкретного размера взятки криптовалютой. В свою очередь, указанные лица могут руководствоваться, например, усредненными курсами различных криптобирж на момент совершения преступления, а также оговоренный сторонами взяточничества размер эквивалента в фиатных валютах. При этом суд должен принимать наименьший из установленных показателей стоимости криптовалюты, приведенный в заключении эксперта за конкретный период [13].

Точное установление суммы взятки важно не только для правильной квалификации взяточничества, но и для назначения наказания, так как санкции соответствующих статей Уголовного кодекса Российской Федерации предусматривают возможность назначения кратных штрафов.

Список литературы

1. Суханов Е. А. О гражданско-правовой природе цифрового имущества // Вестник гражданского права. 2021. № 6. С. 7–29.

2. Лопатина Т. М. Криптовалюта как объективный признак состава легализации (отмывания) денежных средств или иного имущества, добытого преступным путем // Российский следователь. 2022. № 2. С. 51–55.

3. Ображиев К. В. Преступные посягательства на цифровые финансовые активы и цифровую валюту: проблемы квалификации и законодательной регламентации // Журнал российского права. 2022. № 2. С. 71–87.

4. Ермолович Е. Н. О коррупционных и должностных преступлениях должностных лиц и сотрудников организаций ОПК // Оборонно-промышленный комплекс: вопросы права. 2020. № 2. С. 62–72.

5. Ильяшенко Е. А. О перспективах привлечения к уголовной ответственности за использование криптовалют в преступных целях // Российский следователь. 2018. № 8. С. 51–54.

6. Петров В. А. Квалификация действий лиц, совершающих преступления с использованием криптовалюты на территории Российской Федерации // Российский следователь. 2018. № 4. С. 54–57.

7. Долгиева М. М. Конфискация криптовалюты // Законность. 2018. № 11. С. 45–49.

8. Решение Всеволожского городского суда Ленинградской области от 14 марта 2017 г. по делу № 2-1364/2017(2-8091/2016;)-М-7668/16 ; Решение Центрального районного суда г. Оренбурга от 20 мая 2019 г. по делу № 2А-2882/2019 ; Решение Ленинского районного суда г. Чебоксары от 15 мая 2019 г. по делу № 2а-2309/2019 // СПС «КонсультантПлюс».

9. Суд вынес приговор в отношении А. Колбова и С. Белоусова – 2-й Западный окружной военный суд // URL: http://2zovs.msk.sudrf.ru/modules.php?name=press_dep&op=1&did=907.

10. Приговор по делу № 1-7/2021 (1-141/2020). URL: https://2zovs--msk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=954862&case_uid=d4250b4d-b701-4896-a402947f26763690&delo_id=1540006.

11. Определение Пятого апелляционного суда общей юрисдикции от 12 марта 2021 по делу № 55-15/2021 (55-768/2020;) // URL: https://5ap.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=888491&case_uid=87f73e01-1da2-471e-856f-c7e4d5233ca8&result=1&delo_id=4&new=4.

12. Интервью Генерального прокурора Российской Федерации Игоря Краснова РИА «Новости». URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=67360817.

13. Филатова М. А. Проблема установления размера и ущерба при квалификации посягательства на цифровую валюту // Уголовное право. 2022. № 1. С. 71.

Борисов С. В.[1],
профессор кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
доктор юридических наук, доцент

Чугунов А. А.[2],
заместитель начальника
кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент

АКТУАЛЬНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В современных условиях информационно-коммуникационные технологии активно используются в процессе приготовления к различным преступлениям террористической и экстремистской направленности, а также в ходе их дальнейшего совершения, например, для обучения будущих террористов, вовлечения в ряды террористических и экстремистских сообществ или организаций новых участников, взаимодействия между ними и для осуществления других действий организационного характера. Полагаем, что в общей структуре таких преступных посягательств следует обратить особое внимание на общественно опасные деяния, предусмотренные ст.ст. 205^2, 280, 280^1 и 282 Уголовного кодекса Российской Федерации (далее – УК РФ), преимущественно совершаемые с использованием таких технологий, что учтено в качестве конститутивного или квалифицирующего признака соответствующих составов преступлений.

В диспозиции ч. 1 ст. 205^2 УК РФ указаны такие альтернативные общественно опасные действия, как публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма, пропаганда терроризма. При этом понятия двух последних видов общественно опасных действий, равно как и понятие террористической деятельности, определены непосредственно в примечаниях к ст. 205^2 УК РФ, что, на наш взгляд, способствует обеспечению правовой определенности соответствующих положений уголовного закона [1].

Так, согласно п. 1 примечаний к ст. 205^2 УК РФ публичное оправдание терроризма определено как «…публичное заявление о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании», тогда как пропаганда терроризма, как следует из п. 1^1 этих примечаний,

---

[1] © Борисов С. В., 2022.
[2] © Чугунов А. А, 2022.

представляет собой деятельность, заключающуюся в распространении «…материалов и (или) информации, направленных на формирование у лица идеологии терроризма, убежденности в ее привлекательности либо представления о допустимости осуществления террористической деятельности». Следовательно, оправдание терроризма, наказуемое по ст. 205^2 УК РФ, во всех случаях должно характеризоваться публичностью, предполагающей обращение виновного к широкому, неограниченному кругу лиц, и состоять в открытом заявлении о правильности террористических практики и идеологии, тогда как пропаганда терроризма может быть как публичной, так скрытой, адресной, при этом она всегда ориентирована на конкретные лицо или группу лиц, сознание которых подвергается различного рода воздействию, имеющему определенную цель – сформировать у них мировоззрение, принимающее как соответствующую идеологию, так и ее воплощение в террористической деятельности. При этом понятие такой деятельности раскрыто в п. 2 примечаний к ст. 205^2 УК РФ через указание перечня преступлений террористической направленности, образующих объем этого понятия, тогда как в ст. 280 УК РФ определение экстремистской деятельности не приводится, что ориентирует правоприменителя на ее определение, содержащееся в п. 1 ст. 1 Федерального закона «О противодействии экстремистской деятельности». Между тем, последнее обстоятельство создает предпосылки для привлечения к уголовной ответственности за публичные призывы к осуществлению не только преступлений, но и (или) административных правонарушений экстремистской направленности, например, к публичному демонстрированию нацистской атрибутики или символики, что, на наш взгляд, не в полной мере согласуется с задачами и принципами уголовного законодательства.

В ч. 1 ст. 280 УК РФ речь идет о публичных призывах к осуществлению экстремистской деятельности в той ее части, которая не охватывается ст. 205^2 УК РФ, а в ст. 280^1 УК РФ – о публичных призывах к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации, если те действия, к которым призывает виновный, не относятся к разновидностям террористической деятельности, например, к вооруженному мятежу или к захвату власти. Соответствующие призывы, как показывает изучение судебной практики, как правило, опираются на террористическую или иную экстремистскую идеологию, которую виновные пытаются распространить среди других людей, навязать ее им, тогда как преступления, предусмотренные ст. 282 УК РФ, во всех случаях направлены на формирование у других лиц мотивов национальной, религиозной или иной ненависти либо вражды, а равно на унижение их человеческого достоинства по тем же признакам.

На практике важно учитывать, что указанные выше уголовно-правовые нормы не поглощают друг друга при квалификации содеянного, содержащего признаки двух или более различных составов преступлений, связанных с распространением экстремистской идеологии. Например, виновные лица одновременно либо в разное время могут призывать к осуществлению террористической и иной экстремистской деятельности, что предполагает квалификацию таких действий

с учетом совокупности преступлений, предусмотренных ст.ст. 205^2 и 280 УК РФ.

Так, С. был признан виновным в размещении с целью ознакомления неограниченного круга лиц на личной странице в сети Интернет, свободной для общего доступа, видеофайлов с записью призывов к осуществлению террористической деятельности и оправдания терроризма, а также призывов к осуществлению экстремистской деятельности, которые стали доступны пользователям социальной сети. Его действия были квалифицированы по совокупности преступлений, предусмотренных ст.ст. 205^2 и 280 УК РФ [2].

Отметим, что С. М. Кочои выделяет понятие «идеологический экстремизм» («экстремизм в сфере идеологии»), характеризующееся такими формами проявления, как публичное оправдание терроризма и иная террористическая деятельность; возбуждение социальной, расовой, национальной либо религиозной розни; пропаганда исключительности, превосходства или неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, изготовление таковых или хранение в целях массового распространения; публичное заведомо ложное обвинение лица, замещающего государственную должность на Российской Федерации или ее субъекта, в совершении им в период исполнения своих должностных обязанностей уголовно наказуемых деяний, относящихся к экстремистской деятельности; совершение преступлений экстремистской направленности [3, с. 117–122]. Как видим, данный автор при определении объема понятия идеологического экстремизма (экстремизма в сфере идеологии) указывает как уголовно, так и административно наказуемые деяния, причем отдельные из них, на наш взгляд, не связаны ни с формированием, ни с распространением экстремистской идеологии (например, в случае совершения клеветы в отношении должностного лица). Вместе с тем понятие идеологического экстремизма (экстремизма в сфере идеологии) заслуживает внимания, поскольку в современных условиях оно отражает сущность значительной части экстремистских проявлений, направленных и (или) сопряженных с распространением соответствующих идей и взглядов в обществе.

Как следует из приводимой ниже таблицы 1, содержащей статистические данные Судебного департамента при Верховном Суде Российской Федерации [4], наиболее распространенным в исследуемой группе деяний в последние три года являются преступления, предусмотренные ст.ст. 205^2 и 280 УК РФ, заключающиеся соответственно в публичных призывах к осуществлению террористической деятельности, публичном оправдании терроризма или в его пропаганде, а равно в публичных призывах к осуществлению экстремистской деятельности. Также в таблице наглядно представлено, что после введения в декабре 2018 г. административной преюдиции в ч. 1 ст. 282 УК РФ в качестве криминообразующего признака публичных действий, направленных на возбуждение ненависти, вражды, а равно на унижение человеческого достоинства, совершенных без квалифицирующих обстоятельств, предусмотренных в ч. 2 данной статьи [5], число

осужденных за это преступление сократилась более чем в 14 раз. В конце 2020 г. административная преюдиция также была введена в состав преступления в виде публичных призывов к осуществлению действий, направленных на нарушение территориальной целостности России [6], что, как представляется, сведет к минимуму применение ст. 280[1] УК РФ. Одновременно обратим внимание на заметное увеличение в 2021 г. числа осужденных за преступления, предусмотренные ст.ст. 205[2], 280 и 282 УК РФ, при этом особо отметим значительный рост судимости за публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма, пропаганду терроризма (в 2021 г. число таких осужденных увеличилось более чем в 5 раз), что в сегодняшних условиях может указывать на намечающуюся тенденцию.

Таблица 1

Статья УК РФ и ее части	Число осужденных лиц (по основной и дополнительной квалификации преступления)					
	2016	2017	2018	2019	2020	2021
статья 205[2]	55	96	130	126	47	241
часть 1	51	81	68	57	22	46
часть 2	4	15	52	69	25	195
статья 280	143	170	159	145	184	307
часть 1	42	30	19	13	20	30
часть 2	101	140	140	132	164	277
статья 280[1]	3	8	10	4	4	2
часть 1	0	0	3	1	0	1
часть 2	3	8	7	3	4	1
статья 282	502	571	518	36	18	50
часть 1	482	562	505	23	7	22
часть 2	20	9	13	13	11	28
Всего	703	845	817	311	253	600

Сравнительный анализ данных уголовно-правовых норм позволяет сделать вывод об отсутствии системности в регламентации ответственности за распространение террористической и иной экстремистской идеологии. Так, в ст. 205[2] УК РФ предусмотрены три сходных, но тем не менее различающиеся формы распространения террористической идеологии: 1) публичные призывы к осуществлению террористической деятельности; 2) публичное оправдание терроризма; 3) пропаганда терроризма. Применительно же к иной экстремистской идеологии законодатель предусмотрел только две уголовно-наказуемые формы ее распространения: 1) публичные призывы к осуществлению экстремисткой деятельности либо действий, направленных на нарушение территориальной целостности Российской Федерации (ст.ст. 280 и 280[1] УК РФ); 2) публичные действия, направленные на возбуждение ненависти либо вражды, а равно на унижение достоинства человека или группы лиц по признакам пола, расы, национальности,

языка, происхождения, отношения к религии, принадлежности к какой-либо социальной группе.

По нашему мнению, наиболее полно возможные формы распространения опасной идеологии учтены именно в ст. 205^2 УК РФ, в связи с чем примененный здесь подход целесообразно применить и к регламентации ответственности за распространение не только террористической, но и иной экстремистской идеологии, в том числе рассмотреть вопрос о возможности признания ст. 282 УК РФ утратившей силу. Последнее предложение обосновывается тем, что содержание ст. 282 УК РФ не в полной мере соответствует требованиям правовой определенности и системности уголовно-правовой охраны однородных общественных отношений.

Отметим, что для формирования практики применения рассматриваемых уголовно-правовых норм большое значение имеют разъяснения Пленума Верховного Суда Российской Федерации, содержащиеся в постановлениях от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» [7] и от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» [8]. При этом особо выделим изменения и дополнения, внесенные в первое из данных постановлений Пленума Верховного Суда Российской Федерации в 2018 [9] и 2021 [10] гг., направленные на исключение избыточного применения ст.ст. 280, 280^1, 282 и 282^2 УК РФ, в том числе с учетом возможной малозначительности соответствующих деяний [11]. Среди таких изменений и дополнений выделим те, что в наибольшей степени способствуют исключению необоснованного привлечения к уголовной ответственности за деяния, так или иначе связанные с распространением экстремистской идеологии.

Во-первых, Пленум Верховного Суда Российской Федерации обратил внимание правоприменителей на то, что уже на момент возбуждения уголовного дела должны быть установлены достаточные данные, указывающие на признаки соответствующих преступлений, в том числе на их субъективную сторону. В частности, применительно к деяниям, наказуемым по ст.ст. 280, 280^1, 282 УК РФ, следует устанавливать не только сведения о размещении в сети «Интернет» или иной информационно-телекоммуникационной сети текста, изображения, аудио- или видеофайла, которые содержат признаки призывов к осуществлению экстремистской деятельности или действий, направленных на нарушение территориальной целостности России, возбуждения ненависти либо вражды, унижения достоинства человека либо группы лиц, но и иные сведения, подтверждающие общественную опасность деяния, включая направленность умысла и мотив совершения таких действий.

Во-вторых, в продолжение предыдущего разъяснения Пленум Верховного Суда Российской Федерации подчеркнул, что преступления, предусмотренные ст.ст. 280, 280^1, 282 УК РФ, могут быть совершены исключительно с прямым умыслом и с намерением побудить других лиц к осуществлению экстремистской деятельности, совершению действий, направленных на нарушение территориальной целостности России, либо с целью возбудить ненависть либо вражду,

унизить достоинство человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, принадлежности к какой-либо социальной группе.

При этом особо оговаривается ситуация, когда лицо размещает в информационно-телекоммуникационной сети информацию, которая ранее была признана судом экстремистским материалом, что может быть квалифицировано по ст. 280, ст. 280^1 или ст. 282 УК РФ лишь при условии установления осознания лицом, разместившим этот материал, направленности его действий на нарушение основ конституционного строя, а также его намерения побудить других лиц к осуществлению экстремистской деятельности, совершению действий, направленных на нарушение территориальной целостности Российской Федерации, либо цель возбудить ненависть или вражду, унизить достоинство человека или группы лиц по указанным признакам. Для установления прямого умысла, а также указанных намерений и цели необходимо учитывать всю совокупность обстоятельств, характеризующих содеянное, включая сведения о деятельности соответствующего лица до и после того, как оно разместило информацию, в частности, о его действиях по увеличению количества просмотров и числа пользователей; о личности этого лица (например, о его приверженности радикальной идеологии, участии в экстремистских объединениях и т. п.); об объеме соответствующей информации, частоте и продолжительность ее размещения, интенсивности обновлений.

В-третьих, Пленумом Верховного Суда Российской Федерации обращено внимание судов на особенности практики применения ст. 282^2 УК РФ, в том числе на необходимость установления обстоятельств, подтверждающих совершение обвиняемым конкретных действий и раскрывающих их значение для продолжения или возобновления деятельности экстремистской организации, а также указывающих на мотивы, которыми руководствовалось это лицо при совершении соответствующих действий. При этом действия лиц, не связанные с продолжением или возобновлением деятельности экстремистской организации и заключающиеся только в реализации своего конституционного права на свободу совести и свободу вероисповедания, например, путем индивидуального или совместного исповедования религии, совершения богослужений или других религиозных обрядов и церемоний, при отсутствии признаков экстремизма, не рассматриваются в качестве преступления, предусмотренного ч. 2 ст. 282^2 УК РФ (участие в экстремистской организации). Полагаем, что эти разъяснения имеют большое значение для исключения избыточной уголовно-правовой репрессии в тех случаях, когда правомерное поведение граждан хотя и соприкасается с деятельностью экстремистских объединений, являющихся основными центрами формирования и распространения соответствующей идеологии, но не становится ее частью, не приобретает качества, присущие экстремизму.

В-четвертых, не менее важным является и разъяснение о том, что заключение эксперта по делам о преступлениях экстремистской направленности не должно иметь заранее установленной силы и предопределять выводы о виновности лица

в совершении инкриминируемого деяния, поскольку таковые входят в исключительную компетенцию суда, которому надлежит основывать свои решения на совокупности тщательно исследованных доказательств. При этом подчеркивается, что заключение эксперта не обладает преимуществом перед другими доказательствами и, как все другие доказательства, должно оцениваться по общим правилам в совокупности с другими доказательствами [12].

Считаем, что в настоящее время назрела необходимость внесения сходных изменений и дополнений в постановление Пленума от 9 февраля 2012 г. № 1, в котором также целесообразно разъяснить особенности применения ст. 205^2 УК РФ в части квалификации содеянного в качестве пропаганды терроризма, тем более что определенные позиции по данному вопросу уже сформированы в решениях по конкретным уголовным делам.

Например, по одному из таких дел суд на основе анализа законодательного определения пропаганды терроризма, содержащегося в п. 1^1 примечаний к ст. 205^2 УК РФ, посчитал, что такая пропаганда не требует установления признака публичности совершенных действия, в отличие от публичных призывов к осуществлению террористической деятельности и публичного оправдания терроризма, при этом уголовная ответственность за пропаганду терроризма имеет место и в тех случаях, когда соответствующие действия направлены на идей и взглядов, относящихся к террористической идеологии, даже у одного человека. Кроме того, пропаганда терроризма направлена на тех лиц, у которых еще не сформированы такая идеология и убежденность в ее привлекательности, а также отсутствует представление о допустимости осуществления террористической деятельности. Именно в наличии возможности изменить мировоззрение лиц, на которых ориентирована пропаганда терроризма, состоит общественная опасность этого деяния. Соответственно, те лица, у которых указанная идеология уже сформировалась, имеются убеждение в ее привлекательности и представление о допустимости осуществления террористической деятельности, не могут признаваться участниками рассматриваемых правоотношений, так как соответствующая система взглядов и идей у них сформирована ранее и на этот процесс никоим образом не повлияло лицо, распространяющее террористическую идеологию в их присутствии либо в условиях возможного восприятия ими таких действий [13].

В заключение отметим, что распространение террористической и иной экстремистской идеологии в современных условиях таит в себе все более увеличивающуюся общественную опасность, в особенности при совершении соответствующих противоправных действий с использованием информационно-коммуникационных технологий в целях побуждения неограниченного круга лиц к различным насильственным преступным деяниям. Также повышение уровня общественной опасности таких действий обусловливается ростом геополитической напряженности и сопутствующими негативными социальными явлениями, в том числе эскалацией дискриминации и насилия по мотивам национальной, религиозной, политической и иной ненависти и вражды.

Имеющиеся уголовно-правовые средства противодействия соответствующим деяниям нуждаются в совершенствовании, при этом их дальнейшее развитие целесообразно выстраивать на основе доктринально обоснованных предложений и рекомендаций, в частности, учитывающих требования системности и правовой определенности положений уголовного законодательства, а также необходимости формирования правильной и единообразной правоприменительной практики.

Список литературы

1. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) / под ред. Н. Г. Кадникова. 6-е изд., перераб. и доп. М. : ИД «Юриспруденция», 2019. С. 589–560.

2. Обзор судебной практики Верховного Суда Российской Федерации № 2 (2019) : утвержден Президиумом Верховного Суда Российской Федерации 17 июля 2019 г. // Бюллетень Верховного Суда Российской Федерации. 2020. № 2.

3. Кочои С. М. Уголовно-правовое противодействие идеологическому экстремизму // Журнал российского права. 2021. № 11. С. 117–122.

4. Сайт Судебного департамента при Верховном Суде Российской Федерации. URL: http://www.cdep.ru/.

5. Федеральный закон от 27 декабря 2018 г. № 519-ФЗ «О внесении изменения в статью 282 Уголовного кодекса Российской Федерации» // Собрание законодательства Российской Федерации. 2018. № 53 (ч. I). Ст. 8445.

6. Федеральный закон от 8 декабря 2020 г. № 425-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 30 и 31 Уголовно-процессуального кодекса Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 50 (ч. III). Ст. 8070.

7. Постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (ред. от 28.10.2021) // Сайт Верховного Суда Российской Федерации. URL: http://www.vsrf.ru/.

8. Постановление Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» (ред. от 03.11.2016) // Сайт Верховного Суда Российской Федерации. URL: http://www.vsrf.ru.

9. Постановление Пленума Верховного Суда Российской Федерации от 20 сентября 2018 г. № 32 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // Бюллетень Верховного Суда Российской Федерации. 2018. № 11.

10. Постановление Пленума Верховного Суда Российской Федерации от 28 октября 2021 г. № 32 «О внесении изменений в некоторые постановления Пленума Верховного Суда Российской Федерации по уголовным делам» // Бюллетень Верховного Суда Российской Федерации. 2021. № 12.

11. Зателепин О. К., Борисов С. В. Новые позиции Пленума Верховного Суда Российской Федерации по уголовным делам о преступлениях экстремистской направленности // Уголовный процесс. 2018. № 11. С. 24-33 ; Пейсикова Е. В., Борисов С. В. Новые позиции Пленума Верховного Суда Российской Федерации об освобождении от наказания и уголовной ответственности // Уголовный процесс. 2022. № 2. С. 72–74.

12. Андрюхин Н. Г., Борисов С. В. Предпосылки, содержание и значение новых разъяснений Пленума Верховного Суда Российской Федерации о квалификации и доказывании преступлений экстремистской направленности, совершаемых с использованием сети Интернет // Вестник Московского университета МВД России. 2019. № 4. С. 70.

13. Обзор судебной практики Верховного Суда Российской Федерации № 3 (2019) : утвержден Президиумом Верховного Суда Российской Федерации 27 ноября 2019 г. // Бюллетень Верховного Суда Российской Федерации. 2020. № 4.

Кужиков В. Н.[1],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент

Габдрахманов Р. Л.[2],
профессор кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент

ПРОТИВОДЕЙСТВИЕ ЛЕГАЛИЗАЦИИ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Эволюция законодательства во многом зависит от появления новых видов преступлений. В свою очередь совершение преступлений взаимосвязано, со следствием развития производственно-технической сферы общества, которое создает новые возможности для совершения общественно-опасных деяний. В современных условиях одним из важных факторов, влияющих на совершение преступлений в стране и в мире, вне всякого сомнения, является цифровизация практически всех сторон жизни общества, резкое возрастание объемов информации, стремительное развитие новых технологий. Такое положение вещей является новым вызовом для государственных структур и применения правовых мер для адекватной реакции в сложившейся ситуации по защите законных интересов субъектов правоотношений.

С учетом таких кардинальных преобразований 9 мая 2017 г. был принят Указ Президента Российской Федерации № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [1]. В развитие этой стратегии 28 июля 2017 г. Правительством Российской Федерации № 1632-р была утверждена программа «Цифровая экономика Российской Федерации» [2].

На сегодняшний день чтобы повысить конкурентоспособность на мировом рынке все страны мира занимаются цифровизацией многих сфер деятельности. Эту мировую тенденцию необходимо реализовать и на территории Российской Федерации, как одно из неизбежных ключевых направлений экономической политики, если мы хотим успешно развиваться и конкурировать с другими передовыми странами [3, с. 45].

В целом можно сказать, что цифровая экономика представляет с собой такую организацию экономической деятельности, различных видов сделок и взаимодействия со многими другими сферами деятельности, когда отношения возникают с помощью информационных и коммуникационных технологий (ИКТ).

---

[1] © Кужиков В. Н., 2022.

[2] © Габдрахманов Р. Л., 2022.

В итоге происходит очередная индустриальная революция, когда ИКТ позволяют взаимодействовать между физической и цифровой реальностью. Уже на данном этапе развития цифровая экономика выходит за пределы простой автоматизации процессов или сети Интернет и включает в себя продвинутую аналитику, беспроводные сети, мобильные девайсы, социальные медиа, Интернет вещей (IoT), Big Data и массу других новых технологий. Такое глобальное явление приводит к кардинальным изменениям работы государственных структур, в деятельности предпринимателей, общественных организаций, граждан и т. д.

С учетом цифровизации экономики преступным элементам предоставляются масштабные возможности для совершения легализации доходов, полученных преступным путем. Современные технологии позволяют осуществлять незаконные транзакции с банковскими операциями, и повышать анонимность осуществления таких действий.

В соответствии со ст. 5 Федерального закона от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (в ред. от 16.04.2022 № 111-ФЗ) [4] первичными субъектами финансового мониторинга выступают организации (финансовые посредники), осуществляющие операции с денежными средствами или сделки с иным имуществом. В этой связи, банки признаются основным звеном по противодействию легализации доходов, полученных преступным путем, и от эффективности деятельности банковского внутреннего контроля зависит очень многое. При этом принятие решений банками о блокировке транзакций активов зависит не только от различных инструкций, разработанных Центральным банком России и внутренними локальными нормативными актами организации, но и от субъективного подхода сотрудников банка. В Федеральном законе перечисляются финансовые операции или сделки с имуществом, которые обязаны контролировать сотрудники банков, если, по определенным признакам, они считаются подозрительными. В правоприменительной практике по противодействию легализации доходов, полученных преступным путем, несмотря на ужесточение законодательных требований, с учетом новых возможностей цифровых платежей, виртуальных валют, цифровых кошельков и других технологических возможностей, обеспечивать на высоком уровне осуществление внутреннего контроля стало затруднительным. Поэтому очень важным составляющим контроля операций является продвинутая, самая современная технологическая программа, позволяющая осуществлять качественный мониторинг транзакций и в том числе наблюдать за лицами, принимающими решения управленческого характера в этих организациях.

Конечно, вопросы возникают к поставщикам программных продуктов во всем мире. При переводе различных сведений с традиционных мест хранения в цифровые активы возникает тревога об их сохранности. Тем более в новостных лентах постоянно происходят утечки, какой-либо информации, либо о краже персональных данных граждан, юридических лиц или государственных сведений. В данный момент развития государств поставщики различных программных технологий оказались над всеми гражданами, юридическими лицами и в том

числе государственными структурами. Такое положение нуждается в адекватном осмыслении и регламентации на законодательном уровне.

Развитие цифровых технологий позволяет расширить анализ данных, визуализировать риски и моделирование, чтобы увеличить эффективность в деятельности борьбы с отмыванием активов, полученных преступным путем. Уже имеются программы, которые позволяют без участия человека, по заданному заранее алгоритму осуществлять автоматизированный внутренний контроль над банковскими операциями или сделками. С другой стороны, механизмы анализа информации и принятия решений приводят к тому, что невозможно будет осуществлять классический контроль. Такая ситуация позволяет осуществлять транзакции различных данных, и контролирующие органы при всем желании не могут отменить или приостановить операцию или сделку. На практике были случаи, когда искусственный интеллект заблокировал правильную (чистую) финансовую операцию в банковской сфере в соответствии с требованиями Федерального закона № 115 по причине того, что автоматизированной системе операция оказалась подозрительной.

С учетом вышесказанного, следует констатировать, что цифровое взаимодействие приводит к новому качественному уровню развития сфер деятельности, и в связи с этим контролирующие органы не могут в полном объеме осуществлять необходимый контроль над происходящими процессами. Также стоит сказать о том, что цифровые активы были созданы в том числе, чтобы избавиться от контроля со стороны государства. На сегодняшний день цифровые денежные средства, представленные в виде различных видов криптовалют, официально продаются на рынке. В некоторых странах на них можно приобрести и товары повседневного спроса. В мировом масштабе наиболее криминальными криптовалютами являются: Bitcoin, Bitcoin Cash, Ethereum, Litecoin, Ripple, Dash. Кроме этого, токены, полученные в результате ICO, смарт-карты.

По мнению В. И. Просолова и С. С. Фешиной, «Будь то использование криптовалюты, создание «фейковых» ICO с целью привлечения теневых денег на счет, заключение смарт-контрактов для теневых сделок или уже банально привычные уход букмекерских контор и тотализаторов в Интернет, подмена MCC-кодов, предотвратить эффективно схемную операцию представляется сегодня невозможным как в силу несовершенства законодательной базы, так и в силу отсутствия отечественного опыта применения технологий продвинутого анализа, которые необходимы при работе с массивными данными, чем и характеризуются цифровые технологии» [5, с. 138].

Можно выделить некоторые характерные признаки, которыми обладают цифровые активы:

1. *Анонимность.* Как правило, транзакции не содержат данных о владельце счета, что затрудняет проверку данных при использовании услуг провайдеров в сфере виртуальных активов.

2. *Быстрота и невозвратность транзакции*. Операции проходят быстро, порой за доли секунд, поэтому можно совершить множество операций с небольшим разрывом времени и, соответственно, отслеживать такие действия очень сложно,

они могут отличаться невозвратностью, то есть отсутствовать риск отмены перевода после отправки виртуальной валюты.

3. *Сложные запутанные схемы транзакций.* Отсутствует взаимосвязь между физическим лицом и счетом. Кроме этого, лицо может иметь множество счетов.

4. *Установление фактов использования виртуальных валют.* Такая ситуация возникает в связи с отсутствием достаточной информации о транзакции, и поэтому сложно выяснить стороны финансовой операции.

5. *Отсутствие ограничений по сумме.* Объемы транзакций не влияют на осуществление операций.

Таким образом, влияние цифровизации усложняет не только деятельность финансовых институтов, но и схемы легализации доходов, полученных преступным путем. Эффективное и наступательное противодействие затрудняет тот факт, что представители контролирующих органов не всегда обладают необходимыми специальными познаниями в области цифровых активов и, в связи с этим не могут выстроить системную борьбу. Такие новые вызовы требуют адекватных и своевременных комплексных ответных мер. В первую очередь эти меры должны касаться информационно-коммуникационных технологий, экономической, финансовой, социальной и других сфер. Законодательные изменения в последнюю очередь должны касаться области уголовного права, как крайний вариант борьбы, при условии, что не сработали другие возможности противодействия. Тем более, предполагаемые изменения в области уголовного права в любом случае будут касаться других отраслей права или подзаконных актов различных государственных ведомств, так как диспозиция статьи Уголовного кодекса Российской Федерации будет носить бланкетный характер.

Список литературы

1. URL: http://www.kremlin.ru/acts/bank/41919.
2. URL: https://www.garant.ru/products/ipo/prime/doc/71634878/.
3. Кужиков В. Н. // Вестник АУП, № 2–3, 2021.
4. URL: http://www.consultant.ru/document/cons_doc_LAW_32834/.
5. Просолов В. И., Фешина С. С. URL: http://www.publishing-vak.ru/file/-archive-economy-2020-8/13-prasolov.pdf. С. 138.

Боровиков В. Б.[1],
профессор кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент

Боровикова В. В.[2],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент,

ОСОБЕННОСТИ РОССИЙСКОЙ УГОЛОВНО-ПРАВОВОЙ ПОЛИТИКИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

Цифровизация российского общества, с которой связывается прогресс мировой цивилизации вызывает разнообразные негативные последствия, требующие соответствующей реакции со стороны государства. Причем ее формы зависят от качества прогнозов, складывающейся в ближайшие годы социально-экономической ситуации в Российской Федерации; уровня анализа сфер общества, которые в наибольшей степени будут подвергаться процессу цифровизации, предвидения, в связи с этим появления отрицательных последствий; определения мер, необходимых для их минимизации со стороны государства. Естественно, среди них свое место должны занять и меры уголовно-правового воздействия в случаях, когда распространенность, характер и размеры, названных выше последствий, потребуют вмешательства со стороны уголовного закона.

Конечно, прогнозирование подобного рода – дело сложное и предполагает знание не только положений уголовного права, но и криминологии, философии, политологии, экономики, принципиальных положений об информационной безопасности и даже отдельных литературных произведений (например, о негативных последствиях научно-технического прогресса, в том числе связанных с распространением информационных технологий, полезно изучать произведения Е. Замятина «Мы», Олдоса Хаксли «О новый дивный мир», «Обезьяна и сущность», Станислава Лема «Сумма технологий»). Интерес представляют и публикации ряда специалистов различных отраслей знаний [1].

Вот как видится специалистом в области информационных технологий ближайшее будущее цивилизации.

Цифровизация неизбежно приведет к созданию искусственного интеллекта, широкому распространению роботизации. В связи с этим многие профессии «отомрут», например, водители, продавцы, санитары, грузчики, лаборанты, строительные рабочие определенных специальностей, работающие на конвейере, уборщицы. Значительно сократится потребность в таких профессиях

[1] © Боровиков В. Б., 2022.
[2] © Боровикова В. В., 2022.

как журналисты, литературные критики, композиторы, педагоги. Не будут нужны многие чиновники, секретари, референты, депутаты.

В обществе возникнет новая элита – специалисты в области информационных технологий, имеющих высокие зарплаты и привилегии.

Но взамен обострится социальное расслоение общества, появится высокая безработица, недовольство «лузеров» своим положением в обществе. Не будут нужны и миллионы мигрантов из стран ближнего зарубежья, в силу своей в целом низкой квалификации для получения достойной зарплаты. Однако возвращаться назад домой они не будут стремиться, так как на Родине жить еще труднее. Ухудшится материальное положение большинства населения, получат распространение психические заболевания, поскольку многие будут чувствовать себя лишними в новых условиях.

Отсюда – недалеко от роста социальных протестов, дестабилизации общества и государства, изменения в негативную сторону динамики и структуры преступности (причем она будет развиваться и в сфере использования информационных технологий, но и затронет область так называемой общеуголовной преступности, например, будет иметь рост преступлений против личности, собственности, общественной безопасности, порядка управления).

Мы не собираемся анализировать подобного рода прогнозы (это не тема отдельной публикации двух соавторов, нужны усилия мощных научно-исследовательских учреждений). Отметим лишь, что, на наш взгляд, надо учесть в современной российской уголовно-правовой политике фактор расширяющегося процесса цифровизации российского общества. Она, в связи с этим фактором, должна «работать» на опережение.

Очевидно, нужно адекватно оценивать реальную общественную опасность преступлений, совершаемых с использованием информационных технологий, и предусматривать за их совершение с учетом данного обстоятельства соразмерное наказание.

Конечно, при этом нельзя забывать о целях наказания, предусмотренных ч. 2 ст. 43 Уголовного кодекса Российской Федерации (т. е. восстановление социальной справедливости, исправление осужденного и предупреждение совершения новых преступлений).

Обратимся к гл. 28 Уголовного кодекса Российской Федерации, предусматривающей систему норм об ответственности за преступления в сфере компьютерной информации. По нашему мнению, существует специфика целей наказания, назначаемого за названные выше преступления. Так наивно надеяться, что цель исправления осужденных здесь реалистична. Казалось бы, что многие из тех, кто нарушает положения ст.ст. 272–274.1 Уголовного кодекса Российской Федерации входят в контингент лиц, поддающихся процессу исправления (среди них много несовершеннолетних, молодежи). Но дело в том, что виновные в совершении анализируемых преступлений лица обладают, как правило, несколько нестандартной личностью. Для них использование информационных технологий, по сути, образ жизни, который не представляется им вредоносным, даже в случае совершения какого-либо преступления. Надеяться, что применение

наказания разрушит их антисоциальные установки и поменяет их на позитивные, маловероятно. Этот вывод основывается также на том, что то же «хакерство» и другие злоупотребления в сфере компьютерной информации, нередко являются для данной категории лиц своеобразным способом самоутверждения среди своих друзей, коллег, а также важным источником жизненного существования.

Не очень «работает» в отношении рассматриваемой категории лиц и такая цель наказания как восстановление социальной справедливости. В самом упрощенном виде она сводится к тому, что тяжесть наказания должна соответствовать тяжести совершенного преступления. В действительности же ст. 6 Уголовного кодекса Российской Федерации (принцип справедливости) требует, чтобы применение наказания и иных мер уголовно-правового воздействия помимо соответствия характера и степени общественной опасности преступления объему карательного воздействия, надо учитывать и обстоятельства его совершения, и личность виновного. То есть справедливость наказания требует обязательного учета личности осужденного, а также обстоятельств совершения преступления (смягчающих и отягчающих). Но пока судебная практика не выразила еще четкой позиции в отношении личности осуждаемого за преступления в сфере компьютерной информации. Нет и ясного отношения к этой категории лиц и со стороны общественного мнения (тенденция, конечно, меняется в связи с ростом таких преступлений, но не до такой степени, когда нужно уже кричать: «Караул!»). Обычно вопрос о специфике наказания за преступления, совершаемые с использованием информационных технологий, обходят своим вниманием отечественные средств массовой информации, да и Пленумом Верховного Суда Российской Федерации (до сих пор нет и специального постановления на этот счет). Поэтому реальной по степени достижимости остается цель предупреждения данных деяний. Причем, отдавая приоритет цели специального предупреждения, надо отметить, что цель общей превенции здесь занимает особое место, учитывая непрерывный рост пользователей компьютером. Страх перед наказанием за различные злоупотребления в сфере использования информационных технологий может удержать их только, если будущее наказание действительно станет в глазах этих лиц весомым, способным помешать их жизненным планам, создать серьезную угрозу для реализации различных, например, материальных интересов.

А как в настоящее время выглядят санкции статей за преступления в сфере компьютерной информации?

На наш взгляд, законодатель пока не в полной мере оценил реальную общественную опасность названных выше преступлений. Иначе трудно объяснить, почему ни одно преступление, предусмотренное ст.ст. 272–274.1 Уголовного кодекса Российской Федерации, не относится к категории особо тяжких. В шести случаях эти деяния признаются тяжкими (ч. 4 ст. 272, ч. 3 ст. 273, чч. 2–5 ст. 274.1 Уголовного кодекса Российской Федерации); также в шести ситуациях данные преступления относятся к категории средней тяжести (чч. 2 и 3 ст. 272,

чч. 1 и 2 ст.273, ч. 2 ст.274, ч. 1 ст.274.1 Уголовного кодекса Российской Федерации); в двух случаях – преступлениями небольшой тяжести (ч. 1 ст.272, ч. 1 ст. 274 Уголовного кодекса Российской Федерации).

Из перечисленных выше деяний наиболее строгое наказание может быть назначено за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, т. е. деяния, предусмотренные чч. 1, 2, 3 или 4 ст. 274.1 УК РФ, если они повлекли тяжкие последствия предусматривают наказание в виде лишения свободы на срок от 5 до 10 лет, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Мы не являемся сторонниками безудержного ужесточения наказания за многие преступления. Но логика развития цифрового общества доказывает, что вредоносность деяния в сфере использования информационных технологий будет только возрастать.

Есть все основания полагать, что именно деяния, подпадающие под признаки составов преступлений, предусмотренных ст. 274[1] Уголовного кодекса Российской Федерации, в силу сложной внешнеполитической и экономической ситуации в стране станут активно использоваться противниками Российской Федерации для разрушения государства (примеров этому – великое множество). Но раз это так, то почему законодателю не произвести переоценку санкций норм, включенных в анализируемую статью Уголовного кодекса Российской Федерации? В частности, изначально признавать деяние, указанное в ч. 1 этой статьи, как тяжкое преступление, а не как деяние средней тяжести. Деяние же, предусмотренное ч. 5 этой статьи (при наличии тяжких последствий), следует считать особо тяжким преступлением. В других же статьях главы 28 Уголовного кодекса Российской Федерации целесообразно также произвести изменения, связанные с тем, чтобы отсутствовали нормы, устанавливающие ответственность за преступления небольшой тяжести (на наш взгляд, как минимум, они не должны признаваться преступлениями средней тяжести, учитывая их значительную степень общественной опасности).

В отношении же иных преступлений в сфере компьютерной информации должен быть проявлен со стороны законодателя более дифференцированный подход. В частности, надо исключить при конструировании санкций уголовно-правовых норм за эти деяния санкции без указания минимальных пределов видов наказания. В настоящее время в 10 санкциях различных частей, анализируемых статей Уголовного кодекса Российской Федерации, применительно к лишению свободы на определенный срок нет указания на минимальный предел этого вида наказания (см., например, чч. 1–4 ст. 272, чч. 1–3 ст. 273 Уголовного кодекса Российской Федерации). В итоге получается, что формально можно назначать за рассматриваемые деяния и два месяца лишения свободы.

Думается, такой вид наказания совершенно не отражает реальную общественную опасность содеянного. Полагаем, минимальный предел лишения свободы за подобные деяния, должен составлять шесть месяцев.

Конечно, отмеченные выше критические замечания в адрес санкций статей, предусмотренных гл. 28 Уголовного кодекса Российской Федерации, должен соблюдаться и при конструировании санкций статей Особенной части Уголовного кодекса Российской Федерации, находящихся в других главах этого кодифицированного законодательного акта. Полагаем, что здесь не все так благополучно. Существует та же недооценка общественной опасности содеянного.

Например, вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего, совершенного в информационно-телекоммуникационных сетях (включая сеть Интернет), влечет максимальное наказание в виде лишения свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового. То есть данное деяние с позиции уголовного закона признается преступлением небольшой тяжести. Разве это правильно, когда речь идет о том, что рассматриваемое преступление может привести к лишению жизни несовершеннолетнего?

Полагаем, подобное деяние по характеру и степени своей общественной опасности должно относиться, как минимум, к преступлениям средней тяжести. Следовательно, и наказание за такое преступление должно назначаться в виде лишения свободы на срок до пяти лет.

Удивляет и то, что наказание за мошенничество в сфере компьютерной информации согласно ч. 1 ст.159.6 Уголовного кодекса Российской Федерации в качестве наиболее строгого наказания предусматривает арест на срок до четырех месяцев, который, как известно, до сих пор не применяется в Российской Федерации. Опять-таки констатируем, что данное деяние признается преступлением небольшой тяжести. И это в условиях, когда многие граждане нашей страны становятся жертвами таких преступлений. Очевидно, что и это деяние с учетом специфики его общественной опасности, возможностей нарушить имущественные права многих людей должно рассматриваться как преступление средней тяжести.

Можно привести и другие примеры подобного рода. В частности, нет ответа, почему мошенничество с использованием электронных средств платежа (ч. 1 ст. 159³ Уголовного кодекса Российской Федерации) считается преступлением небольшой тяжести с максимальным наказанием в виде лишения свободы на срок до трех лет?

Итак, требуется соответствующая законотворческая деятельность по оценке тяжести преступлений, совершенных с использованием информационных технологий в части ряда статей Особенной части, не входящих в гл. 28 Уголовного кодекса Российской Федерации.

Уголовно-правовая политика в цифровой сфере, по нашему мнению, должна повлиять и на наши представления об обстоятельствах, отягчающих наказание (ст. 63 Уголовного кодекса Российской Федерации). Конечно, правильным является законодательный процесс включения в отдельные статьи Особенной части Уголовного кодекса Российской Федерации в качестве квалифицирующего при-

знака состава преступления – «использование при совершении преступления информационных технологий». Но это процесс достаточно длительный и не требует суеты. Поэтому, на наш взгляд, целесообразно дополнить ч. 1 ст. 63 УК РФ указанием на такое обстоятельство, как «совершение преступления с использованием информационно- телекоммуникационных сетей, включая сеть Интернет». Кстати, закономерно возникает вопрос и о включении в ч. 1 ст. 63 УК РФ такого обстоятельства как «совершение преступления в отношении лица пожилого возраста». Понятие «пожилого возраста», конечно, заслуживает обсуждения (например, он может касаться лиц старше 70 лет).

Целесообразность появления, названного выше обстоятельства в ст. 63 УК РФ связана как с ростом подобных негативных явлений в Российской Федерации, так и их значительной общественной опасностью и необходимостью защитить наиболее уязвимых граждан, не всегда правильно ориентирующихся в условиях цифровизации общества.

В нашей статье из-за обширности проблем, которые возникают в российской уголовно-правовой политике в цифровой сфере, мы затронули лишь некоторые аспекты. Видимо, есть и другие направления в российской уголовной политике в информационной сфере, например, определение и закрепление в уголовном законе круга новых деяний, которые бы предусматривали в качестве признаков основного или квалифицированного состава преступления; использование при совершении преступления информационных технологий; уточнение на законодательном уровне специфики неоконченного преступления и соучастия в преступлении, в связи с использованием названных выше технологий; изучение специфики субъективных признаков преступления, совершенных с использованием IT-технологий (это имеет большое значение для правоприменительной практики); проблемы установления оценочных признаков составов преступлений, совершенных с использованием информационных технологий; криминализация новых общественно опасных деяний, связанных с использованием этих технологий, например, компьютерного шпионажа, распространения «фейковых» новостей, буллинга (травли, издевательств в компьютерных сетях), незаконного разглашения персональных данных с использованием IT-технологий.

Это далеко не полный перечень проблем, который необходимо изучить в связи с распространением цифровизации. Дело – за исследователями, которые могут совершить прорыв в этом направлении.

Список литературы

1. Таран Д. Цифровая оккупация // Завтра. 2019. № 1 ; Ларина Е., Овчинский В. Новизна // Завтра. 2017. № 11, 12, 14 ; Ларина Е. С., Овчинский В. С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М. : Книжный мир, 2014 ; Мирин И. Не нужен репортеру гонорар // Инновации (приложение к «РГ»). 2021. 20 сент. ; Новоселова Е. История сдается? // Российская газета. 2021. 23 нояб. ; Перетолчин Д. Битва железных матриц // Завтра. 2021. № 45 ; Фефелов А. Храм биоцифры // Завтра. 2021. № 45, 47.

Дарменов А. Д.[1],
начальник Карагандинской академии
МВД Республики Казахстан
имени Баримбека Бейсенова,
кандидат юридических наук

НЕКОТОРЫЕ ВОПРОСЫ ПРОВЕДЕНИЯ ВЫЕМКИ СВЕДЕНИЙ О ПРОИЗВЕДЕННЫХ ПЕРЕГОВОРАХ С АБОНЕНТСКИХ НОМЕРОВ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, В РЕСПУБЛИКЕ КАЗАХСТАН

Современный мир характеризуется стремительным развитием информационно-коммуникационных технологий, информационных сетей и цифровизацией всех сфер жизнедеятельности. На сегодняшний день развитие общества полностью связано с указанными технологиями.

Вместе с тем, стремительный научный прогресс может не только открывать новые возможности для людей и нести блага всему человечеству, но и создавать различные проблемы социально-негативного характера. В качестве одной из таких проблем выступают преступления, совершаемые с применением информационно-коммуникационных технологий.

Особенно в последние годы озабоченность правоохранительных органов вызывает резкое увеличение количества мошенничеств, совершаемых с применением информационно-коммуникационных технологий. Согласно статистическим данным Комитета по правовой статистике и специальным учетам при Генеральной Прокуратуре Республики Казахстан показатели по этому виду уголовного правонарушения (мошенничество путем обмана или злоупотребления доверием пользователя информационной системы (п. 4 ч. 2 ст. 190 Уголовного кодекса Республики Казахстан) с каждым годом увеличиваются: в 2019 г. – 7 769 фактов, в 2020 г. – 14 155, в 2021 г. – 21 405 и за 4 месяца 2022 г. – 6 256 [1].

Главными причинами резкого роста данных преступлений могут служить такие факторы как сокращение доходов населения, чрезмерная доверчивость и низкая осведомленность граждан в области информационных систем. Наряду с этим одним из проблемных вопросов в борьбе с указанным видом мошенничества является некоторые сложности в его расследовании. В совокупности все вышеперечисленные факторы влияют на распространение этого вида преступлений, что в свою очередь вселяет правонарушителям чувство безнаказанности и подрывают веру граждан в справедливость.

[1] © Дарменов А. Д., 2022.

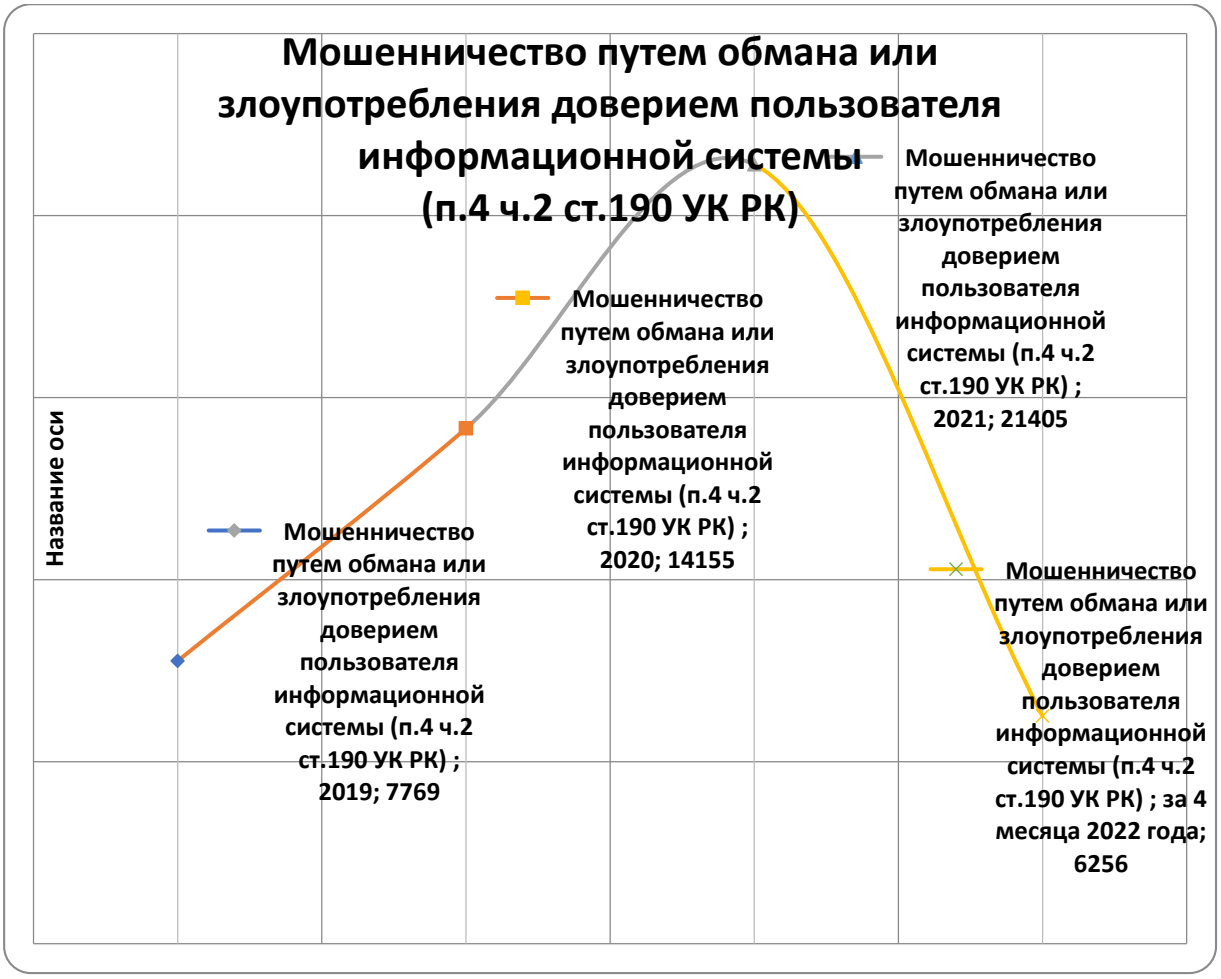

Рис. 1. Статистические данные

При расследовании мошенничеств, совершаемых с применением информационно-коммуникационных технологий, часто возникает необходимость в установлении сведений о произведенных телефонных разговорах сотовой связи потерпевшего. Данная мера предоставляет возможность «сузить круг лиц, могущих быть причастными к преступлению, выдвинуть обоснованные версии о совершении преступного деяния и в конечном счете установить виновных лиц» [2, с. 147].

Анализ практической деятельности следственных подразделений органов внутренних дел Республики Казахстана показал, что при расследовании мошенничеств с использованием информационных систем некоторые возникают сложности в получении сведений о произведенных телефонных разговорах в сотовой связи потерпевшего.

В Республике Казахстан органы досудебного производства вышеуказанные сведения получают посредством проведения их выемки у операторов связи. Согласно порядку производства выемки, закрепленного в ст. 254 Уголовно-процессуального кодекса Республики Казахстан (далее – УПК РК) данное следственное действие должно производиться лицом, осуществляющим досудебное расследование.

Проблема в проведении этого следственного действия при расследовании мошенничеств, совершаемых с применением информационно-коммуникационных

технологий, заключается в том, что сведения о произведенных телефонных разговорах сотовой связи потерпевшего в Республике Казахстане выдаются только головными офисами операторов связи, которые находятся в городах Нур-Султан или Алма-Аты. Соответственно выемка должна производиться в указанных городах с участием лица, осуществляющего досудебное расследование, или иным лицом на основании поручения. К примеру, Специализированный следственный суд г. Караганды удовлетворил ходатайство следователя СО Центрального отдела полиции УП г. Караганды о проведении выемки сведений о произведенных телефонных переговорах с абонентскими номерами: 8-777-736****, 8-777-178****, 8777-749****, обслуженного базовыми станциями сотовой связи компании ТОО «Кар-Тел» «Beeline», расположенной в г. Нур-Султан. В данном случае, выемка сведений о произведенных телефонных разговорах сотовой связи потерпевшего будет проводиться по вышеуказанному адресу. С учетом данного обстоятельства, а также того, что выемка должна производиться с участием лица, осуществляющего досудебное расследование, следователи (дознаватели) вынуждены либо сами осуществлять командировки в указанные города для производства данного следственного действия, либо доверить это другому сотруднику следственного или оперативного подразделения посредством оформления письменной доверенности. Если учесть, что факты мошенничеств с использованием информационных систем в последние годы резко участились, и соответственно количество уголовных дел, находящихся в производстве органов досудебного расследования, увеличилось, то и количество производства выемки по указанным уголовным правонарушениям также пропорционально возросло. Данное обстоятельство отражается на работе следователей (дознавателей). За неимением возможности на постоянной основе осуществлять служебные командировки в города Нур-Султан и Алма-Ата в связи с необходимостью нахождения следователей (дознавателей) на рабочем месте в силу большого объема работы и с существенной нагрузкой на государственный бюджет по оплате служебных командировок, следственные подразделения территориальных органов внутренних дел вынуждены с периодичностью 1–2 раза в месяц направлять сотрудника в указанные города для проведения выемки сведений о произведенных телефонных разговорах сотовой связи по всем находящимся в производстве уголовным делам. Данная мера существенно затягивает сроки расследования.

Безусловно, своевременное получение информации о соединениях между абонентами и (или) абонентскими устройствами позволяет ускорить процесс доказывания по уголовному делу [3, с. 227]. Поэтому некоторые территориальные органы внутренних дел для выхода из сложившейся ситуации находят разные пути решения данной проблемы. К примеру, департамент полиции одного из областей откомандировывает сотрудников в города Нур-Султан и Алма-Ата, где они находятся на постоянной основе и выполняют необходимые мероприятия по заданию руководства, в том числе и производство выемки сведений о произведенных телефонных разговорах сотовой связи потерпевшего. Однако, на наш взгляд, указанная мера не в полной мере сможет решить сложившуюся ситуацию.

Довольно интересная практика получения сведений о произведенных телефонных разговорах сотовой связи потерпевшего была введена в территориальных подразделениях органов внутренних дел некоторых областей во время карантина. В целях минимизации контакта сотрудников полиции с работниками операторов сотовой связи была введена практика получения указанных сведений через почту. Однако, полагаем, что такая практика противоречит требованиям проведения выемки, закрепленным в ст. 254 УПК РК, т. е. производится без участия уполномоченного на это должностного лица.

На наш взгляд, для разрешения этой проблемы необходимо внедрение совершенно иного процессуального механизма, имеющего более упрощенные процедуры получения необходимых сведений, что приведет к более рациональной организации расследования рассматриваемых видов уголовных правонарушений и экономии времени и сил следователей (дознавателей), а также бюджетных средств государства.

В этой связи представляется целесообразным изучение передового опыта зарубежных стран по получению сведений о произведенных телефонных разговорах сотовой связи. Так, в Соединенных Штатах Америки еще с 1999 г. сотовые операторы начали производить записи детализации вызовов (CDR) с информацией о местоположении сотового узла (CSLI), которые предоставлялись правоохранительным органам по решениям суда [4, с. 221; 5].

Интересным также представляется опыт Российской Федерации в данной области. Так, в досудебном производстве Российской Федерации для получения сведений о произведенных телефонных разговорах сотовой связи производится самостоятельное следственное действие – получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 Уголовно-процессуального кодекса Российской Федерации) [6].

Данное следственное действие состоит «в принятии следователем (дознавателем) мотивированного решения об обращении в суд с целью получения судебного решения об истребовании из организаций, осуществляющих услуги телефонной (электронной) связи, сведений о ранее имевших место или возможных в будущем контактах (голосовых, неголосовых) с использованием абонентских устройств, а также в получении и приобщении к делу таких сведений [7].

Весь механизм получения соответствующего ответа на направленный следователем запрос сводится к тому, что данный ответ может быть получен разными способами: вручается непосредственно следователю (дознавателю), направившему данный запрос; оперативно-уполномоченным сотрудникам, действующим по письменной доверенности, выданной следователем (дознавателем). Кроме того, ответ может быть выслан и по почте. При этом он может находиться как на бумажном, так и на электронном носителе. После получения ответа на свой запрос, следователь (дознаватель) при соблюдении необходимых процессуальных требований приобщает сведения о ранее имевших место или возможных в будущем контактах (голосовых, неголосовых) с использованием абонентских устройств в уголовное дело [8, с. 90].

По нашему мнению, данный порядок получения сведений о произведенных телефонных разговорах сотовой связи очень удобен в следственной деятельности. В связи с этим российский опыт может быть полезен для следственных подразделений органов внутренних дел Республики Казахстан. Это обусловлено тем, что одним из важных отличий рассматриваемого следственного действия от выемки является процедура получения интересующей следствие информации. Действия по изъятию предметов и документов при выемке производятся лично следователем, либо лицом на основании доверенности, в то время как информация о соединениях между абонентами копируется работниками операторов связи и направляется следователю [9, с. 59–60]. Говоря обычными словами, должностному лицу, осуществляющему досудебное расследование, не придется лично осуществлять командировку в города Нур-Султан и Алма-Ата, где находятся головные офисы операторов связи, для производства выемки сведений, имеющих значение для следствия или перепоручать данное действие другим должностным лицам органов досудебного расследования.

Немаловажным является и то, что данное следственное действие учеными-процессуалистами оценивается, как эффективное средство формирования и исследования доказательств. Так, по мнению А. А. Цыкоры, В. Ф. Васюкова и А. Богдановского, сведения об абонентах связи как криминалистически значимая информация при раскрытии и расследовании введение в уголовно-процессуальный закон России указанного следственного действия было долгожданным и весьма своевременным законодательным решением [10, с. 13–16], предопределенным как реалиями правоприменительной практики [11, с. 32–36], так и современным уровнем развития телекоммуникационных технологий [12, с. 239].

На основании вышеизложенного предлагается в УПК РК ввести ст. 261-1 в следующей редакции:

«261-1. Получение информации о соединениях между абонентами и (или) абонентскими устройствами.

1. При наличии достаточных оснований полагать, что информация о соединениях между абонентами и (или) абонентскими устройствами имеет значение для уголовного дела, получение лицом, осуществляющим досудебное расследование, указанной информации допускается на основании решения следственного судьи.

2. В ходатайстве лица, осуществляющего досудебное расследование, о производстве следственного действия, касающегося получения информации о соединениях между абонентами и (или) абонентскими устройствами, указываются:

1) уголовное дело, при производстве которого необходимо выполнить данное следственное действие;

2) основания, по которым производится данное следственное действие;

3) период, за который необходимо получить соответствующую информацию, и (или) срок производства данного следственного действия;

4) наименование организации, от которой необходимо получить указанную информацию.

3. В случае принятия следственным судом решения о получении информации о соединениях между абонентами и (или) абонентскими устройствами его копия направляется лицом, осуществляющим досудебное расследование, в соответствующую осуществляющую услуги связи организацию, руководитель которой обязан предоставить указанную информацию, зафиксированную на любом материальном носителе информации. Указанная информация предоставляется в опечатанном виде с сопроводительным письмом, в котором указываются период, за который она предоставлена, и номера абонентов и (или) абонентских устройств.

4. Получение лицом, осуществляющим досудебное расследование, информации о соединениях между абонентами и (или) абонентскими устройствами может быть установлено на срок до шести месяцев. Соответствующая осуществляющая услуги связи организация в течение всего срока производства данного следственного действия обязана предоставлять лицу, осуществляющему досудебное расследование, указанную информацию по мере ее поступления, но не реже одного раза в неделю.

5. Лицо, осуществляющее досудебное расследование, осматривает представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, с участием специалиста (при необходимости), о чем составляет протокол, в котором должна быть указана та часть информации, которая, по мнению лица, осуществляющего досудебное расследование, имеет отношение к уголовному делу (дата, время, продолжительность соединений между абонентами и (или) абонентскими устройствами, номера абонентов и другие данные). Лица, присутствовавшие при составлении протокола, вправе в том же протоколе или отдельно от него изложить свои замечания.

6. Представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, приобщаются к материалам уголовного дела в полном объеме на основании постановления лица, осуществляющего досудебное расследование, как вещественное доказательство и хранятся в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность.

7. Если необходимость в производстве данного следственного действия отпадает, его производство прекращается по постановлению лица, осуществляющего досудебное расследование, но не позднее окончания досудебного расследования по уголовному делу.»

Кроме того, в ч. 1 ст. 55 УПК РК («Полномочия следственного судьи») предлагается ввести п. 19 в следующей редакции:

«19) санкционирует получение информации о соединениях между абонентами и (или) абонентскими устройствами.».

Подытоживая вышесказанное, хотелось бы отметить, что введение в уголовный процесс Республики Казахстан нового следственного действия – получение информации о соединениях между абонентами и (или) абонентскими устрой-

ствами позволило бы существенно упростить процедуру получения необходимых сведений для органов досудебного производства и сократить сроки расследования. Безусловно, данная мера скажется на организацию расследования мошенничеств, совершаемых с применением информационно-коммуникационных технологий и на нагрузку на следователей и дознавателей.

Список литературы

1. Форма отчета № 1-М «О зарегистрированных уголовных правонарушениях» за 2019–2022 гг. Информационный сервис Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан. URL: https://qamqor.gov.kz/crimestat/statistics.

2. Стельмах В. Ю. О Получение информации о соединениях между абонентами и (или) абонентскими устройствами // Совершенствование законодательства. 2017. № 3 (124). С. 141–153.

3. Харзинова В. М. Проблемы получения информации о соединениях между абонентами и (или) абонентскими устройствами // Общество и право. 2014. № 2 (48). С. 226–229.

4. Антонов О. Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами в России: сущность, этапы и пути совершенствования тактического обеспечения // Вестник Томского государственного университета. 2020. № 459. С. 221–229.

5. Minor J. B. (2017) Forensic Cell Site Analysis: A Validation & Error Mitigation Methodology. Journal of Digital Forensics, Security and Law. 12 (2). Article 7. DOI: 10.15394/jdfsl 1474.

6. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/.

7. Комментарий к статье 1861 Уголовно-процессуального кодекса Российской Федерации «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» (введена Федеральным законом от 1 июля 2010 г. № 143-ФЗ). URL: https://mvd.ru/upload/site129/folder_page/013/699/474/-Kommentariy_k_st._186.1_UPK_RF.pdf.

8. Кальницкий В. В., Ларин Е. Г. Следственные действия : учебное пособие. Омск : Омская академия МВД России, 2015.

9. Дерюгин Р. А. Получение информации о соединениях между абонентами и (или) абонентскими устройствами: тактика следственного действия и использование его результатов при расследовании преступлений : дис. … канд. юрид. наук. Екатеринбург, 2018.

10. Васюков В. Ф. Сведения об абонентах связи как криминалистически значимая информация при раскрытии и расследовании грабежей и разбоев, совершенных на открытой местности // Правовые вопросы связи. 2008. № 2. С.13–16.

11. Богдановский А. Может ли ошибаться Конституционный Суд? // Законность. 2006. № 8. С. 32–36.

12. Цыкора А. А. Некоторые проблемы производства следственного действия «получение информации о соединениях между абонентами и (или) абонентскими устройствами» // Юристъ-Правоведъ. 2012. С. 239–244.

Бахур О. И.[1],
начальник кафедры уголовного права
Академии МВД Республики Беларусь,
кандидат юридических наук, доцент

ОСОБЕННОСТИ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ ПО УГОЛОВНОМУ КОДЕКСУ РЕСПУБЛИКИ БЕЛАРУСЬ

Причиной криминализации в уголовном законодательстве противоправных действий в области использования электронной техники и информационных технологий является их высокая общественная опасность, связанная с возможностью наступления тяжких последствий, связанных с причинением физического вреда людям, а также имущественного ущерба. Современная эпоха информационного общества характеризуется доступностью и повсеместным применением компьютерной техники, совершенствованием информационных технологий, таких как электронные платежи и документооборот, социальные сети, стриминговые платформы. Указанные процессы, наряду с пользой для общества, несут в себе и существенный криминогенный потенциал, возник новый вид преступности – компьютерная преступность, или преступность против компьютерной информации (в терминологии УК Республики Беларусь в ред. от 26.05.2021). Концепция информационной безопасности Республики Беларусь, утвержденная постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, указывает на то, что новые вызовы и угрозы, связанные с трансформацией социума в информационное общество, напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов [1]. С использованием компьютерной техники все чаще совершаются преступления террористической направленности и иные тяжкие преступления.

По данным ООН, ущерб, наносимый преступлениями в сфере информационных технологий, сопоставим с доходами от незаконного оборота оружия и наркотиков. Только в США он ежегодно составляет около 100 млрд долларов [2].

Последние изменения в главу 31 УК Беларуси (далее – УК) были внесены 26 мая 2021 г. Законом Республики Беларусь № 112-З, в результате которых она была существенным образом переработана и переименована в главу «Преступления против компьютерной безопасности» (предыдущее название – «Преступления против информационной безопасности».

В Уголовный Кодекс Республики Беларусь 1999 г. (далее – УК) были внесены принципиально новые для отечественного уголовного законодательства виды преступлений, объединенные в самостоятельный Раздел XII «Преступления против компьютерной безопасности», включающий единственную гл. 31 «Преступления против компьютерной безопасности». Данная глава содержит пять статей

[1] © Бахур О. И., 2022.

(349–355, ст.ст. 351, 353 УК исключены – Закон Республики Беларусь от 26 мая 2021 г. № 112-З).

В названии главы УК определен видовой объект рассматриваемых преступлений – компьютерная безопасность, под которой понимается совокупность общественных отношений, обеспечивающих безопасные условия существования и функционирования компьютерной информации и компьютерного оборудования. Дополнительным же объектом могут выступать жизнь, здоровье человека, его честь и достоинство, законные интересы физических и юридических лиц, общества и государства, собственность, общественная безопасность и т. д.

Предметом почти всех преступлений против компьютерной безопасности является компьютерная информация, т. е. информация, хранящаяся в компьютерной системе, сети или на машинных носителях, а также – носители этой информации: компьютерное оборудование, компьютерная система, сеть, машинные носители, компьютерные программы и т. п. Кроме того, в ст. 354 УК в качестве предмета преступления указывается на вредоносные программы или их носители.

Одним из основных нормативных правовых актов в области информационных отношений является Закон Республики Беларусь «Об информации, информатизации и защите информации» [3]. В нем законодательно раскрыто понятие *информации*. Это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Информация становится компьютерной, если она хранится в компьютерной сети, системе или на машинных носителях. Она неотделима от компьютера и доступ к ней может быть обеспечен только с его использованием.

Под компьютерной информацией необходимо понимать информацию, представленную в специальном (машинном) виде, предназначенном и пригодном для ее автоматизированной обработки, хранения и передачи, находящаяся в компьютерной системе, сети или на материальном носителе и имеющая собственника, установившего порядок ее создания (генерации), обработки, передачи и уничтожения. Наиболее важным для правильной квалификации является факт представления этой информации в виде, предназначенном и пригодном для ее обработки, хранения и передачи с использованием электронных технических средств, список которых ныне уже не ограничивается исключительно компьютерами. При этом смысловое содержание информации уходит на второй план, так как в машинном виде оно всегда представлено одинаково – в виде, определяемом физической природой материального носителя информации.

Еще одним важным элементом составов преступлений против компьютерной безопасности является их предмет – «компьютерная система». Основываясь на положениях Закона «Об информации, информатизации и защите информации», компьютерную систему можно определить, как автоматизированную информационную систему, представляющую собой совокупность электронно-вычислительных технологий, ресурсов и программно-технических средств, осуществляющих процессы в человеко-машинном или автоматическом режиме.

Чтобы исключить смешение понятий «объект преступления» и «предмет преступления» применительно к преступлениям против информационной безопасности, разграничение их следует провести следующим образом: противоправное воздействие на компьютерную информацию как предмет преступления посягает на объект преступления – информационную безопасность.

Объективная сторона преступлений против информационной безопасности, как правило, выражается в преступном действии. Лишь в одном преступлении – нарушение правил эксплуатации компьютерной системы или сети (ст. 355 УК) возможно и преступное бездействие виновного.

В своем большинстве рассматриваемые преступления сконструированы по типу *материальных* – предусматривают наступление общественно-опасных последствий.

В основных составах преступлений, предусмотренных ст.ст. 349, 351, 355 УК, в качестве последствий указывается на: изменение, уничтожение, блокирование, приведение в негодное состояние компьютерной информации, программы, вывод из строя компьютерного оборудования, разрушение компьютерной системы, сети или машинного носителя, причинение иного существенного вреда. Только на причинение существенного вреда указывается в ч. 1 ст.ст. 350, 352 УК.

Лишь два состава главы 31 УК относятся к *формальным* – предусмотренные чч. 1, 2 ст. 354 УК. Они считаются оконченными уже с момента совершения общественно опасного деяния.

В том случае, когда результатом совершения преступления против информационной безопасности является наступление последствий материального характера, встает вопрос об их разграничении с преступлениями против собственности, таких как хищение имущества путем модификации компьютерной информации (ст. 212 УК) и причинение имущественного ущерба без признаков хищения (ст. 216 УК), которое также может совершаться путем модификации компьютерной информации.

Законодатель определил модификацию компьютерной информации в примечании к ст. 208 УК («Вымогательство») как – противоправное изменение компьютерной информации либо внесение в компьютерную систему заведомо ложной компьютерной информации. Не является «модификацией» в уголовно-правовом смысле использование программ, модифицирующих данные без изменения их содержания с возможностью восстановления первоначального вида – архиваторов, кодировщиков и т. п.

В том случае, если модификация компьютерной информации производится с целью противоправного завладения имуществом, то в таком случае применяется только ст. 212 УК («Хищение имущества путем модификации компьютерной информации»).

Если же лицо путем использования компьютерной техники пытается извлечь имущественную выгоду, не связанную с хищением, возможны два варианта квалификации. Очевидно, что преступление, предусмотренное ст. 216 УК является корыстным, поэтому при доказанности указанного признака и причинении имущественного ущерба в значительном размере (в 40 и более раз превышает размер

базовой величины, установленной на день совершения преступления), действия виновного следует квалифицировать по ст. 216 УК Республики Беларусь. Если же причиненный ущерб не превышает значительного размера, но наступают последствия в виде существенного вреда нематериального характера (нарушение конституционных прав граждан, значительное ущемление прав и законных интересов органов, организаций и учреждений, создание препятствий их нормальной работе и т. д.) – применяется ст. 350 УК Республики Беларусь «Модификация компьютерной информации».

В случае, когда действия виновного выразились в изменении реквизитов доступа законного пользователя к компьютерной информации (паролей, логинов), что повлекло за собой блокировку доступа к учетной записи или электронному почтовому ящику, они должны оцениваться не как модификация компьютерной информации, а как ее блокирование, с учетом направленности умысла виновного.

Оценочное понятие «существенный вред» представляется достаточно сложно определяемым на практике. Данный признак должен определяться с учетом всех обстоятельств дела. Существенным вредом могут быть признаны: причинение материального ущерба в крупном размере (на сумму в 250 и более раз превышающий размер базовой величины, установленной на день совершения преступления), нарушение конституционных прав граждан, создание препятствий для нормальной работы государственных органов, учреждений, организаций и т. п.

Физическое повреждение или разрушение компьютерной техники, машинных носителей (дискет, дисков), как предметов, обладающих материальной ценностью, квалифицируются по ст. 218 УК (Умышленные уничтожение или повреждение имущества).

Для рассматриваемых преступлений характерно и то, что при их совершении компьютерная система может выступать одновременно и в качестве предмета, и в качестве орудия преступления. Так, компьютер может быть таким же техническим средством совершения преступления, как отмычка, огнестрельное оружие, автомобиль или иное техническое приспособление. Примером может служить преступление, предусмотренное ст. 349 УК «Несанкционированный доступ к компьютерной информации», когда компьютерная система (ПЭВМ) используется как орудие совершения преступления для доступа к предмету преступления – информации, хранящейся в нем, что влечет указанные негативные последствия для этой информации.

Субъективная сторона рассматриваемых преступлений характеризуется как умышленной, так и неосторожной формой вины. Так преступления, предусмотренные чч.1 и 2 ст. 349, ч. 2 ст. 350, ст. 355 УК, являются неосторожными, ст. 354 УК предусматривает умышленное преступление. Совершение же деяний, указанных в ч. 1 ст. 350 и ст.352 УК возможно, как умышленно, так и по неосторожности.

Субъектом преступлений против информационной безопасности в большинстве случаев выступает вменяемое физическое лицо, достигшее 16-летнего возраста. В ст. 355 УК предусмотрен специальный субъект – лицо, имеющее доступ к компьютерной системе или сети.

В заключение отметим, что для обеспечения эффективной защиты человека, общества и государства от общественно опасных посягательств в сфере оборота компьютерной информации необходимо формирование единой правоприменительной практики, отвечающей принципам законности, обоснованности и справедливости.

Список литературы

1. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» // СПС «Консультант Плюс» : Беларусь. Технология Проф. [Электронный ресурс] / ООО «Юрспектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2022.

2. Лосев В. В. Преступления против информационной безопасности : методические рекомендации по курсу «Уголовное право Республики Беларусь. Особенная часть». БрГУ, 2000. С. 3.

3. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» // Национальный реестр правовых актов Республики Беларусь. 2008. № 279, 2/1552. 26 нояб.

Камчатов К. В.[1],
заведующий отделом научного обеспечения
прокурорского надзора за исполнением законов
при осуществлении оперативно-разыскной деятельности
и участия прокурора в уголовном судопроизводстве
Научно-исследовательского института
Университета прокуратуры Российской Федерации,
кандидат юридических наук

ПРОБЛЕМЫ ПРОИЗВОДСТВА ПРОЦЕССУАЛЬНЫХ ДЕЙСТВИЙ В ОТНОШЕНИИ КРИПТОВАЛЮТ

Данный вопрос является крайне актуальный. На фоне отмеченной в последние годы положительной динамики совершения преступлений в сфере ИКТ распространена практика использования криптовалют в целях легализации доходов, полученных в результате совершения преступлений в сфере компьютерной информации [1, с. 13]. Комплексная положительная оценка криптовалюты как нового и перспективного вида актива и финансового инструмента не вызывает сомнения. Для Российской Федерации ее оборот особенно актуален, поскольку неопределенность в сфере регулирования криптовалют в России также делает ее крупнейшим рынком покупки и продажи биткоинов на P2P-платформах [2, с. 64–72]. Согласно ежегодным докладам Европола, до 90 % всех платежей в теневом секторе сети Интернет осуществляется с помощью цифровых валют [3]. В дальнейшем полученные доходы в цифровых валютах нередко конвертируются в фиатную валюту и легализуются.

Так, еще в 2014 г. Банк России в своем письме отметил, что «в связи с анонимным характером деятельности по выпуску «виртуальных валют» неограниченным кругом субъектов и по их использованию по совершению операций граждане и юридические лица, могут быть, в том числе непреднамеренно, вовлечены в противоправную деятельность, включая легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма» [4]. Данную позицию поддерживал Росфинмониторинг, который высказал точку зрения о том, что любые сделки, связанные с использование виртуальной валюты, могут быть рассмотрены как сделки, связанные с легализацией преступных доходов.

В настоящее время деятельность на территории Российской Федерации по обмену криптовалют на фиатные деньги и обратно федеральным законодательством не урегулирован, полностью находится вне правого регулирования. Вся торговля проводится посредством «неофициальных» P2P-бирж. Введенное в 2020 г. положениями Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Закон

[1] © Камчатов К. В., 2022.

№ 259) «оператор обмена цифровых финансовых активов» (ст. 10) относится только к российской юрисдикции.

Поскольку в Российской Федерации криптовалюта официально не введена в гражданский оборот на законодательном уровне, соответственно операции с ней банки не осуществляют и законно определить ее как актив в общепринятом смысле можно весьма опосредовано. Чтобы охарактеризовать данную категорию используются такие определения как это цифровая репрезентация (выражение) стоимости, некая квазивещь, которая хотя и не имеет физического признака, но имеет экономическую ценность сама по себе, а не как документ, закрепляющий право [5, с. 16–23], «денежные суррогаты» [6], своеобразный особый товар, эквивалентом в имущественном обороте [7]. Применительно к понятию имущества, указанного в ст. 5 Уголовно-процессуальный кодекс Российской Федерации, и применяемого на практике, предполагает физическую вещь и информацию в системе государственного учета и статистики. В случае криптовалюты принудительно нельзя установить адрес криптокошелька, данных о владельце. Вместе с тем, информация об операциях (денежных потоках) является общедоступной и размещается в общем реестре операций.

Прокуроры в рамках действующего законодательства могут только обращаться в суд в порядке ст.ст. 45, 245 Гражданско-процессуального кодекса Российской Федерации с заявлениями о признании информации, распространенной посредством сети Интернет на сайте, информацией, распространение которой на территории Российской Федерации запрещено, мотивируя это тем, что «размещение информации об электронной валюте «Bitcoin» является нарушением Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации», подрывает конституционный строй и авторитет Российской Федерации, а также основы материального благополучия граждан России, чем нарушает права и законные интересы неопределенного круг лиц, получающих доступ к незаконной информации». Полагаю, что с учетом обоснования таких заявлений есть процессуальные основания для заявления прокурором гражданского иска в порядке, установленного ст. 44 Уголовно-процессуального кодекса Российской Федерации, если будет доказано использование криптовалюты для легализации преступных доходов и иной противоправной деятельности.

Существующие пробелы законодательства в части регулирования деятельности криптобирж на территории Российской Федерации приводят к блокировке сайтов таких криптобирж. Так, в сентябре 2020 г. Роскомнадзор внес сайт крупнейшей по торговым объемам криптобиржи Binance в реестр запрещенных, письмо о блокировке получил крупнейший в СНГ сервис обмена криптовалют MINE.exchange. Это произошло на основании того, что, по мнению Роскомнадзора, сайты содержат запрещенную к распространению в России информацию, в частности объявления о продаже Bitcoin.

Установление в рамках уголовного судопроизводства обстоятельств использования в механизме преступного поведения криптовалюты предполагает проведение, по сути, отдельного финансового расследования. По информации

из Приволжского федерального округа мониторинг возможных незаконных операций с криптовалютой и идентификация получателя осуществляется во взаимодействии с Росфинмониторингом, в рамках которого анализируются данные деятельности наиболее распространенных для использования на территории Российской Федерации криптовалютных бирж, откуда регулярно запрашивать сведения о лицах, систематически занимающихся приобретением криптовалюты и последующей ее конвертацией в иные расчетные единицы. В настоящее время выработана практика и привлечением Росфинмониторинга и оперативных подразделений органов внутренних дел посредством применения специализированного программного обеспечения установления количество криптовалюты и операций по криптокошельку. Таким образом, само установление факта использования криптовалюты в механизме преступного поведения, не говоря о его фактическом аресте и конфискации, вызывает ряд организационных и правообеспечительных проблем.

Вышеуказанный Закон № 259 отнес в ст. 17 криптовалюту к категории имущества. Вместе с тем процедура ареста и конфискации (изъятие из оборота) криптовалюты связано с обращением с цифровыми кошельками (специализированными программами), представляющих допуск к обращению криптовалюты и одного отнесения криптовалюты к имуществу не создает эффективный правовой механизм обращение с ней. Решением данной проблемы не стало и внесение дополнений в ст. 128 Гражданского кодекса Российской Федерации, поскольку данная норма не отнесла криптовалюту ни к одному из вещных объектов. Закон № 259 также не внес необходимые изменения в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации, что оставило открытым вопрос формальных оснований и механизма конфискации цифровой валюты без юридического признания ее видом имущества в уголовном законодательстве.

Судить о возможном апробации обеспечительных мер в отношении криптовалют посредством установленного в Уголовно-процессуальный кодекс Российской Федерации порядка можно только гипотетически, поскольку вопрос о криптовалюте в приговорах судов практически не указывается. Для этого есть объективные причины, когда осужденные конвертировали криптовалюту на банковские карты российских банков). Практиками апробированы такие процессуальные действия как перевод в фиатную валюту или иное имущество [8, с. 8–14], в том числе в процессе следственного эксперимента. Это подтверждается приговорами по уголовным делам. Однако это никак не может рассматриваться как общепримененимый подход, поскольку существенным условиям таких действия является позитивное посткриминальное поведение. Представляется, что при таком подходе конвертация и хранение денежных средств на специализированном счету более подходит не только к режиму ареста, но и обращения с вещественными доказательствами. Схожесть с вещественными доказательствами также обусловлена обеспечением требуемым режимом хранения, оценки и перспектив реализации криптовалюты или конвертируемых денежных средств ввиду ее высокой волатильности.

В зарубежной практике примеры такого подхода имеются. Законодательство США предусматривает упрощенную процедуру продажи конфискованного при расследовании преступлений имущества, в том числе продажа криптовалюты. В Великобритании в доход государства обращается не сама криптовалюта, а ее денежный эквивалент, что закону не противоречит. Причем для конфискации криптовалюты по этому делу были применены нормы Закона Великобритании о доходах от преступлений (аналогичного нормам главы 15^1 Уголовного кодекса Российской Федерации).

Какие направления совершенствования? Видится, что подход к запрету или даже криминализации использование криптовалют вне отечественного правового поля в условиях глобализации интернет-пространства принципиально не изменить сложившуюся сегодня ситуацию. В определенной степени девальвирует ценность избранного законодателем подхода к регулированию цифровых прав и цифровых валют отсутствие запрета на совершение аналогичных действий с использованием зарубежной информационной инфраструктуры гражданами Российской Федерации. Следовательно, установление фактического способа совершения указанных преступлений (или места их совершения) в каждом конкретном случае потребует нетривиальных усилий правоохранительных органов, в том числе назначения и проведения ряда последовательных технических и информационных судебных экспертиз.

Ранее Правительство Российской Федерации утвердило концепцию законодательного регламентирования механизмов организации оборота цифровых валют, в которой не указано на изменение требований Уголовно-процессуального кодекса Российской Федерации в части механизма ареста и конфискации криптовалюты.

В случае легализации криптовалюты как официального платежного средства, как предлагает Минфин России [9], скорее всего она будет подпадать под категорию «иное имущество» в рамках ст. 128 Гражданского кодекса Российской Федерации [10, с. 45–49].

В этом случае необходимо внести изменения в широкий спектр статей федеральных законов. Так, в Уголовно-процессуальный кодекс Российской Федерации следует включить нормы, регулирующих порядок: изъятие и осмотр электронных носителей информации о цифровых валютах, копирование соответствующей информации; способы установления, фиксации сведений о владельце цифровой валюте и передаче их на ответственное хранение; процедуры проведения оценки их номинальной стоимости в рублях Российской Федерации; наложения ареста на подобное имущество (цифровые валюты либо цифровые активы) (дополнения в ст.ст. 81, 82, 115 и введение новой ст. 116.1 «Особенности и порядок наложения ареста на цифровую валюту» Уголовно-процессуального кодекса Российской Федерации).

Одним из наиболее острых вопросов в рассматриваемой сфере остается применение в практической деятельности механизмов поиска и последующего ареста криминальных доходов и имущества. Этому не соответствует положения ст. 2 закона об ОРД.

В очередной раз указываю на крайнюю востребованность формирования правовых, организационных и технических основ единой системы внутреннего финансового контроля, надлежащего информационного обмена и взаимодействия контролирующих и правоохранительных органов для успешного решения проблем уязвимости финансового рынка, и банковской системы перед попытками их использования в криминальных целях, борьбы с киберпреступлениями. Для преодоления сложившейся ситуации необходима активизация консолидированных усилий и реализация всего инструментария, которым располагают не только силовые ведомства, но и структуры банковской сферы, подразделения службы судебных приставов, налоговые органы в целях достижения возложенных на них задач [11].

Список литературы

1. Колчевский И. Б., Кузнецов А. Г. Криптовалюты на территории стран Содружества: оценка вероятных криминальных рисков и угроз. М., 2018. С. 13.

2. Изгагина Т. Ю. Криминальный рынок криптовалюты. Борьба с криминальными рынками в России: законодательные и правоприменительные проблемы: реализация положений Конвенции ООН против транснациональной организованной преступности : сборник статей / под общ. ред. О. С. Капинус. М. : Университет прокуратуры Российской Федерации, 2020. С. 64–72.

3. Internet Organised Crime Threat Assessment (IOCTA) 2020. URL: https://-www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

4. Информация Банка России от 27 января 2014 г. «Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн» // ИПО «Гарант».

5. Архипов А. В. Цифровые объекты как предмет хищения // Уголовное право. 2020. № 6. С. 16–23.

6. Генпрокуратура: Биткоины в России запрещены // РБК. URL: www.rbc.ru/-economics/06/02/2014/570417179a794761c0ce669d.

7. Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. … канд. юрид. наук. М., 2016.

8. Литвишко П. А. Юрисдикционные и международно-правовые аспекты обеспечительных и конфискационных мер в отношении виртуальных активов // Законность. 2021. № 3. С. 8–14 ; Тутынина И. Б., Химичева О. В. Применение мер уголовно-процессуального принуждения при расследовании преступлений, совершенных использованием криптовалюты : монография. М. : Юрлитинформ, 2022. С. 36.

9. Мантуров. Криптовалюта как платежное средство может быть легализована в России // Российская газета. 2022. 18 мая. URL: https://rg.ru/2022/05/18/manturov-kriptovaliuta-kak-platezhnoe-sredstvo-mozhet-byt-legalizovana-v-rossii.html.

10. Долгиева М. М. Конфискация криптовалюты // Законность. 2018. № 11. С. 45–49.

11. Генпрокуратура подготовила меры по борьбе с киберпреступностью в России. URL: https://tass.ru/obschestvo/9032391.

Ковальчук А. В.[1],
заместитель начальника
кафедры уголовного права
Академии Министерства внутренних дел
Республики Беларусь,
кандидат юридических наук, доцент

Духовник Ю. Е.[2],
доцент кафедры уголовного права
Академии Министерства внутренних дел
Республики Беларусь,
кандидат юридических наук, доцент

ВОПРОСЫ КВАЛИФИКАЦИИ ДЕЯНИЙ, СВЯЗАННЫХ С РАССЫЛКОЙ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, СОДЕРЖАЩИХ ИНФОРМАЦИЮ ОБ УГРОЗАХ ВЗРЫВОВ, В ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКЕ РЕСПУБЛИКИ БЕЛАРУСЬ

Анализ следственно-судебной практики за последние годы демонстрирует значительный рост преступлений, связанных с рассылкой сообщений с использованием информационно-коммуникационных технологий, содержащих информацию об угрозах взрывов [1; 2; 3; 4]. Юридическая оценка таким деяниям, выразившимся в направлении сообщений на электронные почтовые ящики, принадлежащие организациям, учреждениям и предприятиям, расположенным на территории Республики Беларусь, преимущественно осуществляется по ст. 340 «Заведомо ложное сообщение об опасности» Уголовного кодекса Республики Беларусь (далее – УК). В единичных случаях квалификация подобных деяний осуществляется по ст. 290 «Угроза совершением акта терроризма» УК.

В связи с не установлением лица, совершившего анализируемые деяния, а равно о его психическом отношении к содеянному, в правоприменительной деятельности возникает ряд затруднений, связанных с уголовно-правовой оценкой подобного рода фактов. Более того, правоприменитель сталкивается с такими вопросами, как: 1) кто может выступать адресатом сообщений, содержащих информацию об угрозах взрывов (только правоохранительные органы или государственные органы или организации, в задачи которых входит предотвращение действий, создающих опасность, либо любые организации всех форм собственности)?; 2) возможно ли принимать решение о возбуждении уголовного дела по ст. 340 УК без установления лица направившего сообщение, содержащее информацию об угрозе взрыва, тем самым, не установив признак *заведомости* ложно-

[1] © Ковальчук А. В., 2022.
[2] © Духовник Ю. Е., 2022.

сти такого сообщения?; 3) следует ли принимать решение о возбуждении уголовного дела по ст. 290 УК без установления лица направившего сообщение, содержащее информацию об угрозе взрыва, если в сообщаемых сведениях не содержатся требования выполнения каких-либо действий, при отсутствии намерения или возможности реализовать высказанную угрозу? Полагаем, что разрешение данных вопросов сформирует четкую правовую позицию квалификации и будет соответствовать единообразию правоприменительной практики.

Выскажем собственное мнение по обозначенным проблемным вопросам квалификации.

1. Квалифицируя содеянное по ст. 340 УК с учетом адресата, которому передано электронное сообщение об опасности, необходимо учитывать, что таковым может быть любой орган – как правоохранительный, в задачи которого входит предотвращение действий, создающих опасность, так и иной государственный либо негосударственный орган, поскольку диспозиция ст. 340 УК не содержат указания на особенности или исключения, касающиеся адресата.

2. Необходимо отметить, что не существует универсального ответа на вопрос об установлении признака «заведомости ложного сообщения», когда лицо, совершившее общественно опасное деяние, предусмотренное ст. 340 УК, не известно. Для установления данного признака субъективной стороны указанного состава преступления, следует опираться на оценку его объективных признаков, выраженных: в активном противоправном поведении лица (например, в одинаковом способе переданных сведений (посредством e-mail, комментариев на странице, электронного сообщения с абонентского номера иностранного оператора связи); неоднократной рассылке писем с одного IP-адреса; в рассылке одинаковых либо однотипных сообщений об опасности в адрес нескольких организаций; коротком промежутке времени между направленными сообщениями об опасности; сведений о нахождении отправителя за пределами Республики Беларусь; неподтвержденности в ходе проверки сообщаемых сведений и т. п. Указанный перечень является далеко не исчерпывающим и не может однозначно свидетельствовать о «заведомости» ложного сообщения об опасности. В каждом конкретном случае следует учитывать весь комплекс обстоятельств совершенного деяния. Безусловно, не следует забывать законодательный постулат о том, что неустранимые сомнения в виновности должны толковаться в пользу лица, совершившего преступление.

В соответствии со ст. 167 Уголовно-процессуального кодекса Республики Беларусь одним из оснований возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления, при отсутствии обстоятельств, исключающих производство по уголовному делу. При этом следует учесть, что признаки преступления, под которыми законодатель в ст. 11 «Понятие преступления» УК понимает виновность, общественную опасность, противоправность и наказуемость, не являются тождественными признакам состава преступления, содержание которых конкретизируется такими его элементами как объект, объективная сторона, субъект и субъективная сторона преступления. Соответственно для возбуждения уголовного дела по ст. 340 УК необходимо

установить наличие достаточных данных, указывающих на признаки преступления. В то же время возбуждение уголовного дела и его расследование является лишь процессуальной формой, направленной на дальнейшее установление всех признаков как преступления, так и состава преступления.

3. Относительно вопроса, касающегося уголовно-правовой оценки действий неустановленного лица, сообщившего сведения о нахождении в здании (помещении) взрывного устройства, по ст. 290 УК, следует отметить следующее.

Во-первых, для наличия угрозы совершением акта терроризма следует установить признаки самого акта терроризма. Обязательным признаком субъективной стороны состава преступления, предусмотренного ч. 1 ст. 289 «Акт терроризма» УК, являются специальные цели: 1) оказание воздействия на принятие решений органами власти, либо; 2) воспрепятствование политической или иной общественной деятельности, либо; 3) устрашение населения, либо; 4) дестабилизация общественного порядка, в то время как в ст. 340 УК обозначенные цели отсутствуют. Наиболее характерной для преступлений террористической направленности является цель устрашения населения, под которой понимается создание обстановки нервозности и недоверия граждан путем нарушения их нормальной жизнедеятельности путем внушения страха за жизнь и здоровье как самих себя, так и своих близких. При отграничении заведомо ложного сообщения об опасности от угрозы совершения акта терроризма необходимо учитывать, что при направлении электронного сообщения в адрес одного субъекта указанная цель отсутствует, поскольку переданная виновным информация не доводится до сведения населения, т.е. неограниченного круга лиц. При заведомо ложном сообщении об опасности виновный может преследовать любые цели, кроме тех, что указаны в ст. 289 УК (например, корыстные, хулиганские, намерение причинить вред конкуренту и др.). Внешним сходством рассматриваемых видов преступлений обладают такие признаки субъективной стороны состава ст. 289 УК, как дестабилизация общественного порядка и возможные хулиганские побуждения, при совершении преступления, предусмотренного ст. 340 УК. При этом под дестабилизацией общественного порядка следует понимать не любое нарушение общественного порядка, свойственное, по сути, для каждого совершаемого преступления, а существенное нарушение основ стабильности функционирования общества, когда восстановление общепринятого порядка и нормальной деятельности общества является затруднительным.

Во-вторых, важным критерием разграничения ст.ст. 290 и 340 УК является объем действий, совершенных виновным в рамках выполнения объективной стороны этих составов преступлений, характеризующих реальность угрозы и соответствие действительности передаваемых сведений. Реальность угрозы предполагает восприятие неизбежности реализации акта терроризма адресатами распространяемой информации. К примеру, о реальности угрозы свидетельствует факт обнаружения взрывного устройства (либо его муляжа), подтверждение изложенных в сообщении иных сведений. В таком случае деятельность лица будет свидетельствовать о нарушении безопасных условий жизнедеятельности

общества путем создания возможности причинения существенного вреда личности, обществу и государству. При установлении сведений о том, что переданная адресатом информация не соответствует действительности, а угроза объективно не могла быть реализована, то и состав угрозы актом терроризма, на наш взгляд, отсутствует, поскольку не причиняется существенный вред общественной безопасности, не создается реальная угроза причинения указанного вреда.

Таким образом, без установления целей совершения акта терроризма, реальности угрозы и соответствия действительности передаваемых сведений, состав преступления, предусмотренный ст. 290 УК, на наш взгляд, будет отсутствовать.

Список литературы

1. Информация о минировании учебных заведений не подтвердилась – МВД. URL: https://www.belta.by/incident/view/informatsija-o-minirovanii-uchebnyh-zavedenij-ne-podtverdilas-mvd-443786-2021/.

2. МВД: информация о минировании учреждений и организаций не подтверждается. URL: https://www.belta.by/society/view/mvd-informatsija-o-minirovanii-uchrezhdenij-i-organizatsij-ne-podtverzhdaetsja-450795-2021/.

3. Сообщение о минировании столичного ТЦ Outleto оказалось ложным. URL: https://www.belta.by/incident/view/soobschenie-o-minirovanii-stolichnogo-tts-outleto-okazalos-lozhnym-492021-2022/.

Азаренкова Е. А.[1],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук

Осипов В. А.[2],
заместитель начальника кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент

ПУБЛИЧНЫЕ ПРИЗЫВЫ И ДЕЙСТВИЯ КАК ПРИЗНАК ОБЪЕКТИВНОЙ СТОРОНЫ ОТДЕЛЬНЫХ СОСТАВОВ ПРЕСТУПЛЕНИЙ ПРОТИВ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ И ОСНОВ КОНСТИТУЦИОННОГО СТРОЯ И БЕЗОПАСНОСТИ ГОСУДАРСТВА

В действующем Уголовном кодексе Российской Федерации (далее – УК РФ) содержится значительное количество норм, устанавливающих ответственность за публичные действия, публичные призывы, публичное распространение различного рода информации. Настоящая статья посвящена отдельным составам преступлений гл. 24 и гл. 29 УК РФ.

Таблица 1

<table>
<tr><td>205.2</td><td>280</td><td>280.1</td><td>207.1</td><td>207.2</td><td>207.3</td><td>280.3</td><td>282</td></tr>
<tr><td colspan="2">Публичные призывы (+в ст. 205.2 – публичное оправдание…)</td><td colspan="2">Публичное распространение</td><td colspan="2">Публичные действия</td><td colspan="2">Действия, совершенные публично</td></tr>
</table>

Общим в приведенном перечне составов преступлений усматривается признак публичности. Как справедливо отмечается в специальной литературе, признак публичности в ряде статей уголовного законодательства обозначен в качестве конструктивного, в других – усиливает ответственность (является квалифицирующим), в-третьих – «публичные формы совершения преступления проявляются наряду с другими, поэтому законодатель использует либо более широкие понятия, как, например, распространение, разглашение, либо наряду с ними придает публичности самостоятельное значение» [3, с. 104].

Обязательным признаком объективной стороны составов преступлений, предусмотренных ст.ст. 205², 280, 280¹ УК РФ**,** является публичность. Согласно

[1] © Азаренкова Е. А., 2022.
[2] © Осипов В. А., 2022.

толковому словарю Д. Н. Ушакова, под публичным понимается деяние, устроенное для общества, в присутствии общества, публики, то есть открыто, гласно [16]. В толковом словаре Т. Ф. Ефремовой данный термин трактуется аналогично: «публичный, то есть совершающийся в присутствии публики, людей; открытый, гласный» [15].

Значение данного признака разъясняется в ряде постановлений Пленума Верховного Суда Российской Федерации [5, 6]. Так, публичными признаются призывы, осуществленные в любой форме и обращенные к другим лицам с целью побудить их к совершению определенного рода преступлений. Например, Д. В. Антонов при помощи принадлежащего ему мобильного телефона, действуя умышленно, с целью побуждения неограниченного круга лиц к экстремистской деятельности, разместил на общедоступном интернет-ресурсе, то есть публично, текстовые сообщения в виде комментариев к видеозаписи [11].

В другом примере, Абдрахманов в общественном месте – в мечети и на улице в непосредственной близости от нее, публично, в присутствии разновременно нескольких граждан, оправдывал терроризм, призывал с оружием в руках совершать «джихад», т. е. физически истреблять лиц, не исповедующих ислам, к тому же включал на мобильном устройстве видеоролики боевых действий с призывами к джихаду [9].

Таким образом, суды в приговорах обозначают в чем выражалась публичность действий – или размещение текста на общедоступном ресурсе (если преступление совершается посредством использования сети Интернет), или соответствующие высказывания и призывы в присутствии других людей в общественном месте.

Кроме того, необходимо раскрыть еще один признак объективной стороны – «призыв». В толковом словаре В. И. Даля призыв используется в словосочетаниях «призывать кого-либо куда-то, или к чему-либо», то есть звать, кликать, приглашать, просить или требовать [14]. То есть по смыслу анализируемых статей предполагается, что публичный призыв, обращенный к неопределенно широкому кругу людей, должен побуждать других лиц к совершению преступлений террористической или экстремистской направленности, или признанию и одобрению данной идеологии насилия, враждебным или насильственным действиям по отношению к различным социальным группам по национальному или этническому признаку. Так, Али оглы осознавал, что с размещенным им на личной странице в социальной сети «Мой мир» высказыванием может ознакомиться неопределенное количество пользователей, так же он осознавал, что фраза «Русские, вперед, убейте всех *** кроме Кавказцев, а вот Ара – исключение» могла побудить какого-либо пользователя к совершению насильственных действий в отношении так называемых «неверных», то есть не мусульман [12].

Заслуживает отдельного внимания определение квалифицирующих признаков вышеуказанных составов преступлений. Так, в ст.ст. 205.2 и 280.1, помимо распространения призывов посредством использования информационно-телекоммуникационных сетей, говорится еще и об электронных сетях, определение

которых не раскрывается. Кроме того, в одних случаях используется терминология «в том числе сети «Интернет»», а в другом – «(включая сеть «Интернет»)». Отсутствие единообразия указанных законодательных конструкций, на наш взгляд, требует определенной корректировки.

Распространение COVID-19 у некоторых людей вызвало панику. Кроме того, значительно влияние на общественное настроение оказало распространение ложных сведений, касающихся сущности пандемии коронавирусной инфекции, существующей эпидемиологической обстановки. Оперативно реагируя на общественные изменения, сообщение под видом достоверной, заведомо ложной информации неограниченному кругу лиц, законодатель установил ответственность в ст.ст. 207^1 и 207^2 УК РФ за «публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан и заведомо ложной общественно значимой информации, повлекшее тяжкие последствия».

Сам термин «распространение» используется законодателем и при характеристике других составов, например, в ст. 137 УК РФ. Верховный Суд Российской Федерации, под распространением сведений по смыслу данной нормы понимает сообщение (разглашение) их одному или нескольким лицам в устной, письменной или иной форме и любым способом (в частности, путем передачи материалов или размещения информации с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет) [7].

К тому же, в Обзоре по отдельным вопросам судебной практики, сказано, что по смыслу ст.ст. 207^1 и 207^2 УК РФ, под публичным распространением следует понимать доведение информации до сведения других лиц, используя при этом, например, СМИ, сеть Интернет, массовую рассылку сообщений абонентам мобильной связи, отправку сообщений посредством использования мессенджеров (WhatsApp, Viber), путем выступления на собрании, митинге, распространение листовок, вывешивание плакатов [4]. Например, Пичугин, будучи журналистом, в своем блоге, который читает определенное количество людей, разметил заведомо ложную информацию об обстоятельствах, представляющих угрозу жизни и безопасности граждан, а именно: об обстоятельствах эпидемии и распространении новой коронавирусной инфекции. О публичном характере распространенной информации свидетельствует тот факт, что сообщение было размещено в открытом канале, предназначенном для просмотра неограниченным кругом пользователей, имеющим значительное количество подписчиков (лиц, кому информация из данного канала поступает в автоматическом режиме), цитировалось другими пользователями сети Интернет, в том числе, не являющимися подписчиками данного канала. При просмотре публикаций имеется значок, который свидетельствует о количестве просмотров той или иной информации разными людьми. Правоприменитель толкует данную норму следующим образом: ст. 207^1 УК РФ запрещает распространение информации, создающей у получателя такой информации устойчивое мнение о реальном наличии обстоятельств, угрожающих жизни и безопасности граждан, в то время как обстоятельства, о которых

сообщается в рассматриваемой информации, отсутствуют в реальной действительности. При этом значение имеет не только фактически (буквально) изложенная информация, но и обстоятельства ее изложения, форма и способ передачи такой информации. Один из свидетелей по данному делу пояснил, что информацию, содержащуюся в сообщении, он воспринял серьезно, позвонил родственникам, сказал, чтобы не выходили на улицу. Кого-то предупредил устно, кому-то скинул ссылку на размещенное сообщение [8]. Таким образом, было установлено, что данная публикация могла вызвать панику в обществе, а ссылки на определенные источники лишь усиливали это воздействие.

Следует отметить, что распространение определенной информации не является тождественным призывам к совершению каких-либо запрещенных законом действий. Термин «распространение» можно раскрыть как «сделать обширнее, больше, расширить, пропагандировать что-либо, сделать доступным для многих, дать возможность усвоить информацию, сообщить, сделать известным для многих [16]. Да и сам законодатель не отождествляет данные термины. Как справедливо отмечает А. Ю. Сичкаренко, в ряде составов Особенной части УК РФ, в качестве альтернативных отмечены публичные действия и распространение материалов (ст. 242 УК РФ), распространение определенных сведений в публичном выступлении или СМИ (ст. 137 УК РФ). В качестве квалифицирующего признака выделяется совершение публичных призывов или действий, с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет (ч. 2 ст. 205^2, ч. 2 ст. 280 УК РФ). Таким образом, автор заключает, что публичные действия и действия по распространению информации не тождественны [13, с. 22]. Возникает вопрос – изменяется ли степень общественной опасности при выполнении действий публично или их совершении с использованием информационно-телекоммуникационных сетей. Ответ на данный вопрос может стать предметом самостоятельного научного исследования не в рамках данной статьи.

В этом году УК РФ был дополнен ст. 207^3, которая призвана защитить общественную безопасность от распространения так называемых «фейковых» новостей в связи с проведением специальной операции на Украине. Здесь используется тот же прием законодательной техники, что и в ранее рассмотренных статьях. Публичность в ст. 207^3 УК РФ определяется с учетом места, способа, обстановки и других обстоятельств дела (например, обращения к группе людей в общественных местах, на учебных занятиях, собраниях, публикация в соцсетях и т. п.). Распространение таких «фейков» является общественно-опасным, поскольку может привести к дестабилизации обстановки внутри страны.

Несмотря на довольно непродолжительное время существования исследуемой статьи, было возбуждено несколько уголовных дел. В марте 2022 г. блогер Белоцерковская на своей странице в «Инстаграм»[1] опубликовала несколько записей, в которых содержатся заведомо ложные сведения об использовании Вооруженных сил Российской Федерации для уничтожения городов и гражданского населения Украины [2]. Еще одно уголовное дело по п. «д» ч. 2 ст. 207^3 УК РФ

[1] Признана экстремистской организацией и запрещена на территории Российской Федерации.

было возбуждено против Клокова, который позвонил нескольким лицам в Крыму и Подмосковье и тем самым «публично распространил под видом достоверных сообщений заведомо ложную информацию» о действиях Вооруженных сил Российской Федерации [1].

Используемая законодателем в ст. 280³ УК РФ формулировка «публичные действия» не является новеллой. В то же время, необходимы разъяснения – какие действия, выполняемые публично, будут считаться уголовно наказуемыми. Так, в частности, диспозиция ст. 148 УК РФ содержит аналогичную формулировку – «публичные действия». По смыслу данной статьи, под уголовно наказуемые действия подпадают, например, карикатуры, сатирические высказывания, видеоролики и т. п.

Публичными следует считать такие действия, которые совершаются: 1) в общественном месте (например, на улицах, в парках, на общественном транспорте), при этом обязательно присутствие других лиц в вышеуказанных общественных местах (наличие двух и более лиц); 2) посредством трансляции по телевидению и радио, а также путем распространения листовок, распространение обращений путем массовой рассылки электронных сообщений и т. п. При этом количество просмотров публикации не влияет на квалификацию деяния как преступления, запрещенного исследуемой статьей.

В диспозиции ст. 282 УК РФ говорится о публичном совершении действий (в том числе с использованием средств массовой информации либо информационно-телекоммуникационных сетей, включая сеть Интернет), которые способны вызвать у людей ненависть либо вражду по отношению к другим лицам по признакам пола, расы, национальности, и т. д. Верховный Суд Российской Федерации разъяснил, что к таким действиям могут быть отнесены высказывания, обосновывающие или утверждающие необходимость геноцида, массовых репрессий, депортаций, применения насилия, в отношении представителей какой-либо нации, расы, социальной группы, приверженцев той или иной религии. Например, 14 октября 2015 г. Васильев и Андреев, на светлый фасад жилого дома крупным шрифтом черной краской нанесли надписи, осознавая, что данный текст будет доступен для ознакомления и восприятия неограниченному кругу лиц, то есть понимая, что они действуют публично. Согласно заключению экспертизы, соответствующая надпись унижает и оскорбляет отдельные группы лиц и направлена на возбуждение розни (вражды, ненависти), содержит призыв к насильственным действиям (уничтожению) по отношению к темнокожим как к группе лиц, выделяемой по расовому признаку, кавказцам и азиатам как группам лиц, выделяемым по этническому признаку [10].

Таким образом, мы пришли к следующим выводам. Публичность как признак объективной стороны отдельных составов преступлений означает, что деяние носит открытый характер, совершается в присутствии других лиц или совершается таким образом, что может стать доступным для восприятия несколькими лицами. Значение для квалификации могут иметь и обстоятельства, при которых происходит деяние, например, место, время, массовая рассылка сообщений в мессенджерах, открытый доступ к определенному ресурсу в сети Интернет.

Призыв – определенное побуждение других лиц совершить преступление экстремистской или террористической направленности [17, с. 868–871]. Публичное распространение – доведение различного рода информации до сведения других лиц. При этом, публичные действия, запрещенные законом и публичное распространение соответствующей информации не следует отождествлять.

Список литературы

1. В Башкирии возбуждено первое уголовное дело о фейках о российской армии. URL: https://ufa.rbc.ru/ufa/14/04/2022/625808db9a7947ab93f03731?.

2. В России завели первые уголовные дела за фейки о военных. URL: https://www.forbes.ru/society/459297-v-rossii-zaveli-pervye-ugolovnye-dela-protiv-rossian-za-fejki-o-voennyh?utm_source=yxnews&utm_medium=desktop.

3. Маталаев Ш. З. Признак «публичности» и проблемы квалификации преступлений экстремистской направленности // Актуальные проблемы уголовного и уголовно-процессуального права: современное состояние и перспективы развития : сборник научных трудов. М. : Саратовский источник, 2016. С. 103–115.

4. Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2 : утвержден Президиумом Верховного Суда Российской Федерации 30 апреля 2020 г.

5. Постановление Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» (ред. от 03.11.2016) // СПС «КонсультантПлюс».

6. Постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // СПС «КонсультантПлюс».

7. Постановление Пленума Верховного Суда Российской Федерации от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (ст.ст. 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // СПС «КонсультантПлюс».

8. Приговор Богородского городского суда (Нижегородская область)от 11 ноября 2020 г. № 1-194/2020 по делу № 1-194/2020. URL: //sudact.ru/regular/-doc/wCYwnZ3Sx1gP/.

9. Приговор Верховного Суда Чеченской Республики от 27 января 2014 г. № 2-24/2013 2-6/2014 по делу № 2-24/2013. URL: //sudact.ru/regular/doc/o4c-RjjRCuVrT/.

10. Приговор Головинского районного суда г. Москвы № 1-447/2014. URL:https://sud-praktika.ru/precedent/59814.html.

11. Приговор Киселевского городского суда (Кемеровская область) от 27 июля 2020 г. № 1-310/2020 по делу № 1-310/2020. URL: //sudact.ru/regular/doc/-pp9Z2ZHRxjVQ/.

12. Приговор Центрального районного суда г. Хабаровска (Хабаровский край) от 19 сентября 2014 г. № 1-367/2014 по делу № 1-367/2014. URL: //sudact.-ru/regular/doc/JHhdU9cfXEln/.

13. Сичкаренко А. Ю. Публичность как признак преступного нарушения права на свободу совести и вероисповеданий // Вестник КРУ МВД России. 2019. №4 (46). С. 21–25.

14. Толковый словарь В. И. Даля. URL: https://www.slovardalja.net/word.-php?wordid=32917.

15. Толковый словарь Т. Ф. Ефремовой. URL: https://onlinedic.net/efremova/-page/word88024.php.

16. Толковый словарь Д. Н. Ушакова. URL: https://onlinedic.net/ushakov/page/-word59738.php.

17. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) / под ред. Н. Г. Кадникова. 6-е изд., перераб. и доп. М. : ИД «Юриспруденция», 2019. С. 868–871.

Горач Н. Н.[1],
доцент кафедры судебно-экспертной
и оперативно-разыскной деятельности
Московской академии Следственного комитета
Российской Федерации,
кандидат педагогических наук

Лаврова О. Н.[2],
заместитель начальника кафедры уголовного процесса
Московского областного филиала
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент

О НЕКОТОРЫХ ВОПРОСАХ ПРИЗНАНИЯ КРИПТОВАЛЮТЫ ПРЕДМЕТОМ ПРЕСТУПЛЕНИЯ ПО УГОЛОВНЫМ ДЕЛАМ, СВЯЗАННЫМ С РАССЛЕДОВАНИЕМ ВЗЯТОЧНИЧЕСТВА

Криптовалюта является своеобразным платежным средством за оказанные или подлежащие оказанию услуги взяткополучателя.

Вместе с тем, криптовалюта должна получить юридическую оценку в как предмет преступления. И если из-за неопределенности статуса криптовалюты с момента выявления самых первых фактов торговли наркотическими средствами за нее никто из авторов не считал это непреступными действиями, то применительно к взяточничеству некоторые авторы утверждают о непреступности таких действий именно по той причине, что Уголовный кодекс Российской Федерации соответствующие признаки прямо не предусматривает. Так, по мнению, Я. Н. Ермоловича, «с учетом отсутствия правового регулирования, скорее всего, криптовалюты не могут признаваться предметом взятки или коммерческого подкупа…» [1]. Данная ситуация схожа с научной дискуссией о признании криптовалюты предметом имущественных преступлений, однако имеется определенная специфика. В отличие от преступлений против собственности, где есть конкретный потерпевший, заинтересованный в возбуждении и расследовании уголовного дела, как правило, и взяткодатель, и взяткополучатель обычно скрывают факт совершенного преступления и противодействуют предварительному расследованию. Кроме того, латентность криптовалютного взяточничества максимальна.

Справедливым представляется замечание В. А. Петрова, что «если принять точку зрения о том, что криптовалюта не является имуществом и не может быть предметом преступного посягательства, в том числе и предметом взятки, то противодействие совершению такого рода преступлений будет приближаться к нулю» [2].

---

[1] © Горач Н. Н., 2022.
[2] © Лаврова О. Н., 2022.

В настоящее время разработаны криптовалюты, анонимность которых намного превосходит таковую у биткоинов, которые практические работники даже называют «прозрачной криптовалютой» [3]. Более анонимными криптовалютами, например, являются: Monero, ZCash, PIVX, Komodo, Zcoin, NAV coin, ZenCash, Verge, DASH, SmartCash, BlackCoin и пр.

Криптовалюты уже сейчас активно используются для подкупа должностных лиц. Преступный мир не ожидает пока государство окончательно нормативно урегулирует порядок обращения криптовалют на своей территории.

Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 112^4 части третьей Гражданского кодекса Российской Федерации» (далее – ФЗ) ввел в Гражданский кодекс Российской Федерации (далее – ГК РФ) понятие «цифровые права» (ст. 141) [4], отнеся их к категории иного имущества. Указанный ФЗ стал одновременно и революционным, и компромиссным, поскольку термин «криптовалюта» так и не появился в ГК РФ.

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» также дает определения криптовалюты, хотя и содержит понятие «цифровая валюта», одним из ее признаков называя легальное использование в качестве средства платежа. При этом использование криптовалюты в качестве средства платежа в Российской Федерации в настоящее время запрещено.

Постановление Пленума Верховного Суда Российской Федерации от 9 июля 2013 г. № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях»[5] (далее – Постановление по делам о взяточничестве) упоминает о цифровых правах раскрывая содержание имущественных прав – «в тех случаях, когда предметом взятки являются имущественные права, у должностного лица, получившего такое незаконное вознаграждение, возникает возможность вступить во владение или распорядиться чужим имуществом как своим собственным, требовать от должника исполнения в свою пользу имущественных обязательств, получать доходы от использования бездокументарных ценных бумаг или цифровых прав и др.» (пункт 9). На основании вышеизложенного следует, что в данном случае пленум разъясняет, что необходимо говорить не о передаче (переходе) цифровых прав лицу получающему взятку, а о приобретении дохода в результате использования цифровых прав.

Можно предположить, что приобретение лицом, занимающим определенное должностное положение цифровых прав следует квалифицировать в виде получения взятки по такому признаку как «иное имущество» в случае, если сами права не переходят к взяткополучателю, а им приобретается только возможность извлечения дохода от их использования.

Следует отметить, что учетом современного системного толкования норм права в случае, если криптовалюту используют в качестве предмета взятки, это возможно осуществить по такому признаку как «иное имущество». Такой

подход в целом отвечает и судебной практике отнесения криптовалют к предмету преступлений против собственности, и представлениям большинства исследователей об ее месте в системе объектов гражданского права.

Современные проблемы в отечественном законодательстве, связанные с формированием института правового регулирования криптовалют, не должно препятствовать в установленном законом порядке признанием их в качестве предмета получения взятки. Закон предусматривает, и правоприменительная практика это подтверждает, что в качестве взятки могут признаваться даже предметы ограниченные или запрещенные, то есть изъятые из гражданского оборота (к примеру, наркотические средства).

Соответственно, если криптовалюты будут урегулированы отечественным законодательством, это не повлияет на фактическую возможность криптовалют выступать эквивалентом стоимости товаров и услуг, не будет препятствием для незаконного оборота криптовалют, в том числе и в коррупционных отношениях, следовательно, не повлияет на возможность их квалификации в качестве предмета взятки, что подтверждается правоприменительной практикой.

Так, 26 февраля 2021 г. Вторым Западным окружным военным судом Российской Федерации Б. и К. были осуждены по ч. 6 ст. 290 УК РФ и приговорены к 9 и 12 годам колонии строгого режима соответственно. Им было вменено получение взятки в биткоинах. Полученные преступниками биткоины были конфискованы в доход государства [6].

С учетом изложенного мы можем резюмировать, что современное состояние отечественного уголовного права уже в настоящий момент дает возможность без каких-либо дополнений и изменений законодательства признавать криптовалюту в предусмотренных законом случаях предметом взятки и привлекать к уголовной ответственности лиц, которые ее используют для дачи или получения взятки.

Таким образом, осуществляя уголовно-правовую квалификацию взятки, криптовалюту можно оценивать в качестве предмета преступления, относя ее к иному имуществу.

Само же преступление следует считать оконченным в тот момент, когда у лица, занимающего определенную должность, возникла реальная возможность указанной криптовалютой распорядиться, либо воспользоваться.

Список литературы

1. Ермолович Е. Н. О коррупционных и должностных преступлениях должностных лиц и сотрудников организаций ОПК // Оборонно-промышленный комплекс: вопросы права. 2020. № 2.

2. Петров В. А. Квалификация действий лиц, совершающих преступления с использованием криптовалюты на территории Российской Федерации // Российский следователь. 2018. № 4.

3. Долгиева М. М. Конфискация криптовалюты // Законность. 2018. № 11.

4. 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» // Российская газета. 2020. № 173. 6 авг.

5. Постановление Пленума Верховного Суда Российской Федерации от 9 июля 2013 г. № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях (ред. от 24.12.2019) // Российская газета. 2013. № 154. 17 июля.

6. Приговор по делу № 1-7/2021 // Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru.

Андреев А. А.[1],
заместитель начальника
факультета заочного обучения
Московского областного филиала
Московского университета МВД России
имени В.Я. Кикотя

Куликова О. Н.[2],
доцент кафедры уголовно-правовых дисциплин
Смоленского филиала
Саратовской государственной юридической академии,
кандидат юридических наук, доцент

ТРАНСФОРМАЦИЯ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА В УСЛОВИЯХ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ

Основная идея нашего исследования отражает изменение уголовного законодательства Российской Федерации посредством включения в отдельные составы преступлений отягчающих признаков, сопряженных с использованием интернет-платформ. Целью работы является систематизация положений действующего российского закона, определяющего общественную опасность деяний, совершаемых с использованием телекоммуникационной глобальной системы компьютерной сети. Новизной исследования выступает авторское понятие трансформации отечественного уголовного законодательства в условиях актуальных информационных процессов современного периода развития государства, общества, их институтов, правосознания и правовой культуры граждан.

Как отмечают современные правоведы: «Юридическая наука современного периода приобрела ярко выраженный практико-ориентированный характер. Основной задачей видится совершенствование юридической техники, оптимизация законотворческого процесса и правоприменительной практики, систематизация и кодификация законодательства» [2, с. 9]. Вопросы изменения уголовного законодательства в российском государстве, в свою очередь, отражают качественно-позитивный своевременный подход видения отдельных положений Уголовного кодекса в части криминализации деяний, совершаемых в условиях глобальных процессов информатизации, цифровизации, развития в обществе киберкультуры.

По прогнозам компании Cisco в отчете Visual Networking Index (VNI) [3] в России на начало 2022 г. 867 млн граждан России подключатся к глобальной сети, что составит около 6 устройств на человека (в сравнении с 2017 г. – 3,6 шт.). В 2021 г. российская интернет-аудитория составила почти 124 млн граждан [1]. Так, руководитель Роскомнадзора А. Липов активизировал внимание россиян о том, что множество угроз влечет за собой стремительное развитие технологий, информатизации, цифровизации. Глава ведомства отметил: «Постоянные атаки

[1] © Андреев А. А., 2022.
[2] © Куликова О. Н., 2022.

на критически важные инфраструктуры в мире, интернет-платформы требует все больше технологичности и проактивности для обеспечения защиты людей. Государство должно оградить граждан от опасного контента, бесконтрольного распространения персональных данных, мошенничества, посягательства на детей и подростков» [5]. Поэтому вопросы трансформации российских законов, устанавливающих уголовную ответственность в случае совершения опасных деяний с использованием интернет-пространства является крайне актуальным.

Приводимые нами данные свидетельствуют о повышенной социально-правовой значимости необходимости законодательного установления уголовной ответственности за определенные виды общественно-опасного преступного поведения в сфере информационных технологий, цифровизации, которое следует признавать незаконным. Мы отмечаем, что действующий Уголовный кодекс Российской Федерации должен успевать реагировать на любые правовые, технические и иные условия и обстоятельства в сфере информационной безопасности российского государства. Эти условия обязательно должны составлять либо быть связанными с составляющими национальную, в том числе информационную, безопасность компонентами, которые законодателю необходимо включить в уголовный закон. Отечественные уголовно-правовые нормы могут их включать как в основной состав в качестве обязательных признаков содеянного, так и выступить отягчающими признаками путем их введения в уже имеющиеся статьи Уголовного кодекса Российской Федерации. При указанных обстоятельствах можно будет свидетельствовать о перспективах и положительных тенденциях информационного развития в российском государстве и правовом регулировании общественных отношений в этой области действующим законодательством.

Как нами отмечалось в монографическом исследовании, в вопросах трансформации уголовного законодательства Российской Федерации наиболее актуален процесс криминализации и пенализации законов, так как именно они учитывают научные доводы и обоснования необходимости введения определенных рычагов уголовно-правового воздействия в отношении лиц, совершивших преступления. Научные подтверждения законодательного дополнения, включения дополнительных уголовно-правовых мер в Уголовный и Уголовно-исполнительный кодексы Российской Федерации, по нашему мнению, опираются на положения науки, реализуемые в практической деятельности [4, с. 94].

Действующее национальное законодательство в области уголовно-правовых отношений, на протяжении более двух десятков лет претерпело свыше 170 существенных дополнений и изменений (в части описания общих положений, введения новых преступных деяний, отдельных признаков составов преступлений, порядка исполнения наказаний за их совершение). В частности, в вопросах отражения «Интернет способа» совершения преступления и в части изменения собственно компьютерных видов преступлений и их признаков с момента вступления Уголовного кодекса Российской Федерации 1996 г. в силу и по настоящее время введено в действие 23 законодательных дополнения.

В контексте законодательного изменения, свидетельствующего о трансформации российского Уголовного кодекса, следует указать ряд отдельных положений, отражающих содержание системы общественно-опасных деяний, совершаемых с использованием Интернета за последние годы. Ряд преступлений был изменен законодателем и основной состав ряда противоправных деяний стал сопряжен с заведомым использованием виновным лицом телекоммуникационного пространства для совершения посягательства. Иные уголовно-правовые характеристики отягчающих признаков вводились в соответствующие статьи Особенной части уголовного закона Российской Федерации с учетом увеличения случаев преступных действий с использованием Интернета, социальных сетей, изменения социально-воспитательных ориентиров в обществе, случаев преступлений морально-нравственного характера, последствий деяний либо уверенности виновных в их не установлении при совершении деяний таким способом.

К указанным преступным деяниям относятся следующие виды преступлений, которые претерпели законодательную трансформацию, как и сам уголовный закон, когда такой процесс охватил законодательное включение новых составов преступлений в Уголовный кодекс Российской Федерации. В первую очередь это компьютерные преступления, расположенные в гл. 28 Уголовного кодекса Российской Федерации, которые впоследствии в 2017 г. пополнились самостоятельным преступным деянием в виде неправомерного воздействия на критическую информационную инфраструктуру российского государства, регулируемую Федеральным законом от 26.07.2017 № 194-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Конституционные права человека, такие как жизнь и неприкосновенность частной жизни лица, охраняются действующим законодательством в случае совершения такого посягательства с использованием сети Интернет (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110^1, ч. 2 ст. 110^2, ч. 3 ст. 137 Уголовного кодекса Российской Федерации). Интересы несовершеннолетнего, такие как здоровье, телесная неприкосновенность, жизнь охраняются действующим законом с 2017 г. Так, п. «в» ч. 2 ст. 151^2 Уголовного кодекса охватывает вовлечение взрослым несовершеннолетнего в совершение действий, представляющих опасность для жизни последнего посредством информационно-телекоммуникационных сетей.

Экономическая сфера обеспечивается уголовно-правовой охраной при использовании информационных платформ Интернета. В частности, это мошенничество в сфере компьютерной информации (ст. 159^6 Уголовного кодекса Российской Федерации), введенное законодателем в 2012 г., и ст. 187 Уголовного кодекса Российской Федерации, в которой были наказуемы изготовление, сбыт поддельных кредитных либо расчетных карт и иных платежных документов, а после 2015 г. законом охватывался неправомерный оборот средств платежей.

Далее отметим введение отягчающего обстоятельства в ст. 205^2 Уголовного кодекса Российской Федерации такого способа, как совершение через сеть Интернет, в состав о публичных призывах к осуществлению террористической деятельности, публичному оправданию терроризма или пропаганде терроризма.

В уголовном законодательстве по вопросу охраны здоровья населения были введены изменения, когда совершение незаконного производства, сбыта, пересылки наркотикосодержащих веществ и обращение фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и оборот фальсифицированных биологически активных добавок охватывало использование информационно-телекоммуникационных сетей (п. «б» ч. 2 ст. 228^1, ч. 1^1 ст. 238^1 Уголовного кодекса Российской Федерации).

Пункт «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242^1, п. «г» ч. 2 ст. 242^2 и п. «г» ч. 2 ст. 245 Уголовного кодекса Российской Федерации в 2012 и 2017 гг. соответственно охватили рассматриваемый вид способа совершения посягательств в области национальной нравственности. Указанные преступления охватывают оборот порнографических материалов с изображением, участием несовершеннолетнего лица либо при жестоком обращении с животными. Посягательства с использованием интернет-платформ охватили и экологические преступления. Так предметом посягательства с 2019 г. выступают особо ценные дикие животные и водные биологические ресурсы, принадлежащие к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации (ч. 1^1 ст. 258^1 Уголовного кодекса Российской Федерации).

В области общественной безопасности как компонента в целом национальной безопасности России отметим трансформацию законодательного охвата уголовно-правовых норм, когда с использованием информационно-коммуникационных технологий совершаются деяния экстремистской направленности (ст.ст. 280, 280^1, 282 Уголовного кодекса Российской Федерации).

Изложенное позволяет нам сделать вывод о том, что отечественное уголовное законодательство охраняет наиболее важные общественные отношения и блага, охватывающие развитие институтов государства и общества, правосознание населения и правовую культуру граждан, которые могут претерпеть негативное воздействие при использовании ресурсов сети Интернет. Постоянные законодательные интерпретации норм уголовного закона посредством его изменения (дополнения) отражают процесс трансформации, затрагивающий актуальные для нашего поколения информационные процессы, которые без информационно-технических ресурсов существовать не могут.

Тем самым рассмотренный нами процесс изменения уголовно-правовых норм, именуемый в теории уголовного права криминализацией деяния, становящегося преступным и наказуемым, при законодательном включении в Уголовный кодекс Российской Федерации, связан с внесением дополнений в этот нормативно-правовой акт государства. А любой процесс перемены, преобразования, изменения, перехода, превращения в той или иной области или сфере в общем ее понимании свидетельствует о трансформации. Тем самым, мы можем говорить о трансформации действующего с января 1997 г. в российском государстве Уголовного кодекса Российской Федерации при совершении преступлений посредством интернет-ресурсов.

Итак, трансформация уголовного законодательства Российской Федерации в условиях информационных процессов – это изменение уголовного закона, поставившего под охрану широкий перечень важных для личности, государства и общества объектов и общественных отношений посредством введения уголовной ответственности с учетом социально-экономических, правовых и иных потребностей жизни современного человека в условиях использования информационно-коммуникационных технологий, интернет-платформ.

Список литературы

1. Digital 2021: главная статистика по России и всему миру. URL: https://spark.ru/user/115680/blog/74085/digital-2021-glavnaya-statistika-po-rossii-i-vsemu-miru.

2. Матанцев Д. А., Рыжова Ю. В., Токмачева А. Ю. История и методология юридической науки : учебно-практическое пособие. М. : Академия управления МВД России, 2020.

3. К 2022 г. пользоваться интернетом будут 69 % россиян. URL: https://vc.ru/-future/54678-k-2022-g-polzovatsya-internetom-budut-69-rossiyan.

4. Куликова О. Н., Масягина Ю. Б. Правовая форма и правовые средства в правовом регулировании. М. : Юрлитинформ, 2022.

5. Число пользователей интернета в России достигло 124 млн. URL: https://-tass.ru/obschestvo/12698757.

Хакимова Э. Р.[1],
заместитель начальника кафедры криминалистики
Уфимского юридического института МВД России,
кандидат юридических наук, доцент

Дайшутов М. М.[2],
начальник кафедры уголовного права
Московского университета МВД России
имени В..Я. Кикотя,
кандидат юридических наук, доцент

НЕКОТОРЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Появление цифровых денег, криптовалют, массовое внедрение умных часов, домов, других интернет-вещей, использование квадракоптеров, навигаторов, флеш-карт, каждодневное увеличение передачи пользовательских данных в Интернете, масштабный уход в онлайн многих сфер жизнедеятельности общества в связи с пандемией COVID-19 неизбежно повлияли на резкое увеличение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Выступая на расширенном заседании коллегии МВД России в 2022 г., Президент Российской Федерации Владимир Владимирович Путин подчеркнул, что задачей силовиков является обеспечение кибербезопасности граждан [1].

Действительно, возникла острая необходимость в изучении особенностей расследования преступлений, совершенных с применением информационно-телекоммуникационных технологий. Рассмотрим особенности некоторых следственных действий при расследовании указанных преступлений.

Осмотр места происшествия по рассматриваемым преступлениям – важное следственное действие. Так, в ходе подготовительного этапа к осмотру необходимо заранее взять объяснения у руководителя организации, лица, отвечающего за обслуживание компьютерного оборудования, выяснив обстоятельства, связанные блокированием помещения, где находится вычислительная техника, охранная сигнализация, логины, пароли, коды, документация для последующего беспрепятственного доступа к ним. Важно помнить, что дистанционное блокирование помещения или компьютера часто связано с самоуничтожением либо всей информации, либо наиболее значимой для расследования уголовного дела. Так, например, при несоблюдении правил входа в помещение может включаться устройство защиты, и компьютерная техника уничтожает необходимую информацию. При осмотре места происшествия также необходимо выяснить

[1] © Хакимова Э. Р., 2022.
[2] © Дайшутов М. М., 2022.

осуществление резервного копирования информации, ведение протокола деятельности работы компьютерной техники в течение дня. Установив, что на предприятии имеется сеть Интернет, нужно определить условия предоставления указанных услуг.

Перед производством рабочего этапа осмотра места происшествия рекомендуется ознакомить специалиста, который будет участвовать в следственном действии, с протоколами объяснений, допросов, изъятой документацией.

Состав следственно-оперативной группы при расследовании киберпреступлений весьма разнообразен: это специалист-криминалист, специалист по средствам вычислительной техники, сотрудник ФСТЭК России, Центра защиты информации (при обнаружении на месте осмотра конфиденциальной компьютерной информации, машинных носителей, специальных средств защиты от несанкционированного доступа и (или) технических средств негласного получения (уничтожения, блокирования) компьютерной информации), специалист по сетевым технологиям (в случае наличия периферийного оборудования удаленного доступа или локальной компьютерной сети), специалист по системам электросвязи (при использовании для дистанционной передачи данных каналов электросвязи), оперативные сотрудники БСТМ. Также в состав группы могут входить бухгалтеры, специалисты спутниковых систем связи, операторы компьютерных систем и сетей электросвязи и др.

По прибытии на место совершения преступления следователю необходимо обеспечить недопущение воздействия на имеющуюся информацию. Важно оперативно отстранить сотрудников организации от компьютерных средств и иных гаджетов, установить наличие локальной сети в организации. При осмотре монитора необходимо зафиксировать имеющуюся информацию на нем путем фотографирования или составления рисунка, схемы, в ходе детального осмотра выявить программы, запущенные на техническом устройстве. Помимо этого, нужно зафиксировать наличие подключения внешних кабелей к компьютерным средствам для того, чтобы в последующем правильно восстановить их соединения.

Рабочий этап осмотра начинается со сбора традиционных доказательств: следов пальцев рук, следов обуви, орудий взлома, тетрадей с записями и др. Важным является проведение указанного следственного действия на месте. Так, специалист в присутствии понятых подключает свой ноутбук к сети или компьютеру для проведения антивирусного тестирования системы, проверяет наличие (отсутствие) вредоносных программ. Для получения образцов для сравнительного исследования файлов специалист осуществляет копирование файлов системы. Важно отметить, что при обнаружении «зараженных» файлов, они не должны вылечиваться. Факты их обнаружения фиксируются в протоколе осмотра, в дальнейшем экспертиза определит групповую принадлежность обнаруженных вирусов, вредоносность последствий их применения, дату создания, квалификацию лица, их создавшего.

Важно отметить, что при осмотре велика роль понятых, так как в суде сторона обвинения может попытаться опровергнуть факт наличия вредоносных программ на компьютере в момент осмотра.

Помимо результатов осмотра места происшествия, доказательства, собранные при проведении обыска, также способствуют успешному расследованию рассматриваемых преступлений. Чаще всего он проводится в жилище (помещении), также проводится личный обыск подозреваемого (обвиняемого) лица.

Подготовительный этап – важная часть этого следственного действия. Определение круга участников обыска, консультация с оперативными сотрудниками, сотрудниками БСТМ дают возможность следователю выработать эффективные тактические приемы проведения указанного следственного действия. При подготовке к обыску следователь решает вопросы, схожие с подготовкой к осмотру места происшествия: о виде и конфигурации используемой компьютерной техники; о том, подключена ли она к локальной сети или Интернету; о наличии службы информационной безопасности и защиты от несанкционированного доступа; системе электропитания помещений, где установлена техника; квалификации пользователей. Владение такой информацией облегчит следователю доступ к хранящейся в компьютере информации и максимально повысит ее доказательственную базу.

Внезапность обыска часто имеет решающее значение. Это позволит избежать быстрого уничтожения компьютерной информации. Если получены сведения о том, что компьютеры организованы в локальную сеть, следует заранее установить местонахождение всех средств компьютерной техники, подключенных к этой сети (принтеров, сканеров) и организовать групповой обыск одновременно во всех помещениях, где установлены компьютеры [2, с. 30].

Необходимо учесть, что при обыске следует организовать охрану обыскиваемых площадей, компьютеров, хранилищ машинных носителей информации, всех пунктов (пультов) связи, охраны и электропитания, находящихся на объекте обыска, специальных средств защиты от несанкционированного доступа, помещений и других объектов (стендов, сейфов и т. п.).

При обзорной стадии обыска необходимо определить местонахождение подозреваемого (обвиняемого) на объекте обыска, отстранить его от осуществления любых действий, никого не впускать и не выпускать на время проведении данного следственного действия.

Так, при производстве обыска у Б. сотрудниками отдела «БСТМ» были изъяты листы бумаги, содержащие 19 конфиденциальных логинов и паролей пользователей сети Интернет. При расследовании уголовного дела, возбужденного по ч. 1 ст. 165 и ч. 1 ст. 272 Уголовного кодекса Российской Федерации, было установлено, что записи выполнены собственноручно Б., полностью соответствуют реквизитам протокола провайдера, отражающим все сеансы работы пользователей в сети Интернет. Эти вещественные доказательства в совокупности с другими доказательствами, даже с учетом противодействия следствию со стороны Б., позволили привлечь его к уголовной ответственности за совершение более 38 преступлений [3, с. 32].

Подводя итог, отметим, что в статье рассмотрены некоторые особенности проведения осмотра места происшествия и обыска при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных

технологий. Но успех расследования конкретного киберинцидента зависит только от профессионализма следователя, его специальных познаний и опыта расследования подобных преступлений, от качественно подобранных членов следственно-оперативной группы, особенно специалиста, а также исходной информации, которая находится в распоряжении у следователя в начале расследования.

Список литературы

1. Расширенное заседание коллегии МВД России // URL: http://www.kremlin.-ru/events/president/transcripts/comminity_meetings/67795.

2. Архипова И. А. Актуальные проблемы расследования преступлений в сфере компьютерной информации // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : сборник статей. М. : Академия управления МВД России, 2018. С. 29–31.

3. Дуленко В. А. Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации : учебное пособие // Уфа : Уфимский юридический институт МВД России, 2007. С. 32. URL: https://-nashaucheba.ru/v54450/.

Чуканова Е. С.[1]*,*
заместитель начальника
кафедры уголовного права и криминологии
Московского областного филиала
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент

Бабченко А. И.[2]*,*
курсант 2 курса 202 учебного взвода
Московского областного филиала
Московского университета МВД России
имени В.Я. Кикотя

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В УГОЛОВНОМ ПРАВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

На сегодняшний день происходит глобальная трансформация всего общества под влиянием цифровизации многих сфер жизни и внедрение технологий искусственного интеллекта. Термин искусственный интеллект – многогранный и его рассмотрение возможно с нескольких сторон. Например, как современные высокотехнологические средства, применяемые при расследовании преступлений. Однако, наиболее интересным аспектом являются проблемы уголовной ответственности за вред, причиненный при использовании систем искусственного интеллекта.

Современное уголовное право не в полной мере отвечает уровню научно-технического прогресса, а также уровню достижений науки и техники. Исходя из этого, идет активная работа над совершенствованием уголовно-правовых норм в сфере регулирования общественных отношений, связанных с использованием искусственного интеллекта. Законодательное закрепление данного понятия указано в Федеральном законе «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве» представляет собой комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека» [9]. Полностью идентичное понятие указано в п. «а» ст. 5 Указа Президента Российской Федерации «О развитии искусственного интеллекта в Российской Федерации» [8].

---

[1] © Чуканова Е. С., 2022.
[2] © Бабченко А. И., 2022.

Как отметил И. Н. Мосечкин, формулирование авторского понятия «искусственный интеллект» осложняется значительным количеством видов таких систем, в связи с чем классифицировал технологии искусственного интеллекта по следующим основаниям:

1. В зависимости от сферы применения: механический (выполняет рутинную работу); аналитический (обрабатывает большой массив данных); интуитивный (способен приспосабливаться к различным ситуациям); эмпатический (способен распознавать эмоции людей).

2. В зависимости от конкретных функций: генерация текста, распознавание речи и др.

3. В зависимости от функциональных возможностей: сильный и слабый.

4. В зависимости от цели создания: для законной деятельности; для противоправной деятельности [2, с. 13–14].

Искусственный интеллект в рамках уголовного закона можно рассматривать в разных аспектах. Целью создания и внедрения искусственного интеллекта в деятельность правоохранительных органов служит, прежде всего, повышение эффективности расследования и раскрытия преступлений. Одним из принципов, провозглашенных в Национальной стратегии развития искусственного интеллекта, является защита прав и свобод человека при использовании систем искусственного интеллекта. Однако, преступные замыслы полностью нарушают данный принцип – статистические данные МВД России за январь–март 2022 г. показывают, что каждое четвертое преступление совершается с использованием IT-технологий [3].

Также И. Н. Мосечкин рассматривает возможность обособления общественных отношений, связанных с применением технологий искусственного интеллекта, в отдельный непосредственный объект. По нашему мнению, данное положение довольно актуально, так как искусственный интеллект имеет существенные различия от компьютерных программ, например, функция самообучения. Такой функцией обладает искусственный интеллект, что и приближает его возможности к когнитивным способностям человека [2, с. 13–14].

Кроме этого, представляется возможным рассматривать искусственный интеллект как предмет преступного посягательства, так как, программы, созданные на основе искусственного интеллекта, помещены в материальную оболочку и на основании ст. 128 и п. 1 ст. 129 Гражданского кодекса Российской Федерации искусственный интеллект можно отнести к имуществу, которое может отчуждаться и переходить от одного лица к другому [1]. Беспилотные дроны, роботы могут быть украдены либо повреждены. На основании этого, искусственный интеллект может выступать в качестве предмета преступления, предусмотренного в статьях главы 21 Уголовного кодекса Российской Федерации («Преступления против собственности») [6], т. е. в как чужое имущество. Предметом посягательства могут выступать программы, базирующиеся на технологиях искусственного интеллекта, например, предметом преступлений, предусмотренных в ст. 272 и ст. 273 Уголовного кодекса Российской Федерации. Однако, в данном случае возникает еще одна дискуссионная проблема по поводу

признания компьютерной информации предметом преступления. Стоит согласиться с мнением профессора Л. М. Прозументова, который признает компьютерную информацию предметом преступления, закрепленного в ст. 272 Уголовного кодекса Российской Федерации [5].

При этом сущность технологий искусственного интеллекта отличается от сущности имущества или компьютерной информации, что требует совершенствование уголовного законодательства и выделения деяния, направленного на причинение вреда технологиям искусственного интеллекта в качестве самостоятельного преступления.

В настоящий момент рассмотрение искусственного интеллекта в качестве потерпевшего следует признать нецелесообразным, так как в соответствии со ст. 42 Уголовно-процессуального кодекса Российской Федерации потерпевшими являются физические и юридические лица [7]. Кроме того, степень самообучаемости и независимости систем искусственного интеллекта от человека не достигла должного уровня развития на сегодняшний день. Несмотря на это, имеет место быть дискуссия о квалификации категории вреда, причиненного здоровью человека при повреждении искусственных органов и тканей, а также таких средств реабилитации, которые управляются за счет нейронных сигналов, посылаемых головным мозгом человека, и функционируют с остальным человеческим организмом как единое целое. И. О. Ткачев предлагает расширить границы человеческого организма при рассмотрении вопроса о причинении вреда личности путем включения в них вышеуказанных понятий [4, с. 49].

Рассмотрев искусственный интеллект с точки зрения объективных признаков, стоит его проанализировать и со стороны субъективных признаков, в частности субъекта преступления, что является актуальным дискуссионным вопросом. С точки зрения действующего законодательства в качестве субъекта преступления выступает только физическое лицо (ст. 19 Уголовного кодекса Российской Федерации) [6], т. е. с точки зрения законодателя искусственный интеллект на сегодняшний день не подлежит уголовной ответственности. Однако, в условиях постоянно изменяющегося общества можно предположить, что и правовой статус искусственного интеллекта будет претерпевать изменения. И. Н. Мосечкин отмечает, что современные технологии искусственного интеллекта не обладают должным уровнем самосознания. В связи с этим их нельзя признать в качестве субъектов преступлений сейчас. В будущем все же возможность совершения преступлений искусственным интеллектом имеет место быть. На основе этого автор подчеркивает необходимость разработки исследований, посвященных определению перечня предполагаемых субъектов преступления [2, с. 13–14].

Вышесказанное подчеркивает актуальность исследуемой проблемы и необходимость разработки теоретических обоснований привлечения к уголовной ответственности за преступления, связанные с искусственным интеллектом.

Таким образом, искусственный интеллект в научной литературе рассматривается в нескольких аспектах: как средство совершения преступления, как объ-

ект и предмет преступления, а также как предполагаемый в будущем субъект общественно опасных деяний. Это, конечно же, требует модернизации уголовно-правовых норм, рассматривающих общественные отношения по поводу причинения вреда технологиям искусственного интеллекта в качестве самостоятельного объекта преступления.

Список литературы

1. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ (ред. от 25.02.2022) // СПС «КонсультантПлюс».

2. Мосечкин И. Н. Искусственный интеллект в уголовном праве: перспективы совершенствования охраны и регулирования : монография. Киров : Вятский государственный университет, 2020. С. 13–14.

3. Краткая характеристика состояния преступности в Российской Федерации за январь – март 2022 года // МВД России: сайт. URL: https://мвд.рф/reports/item/-29705686/.

4. Ткачев И. О. К вопросу о понятии вреда здоровью // Уголовное право. 2021. № 7 (131). С. 49.

5. Уголовное право. Особенная часть : учебник для вузов / [В. В. Агильдин и др.] ; под общ. ред. Л. М. Прозументова. Томск: Издательский дом Томского государственного университета, 2019. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000666293.

6. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 25.03.2022) // СПС «КонсультантПлюс».

7. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 25.03.2022) // СПС «КонсультантПлюс».

8. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // СПС «КонсультантПлюс».

9. Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // СПС «КонсультантПлюс».

Лаврентьева М. С.[1],
заведующий аспирантурой и докторантурой
Российской государственной академии
интеллектуальной собственности,
кандидат юридических наук, доцент

Туркин М. М.[2],
преподаватель
Государственного бюджетного
профессионального образовательного учреждения
города Москвы «Юридический колледж»,
кандидат юридических наук

КИБЕРМОШЕННИЧЕСТВО В СФЕРЕ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Правовая природа кибермошенничества, как следует из названия самого понятия, основана на мошенничестве. Перечень противоправных деликтов приведен в ст.ст. 159–159.6 Уголовного кодекса Российской Федерации (далее – Уголовный кодекс, УК РФ). Уголовный кодекс дает данному противоправному деянию следующее определение: «мошенничество, то есть хищение чужого имущества или приобретения права на чужое имущество путем обмана или злоупотребления доверием». Как известно объектом данного преступления являются отношения определенной формы собственности. Объективная сторона мошенничества выражается в хищении чужого имущества или приобретение права на чужое имущество путем обмана или злоупотреблением доверием. [3, с. 8]

Мошенничество, совершенное в цифровой реальности, является кибермошенничеством. Кибермошенничество – доктринальное понятие, точного определения данному виду преступления в законодательстве не дано. [5, с. 43]

Полагаем, что в этом случае допустимо провести некую параллель, и исходя из признаков мошенничества и киберпространства, возможно констатировать, что кибермошенничество – это один из видов противоправной деятельности по своим основным объективным признакам, совпадающей с мошенничеством, но совершенное в киберпространстве. Таким образом, стоит признать тот факт, что основным отличием, на наш взгляд, между мошенничеством и кибермошенничеством является «место совершения» противоправных деяний.

При этом некоторые действия кибермошенников выражаются не только в незаконном завладении имуществом или правом на него, но и противоправном завладением различными данными (персональными данными, информации о счетах, кодами, паролями и др.), которые в последующем используются как способ совершения преступления. Данные деяния совершаются в цифровом простран-

---

[1] © Лаврентьева М. С., 2022.
[2] © Туркин М. М., 2022.

стве. В свою очередь имущество или права на него мошенникам, будущий пострадавший сам передает лично, не подозревая о совершении в отношении него противоправных деяний [4, с. 191].

Переходя непосредственно к объекту нашей статьи, целесообразно пояснить, что право интеллектуальной собственности (далее – ПИС, ИС) провозглашается ст. 44 Конституции Российской Федерации, кроме того, ею гарантируется охрана прав на результаты литературного, научного, технического, художественного, а также других видов творчества.

Благодаря повсеместному введению ИС в информационную среду, стала очевидна ее роль как одного из основных элементов в сфере кибербезопасности. Способы охраны ИС и защиты ПИС выходят на первоочередные места, становясь одной из частей общей системы информационной безопасности в киберпространстве. При существовании высокого уровня динамики, остро стоит вопрос о реализации разрабатываемых механизмов защиты ИС в данной среде. Одновременно значимость поднятых вопросов проявляется в реализации Закона Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и других нормативных правовых актах в глобальной информационно-коммуникационной среде, а, следовательно, выступает некой защитой от киберпреступности в целом, и кибермошенничества в частности.

Кибермошенничество в сфере ИС сопоставимо с мошенничеством в реальной жизни. Различие заключается в том, что кибермошенничество в сфере интеллектуальной собственности совершается в цифровом пространстве, в то время как обычное мошенничество совершается в обыденной реальности. Еще одним главным различием являются методы совершения таких преступлений [6, с. 1].

Мошенничество в области интеллектуальной собственности включает в себя мошенничество, при котором изобретателей и других правообладателей заманивают заплатить деньги за явно официальную регистрацию своей интеллектуальной собственности или за профессиональное развитие и продвижение своих идей, но они не получают ожидаемых услуг. Одной из главных проблем современности в кибермошенничестве в период цифровизации в сфере интеллектуальной собственности, на наш взгляд, является не только недостаточное, правовое регулирование данных вопросов, но и слабая материальная база, небольшое количество специалистов в этой сфере, состоящих на службе в правоохранительных органах и др.

При этом зачастую преступники пытаются придать своим действиям легитимный характер, закамуфлировав их под видом, например, гражданско-правовых отношений. В этой связи, некоторые правовые пробелы приходится решать уже в судебном порядке. Так, в России 28 марта 2014 г. Суд по интеллектуальным правам (далее – Суд, СИП) утвердил: «Справку по вопросам, возникающим при рассмотрении доменных споров». В свою очередь, постановление президиума СИП №СП-21/4 представляет собой ряд «общих положений», основным предназначением которых выступает разрешение вопросов по доменным спорам и упорядочение сложившейся судебной практики.

При этом Суд рекомендует: «доменные споры рассматриваются с учетом Парижской конвенции по охране промышленной собственности, ст. 10 Гражданского кодекса Российской Федерации и Единообразной политики по разрешению споров (UDRP) в связи с доменными именами (ICANN).», а международные доменные споры должны рассматривать Административные трибуналы при ВОИС.

Как уже отмечалось, вопросы охраны и защиты ПИС в глобальной информационно-коммуникационной среде – сети Интернет, а, следовательно, и противодействие таким деяниям, носит комплексный характер и должно разрешаться единовременно. Названный аспект обусловлен следующими положениями:

1. Местом совершения правонарушений является не только сеть Интернет, но и другие, различные информационно-телекоммуникационные сети, например, сети подвижной радиотелефонной связи.

2. При использовании их, могут совершаться самые многообразные деликты: плагиат; незаконная торговля объектами ПИС; торговля контрафактной продукцией через «Интернет-магазины». При этом правонарушитель может находиться в другом государстве, т. е. такие деяния носят транснациональный характер.

3. Объектами деликтов могут выступать как сами права ИС, так и результаты интеллектуальной деятельности.

4. Данные правонарушения также могут, а зачастую и сопровождаются другими преступными деяниями, к которым можно отнести: распространение вредоносных программ, нарушение правил обработки персональных данных, распространение «фейков» и др.

Методы защиты от нарушений прав интеллектуальной собственности в киберпространстве определяются комплексностью их характера. Одним из актуальных вопросов в Российской Федерации остается ответственность провайдеров (Интернет-сервисов) за нарушения прав, в том числе и за киберпреступность, и кибермошенничество в сфере ИС [7, с. 1, 8, 12]. Однако до настоящего времени названная проблема не разрешена.

Таким образом, борьба с кибермошенничеством в сфере ИС остается значимой задачей для всех уровней государственных органов, при этом затрагивая интересы не только коммерческих организаций, но и простых граждан. С учетом динамики развития ИС в глобальной информационно-коммуникационной среде, и перехода многих участников правоотношений в «ОН-ЛАЙН» режим, вопрос о создании эффективной защиты и охраны ПИС в киберпространстве, в том числе защита от киберпреступности и кибермошенничества приобретает первостепенное значение. Полагаем, что чем выше уровень законотворческой деятельности по защите и охране ПИС, особенно от кибермошенничества, тем эффективнее становится механизм разрешения возникающих проблем, в том числе и безопасность в сети Интернет.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ,

от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // Собрание законодательства Российской Федерации. 2020. № 31. Ст. 4398.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 31.07.2020) // Собрание законодательства Российской Федерации. 1996. № 25.

3. Аванесян С. Р. Мошенничество как форма хищения // Право: теория и практика. 2007. № 4 (93).

4. Блинников В. А., Бриллиантов А. В., Вагин О. А. Уголовное право России. Части общая и особенная : учебник / под ред. А. В. Бриллиантова. 2-е изд., перераб. и доп. М. : Проспект, 2017.

5. Завидов Б. Д., Ибрагимова З. А. Мошенничество в СВТ // Современное право. 2001. № 4.

6. РБК. ТОП-5 кибермошенничеств с самым большим ущербом в Башкирии. URL: https://ufa.rbc.ru/ufa/19/07/2020/.

7. Черников В. В. Борьба с пиратством в IT-отрасли: тренды 2017 года. URL: https://consultant19.ru/wp-content/uploads/sites/31/2017/09/Statya.pdf.

8. Юрочкин Н. С. Кибермошенничество: характеристика, приемы и методы его совершения // Таврический научный обозреватель. 2016. № 12-2.

9. Директива 2000/31/ЕС Европейского парламента и Совета Европейского Союза «О некоторых правовых аспектах информационных услуг на внутреннем рынке, в частности, об электронной коммерции (Директива об электронной коммерции)» [рус., англ.] (Вместе с «Исключениями из статьи 3») (Принята в г. Люксембурге 08.06.2000) // СПС «Гарант». URL: https://base.garant.ru/2568904/.

10. Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «Гарант». URL: https://www.garant.ru/products/ipo/prime/doc/1685377/.

11. Постановление Президиума Суда по интеллектуальным правам от 28 марта 2014 г. № СП-21/4 «Об утверждении справки по вопросам, возникающим при рассмотрении доменных споров» // СПС «Гарант» URL: https://www.garant.ru/products/ipo/prime/doc/70579692/.

Ларина Л. Ю.[1],
директор юридического института
Рязанского государственного университета
имени С.А. Есенина,
кандидат юридических наук, доцент

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ КАК ПРИЗНАК СОСТАВА ПРЕСТУПЛЕНИЯ

С развитием современных технологий и в условиях масштабной цифровизации, затрагивающей практически все сферы общественных отношений, увеличиваются риски использования таких технологий при совершении преступлений. В п. 42 Стратегии национальной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 2 июля 2021 г., указано, что в нашем государстве растет число преступлений, совершаемых с использованием информационно-коммуникационных технологий. В научной среде также обращается внимание на увеличение количества таких деяний [3, с. 34]. При этом отдельными авторами отмечается, что за последние годы количество совершаемых таким способом преступлений увеличилось в двадцать пять раз [2, с. 172].

Действующее российское уголовное законодательство содержит признак, выражающийся в использовании информационно-телекоммуникационных сетей (далее – ИТС), в 28 статьях Особенной части. В большинстве случаев он представляет собой квалифицирующий или особо квалифицирующий признак, характеризующий, как правило, способ совершения преступления. Лишь в нескольких случаях законодатель использует термин ИТС в основном составе преступления. Так, например, применительно к мошенничеству в сфере компьютерной информации (ст. 159⁶ Уголовного кодекса Российской Федерации) в качестве альтернативного выступает совершение этого деяния путем вмешательства в функционирование ИТС. В данном случае речь идет не просто об использовании этих сетей, а о совершении в отношении них целенаправленных действий, которые нарушают установленный процесс обработки, хранения, передачи компьютерной информации. С этой точки зрения указанные сети представляют собой средство совершения преступления.

В преступлениях, регламентированных в ст.ст. 171², 185³ Уголовного кодекса Российской Федерации, законодатель указывает на использование ИТС в качестве способа совершения преступления. Статья 274 Уголовного кодекса Российской Федерации в числе прочего содержит норму об ответственности за нарушение правил эксплуатации ИТС, а ч. 3 ст. 274¹ Уголовного кодекса Российской Федерации – за нарушение правил доступа к таким сетям. В последних случаях указание на ИТС характеризует предмет преступления.

Нормативное определение ИТС раскрывается в ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях

---

[1] © Ларина Л. Ю., 2022.

и о защите информации». В частности, под таковой понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Данное определение перегружено специальными терминами, значение которых понятно не каждому человеку. В самом общем виде к таким сетям относятся сети мобильной (сотовой) связи, локальные и глобальные компьютерные сети, которые используются при помощи сотовых или IP-телефонов, компьютеров, ноутбуков, нетбуков, планшетов, смарт-часов, других «умных» устройств и специальных технических средств.

Законодатель, конструируя признаки отдельных преступлений, во всех случаях, когда речь идет о способе в форме использования ИТС, делает конкретизацию, указывая формулировку «в том числе сети "Интернет"». Такая детализация, на первый взгляд, является лишней, поскольку отнесение сети Интернет к числу ИТС является общепризнанным и никем не оспаривается. Более того, сеть Интернет является самой распространенной ИТС, используемой при совершении преступлений. Однако указанная конкретизация, на наш взгляд, в данном случае должна иметь место, поскольку уголовный закон обращен, прежде всего, к обычному гражданину, у которого должно сформироваться четкое представление о том, какие именно действия находятся под уголовно-правовым запретом.

Стоит обратить внимание, что само по себе указание на сеть Интернет сделано законодателем различными юридико-языковыми средствами. В одних случаях используется формулировка «в том числе сети "Интернет"» (ст. ст. 205^2, 222–222.2, 242^1, 280 Уголовного кодекса Российской Федерации), а в других «включая сеть "Интернет"» (ст. ст. 110, 110^1, 128^1, 228^1, 242^2, 280^1 Уголовного кодекса Российской Федерации и др.). Смысл обоих конструкций одинаков, однако использование различных языковых форм может создать у граждан ложное впечатление об их различии. Целесообразно хотя бы в рамках одного кодекса использовать единообразные языковые конструкции построения норм, оставив один из вариантов.

В четырех статьях Уголовном кодекса Российской Федерации законодатель наряду с ИТС указывает в качестве альтернативы электронные сети (ст. 205^2, ст. 228^1, ч. 1.1 ст. 258^1, ст. 280^1 Уголовного кодекса Российской Федерации). При этом действующее законодательство такого понятия не только не раскрывает, но и не использует нигде, кроме Уголовного кодекса Российской Федерации. В комментариях к Уголовному кодексу Российской Федерации можно встретить разъяснение о том, что «электронная сеть – это электронная почта, технология и служба по пересылке и получению электронных сообщений (писем) между пользователями компьютерной сети, в том числе Интернет» [5, с. 36]. Кроме тавтологичности, это определение методологически не верно, поскольку электронная сеть рассматривается частью ИТС.

В судебной практике вменение альтернативного признака «с использованием электронной сети» нам не удалось встретить. Однако он встречается в комплексном варианте: «с использованием электронной или информационно-телекомму-

никационной сети» [1; 8]. Указанные два признака разделяет союз «или», предполагающий альтернативу, т. е. применение одного из этих признаков. Поскольку при признании лица виновным суд должен установить конкретные действия, за совершение которых виновный подвергается уголовной ответственности, то указание альтернатив недопустимо. Суд должен четко в приговоре определить, какие именно сети использовал виновный.

Встречается в судебной практике и другой тип ошибок – указание в описании преступного деяния как электронных, так и ИТС, перечисляя их через союз «и» или через запятую [7; 8].

Подобные судебные ошибки возникают из-за сложностей понимания правоприменителем содержания понятия «электронная сеть». Е. А. Русскевич очень точно отметил, что «указание на электронную сеть в ряду квалифицирующих признаков статей Особенной части Уголовного кодекса Российской Федерации явилось следствием ситуативного и необдуманного законотворчества» [9, с. 361]. Действительно, использование термина «электронная сеть» в приведенных уголовно-правовых нормах создает сложности на практике, является излишним и подлежит исключению.

Использование ИТС при совершении преступлений по-разному отражается в оценке общественной опасности совершенных таким образом деяний. В тех случаях, когда использование таких сетей характеризует предмет преступления (например, ст. 274 Уголовного кодекса Российской Федерации), общественная опасность имеет теснейшую связь с содержанием непосредственного объекта. Иным образом происходит, когда рассматриваемый признак характеризует способ или средство совершения преступления. Анализ содержащих такие признаки норм показывает, что их можно разделить на три группы. К первой группе следует отнести преступления, при совершении которых рассматриваемый способ направлен на облегчение совершения преступления, на усложнение его раскрытия или расширение масштабов преступной деятельности (ст.ст. 171^2, 222 – 222^2, 228^1, 230, 238^1, 242 – 242^2 Уголовного кодекса Российской Федерации). В таких случаях специфика и технические особенности используемых сетей телекоммуникации принципиального значения не имеет. Например, через сеть Интернет можно охватить широкий круг лиц, которые могут стать покупателями оружия или наркотических средств. Здесь не имеет значения насколько публично действует виновный: размещает ли он информацию в общедоступной группе или общается индивидуально.

К второй группе относятся преступления, при совершении которых использование ИТС является проявлением публичного характера и направлено на распространение информации среди максимально широкого круга лиц, что и обусловливает повышенную общественную опасность таких деяний (ст.ст. 128^1, 205^2, 280, 280^1, 282, 354^1 Уголовного кодекса Российской Федерации). В таких случаях рассматриваемый признак касается не любого использования ИТС. К примеру, если информацию, содержащую реабилитацию нацизма направить ограниченному кругу лиц в личных сообщениях в социальной сети или пись-

мами конкретным адресатам по электронной почте, то нельзя делать вывод о повышении общественной опасности содеянного по сравнению с теми же действиями, совершенными в ходе публичного выступления. Изменение общественной опасности будет иметь место лишь в тех случаях, когда рассматриваемые сети использовались виновным для придания своим действиям максимально публичного характера, для доступности преступной информации неограниченному кругу лиц.

Третья группа преступлений носит смешанный характер, то есть в зависимости от обстоятельств дела может иметь признаки как первой, так и второй группы преступлений (например, ст.ст. 110–110² Уголовного кодекса Российской Федерации).

Таким образом, толкование и практическое применение признака, выражающегося в использовании при совершении преступления ИТС, зависит от того, как он влияет на общественную опасность содеянного.

Еще одним вопросом, требующим обсуждения, является определение перечня преступлений, в которых рассматриваемый признак может играть квалификационное значение. Например, первую группу преступлений можно дополнить близкими по механизму их совершения (ст.ст. 234 и 234¹ Уголовного кодекса Российской Федерации).

Стоит отметить, что в науке уголовного права есть позиция о том, что рассматриваемые признаки следует исключить из Уголовного кодекса Российской Федерации. Это предлагает сделать Н. В. Летёлкин, одновременно дополнив уголовный закон новым составом преступления «Использование информационно-телекоммуникационных сетей (включая сеть «Интернет») при совершении преступления» [6, с. 12]. Схожую позицию занимает И. В. Савельев, предлагающий сохранить рассматриваемый признак только для случаев, когда он «не повышает общественную опасность деяния существенно (нет смены категории преступления на тяжкую)» [10, с. 484–485]. Н. В. Летёлкин главным признаком преступлений, совершаемых с использованием ИТС, определяет направленность посягательства на общественные отношения в сфере охраны правомерного пользования сетями коммуникации [6, с. 10–11]. Такой подход вызывает возражения, поскольку подобные преступления могут не причинять никакого ущерба указанным отношениям. Кроме того, при совершении преступлений само по себе использование указанных сетей может быть вполне правомерным. На наш взгляд, абсолютно верно законодатель при конструировании квалифицирующих и особо квалифицирующих признаков, не указывает на неправомерный характер использования указанных сетей.

Представляется, что включение в Уголовный кодекс Российской Федерации предлагаемого состава ничем не обосновано и нецелесообразно. Суть предлагаемой авторами нормы состоит в запрете совершить преступление определенным способом. Такой подход нарушает принцип non bis in idem, допуская двойную ответственность за одно и то же деяние.

Список литературы

1. Апелляционное определение Верховного суда Чувашской Республики от 27 мая 2020 г. по делу № 22-748/2020 // СПС «КонсультанПлюс».

2. Глазкова Л. В. Преступления экстремистской направленности, совершаемые с использованием сферы телекоммуникаций и компьютерной информации // Актуальные проблемы российского права. 2021. № 12. С. 167–176.

3. Евдокимов К. Н. Уголовная ответственность за преступления против жизни и здоровья, совершенные с использованием информационно-коммуникационных технологий // Российский следователь. 2021. № 12. С. 34–38.

4. Кассационное определение Второго кассационного суда общей юрисдикции от 9 ноября 2021 г. № 7У-10814/2021[77-3586/2021] // СПС «КонсультантПлюс».

5. Комментарий к Уголовному кодексу Российской Федерации в 4 т. Т. 3. Особенная часть. Раздел IX. М.: Юрайт, 2022.

6. Летелкин Н. В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей: включая сеть «Интернет» : автореф. дис. … канд. юрид. наук. Н. Новгород, 2018.

7. Определение Первого кассационного суда общей юрисдикции от 1 июня 2021 г. № 77-1947/2021 // СПС «КонсультантПлюс».

8. Определение Первого кассационного суда общей юрисдикции от 19 ноября 2019 г. № 77-7/2019 // СПС «КонсультантПлюс».

9. Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук.

10. Савельев И. В. Преступление, осложненное искусственным интеллектом: перспективы ближайших уголовно-правовых преобразований // Вопросы российской юстиции. 2020. № 7. С. 475–488.

Горенская Е. В.[1],
старший научный сотрудник
Института законодательства и сравнительного правоведения
при Правительстве Российской Федерации,
кандидат юридических наук, доцент

ПРОБЛЕМЫ КВАЛИФИКАЦИИ НЕЗАКОННОГО ПРЕДПРИНИМАТЕЛЬСТВА В ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОМ КОМПЛЕКСЕ ПРИ ВЫДАЧЕ ЛИЦЕНЗИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Нефть, газ и уголь – главные полезные ископаемые (далее также – ПИ), имеющие не только экономическое, но и стратегическое значение для России. Они оказывают значительное влияние на формирование энергетической политики и обеспечение энергетической безопасности Российской Федерации.

Отечественный топливно-энергетический комплекс (далее – ТЭК) включает нефтяную, газовую, угледобывающую и энергетическую отрасли. В состав ТЭК входят предприятия по добыче, переработке и транспортировке нефти, газа, угля, а также электростанции. По итогам в 2021 г. объем добычи нефти и газового конденсата в России составил 524,05 млн тонн (+2,2 % к 2020 г.), газа – 762,3 млрд кубометров (+10 %), угля – 438,09 млн тонн угля (+8,9 %). Выработка электроэнергии в 2021 г. выросла до 1,131 трлн кВт.ч (+6,4 %).

Основным разрешительным документом для осуществления большинства профильных видов деятельности в ТЭК является лицензия. Хозяйствующие субъекты ТЭК должны в зависимости от вида своей деятельности иметь лицензии: на пользование недрами (несколько различных видов лицензий); на эксплуатацию опасных производственных объектов; на погрузочно-разгрузочную деятельность применительно к опасным грузам на транспорте; на производство маркшейдерских работ; на геодезическую деятельность; на деятельность по осуществлению буксировок морским транспортом. Все эти виды лицензий и порядок их получения урегулированы нормативными правовыми актами, в основном, постановлениями Правительства Российской Федерации (от 12.10.2020 № 1661; от 16.09.2020 № 1467; от 28.07.2020 № 1126; от 30.11.2021 № 2111; от 31.12.2020 № 2417; от 21.07.2021 № 1243 и др.).

Следует также отметить, что наличие лицензий является вторым из важнейших условий законности деятельности субъектов ТЭК (первым таким условием является государственная регистрация). Например, в 2021 г. сотрудниками УЭБиПК МВД по Республике Саха (Якутия) при участии Росгвардии пресечена незаконная деятельность по производству нефтепродуктов. Установлено, что руководитель организации, занимавшейся торговлей твердым, жидким и газообразным топливом, то есть зарегистрированной в установленном законом порядке, *не имея лицензии на эксплуатацию объектов повышенной опасности*, создал на территории базы цех по производству дизельного топлива и других

[1] © Горенская Е. В., 2022.

нефтепродуктов, в котором трудились несколько жителей Мирнинского района. В дальнейшем нефтепродукты сбывались другим предприятиям отрасли. При этом на производстве не соблюдались требования безопасности. По предварительным подсчетам незаконный доход превысил 72 млн руб. Также указанный руководитель осуществил *незаконное подключение к газопроводу*, установив специальное оборудование на территории базы. С июня по декабрь 2020 г. с его помощью было похищено более 1 млн кубометров природного газа. Газовой компании причинен ущерб, превышающий 5,5 млн руб. В ходе обысков изъята документация, электронные носители информации и другие предметы, имеющие доказательственное значение. СО ОМВД России по Мирнинскому району возбуждены уголовные дела по ч. 1 ст. 171 и ч. 4 ст. 158 Уголовного кодекса Российской Федерации.

Таким образом, лица, нарушившие указанные условия, привлекаются к административной либо к уголовной ответственности (см. приговоры судов № 1-2/2020, 1-76/2019 от 26.02.2020, по делу № 1-2/2020; 1-43/2017 от 04.07.2017 по делу № 1-43/2017№ и т. д.) [6, с. 48]. В феврале 2018 г. сотрудниками ЛУ МВД России по Кемеровской области задокументирован факт незаконной добычи угля ООО «Энергоуголь» в течение двух предшествующих лет на территории Бунгурского каменноугольного месторождения без получения лицензии. Установлено, что в 2016 г. ООО «Энергоуголь» заключило договор на выполнение подрядных работ по разработке участка недр, однако на самом деле велась *добыча угля*, при этом из недр было незаконно извлечено 291 тыс. тонн каменного угля марки «Т», в результате чего получен доход более 430 млн руб. По факту осуществления предпринимательской деятельности *без лицензии* с причинением ущерба в особо крупном размере возбуждено уголовное дело по п. «б» ч. 2 ст. 171 Уголовного кодекса Российской Федерации [1, с. 37]. Аналогичные преступления совершаются в нефтяной отрасли [4, с. 34].

В последние годы российские предприниматели испытывают на себе последствия различных кризисов и конфликтов, в том числе мирового масштаба (например, пандемия COVID-19). Следует отметить, что государство пытается смягчить тяжесть таких последствий. Так, согласно постановлению Правительства Российской Федерации от 30 ноября 2021 г. № 2125 «О внесении изменений в постановление Правительства Российской Федерации от 31 декабря 2020 г. № 2417», с 14 марта 2022 г. и до конца года погрузочно-разгрузочная деятельность применительно к опасным грузам на железнодорожном транспорте (например, нефти и нефтепродуктов) и перевозка таких грузов могут осуществляться *без лицензии при условии уведомления о начале их осуществления*. Помимо этого, принято постановление Правительства Российской Федерации от 12 марта 2022 г. № 353 «Об особенностях разрешительной деятельности в Российской Федерации в 2022 году» (далее – постановление № 353), в котором урегулированы вопросы *автоматического продления* сроков действия разрешительных документов на 12 месяцев, их упрощенного получения или переоформления. Основной целью указанного постановления является снижение нагрузки на организации и предпринимателей, сокращение издержек, связанных с прохождением

разрешительных процедур. Всего автоматически будет продлено действие или переоформлено в упрощенном порядке более 2,5 млн разрешений. Этим же постановлением расширены полномочия государственных органов относительно принятия решений о сокращении сроков услуг в сфере разрешительной деятельности и т. п.

Для нашего исследования представляет интерес Приложение № 11 к постановлению № 353 «Особенности разрешительных режимов в сфере геологии и недропользования», в соответствии с которым с 14 марта 2022 по 31 декабря 2022 года «допускается приостановление осуществления права пользования недрами сроком до двух лет по заявке пользователя недр, направленной в орган, предоставивший лицензию». В Приложении № 11 также закреплена возможность продления до двух лет сроков выполнения работ, связанных с пользованием недрами, предусмотренных лицензией на пользование недрами и (или) проектной документацией, для чего пользователь недр должен подать заявку.

По данным Роснедра, в 2021 г. выдано 120 лицензий на углеводородное сырье (УВС) без учета переоформленных, в том числе, 44 лицензии на геологическое изучение, включающее поиски и оценку УВС (вида НП) (из них 22 – по заявительному механизму), 30 лицензий на разведку и добычу УВС (вида НЭ) и 46 лицензий на геологическое изучение, включающее поиски и оценку УВС, разведку и добычу УВС (вида НР). По факту открытия месторождений УВС выдано 13 лицензий, по заявительному механизму – 22 лицензии. За 2021 г. переоформлены 367 лицензий (34 вида НП, 236 вида НЭ и 97 вида НР). За этот же период были аннулированы 103 лицензии. В связи с окончанием действия лицензий аннулированы 67 лицензий. Столь большое их количество обусловлено тем, что в связи с пандемией коронавируса и массовой самоизоляцией граждан был издан Роснедром приказ от 16 апреля 2020 г. № 157, в соответствии с которым были продлены на 12 месяцев сроки пользования участками недр по лицензиям, действие которых истекало в период с 15 марта 2020 по 31 декабря 2020 года. Поэтому в 2021 г. были аннулированы лицензии как продленные с 2020 г., так и те, срок действия которых по лицензионному соглашению заканчивался в 2021 г. Досрочно аннулированы 36 лицензий, из них 8 – в связи с невыполнением условий пользования. Таким образом, на 01.01.2022 действовало 3915 лицензий на право пользования недрами в части УВС (НП – 566, НЭ – 2140, НР – 1209).

Не секрет, что ТЭК является самым важным сегментом российской экономики. Топливно-энергетические ресурсы – товар всесезонного спроса. Они также являются предметом повышенного интереса преступной среды. В этой связи ТЭК является одним из наиболее криминализованных сегментов национальной экономики, причем достаточно высокий уровень криминализации наблюдается в ТЭК на протяжении многих лет [2; 8]. По данным ГИАЦ МВД России, в 2021 г. в ТЭК было зарегистрировано 1593 преступления экономической направленности (далее – ЭН), из них в сфере экономической деятельности – 301, в том числе 51 (17 %) факт незаконного предпринимательства (ст. 171 Уголовного кодекса Российской Федерации).

И вот здесь возникают проблемы. Для квалификации деяния как незаконного предпринимательства необходимо наличие действующей лицензии на определенный вид деятельности, которую хозяйствующий субъект должен представить по требованию уполномоченных лиц / органов. Однако в настоящее время в соответствии с Федеральным законом от 27 декабря 2019 г. № 478-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части внедрения реестровой модели предоставления государственных услуг по лицензированию отдельных видов деятельности» заявление и документы на выдачу (продление) лицензии можно подавать в электронном виде (с обязательным использованием электронной цифровой подписи). С учетом нововведений также имеется возможность уведомления о начале осуществления деятельности. И, наконец, предприниматели могут рассчитывать на автоматическое продление сроков действия лицензий.

Соискатель лицензии может представить в лицензирующий орган заявление о предоставлении лицензии и приложения к нему в форме электронных документов (пакета таких документов) с использованием федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее – ЕСИА). Он также вправе представить эти документы в лицензирующий орган или в многофункциональный центр предоставления государственных и муниципальных услуг (МФЦ) в бумажном варианте самостоятельно или направить заказным почтовым отправлением с уведомлением о вручении. Несомненно, что все эти нововведения предназначены «облегчить жизнь» предпринимателям, снизить давление административных барьеров на бизнес. По мнению специалистов, лицензии на государственных бланках строго установленной формы утратили свою актуальность. Теперь в оборот включаются стандартные выписки из соответствующего реестра. При этом министерства и ведомства (Ростехнадзор, Росприроднадзор, Роснедр, Росздравнадзор и др.) обязаны привести в соответствие свои Положения о лицензировании, в том числе в части порядка оказания услуг в электронной форме и порядка взаимодействия с МФЦ. Кроме того, все организации, обязаны исключить из локальных нормативных актов требования о предъявлении лицензий на бумаге.

На практике уже возникают проблемы квалификации незаконного предпринимательства, связанные с установлением наличия лицензии, ее вида, сроков действия. Тем более что сегодня это, чаще всего, не документ установленной формы, а выписка из Государственного реестра участков недр, предоставленных в пользование, и лицензий на пользование недрами (далее – Реестр), находящегося в соответствии с приказом Минприроды России от 29 октября 2020 г. № 865 в ведении Роснедр. Возникают различные ситуации, при которых лица, подозреваемые в совершении незаконного предпринимательства, приводят следующие аргументы: 1) документы на получение лицензии отправлены через ЕСИА, ждем

результат; 2) лицензия есть, срок истек, думали, что она продлена автоматически; 3) есть выписка из Реестра (чаще – ксерокопия выписки, а сама выписка «в головном офисе»). При действующих сроках предварительного следствия (ст. 162 Уголовно-процессуального кодекса Российской Федерации) установление наличия лицензии, уточнение ее статуса оказывают негативное влияние на ход расследования уголовного дела.

Одновременно правоохранительные органы также испытывают обоснованные сомнения в допустимости использования в уголовном процессе в качестве доказательств новых форм подтверждения наличия лицензий на определенный вид деятельности, полученных с использованием информационных технологий и электронных форм, при отсутствии типового государственного бланка и установленных обязательных реквизитов лицензии [3, с. 150; 7]. Хотя законодатель, очевидно, планирует полный переход на электронное лицензирование, в данном случае необходимо более глубоко изучить проблему и предложить несколько альтернативных путей решения с учетом того, что любой реестр может подвергнуться кибератаке либо иному незаконному изменению, и данные о лицензиях могут быть изменены или вовсе утрачены.

Список литературы

1. Горенская Е. В., Попов А. И., Артюшенко Е. И. Сфера добычи, переработки и транспортировки угля как предмет преступного интереса // Научный портал МВД России. 2020. № 3 (51). С. 33–41.

2. Горенская Е. В., Фомин В. В. Криминогенная ситуация в топливно-энергетическом комплексе. М. : ВНИИ МВД России, 2013.

3. Горенская Е. В., Денисов Н. Л. К вопросу обеспечения органами внутренних дел экономической безопасности топливно-энергетического комплекса // Уголовно-правовая охрана конституционных прав и свобод граждан, суверенитета и территориальной целостности Российской Федерации : сборник научных трудов. М. : Московский университет МВД России имени В.Я. Кикотя, 2021. С. 146–151.

4. Горенская Е. В. Характеристика экономических преступлений в сфере добычи и транспортировки нефти // Вестник Восточно-Сибирского института Министерства внутренних дел Российской Федерации. 2021. № 2 (97). С. 31–45.

5. Горенская Е. В. Отдельные аспекты противодействия экономическим преступлениям в сфере электроэнергетики // Наукосфера. 2022. № 3–1. С. 249–254.

6. Зайцев О. А., Кашепов В. П., Нудель С. Л. Уголовная политика в отношении преступлений, совершаемых в сфере предпринимательской деятельности // Вестник Томского государственного университета. 2020. № 37. С.40–56.

7. Нудель С. Л. Тенденции современной российской уголовной политики в контексте криминализации // Человек: преступление и наказание. 2019. № 1. С. 18–26.

8. Преступность в сфере оборота нефти и нефтепродуктов в Российской Федерации : научно-практическое пособие / [С. Л. Нудель и др.]. М. : ВНИИ МВД России, 2012.

Нгуен Дык Фук[1]*,*
начальник Юридического Факультета
Полицейской Народной Академии
Министерства Общественной безопасности Вьетнама,
доктор юридических наук, доцент

ПРАВОВАЯ РЕГЛАМЕНТАЦИЯ И ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ В СООТВЕТСТВИИ С УГОЛОВНЫМ ЗАКОНОДАТЕЛЬСТВОМ ВЬЕТНАМА

В настоящее время уголовное законодательство многих государств, таких как Австралия, США и Великобритания, выделяет в отдельную группу преступления, совершаемые с использованием высоких технологий. Во Вьетнаме указанные правоотношения стали регулироваться сравнительно недавно, с момента вступления в законную силу Постановления Правительства Социалистической Республики Вьетнам (далее – Вьетнам) № 25/2014/ND-CP от 7 апреля 2014 г., предусматривающего в ч. 1 ст. 3, что «преступлениями в сфере высоких технологий являются общественно опасные деяния, предусмотренные в Уголовном кодексе, совершаемые с использованием высоких технологий». Согласно ч. 1 ст. 3 Закона «О высоких технологиях» 2008 г. под высокими технологиями понимается «технология с высоким содержанием научных исследований и технологических разработок, интегрированная в определенный вид деятельности…».

Таким образом, преступлениями, совершаемыми с использованием высоких технологий, являются: *«Преступления, совершаемые умышленно с использованием высокого уровня знаний, навыков и специальных информационных технологий для неправомерного воздействия на цифровую информацию, хранимую, обрабатываемую и передаваемую в сети Интернет, компьютерные системы, посягающее на порядок и сохранность информации, причиняющие вред интересам государства, правам и законным интересам организаций и граждан».*

Уголовный кодекс Вьетнама 2015 г. (УК Вьетнама) выделяет преступления, связанные с использованием компьютеров, цифровых устройств, компьютерных сетей и телекоммуникационных сетей. Эти виды высокотехнологичных преступлений возможно условно разделить на следующие две группы преступлений:

Первая группа – преступления, которые наносят ущерб безопасности, целостности и доступности к компьютерной системе, совершаемые группой лиц, использующих исключительно высокие технологии, в том числе: 1) Производство, покупка, продажа, обмен или дарение инструментов, оборудования и программного обеспечения для использования в незаконных целях (ст. 285 УК Вьетнама); 2) Распространение информационных программ, наносящих ущерб работе компьютерных сетей, телекоммуникационных сетей и электронных средств (ст. 286

[1] © Нгуен Дык Фук, 2022.

УК Вьетнама); 3) Воспрепятствование работе или нарушение работы компьютерных сетей, телекоммуникационных сетей и электронных средств (ст. 287 УК Вьетнама); 4) Незаконное предоставление или использование информации о компьютерных сетях или телекоммуникационных сетях (ст. 288 УК Вьетнама); 5) Неправомерный доступ к компьютерные сети, телекоммуникационной сети или электронным средствам (ст. 289 УК Вьетнама).

Вторая группа – «традиционные» преступления, где компьютеры, цифровые устройства, компьютерные сети и телекоммуникационные сети используются в качестве средств совершения преступлений, в том числе: 1) Хищение чужого имущества с использованием компьютерных сетей, телекоммуникационных сетей и электронных средств (ст. 290 УК Вьетнама); 2) Размещение информации и услуг на информационных сайтах, ущемляющие права и законные интересы физических и юридических лиц. В настоящее время последний вид противоправной деятельности не определен как преступление в УК Вьетнама, несмотря на опасность наступления общественно опасных последствий.

Санкции, предусматриваемые для лиц, совершивших вышеуказанные преступления, установлены в виде штрафа и лишения свободы, при этом самое тяжкое наказание в виде штрафа – 1 миллиард донгов, а лишение свободы – до семи лет.

Криминогенная обстановка в условиях активного применения высоких технологий при совершении преступлений заметно ухудшается, при этом увеличивается не только количество уголовных дел, представляющих сложность в расследовании, но и характер и масштаб общественно опасных последствий. Высокой регистрации противоправных деяний сопутствует низкое количество раскрываемых преступлений, поскольку лица, совершая преступления в киберпространстве, может находиться за пределами Вьетнама, как и сервисы, используемые при совершении преступлений.

По данным Департамента полиции высоких технологий Министерства общественной безопасности, наибольшее распространение получили следующие виды противоправных действий, связанные с применением высоких технологий:

Во-первых, атаки с компьютеров и компьютерных сетей путем обнаружения уязвимости в системе безопасности, получение доступа к информации, ее похищение и уничтожение (взлом ПК и сетей - Hacking of PCs and networks); распространение вирусов, шпионского ПО (трояны, черви, вредоносное ПО...); атаки типа «отказ в обслуживании» (Denial of service attacks - Botnet).

Во-вторых, хищение имущества, которое может быть осуществлено путем совершения мошенничества с кредитными картами; онлайн-мошенничества с использованием многоуровневых бизнес-уловок, связанных с инвестициями, бизнес-услугами, такими как кейс MB24, vicongdongviet, торговыми площадка с золотом, виртуальной иностранной валютой, в сфере электронной коммерции C2C, B2C, B2B; мошенничество по электронной почте, в ник-чате, CMC-Массовый маркетинг; направление сообщений с целью получения данных об учетной записи электронной почты и паролей, запросов о направлении денежных переводов и т. п.

Киберпреступники зачастую распространяют вредоносные программы через спам по электронной почте, веб-сайты, форумы, такие как Twitter, Facebook, YouTube и популярное программное обеспечение, такое как Unikey, Windows, Adobe и т. д. Вредоносный код, содержащийся в программе, позволяет получить личную информацию, такую, как пароль электронной почты, ник в чате. Особую тревогу вызывают атаки на национальные системы информационной и коммуникационной инфраструктуры.

По данным Департамента полиции Вьетнама, хакеры иностранного происхождения, используя высокие технологии, атакуют и получают доступ к сетевым системам государственных органов и некоторых крупных предприятий, похищая конфиденциальные данные, нанося огромный ущерб. Основываясь на данных мониторинга иностранных хакерских серверов или серверов, где размещаются объявления о продаже похищенных данных, согласно статистике компании TrendMicro, Вьетнам подвергается атакам на сайты Правительства, Министерств и ведомств в основном со стороны. Вьетнам имеет в общей сложности 394 сервера министерств и ведомств, которые и постоянно подключены к зарубежным серверам без уведомления сетевых администраторов этих подразделений, что безусловно вызывает тревогу для работы правительства в сфере информационной безопасности.

Что касается предупреждения и пресечения высокотехнологичных преступлений во Вьетнаме, то, исходя из анализа практики общемировой практики борьбы с данными видами преступлений, необходимо:

Во-первых, продолжать вносить изменения и дополнения в нормы УК Вьетнама, касающиеся конкретизации регулирования правоотношений в сфере высокотехнологичных преступлений в соответствии с Законом Вьетнама «Об информационной безопасности» 2018 г.

Поскольку для совершения преступных действий используются популярные компьютерные игры, онлайн-казино, ставки на спортивные мероприятия через сеть Интернет, УК Вьетнама должен регулировать правоотношения, связанные с пресечением преступлений, совершаемыми подобными средствами. Требуется оперативно издать методические указания, способствующие процессуальным органам координировать работу по выявлению, предупреждению и пресечению преступлений в сфере высоких технологий. Вместе с тем, внесение изменений в УК Вьетнама должно классифицировать киберпреступников, в соответствии с рекомендациями Интерпола, выделив преступления в сфере высоких технологий в отдельную главу уголовного закона.

В случае, если выделение отдельной главы не представится возможным, необходимо усилить ответственность за совершение финансовых преступлений, совершаемых с использованием высоких технологий. Кроме того, необходимо продолжить работу по совершенствованию Уголовно-процессуального кодекса, Закона Вьетнама «Об электронных сделках», Закона Вьетнама «О рассмотрении административных правонарушений», Закона «О связи» и др. с учетом особенностей и требований противодействия преступлениям с использованием высоких технологий.

Во-вторых, помимо нормотворчества, необходимо усилить практическую деятельность по предупреждению преступности в ИТ-телекоммуникации. Так, например, необходимо: 1) использовать технические средства предотвращения несанкционированного доступа, распространения вирусов, краж данных, защиты серверов, веб-сайтов, баз данных, с помощью устройств безопасности, сетевой безопасности (аппаратное обеспечение), антивирусного программного обеспечения и другие меры; 2) создать программное обеспечение для системного администрирования, децентрализовать соответствующих пользователей баз данных, принять меры для обеспечения сетевой безопасности, чтобы не подвергаться атакам изнутри; 3) усилить пропаганду, повышение квалификации с целью распространения знаний о нормах законодательства в области ИТ среди населения, особенно в средних школах, университетах и колледжах, чтобы вооружить учащихся знаниями об информационной безопасности.

В-третьих, повысить квалификацию должностных лиц и государственных служащих, непосредственно осуществляющих работу по предупреждению и борьбе с преступлениями в сфере высоких технологий. Внести предложения в Национальное собрание по внесению изменений в Закон «Об организации органов уголовного розыска» 2015 г., в котором установить положение о том, что Департамент полиции по предупреждению высокотехнологичной преступности является «органом народной общественной безопасности, которому поручено проведение ряда следственных действий». Полицейские силы по борьбе с преступлениями в сфере высоких технологий, должны исследовать и применять форму «онлайн-патрулирования», назначая ИТ-разведчиков для регулярного доступа к веб-сайтам и проникновения на ИТ-форумы, особенно на форумы киберпреступников, где размещается информация о методах, орудиях и средствах, используемых преступниками.

В-четвертых, продолжать эффективно осуществлять международное сотрудничество в борьбе с преступлениями в сфере высоких технологий, в том числе, использование опыта других стран в борьбе с преступностью, опыт сетевого администрирования и эксплуатации ресурсов, финансирования проектов в сфере информационной безопасности; организация международных учебных курсов, конференций и семинаров, и координация совместной деятельности по эффективному противодействию преступлениям в сфере высоких технологий.

Список литературы

1. Уголовный кодекс Вьетнама 2015 г.
2. Уголовно-процессуальный Кодекс Вьетнама 2015 г.
3. Закон «Об административных правонарушениях» 2012 г.
4. Постановление Правительства от 7 апреля 2014 г. № 25/2014/НД-КП.

Нгуен Тхи Тхань Тхуи[1],
заместитель Юридического факультета
Полицейской Народной Академии
Министерства Общественной безопасности Вьетнама,
кандидат юридических наук

ПРОБЛЕМА ПРЕСТУПНОСТИ, СВЯЗАННОЙ С ИНВЕСТИРОВАНИЕМ В ВИРТУАЛЬНУЮ ВАЛЮТУ ВО ВЬЕТНАМЕ

Криптовалюты или цифровые валюты, обычно называемые виртуальными валютами, уже не являются новой проблемой в правовом регулировании для многих стран мира, поскольку торговля ими происходит достаточно активно, однако единого понятия виртуальной валюты пока не существует. Виртуальная валюта – это электронное представление денежной стоимости, которое может выпускаться, управляться и контролироваться частными эмитентами, разработчиками или организациями-учредителями. Такие виртуальные валюты часто представлены в виде токенов и не обязательно привязаны к фиату.

Виртуальные валюты можно охарактеризовать следующим образом:

Во-первых, в отличие от обычных денег виртуальная валюта не может быть выпущена центральным банком или другим банковским регулятором. Виртуальная валюта создается человеком или группой лиц на основе применения современных технологий, зашифровывается и хранится в компьютерной системе с обменной стоимостью, выраженной через традиционную валюту. Другими словами, стоимость виртуальной валюты измеряется национальной валютой, а также любым другим имуществом, находящимся в обороте. Это делает криптовалюту средством сбережения и инвестиционным инструментом. Сама по себе виртуальная валюта может стать только платежным средством для электронных транзакций, но не платежной валютой для транзакций, совершаемых традиционными способами, поскольку ее не существует в объективном мире. Создание виртуальной валюты также не основано ни на каких гарантиях стоимости, ни на каких-либо принципах валютного рынка.

Во-вторых, коммерческие или гражданские транзакции, оплачиваемые виртуальной валютой, в основном анонимны. Субъекты отношений не могут быть идентифицированы, а лица, совершающие операции друг с другом не знают друг друга, поскольку общение осуществляется через Интернет. В этой связи, когда имеет место факт ограничения интересов участников операций с виртуальной валютой, защита их прав и законных интересов столкнется со многими трудностями, когда нарушитель преднамеренно найдет способ скрыться в киберпространстве. Кроме того, из-за высокой анонимности использование виртуальной валюты может быть использовано преступниками как средство отмывания денег, торговли запрещенными товарами, уклонения от уплаты налогов и т. д.

[1] © Нгуен Тхи Тхань Тхуи, 2022.

В-третьих, поскольку отсутствует надзорный орган или организация-посредник отношения с виртуальной валютой складываются по соглашению между анонимными сторонами, участвующими в транзакции. Стоимость виртуальной валюты может сильно колебаться в течение короткого периода, поэтому она содержит много рисков «лопнуть как пузырь». Сама виртуальная валюта не регулируется и не контролируется каким-либо государственным регулирующим органом, поэтому в этой ситуации владельцы виртуальной валюты должны принять на себя все риски.

Сопоставление функций, принципов эмиссии и обращения валют показывает, что виртуальная валюта по своей сути не может считаться подлинной валютой, поскольку не отвечает международным требованиям, принципам и практике эмиссии и обращения денег. Во Вьетнаме отсутствует правовое регулирование виртуальной валюты в качестве объекта обмена и продажи, то есть виртуальная валюта не признана законным платежным средством.

В Постановлении № 5747/NHNN-PC Государственного банка Вьетнама, направленном в Аппарат Правительства для ответа на вопрос о выпуске виртуальной валюты, Государственный банк подтвердил:

«Виртуальные деньги не являются валютой и не являются законным платежным средством в соответствии с вьетнамским законодательством. Выпуск, поставка и использование виртуальной валюты в качестве платежного средства запрещены положениями Постановления Правительства 96/2014/ND-CP о санкциях за административные правонарушения в денежно-кредитной и банковской сферах и Уголовным кодексом 2015 года (с изменениями и дополнениями). При инвестировании в виртуальную валюту Государственный банк Вьетнама много раз предупреждал, что эти инвестиции представляют большие риски для инвесторов».

В последнее время во Вьетнаме появилось множество финансовых бирж, использующих виртуальные валюты, такие как Airbitclub, Bitkingdom, BMW и др.; некоторые используют площадки для получения финансов с использованием вьетнамских денег, работающие аналогично M5, G5, Ex101, sm99, srow и т. д. Данные биржи уже принимают финансирование через виртуальные валюты, работая по многоуровневой модели, используя денежные средства последних участников для оплаты услуг первым участникам. Суть в многоуровневой трансформации заключается в возврате инвестированных средств с высокими процентами, достигающими 80 % в год. Форма бизнеса с виртуальной валютой во Вьетнаме складывается стихийно, покупка и продажа виртуальной валюты осуществляется без регистрации в каком-либо государственном органе управления. С другой стороны, торговля виртуальной валютой с ее анонимностью становится опасной для деятельности государственного управления, поскольку ее трудно контролировать и обнаруживать незаконные транзакции.

Несмотря на рекомендации органов государственной власти, во Вьетнаме используется множество виртуальных валют. Эти виртуальные валюты «добыва-

ется» отдельными лицами и организациями во Вьетнаме. Так, большое количество «майнеров» виртуальной валюты «Биткойн» осуществляют свою деятельность на территории Вьетнама.

В этом контексте многие виды деятельности, связанные с виртуальной валютой, используют пробелы в законодательстве, технологическую сложность и неосведомленность общественности для незаконного привлечения капитала, мошеннического присвоения имущества, отмывания денег, финансирования терроризма, организации азартных игр и т. д., что отрицательно сказывается на ситуации с безопасностью и порядком во Вьетнаме. Кроме того, большое количество вьетнамцев, занимающихся инвестированием и покупкой виртуальных валют на международных биржах, привело к тому, что огромные суммы денег – сотни и тысячи миллиардов донгов уходят за границу каждый день, а поступающая прибыль лиц и организаций не декларируется и не облагается налогами, что приводит к потере доходов государственного бюджета. Так, компания Modern Tech и команда разработчиков iFan, Pincoin мошенническим образом присвоил активы на сумму до 15000 миллиардов донгов, число жертв составило около 32000 (в 2018 г.); другим примером является случай, когда основатель Plus Token (Pluscoin) в Китае скрылся со средствами инвесторов из Вьетнама в три миллиарда долларов США (в 2019 г.), что является крупнейшей аферой, связанной с зарегистрированной виртуальной валютой на сегодняшний день.

Инвестиционная, торговая деятельность и деятельность по привлечению капитала с использованием виртуальной валюты широко распространены во Вьетнаме, хотя нормативно-правовая база отсутствует. Согласно статистике, Государственный банк Вьетнама выдал лицензии девяти небанковским кредитным организациям на использование услуг электронных кошельков (разновидность виртуальной валюты), в том числе: MobiVi, VietUnion, VNPay, VinaPay, Smartlink и т. д., M_Service, VNPT-EPAY и т. д., что потребовало создание правовой базы для управления виртуальной валютой во Вьетнаме.

В целях повышения эффективности противодействия использования преступниками транзакций с виртуальной валютой во Вьетнаме сегодня, необходимо применение следующих мер:

Во-первых, необходимо повышать осведомленность людей в вопросах, связанных с виртуальной валютой путем пропаганды и распространения знаний о природе виртуальной валюты и сути операций с виртуальной валютой. Требуется раскрывать положения норм действующего законодательства, связанного с виртуальной валютой, на примерах указывать методы совершения преступлений с виртуальной валютой. Пояснить, что неосведомленность в операциях приводит к отмыванию денег, финансированию терроризма, организации незаконных азартных игр и т. д.

Во-вторых, необходимо совершенствовать правовую базу, регулирующую виртуальную валюту во Вьетнаме. Столкнувшись с вышеуказанным фактом и тенденциями развития использования виртуальных валют, Вьетнаму необходимо изучить опыт зарубежных стран и создать правовую основу для регулиро-

вания виртуальной валюты. Это требование полностью соответствует общемировой тенденции развития стран, а также является решением, которое соответствует влиянию технологической революции 4.0. Более того, правоотношения, связанные с виртуальной валютой, должны быть выстроены таким образом, чтобы управление ими и надзор осуществлялся государственными органами. При таких обстоятельствах инвесторы будут чувствовать себя более защищенными в процессе ведения бизнеса, что будет способствовать созданию здоровой деловой среды и социально-экономической стабильности.

Стоит заметить, что применение общемировой практик должно быть интегрировано в экономику Вьетнама с учетом особенностей и традиций страны, не ставило под угрозу национальную денежно-кредитную политику и функционирование экономики. Вьетнам должен признать виртуальные валюты в качестве особого класса активов, не рассматривать виртуальную валюту как вид платежного средства.

В-третьих, участие в трансграничной координации международных организаций, таких как Международная финансовая целевая группа (FATF – Financial Action Task Force), содействие сотрудничеству между правительствами в разработке соответствующего правового регулирования и правоприменения в отношении виртуальных валют. Поощрять и облегчать соответствующий обмен информацией на региональных форумах, посвященных подходам к управлению рисками, контролю за незаконными веб-сайтами и т. д.

В-четвертых, увеличение финансирования и обучения в целях обеспечения сотрудников правоохранительных органов достаточными знаниями о виртуальных валютах, знаниях в области идентификации, а также о методах выявления финансовых преступлений с использованием виртуальных валют.

Таким образом, виртуальная валюта таит в себе множество рисков стать инструментом совершения многих особо тяжких преступлений, в том числе транснациональных. Этот вызов ставит перед законодателями требования по скорейшему совершенствованию правовой базы, связанной с виртуальными валютами, создавая прочную основу для государственных органов в сфере защиты виртуальных валют, законных прав и интересов участников операций с виртуальными валютами. Создание правовой базы регулирования виртуальной валюты во Вьетнаме должно способствовать защите прав и законных интересов отечественных и иностранных инвесторов, эффективно ограничивая, предотвращая и контролируя риски и злоупотребления, связанные с торговлей виртуальной валютой.

Список литературы

1. Ле Тхи Тует Хоа, Нгуен Тхи Нхунг (2011), Банковская валюта, Orient Publishing House, стр. 1.

2. Ле Ань Зунг (2018 г.), Взгляд на виртуальные деньги – предложения по управлению виртуальными деньгами на примере Таиланда, Материалы конференции «Правовая база для виртуальных денег и виртуальных активов во Вьетнаме в контексте технологической революции 4.0»; организовано Министерством юстиции в июне 2018 г. в Хошимине.

3. Нгуен Хуинь Фуонг Тхао (2018 г.), Исследование налогового законодательства стран, связанных с криптовалютами, и опыт Вьетнама. Магистерская диссертация по юриспруденции, Университет экономики и права.

Нгуен Тхи Хай Иен[1],
заместитель начальника Юридического факультета
Полицейской Народной Академии
Министерства Общественной безопасности Вьетнама,
кандидат юридических наук

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НЕЗАКОННУЮ ОРГАНИЗАЦИЮ И ПРОВЕДЕНИЕ АЗАРТНЫХ ИГР В КИБЕРПРОСТРАНСТВЕ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ ВЬЕТНАМА

Незаконная организация и проведение азартных игр является тяжким преступлением в уголовном праве Вьетнама. Развитие информационных технологий, разнообразие социальных сетей, организация онлайн-гемблинга способствовали вовлечению в теневой оборот до десятков тысяч миллиардов донгов, нанося большой ущерб общественному порядку и общественной безопасности.

В уголовном праве Вьетнама организация и проведение азартных игр в киберпространстве регулируется ст. 26 Указа 167/2013/ND-CP «Об административных правонарушениях в области безопасности, общественного порядка и безопасности; о профилактике и тушении пожаров; о профилактике и борьбе с насилием в семье» и ст.ст. 321 и 322 Уголовного кодекса Вьетнама 2015 г. (далее – УК Вьетнама).

Незаконные азартные игры согласно ст. 321 УК Вьетнама – это азартные игры в любой форме, такие как «диск-жокей», «выборы крабов», «гнездо креветок», «три хризантемы», «числа», петушиные бои, скачки, пари и др., где возможны ставки в виде денежных средств или иных ценностей.

Вместе с тем, согласно ст. 322 УК Вьетнама, организация азартных игр включает действия по даче приказа, принуждения других лиц к участию в азартных играх путем угроз, использования места для проведения азартных игр.

Проведение азартных игр и организация азартных игр - это два вида преступления, предусмотренные не только УК Вьетнама, но и административным законодательством в соответствии с Указом 167/2013/ND-CP. Проведение азартных игр предусматривает административное наказание в виде штрафа в размере от 200 тысяч донгов до 2 миллиона донгов, уголовное наказание – лишение свободы на срок до семи лет либо штраф в размере до 50 миллионов донгов. Организация азартных игр предусматривает административное наказание в виде штрафа в размере от 5 миллионов до 20 миллионов донгов, уголовное наказание – лишение свободы на срок до десяти лет либо штраф в размере от 50 миллионов донгов до 300 миллионов донгов.

Незаконные организация и проведение азартных игр в киберпространстве совершаются в основном в двух формах:

---

[1] © Нгуен Тхи Хай Иен, 2022.

1) Путем осуществления постоплатного участия. Различные букмекерские конторы для организации игр привлекают лидеров отечественных сетей. Каждому игроку передается определенная сумма денежных средств для участия в азартных играх. По прошествии определенного срока игрок должен вернуть предоставленные средства. В настоящее время во Вьетнаме функционирует более 10 букмекерских контор, организующих азартные игры таким образом (ставки на спорт, лотереи и онлайн-покер).

2) Путем осуществления предоплатного участия. После регистрации игорного счета участнику азартных игр необходимо перевести денежные средства на банковский счет организации либо пополнить телефонную карту и следовать инструкциям игорного сайта. Сумма, внесенная на счет, будет конвертирована в очки (виртуальные деньги), которые игроки смогут использовать для игры. Однако в дальнейшем перевести денежные средства букмекером игроку напрямую сложно, поскольку организатор находится за границей, зачастую используются вьетнамские посредники.

В настоящее время преступники организовывают азартные игры в киберпространстве, используя все более изощренные метод, побуждающие людей принимать участие в азартных играх, при этом оказывая противодействие выявлению и расследованию преступлений. Примечательно, что преступники постоянно настраивают множество доменов и веб-сайтов игорных организаций для предотвращения возможной блокировкой доступа правоохранительными органами. Существенным образом на развитие преступности в данной сфере оказала пандемия COVID-19, когда букмекерские конторы Вьетнама изменили свое направление деятельности, привлекая делать ставки на виртуальные спортивные турниры (Virtual Sport), киберспорт.

Особую проблему вызывает создание привлечение вьетнамских граждан для участия в игорных онлайн-заведениях на территории Камбоджи. Общение организаторов осуществляется через социальные сети (Zalo, Facebook, Weibo и др.). Их целевая аудитория – люди, которые знают китайский язык, получают высокие заработные платы и комиссионные от 800 до 1000 долларов США в месяц, прибывающие в Камбоджу для участия в казино, и становящиеся жертвами преступлений. После достижения цели, преступники удаляют старые аккаунты и создают новые аккаунты для продолжения поиска новых жертв.

В начале 2022 г. Департамент кибербезопасности и борьбы с преступлениями в сфере высоких технологий Министерства общественной безопасности Вьетнама расследовал уголовное дело по незаконным организации и проведению азартных игр в городе Ханое. Первоначальные результаты расследования показали, что только с начала 2020 г. сумма игорных транзакций составила более 1500 миллиардов донгов. Преступники использовали веб-сайт «Bong88.com», сервер которого находится за границей, организуя азартные игры, в том числе ставки на спорт: футбол, баскетбол, теннис и др. Кроме того, в августе 2020 г. Следственное полицейское управление полиции провинции Хатинь согласовало проведение полицейских операций с целью пресечения деятельности организации, занимающейся онлайн-ставками на футбол с суммой транзакции

до 10000 миллиардов донгов. Правоохранительные органы власти установили, что эта линия ставок на футбол существует уже много лет и насчитывает около 1000 активных счетов.

С целью предупреждения и пресечения незаконных организаций и проведения азартных игр необходимо предпринять следующие меры:

Во-первых, необходимо совершенствовать нормативное правовое регулирование правоотношений в данной сфере. Поскольку это тяжкое преступление, наносящее большой ущерб общественному порядку и общественной безопасности, необходимо ужесточить наказание за их совершение. В частности, выделение незаконных организации и проведения азартных игр с использованием высоких технологий в отдельный вид преступлений с более тяжким наказанием, соразмерного последствиям их совершения.

Законодатели Вьетнама приняли множество нормативных правовых актов в целях повышения эффективности борьбы с преступностью в сфере высоких технологий, однако до сих пор существуют нормативные акты, не реализуемые на практике и не решающие проблем правоприменителей. Статьи 321 и 322 УК Вьетнама 2015 г. определяют, как преступление незаконные организацию и проведение азартных игр, несмотря на то, что те же деяние, совершенные с применением высоких технологий, являются квалифицированными составами, а не выделены в отдельные преступления, поэтому уровень их противодействия невысок. В этой связи, полагаем, что необходимо выделить данные преступления в самостоятельные с более строгим наказанием, чем за организацию и проведение традиционных азартных игр. Кроме того, требуется разработка нормативных правовых актов по усилению контроля за кредитными учреждениями и поставщиками высоких технологий. При обнаружении сомнительных операций, например, перевод денежных средств, использование электронной почты, социальных сетей, сетей телекоммуникаций и т. д., указанным организациям следует ограничить или прекратить оказание услуг, потребовать направить отчетность компетентным органам для проверки и уточнения.

Во-вторых, необходимо усилить контроль за транзакциями в киберпространстве; своевременно обнаруживать, отслеживать и уничтожать игровые линии. Поскольку характерным для этих преступлений является применение высоких технологий, необходимо, чтобы полиция обладала высокой профессиональной квалификацией, современными техническими средствами противодействия преступности.

Законодательство Вьетнама имеет относительно полную и четкую систему правил открытия и использования счетов и денежных переводов за границу (Постановление Правительства Вьетнама 101/2012/ND-CP «О регулировании безналичных расчетов»; Циркуляр 16/2014/TT-NHNN «О руководстве по использованию счетов в иностранной валюте, счетах резидентов, нерезидентов в лицензионных банках», Закон «О борьбе с отмыванием денег и связанные с ним законы» и руководящие документы).

В целях контроля и управления за финансовыми, а также предотвращения оттока капитала, поставщики платежных услуг должны строго следить за процессом предоставления кредитных услуг.

Вместе с тем, необходимо проводить проверку и классифицировать клиентов на основе информации, предоставленной клиентами, для оперативного выявления рисков и принятия соответствующих мер по их ограничению, и в то же время обеспечивать координацию действий компетентных органов при совершении клиентом преступления. Для транзакций на крупную сумму, связанных с международным переводом электронных денег во Вьетнам и из него, или в случае, когда имеются основания подозревать, что активы в транзакции имеют преступное происхождение или связаны с отмыванием денег, необходимо незамедлительно сообщать об этом в Государственный банк для консультации и принятия управленческого решения.

Требует усиления надзор за деятельностью банков и организаций, занимающихся управлением электронными кошельками, нарушающими правила открытия и использования счетов, проводящих сомнительные транзакции.

Список литературы

1. Уголовный кодекс Вьетнама 2015 г.

2. Постановление Правительства Вьетнама 101/2012/ND-CP «О регулировании безналичных расчетов».

3. Циркуляр 16/2014/TT-NHNN «О руководстве по использованию счетов в иностранной валюте, счетах резидентов, нерезидентов в лицензионных банках».

4. Закон № 07/2012/QH13 «О борьбе с отмыванием денег и связанные с ним законы» 2012 г.

Хоанг Тхи Тху Нга[1]*,*
преподаватель Юридического факультета
Полицейской Народной Академии
Министерства Общественной безопасности Вьетнама

К ВОПРОСУ О НЕКОТОРЫХ МЕРАХ ПРЕДУПРЕЖДЕНИЯ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ

Преступления, совершаемые с использованием высоких технологий, являются формой нетрадиционной преступности, имеющей в современный период особо опасный характер. В мире они входят в число самых серьезных угроз безопасности наравне с терактами, угрозой применения химического и ядерного оружия. Уголовный кодекс Вьетнама 2015 г., измененный и дополненный в 2017 г. (далее – УК Вьетнама), содержит нормы, регламентирующие преступления в сфере информационных технологий и телекоммуникационных сетей (ст.ст. 285–294 УК Вьетнама).

Многие экономические, социальные и культурные сферы жизни общества зависят от новых информационных технологий. Как и в случае внедрения любого научного достижения они способствуют облегчению решения повседневных задач, просты в использовании, вовлекают в оборот значительные денежные средства, которые становятся целью хищения для преступников. В настоящее время это считается одной из забот всего мирового сообщества и представляет собой новую задачу для законодателей, а также правоохранительных органов в определении соответствующих правил, позволяющих эффективно предупреждать и пресекать преступления, совершаемые с использованием высоких технологий.

Согласно данным статистики, предоставленной Департаментом кибербезопасности и предупреждения преступлений в сфере высоких технологий Министерства Общественной безопасности Вьетнама с 2016 по 2021 гг. выявлено и рассмотрено более 2400 материалов проверки, возбуждено более 1000 уголовных дел в отношении 1055 лиц, применены меры административного воздействия в отношении 51 лиц, совершивших присвоением имущества через киберпространство.

Статистика – это лишь малая часть реальности преступлений с использованием высоких технологий, на самом деле это вид преступлений с очень высоким «скрытым» уровнем, количество не выявленных правонарушений по-прежнему остается достаточно большим. Раскрытые преступления показывают, что они могут затронуть все сферы общественной жизни, в том числе общественный порядок и национальную безопасность.

Лица, совершающие данные преступления, в основном имеют квалификацию в области информационных технологий, имеют образование или профессию в этой области, что способствует использованию последних достижений науки и техники в преступной деятельности, имеют доступ к форумам в Интернете

[1] © Хоанг Тхи Тху Нга, 2022.

для обмена опытом совершения преступлений. Поскольку преступления совершаются в киберпространстве, «безграничной» среде, характерной чертой этих преступлений является международный характер. Используя Интернет, преступники могут совершать преступления, находясь в любой стране мира, размер причиняемого вреда может достичь больших размеров за короткий промежуток времени, при этом следы преступления удаляются, что затрудняет поиск преступников. Методы совершения преступлений становятся все более изощренными, постоянно меняются, что усложняет работу правоохранительных органов по их противодействию.

Благодаря практике предупреждения, пресечения и раскрытия преступлений, совершаемых с использованием высоких технологий, правоохранительные органы Вьетнама определили методы, которые часто используют преступники для хищения имущества:

Во-первых, путем телефонных звонков обманывают и склоняют самостоятельно переводить денежные средства на счета преступников. Например, представляясь сотрудниками следственных органов, просят клиентов перевести денежные средства для проведения качественного расследования; сообщают ложную информацию о выигрыше в лотереи; выдают себя за родственников и друзей, которые просят финансовой помощи.

Во-вторых, преступники используют социальные сети, такие как Zalo, Facebook, Telegram, Tinder и т. д., чтобы познакомиться, а затем подружиться с жертвой. После знакомства преступники склоняют жертву инвестировать деньги на электронные биржи, якобы имеющие высокий процент при их возврате. Через некоторое время биржа объявляет, что закрывается на техническое обслуживание или вовсе закрывает доступ, клиенты не могут войти в систему для вывода инвестированных средств, теряют все средства на своих счетах, а лица, пригласившие их для участия, удаляют аккаунты в Facebook, Zalo, Telegram, Tinder.

В-третьих, кража конфиденциальной информации у клиентов: выдача себя за сотрудника банка с целью запроса паролей, PIN-кодов или информации о карте для решения проблем, связанных с банковскими услугами или карточными услугами; отправление электронного письма/сообщения, содержащего ссылку для доступа к веб-сайту службы денежных переводов, с целью якобы получения денег из-за границы. Клиент вводит данные для входа в Интернет-банке или данные карты для получения денежных средств, а подделанные веб-сайты, устанавливая вредоносное программное обеспечение, похищают значимую для клиента информацию.

В-четвертых, использование высокотехнологичного программного обеспечения (передача голоса по IP) для подделки номера телефона полиции с целью обмана и присвоения имущества: злоумышленники используют высокотехнологичное программное приложение «Передача голоса по IP», совершают звонки с телефонных номеров, отображаемых на экране телефона получателя с номерами, похожими на номер Департамента полиции и т. д. Затем, выдавая себя за сотрудника полиции, угрожая и шантажируя, требуют перевода денежных

средств. Мошеннические номера телефонов, как правило, отображаются при звонке, как: 1080, +084028 или +028 и др.

В целях предупреждения и пресечения преступлений, совершаемых в сфере информационных технологий, предотвращению и ограничению ущерба, причиняемого преступниками, необходимо предпринять следующие меры:

Во-первых, активизировать и усилить работу по информированию, пропаганде граждан по правовому просвещению и способах совершения преступлений, а также об угрозах безопасности и незащищенности сети. Людям рекомендуется не верить сообщениям незнакомцев, переходить по сомнительным ссылкам в социальных сетях, не участвовать в инвестировании средств на биржах, в виртуальные валюты без понимания работы информационных технологий и интернета.

Особое внимание следует уделить охране личной информации, проверять поступающие звонки якобы от сотрудников государственных органов, банков, кредитных учреждений и т. д.; не заказывать товары или продукты через социальные сети zalo, facebook; не принимать участия в онлайн-играх, что может привести к краже личной информации и информации об учетной записи, а также следует стремиться к ограничению публикации и обмену личной информацией, о жизненных проблемах в социальных сетях, поскольку это может стать ключом для преступников в целях шантажа.

Во-вторых, применять меры по защите данных клиентов и информационной деятельности банков и кредитных организаций. Банкам рекомендуется регулярно контролировать работу банкоматов в целях обнаружения скимминговых устройств, регулярно проверять наличие поддельных веб-сайтов и предупреждать клиентов о том, чтобы они не заходили на подозрительные веб-сайты, совершали переходы по сомнительным ссылкам и не предоставляли информацию о счете и карте по этим ссылкам. Полицейские органы также предлагают кредитным учреждениям настроить оповещения клиентов, когда вход в учетную запись осуществляется с неизвестного устройства или, когда изменяется метод аутентификации.

В-третьих, продолжать совершенствование нормативных правовых актов для создания прочной правовой базы в целях борьбы с преступлениями (УК, УПК Вьетнама, Закон об административных правонарушениях и др.).

В-четвертых, повысить способность полиции предупреждать преступления, совершаемые с использованием высоких технологий, при этом следует обновлять современное оборудование, техническую инфраструктуру и специализированное программное обеспечение. Необходимо продолжать разработку и выдачу инвестиционных проектов на закупку оборудования для специализированных учреждений в дополнение к утвержденному Проекту 5 Национальной программы предупреждения преступности «Борьба и предупреждение преступности с использованием высоких технологий». Принять разумную политику для привлечения и найма высококвалифицированных сотрудников в области науки и техники, способных бороться с преступностью, совершаемых с использованием высоких технологий, в специализированных учреждениях. В то же время

следует разработать долгосрочные программы и планы обучения в образовательных организациях, специализирующихся на подготовке кадров в сфере информационных технологий, банковского, финансового и кредитного секторов.

В-пятых, укреплять международное сотрудничество в предупреждении и борьбе с преступностью с использованием высоких технологий в целях расширения пространства для предупреждения преступности, использовать опыт передовых стран для повышения эффективности в борьбе с преступлениями в сфере высоких технологий.

Список литературы

1. Уголовный кодекс Вьетнама 2015 г.
2. Уголовно-процессуальный Кодекс Вьетнама 2015 г.
3. Закон «Об административных правонарушениях» 2012 г.

Байтеленова С. Г.[1],
научный сотрудник Центра по исследованию проблем
уголовной политики и профилактики преступности
НИИ Карагандинской академии
МВД Республики Казахстан
имени Б. Бейсенова,
магистр юридических наук

Еспергенова Е. В.[2],
старший научный сотрудник Центра по исследованию
проблем уголовной политики и профилактики преступности
НИИ Карагандинской академии
МВД Республики Казахстан
имени Б. Бейсенова,
доктор философии (PhD)

ПОРТРЕТ ЛИЧНОСТИ ЖЕРТВ ПРЕСТУПЛЕНИЙ В СФЕРЕ СЕТЕЙ ТЕЛЕКОММУНИКАЦИИ, В ТОМ ЧИСЛЕ СЕТИ ИНТЕРНЕТ

В последнее время все большие обороты набирают уголовные правонарушения, совершаемые в сфере сетей телекоммуникации, в том числе сети Интернет. Данное обстоятельство представляется актуальным, если учесть, что статистические данные, которые указывают, что по состоянию на 2020 г. мобильными и/или телекоммуникационными сетями было охвачено около 7 млрд человек (94 % мирового населения) [1]. Так, согласно данным Комитета по статистике РК за период 2010 по 2021 год общее количество пользователей сети Интернет в Казахстане выросло с 36,1 % до 84,2 % всего населения Республики, к концу 2022 г. количество пользователей увеличится и составит 99,3 % населения [2].

С ростом пользователей сети Интернет, число жертв преступлений, совершаемых в сфере сетей телекоммуникации, в том числе сети Интернет, также увеличивается. В этой связи, считаем целесообразным провести анализ личности жертв по вышеуказанным уголовным правонарушениям.

Существуют различные типы уголовных правонарушений, совершаемых посредством использования сетей телекоммуникаций, в том числе сети Интернет. Так, в УК Республики Казахстан содержится 34 статьи, относящиеся к данной категории уголовных правонарушений.

Проведенный анализ статистических данных, научных работ, посвященных личности жертв преступлений, совершаемых посредством использования сетей телекоммуникации, в том числе сети Интернет, позволил сформулировать обобщенный портрет жертвы и привести его типологизацию.

---

[1] © Байтеленова С. Г., 2022.
[2] © Еспергенова Е. В., 2022.

Портрет личности жертвы как правило складывается из определенной совокупности признаков, среди которых, в основном выделяют пол, возраст, образование, социальное положение и т. д.

Согласно статистическим данным Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан с 2017 по 2021 год возрастные характеристики жертв по уголовным правонарушениям в сфере сетей телекоммуникации, в том числе сети Интернет, классифицируется по следующим категориям:

- до 18 лет – 0,2 %;
- от 18 до 20 лет – 6,1 %;
- лица в возрасте от 21 до 29 лет – 27,8 %;
- лица в возрасте от 30 до 39 лет – 30,6 %;
- лица в возрасте от 40 до 49 лет – 18,8 %;
- лица в возрасте от 50 до 59 лет – 10,2 %;
- от 60 и выше – 6,2 %.

Таким образом, средний возрастпотерпевших по данным преступлениям составил 21–39 лет [3]. Представляется, что указанная категория граждан является активными пользователями сети Интернет. О. С. Гузеева также отмечает, что наиболее активна в овладении сетью Интернет молодежь, составляющая 48 % от всех пользователей [4, с. 4].

Жертвами преступлений данного вида деяния в подавляющем большинстве становятся женщины – 58 %, доля мужчин составляет 42 % среди потерпевших этой категории [5]. Такая статистика может объясняться тем, что зачастую методы, как убеждение и психологическое давление, больше воздействует на женщин, чем на мужчин. Если рассматривать, жертв хакерских атак, то в большинстве случаев, целью преступников, как правило является завладение чужими денежными средствами, поэтому здесь не важны личность и физические особенности жертвы, поскольку он с ней не имеет прямого контакта.

Как показывают статистические данные, 49 % потерпевших лиц, не имеют постоянного места работы. Большая часть 51 % занимают лица, имеющие постоянный заработок, так как в большей степени целью преступника, как правило является завладение чужими денежными средствами. Однако зачастую, уголовные правонарушения данной категории не связаны с социальным положением лица. Преступники могут завладеть как 5000000 тенге, так и 5000 тенге. Соответственно типичная жертва имеет два признака: первый – является пользователем сети Интернет, второй – неграмотно распространяет свои персональные данные и сведения о паролях и лицевых счетах [6, с. 167].

Следующим немаловажным признаком в портрете жертвы является уровень образования, которое также влияет на виктимность пользователей сети Интернет. Многие ученые неоднократно отмечали о том, что низкий уровень технического образования, низкий уровень культуры информационной безопасности является одним из наиболее виктимных факторов киберпреступности [6, с. 167].

Так, в соответствии с отчетом по утечкам конфиденциальной информации агентства InfoWatch за 2018–2020 гг. в Республике Казахстан в открытом доступе

было обнаружено более 11 млн записей конфиденциальных персональных данных и платежных карт [7].

Согласно исследованию, доля утечек, произошедших по вине внешних кибератак, составляет 27,3 %. Соответственно, 72,7 % от общего количества инцидентов спровоцированы действиями внутренних нарушителей – т. е. сотрудников, имеющих доступ к персональным и другим конфиденциальным данным, а также самими лицами. Основной причиной утечки конфиденциальной информации является недостаточная осведомленность о методах защиты информации и низкая обеспеченность в системах информационной безопасности, в том числе занятых в сфере оказания информационно-коммуникационных услуг, приводят к большому количеству не анализируемых событий и инцидентов информационной безопасности.

По оценкам специалистов рабочей группы по программному обеспечению в Казахстане в 2019 г. у примерно 74 % программного обеспечения, установленного на компьютерах, было нелицензионным, так называемым «пиратским» [8]. Пользователи предпочитают устанавливать бесплатные «пиратские» программные продукты, безвозмездно пользоваться другими результатами интеллектуальной деятельности, охраняемыми авторским правом (просмотр фильмов, скачивание музыки и т. д.).

Таким образом, приходим к выводу, что на виктимность личности (склонность становиться жертвой) влияет его уровень технических знаний.

Поскольку, лица, обладающие такими знаниями, более осведомлены об основных методах хакерских атак и, следовательно, защищены от них. Такие люди не редко следят за последними техническими новинками в области защиты персональных данных и знают самые эффективные способы борьбы с кибер-атаками, вирусами и иными вредоносными программами, знают самые незащищенные области каждой из используемых операционных систем и зачастую используют более старую, но надежную версию. Однако в масштабе страны общее количество людей, обладающих подобными знаниями, объективно мало.

Как правило, жертвы в сфере сетей телекоммуникации имеет активность в киберпространстве. К примеру, жертвами п. 4 ч. 2 ст. 190 УК РК чаще всего становятся менее опытные покупатели, либо лица, впервые зашедшие на данный сайт. Для обмана покупателей в Интернет-магазине преступник может установить сумму за товар в несколько раз ниже средне-розничной с условием определенного процента предоплаты. Пользователи, которые не раз совершали покупки на таких сайтах, обходят подобные объявления стороной, осознавая возможность мошенничества, в то время как менее опытные пользователи могут заинтересоваться «выгодным предложением» [6, с. 169].

По преступлениям, предусмотренным ч. 2 ст. 132 и п. 1-1 ч. 3 ст. 134 УК РК, поведение самих несовершеннолетних все чаще приобретают формы кокетства, демонстрации взрослости, самостоятельности и нередко способствуя совершению в отношении них преступлений сексуального и иного характера. Несовершеннолетние как правило, привлекают интерес преступников своей незрелостью, неопытностью, а в отдельных случаях зависимое положение потерпевших

в физическом, психологическом, материальном отношений, дает виновным некую власть.

Так, учитывая вышеизложенное, по нашему мнению, личность жертвы по преступлениям, совершаемым посредством использования сетей телекоммуникации, в том числе сети Интернет, можно разделить на следующие группы:

– жертвы, находящиеся в контакте с преступником;
– жертвы хакерских атак.

К первой группе относятся, когда преступник вступает в контакт с жертвой посредством личной переписки в социальной сети, аудио- (видео-) чате или через электронную почту либо вещает посредством использования сетей телекоммуникаций, в том числе сети Интернет. Так, для совершения таких преступлений, как: доведение до самоубийства (п. 4 ч. 2 ст. 105 УК РК), вовлечение несовершеннолетнего в совершение уголовных правонарушений (ч. 2 ст. 132 УК РК), вовлечение несовершеннолетнего в занятие проституцией (п. 1-1 ч. 3 ст. 134 УК РК), мошенничество (п. 4 ч. 2 ст. 190 УК РК), принуждение к передаче информации (ст. 209 УК РК), распространение заведомо ложной информации (п. 3 ч. 2 ст. 274 УК РК), склонение к потреблению наркотических средств, психотропных веществ, их аналогов (п. 3 ч. 2 ст. 299 УК РК) и др.

В таком случае основными виктимогенными факторами могут выступать: необразованность, излишняя доверчивость, неопытность.

Ко второй группе относятся, когда жертва и преступник не вступают в контакт друг с другом, поскольку преступник при совершении данных преступлений может использовать вредоносные программы, то главную роль будут играть уже такие виктимогенные факторы, как низкий уровень технической защищенности, наличие либо отсутствие антивируса и т. д.

В зависимости от того, к какой группе принадлежит та или иная жертва уголовного правонарушения в сфере сетей телекоммуникаций, в том числе сети Интернет, прослеживаются те или иные виктимогенные факторы, следовательно, к разным типам жертв должны применяться разные меры противодействия преступлениям. Так как никакие антивирусные программы не уберегут самого опытного программиста от простого интернет-мошенничества, как и никакие знания не уберегут опытного юриста от банального компьютерного вируса [6, с. 171].

Подводя итог, можно составить общие черты характеристики жертв по уголовным правонарушениям в сфере сетей телекоммуникаций, в том числе сети Интернет в Республике Казахстан: лицо, женского пола, в возрасте от 21 до 39 лет, являющееся активным пользователем сети Интернет, с низкой культурой информационной безопасности или пренебрегающий средствами компьютерной защиты.

Анализ портрета личности потерпевшего по преступлениям в сфере сетей телекоммуникации, в том числе сети Интернет позволит эффективно проводить профилактические мероприятия в отношении лиц, поведение и личные качества которых позволяют предполагать, что данные лица могут оказаться жертвами преступлений, что в свою очередь создает более эффективные меры противодействия данной категории преступлений [9, с. 549]. Поскольку в отдельных случаях

само поведение жертвы может служить фактором, подталкивающим лиц к совершению уголовного правонарушения.

Список литературы

1. Committed to connecting the world. URL: http://www.itu.int/.

2. Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан. URL: https://stat.gov.kz/official/industry/-29/statistic/7.

3. Портал органов правовой статистики и специальных учетов. URL: https://-qamqor.gov.kz/crimestat/statistics.

4. Гузеева О. С. Предупреждение размещения информации, способствующей распространению наркотических средств, в российском сегменте сети Интернет (криминологические и уголовно-правовые проблемы) : автореф. дис. … канд. юрид. наук. М., 2008. С. 4.

5. Информация с КПСУ ГП РК (исх. от 15.04.2022 № 2-20-22-03519).

6. Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. … канд. юрид. наук : 12.00.08. М., 2016. С. 167.

7. В результате утечек в Казахстане скомпрометировано более 11 млн записей персданных. URL:https://www.infowatch.ru/company/presscenter/news/32794.

8. URL: https://kapital.kz/gosudarstvo/71001/issledovaniye-ispol-zovaniye-nelit-senzionnogo-po-v-kazakhstane.

9. Карасева М. Ю. Криминологическая характеристика потерпевшего // Актуальные проблемы российского права : сборник статей. 2007. С. 549–554.

Абдульманов А. А.[1],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент

К ВОПРОСУ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА СБЫТ НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ ИЛИ ИХ АНАЛОГОВ, СОВЕРШЕННЫЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СЕТЕЙ

Актуальность проблемы борьбы с преступлениями связанными с распространением наркотических средств, психотропных веществ или их аналогов на территории Российской Федерации свидетельствуют следующие статистические данные: в 2018 г. было зарегистрировано 11285 преступлений, связанных со сбытом наркотических средств, психотропных веществ или их аналогов, что на +5 % больше, чем в 2017 г., в 2019 г. – 112651 преступлений, что на –0,2 % меньше, чем в 2018 г., в 2020 г. – 112267 преступлений, что на –0,3 % меньше чем в 2019 г., в 2021 г. было зарегистрировано 103446 преступлений, что на –7,9 % меньше, чем в 2020 г. [1] Анализируя эти данные, необходимо обратить внимание на латентность этой категории преступлений, что влияет на сложности их выявления и расследования.

Проводя анализ п. «б» ч. 2 ст. 228.1 УК РФ [2], в контексте п. 13 постановление Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14 (ред. от 16.05.2017) «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» [3], следует признать, что объективная сторона выражается в незаконной деятельности, направленной на возмездную или безвозмездную реализацию наркотиков в СМИ или Интернете. Анализ же судебной практики свидетельствует, что данное положение в полной мере не отражает характер и особенности сбыта наркотиков в СМИ или интернете.

Например, А. был привлечен к ответственности за незаконный сбыт наркотиков через Интернет, который выражался в том, что он в специальном приложении «Соль земли» размещал объявление о продаже «зернистой соли». Откликнувшимся лицам сообщалось место и время, когда они смогут забрать «зернистую соль» и способ оплаты. Как было установлено в ходе проведения оперативно-розыскного мероприятия, А. делал закладку в лесу пакет с «зернистой солью». Заключение судебного эксперта свидетельствует о том, что «зернистая соль» представляет собой вещество тетраметилциклопирил, которое является производным наркотическим средством общей массой 397,522 г веществ. Помимо этого, у А. было изъяты еще шесть пакетов с наркотиками. Осмотр ве-

[1] © Абдульманов А. А., 2022.

щественного доказательства, в качестве которого выступал «мобильный телефон» показал, что предложение о сбыте наркотиков и последующее обсуждение велось в приложении [4]. В итоге действия А. были квалифицированы в качестве сбыта наркотиков посредством сети Интернет в составе организованной группы в особо крупном размере, т. е. по ч. 5 ст. 228.1 УК РФ.

В данном случае объективная сторона выражалась в размещении информации о сбыте наркотиков. Аналогичная ситуация прослеживается и в других судебных решениях по схожим делам. Следовательно, определение понятия сбыта наркотиков в Интернете или СМИ отличается от сбыта в реальной жизни. Фактически в Интернете или СМИ лицо размещает сообщение о сбыте наркотиков. Однако, как указывалось ранее, законодатель дает иное определение исследуемому понятию. Подобная ситуация обусловлена тем, что законодатель не учитывает особенности Интернет и СМИ, которая связана в первую очередь с информационной сферой. Поэтому считаем необходимым сформулировать определение понятия сбыта наркотиков в СМИ или Интернета с учетом особенностей распространение информации на данных ресурсах.

Основная проблема, связанная с привлечением лиц к ответственности по п. «б» ч. 2 ст. 228.1 УК РФ, обусловлена тем, что объективная сторона не раскрыта должным образом. В частности, не урегулированы следующие моменты:

1. Не установлен перечень действий направленных на сбыт наркотиков в Интернете или СМИ, которые следует квалифицировать по п. «б» ч. 2 ст. 228.1 УК РФ. Как было установлено ранее, действия, направленные на сбыт наркотиков в Интернете или СМИ, несколько отличается от сбыта в реальной жизни. В первую очередь он выражается в передаче информации неопределенному кругу лиц о намерении сбыть наркотики посредством таких ресурсов, как СМИ, электронных или информационно-телекоммуникационных сетей. Анализ законодательства позволяет прийти к выводу о том, что представленные способы передачи информации можно условно подразделить на СМИ, средства сотовой связи и Интернет.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» регулирует отношения, связанные с осуществлением права на поиск, получение, передачу, производство и распространение информации, применение информационных технологий и обеспечение защиты информации. В данном законе определены особенности обращения с информацией, которая получается в рамках проведения оперативно-розыскных мероприятий.

Однако, в российском законодательстве отсутствует определение понятий «сотовая связь», «мобильная связь», «средства сотовой связи». Отсутствие данных определений не способствует совершенствованию подхода к определению приемов и способов сбыта наркотиков в Интернете, СМИ и посредством средств сотовой связи.

Подобная ситуация сложилась ввиду несовершенства законодательства, а отчасти наличием технических стандартов. Однако, такой подход не может считаться верным. Во-первых, в технической литературе понятия «мобильная связь»

и «сотовая связь» рассматриваются в качестве синонимов. Данное понятие раскрывается в качестве особого вида телекоммуникаций, при котором голосовая, текстовая и графическая информация передается на абонентские беспроводные терминалы, не привязанные к определенному месту или территории [5]. В технической литературе выделяют спутниковую, сотовую, транкинговую и другие виды мобильной связи [6, с. 25]. Следовательно, мобильная и сотовая связь являются схожими, но не эквивалентными понятиями.

Поэтому не понятно, каким образом следует квалифицировать сбыт наркотиков посредством средств сотовой связи через приложения. Является ли подобный способ распространение наркотиков через электронные или информационно-телекоммуникационных сети или нет. В судебной практике данное положение также не нашло однозначного ответа.

2. Не определены способы распространения информации о сбыте наркотиков в Интернете или СМИ. По факту происходит сбыт наркотиков в виртуальном пространстве, который отличается рядом особенностей.

Рассматривая данную проблему, следует указать, что законодатель не объяснил является ли создание приложений в App-store или Google-play, посредством которого распространяется наркотики преступлением, квалифицируемым по п. «б» ч. 2 ст. 228.1 УК РФ.

Например, действия С. были квалифицированы как сбыт наркотических средств в крупном размере, организованной группы с использованием электронных и информационно-телекоммуникационных средств, в том числе Интернет. Так, С. создала приложение «Т-Т», в котором осуществлялся сбыт наркотических средств. С. осуществляла рассылку в чате Телеграмм-канала «Т-Т» о том, что каждый, кто хочет приобрести «сами знаете, что» должен получить приглашение в закрытое приложение. В данном приложении, посредством осуществления игры, осуществлялась переписка между участниками отдельных групп, которые участвовали в виртуальном соревновании о том, каким образом можно приобрести наркотическое средство. После того как договоренность была достигнута, соответствующие игроки получила информацию об оплате наркотических средств через криптовалюту, а после произведение оплаты данные о месте, где они могут забрать наркотические средства. С. привлекла к своей деятельности Г. и Е., которые выполняли роль курьеров и осуществляли закладки.

Суд, рассмотрев материалы дела, пришел к выводу о том, что несмотря на то, что способ совершения сбыта некротических средств прямо и не определен в законе, данные действия следует квалифицировать по п. «б» ч. 2 ст. 281.1 УК РФ [7].

Однако, следует признать, что законодатель не установил ответственность за создание приложений, деятельность которых связана со сбытом наркотических средств.

3. Не определены инструменты распространения информации о сбыте наркотиков в Интернете или СМИ.

В правовой и судебной литературе остается не определен вопрос о том, является ли средство сотовой связи инструментом для распространения информации

о сбыте наркотиков или нет. Во-первых, данная проблема связана с тем, что законодатель в полной мере не дал определение самому понятию «средство сотовой связи». Во-вторых, существует правовая и судебная неопределенность в рассмотрении инструментов распространении информации о сбыте наркотиков.

В научной литературе средства сотовой связи классифицируются по различным основаниям. Так, например, С. С. Медведев [8, с. 145–146] предлагает следующую классификацию:

1. В зависимости от функциональности средств сотовой связи, выделяют:

– абонентские устройства, в качестве которых выступают планшетные компьютеры, смартфоны или телефоны, предназначенные для осуществления связи в виде голосовой передачи данных;

– оборудование, обеспечивающее подвижную радиосвязь и базовые станции.

2. В зависимости от характеристики абонентских устройств подразделяют на:

– мобильные телефоны первого уровня, которые позволяют осуществлять голосовую и текстовую передачу данных;

– мобильные телефоны и смартфоны, которые включают в себя функции мобильных телефонов первого уровня, а также обладают характеристиками персонального компьютера, данные устройства относятся к категории мобильных телефонов второго уровня;

– планшеты и телефоны, которые включают в себя функции телефона и компьютера, но имеют диагональ устройства больше, чем у смартфонов.

Сложность выявления мошенничеств, совершаемых с помощью средств сотовой связи, состоит в определении следов преступления.

В отличие, от преступлений, которые совершаются в реальной жизни, следами мошенничества, совершаемого с помощью средств сотовой связи, выступают следы, которые не имеют явного материального выражения.

По мнению ряда правоведов, данные следы являются «виртуальными следами». Так, например, В. Ю. Агибалов указывает, что под виртуальными следами следует понимать следы, которые были «зафиксированы компьютерной системой на цифровом материальном носителе результат отражения реального (физического) процесса или действия иной компьютерной системы, связанный с преступлением (имеющий уголовно-релевантное значение) в виде цифрового образа формальной модели этого процесса» [9, с. 7].

Однако, не все специалисты считают, что само понятие «виртуальный след» не точно трактует сущность следа, который оставляет преступник, используя средства сотовой связи для совершения преступления. Б. В. Вехов указывает, что более правильно использовать понятие «электронно-цифровой след», так как он отображает сущность и содержание действий средств сотовой связи. Поэтому в качестве электронно-цифрового следа правовед предлагает понимать «любую криминалистически значимую компьютерную информацию, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе либо передающиеся по каналам связи электромагнитных сигналов» [10, с. 28–29].

Данное определение позволяет конкретизировать сущность всех следов, которые совершаются удаленно посредством средств коммуникации или компьютеров. Вместе с тем, след, который остается от использования средств сотовой связи, хоть и является электронно-цифровым следом, однако, указывает на тот факт, что он был оставлен на конкретном устройстве.

Другая группа специалистов, указывает, что термины «виртуальные» и «электро-цифровые следы» не является идентичными понятиями.

Во-первых, виртуальность, в данном контексте, представляет собой особое специфическое состояние, которое не существует в реальности, однако при наличии конкретных условий может возникнуть в форме реального объекта, который и оставляет след, и отображается в действительности на материальных объектах.

Во-вторых, электроцифровое пространство представляет собой такое пространство, которое воплощается посредством программ, подключенного оборудования, передачи информации в виде фотонов и прочее.

Так, Е. Р. Россинская отмечает, что следы, оставляемые средствами сотовой связи, являются материальными, так как «зафиксированы на материальных носителях путем изменений свойств или состояния отдельных их элементов… Если выделять информацию, формирующуюся в процессе работы с вычислительной техникой в особую группу материальных следов, то наиболее рациональным полагаем обозначить их в качестве информационно-технологических, поскольку образование данных следов обусловлено спецификой реализации информационных технологий, а для их преобразования в доступную для восприятия форму информационные технологии также применяются» [11, с. 317–318].

Однако, данное определение понятия также нельзя назвать корректным, так как следы средств сотовой связи носят скорее не технологический характер, а отображают электронную сущность рассматриваемого явления. Поэтому в качестве следов средств сотовой связи следует понимать информационно-электронные следы. Для того чтобы определить понятие «информационно-электронные следы», необходимо рассмотреть их видовое разнообразие.

Н. В. Яджин и В. А. Егоров [12, с. 27] предлагают следующую классификацию информационно-электронных следов:

1. Следы на электронных носителях, содержащих сведения о соединениях между абонентами, о произведенных финансовых операциях, системе сотовой связи и иных обстоятельствах, хранящихся у сотовых операторов либо на компьютерах.

2. Следы на мобильных устройствах в виде информации о проведенных финансовых операциях, реальном ущербе от совершенного преступления, местах обналичивания денежных средств, круге лиц, причастных к совершению преступления и т. д. Кроме того, указанные следы способствуют установлению местонахождения преступников, лиц с которыми они контактировали, включая и потерпевших от их действий лиц, а также расширить круг свидетелей и определить IMEI-номера используемых телефонных аппаратов.

3. Следы на мобильном устройстве, содержащие сведения об абонентской книге телефона, соединениях абонентов сетей сотовой связи (журнал звонков,

сообщения формата SMS1, MMS2), о произведенных финансовых операциях, системе сотовой связи, специальных программных средств для «прошивки» мобильных телефонов, SIM-карт, из имеющихся на устройстве приложений, таких как Viber, Skype, WhatsApp, Facebook, Telegram, Vkontakte, Одноклассники и т. д. Они могут содержать данные о пользователях мобильных телефонов, используемых телефонных номеров, фотографиях и видеозаписях, а также следы пальцев рук, микрообъекты.

4. Следы на SIM-карте, содержащих сведения в виде абонентской книги, журнал звонков, текстовые сообщения. Наличие указанной информации, способствует установлению членов преступной группы, определению круга потерпевших и свидетелей, установлению временных промежутков совершенных преступлений.

Информационно-электронный след может быть обнаружен на мобильном устройстве, SIM-карте, на иных электронных носителях.

Таким образом, информационно-электронные следы – представляют собой след, который находит материальное отображение на мобильном устройстве, SIM-карте или иных электронных носителях, которые связанные с реализацией информационных технологий.

Таким образом, учитывая специфику и особенность совершения преступления, которое предусмотрено п. «б» ч. 2 ст. 228.1 УК РФ, объективная сторона выражается именно в распространении информации о сбыте наркотиков в СМИ, электронных или информационно-телекоммуникационных сетей. Инструментом распространения информации выступает Интернет или средство сотовой связи.

В то же время данный момент в полной мере не урегулирован в законодательстве. Отсутствие законодательного разграничения данных понятий является важной проблемой в квалификации преступлений по п. «б» ч. 2 ст. 228.1 УК РФ.

Другая проблема квалификации по п. «б» ч. 2 ст. 228.1 УК РФ заключается в том, что законодатель не определил ответственность за создание Интернет-магазина, который занимается сбытом наркотиков. По нашему мнению, не решение данного вопроса не способствует предупреждению сбыта наркотиков в интернет-среде.

Привлечение лиц к уголовной ответственности за сбыт наркотических веществ, совершенных с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей должно быть направлено в первую очередь на уголовно-правовое предупреждение преступлений данной категории. В данном контексте следует указать, что отсутствует дифференциации уголовной ответственности по п. «б» ч. 2 ст. 228.1 УК РФ. Особенно актуально стоит вопрос не просто ответственности за организацию сбыта наркотиков в Интернете или СМИ, а за организацию постоянной виртуальной точки, в виде Интернет-магазина или объявления, публикуемого в СМИ.

В настоящее время уголовная ответственность за сбыт наркотиков в Интернете или СМИ по п. «б» ч. 2 ст. 228.1 УК РФ рассматривается в общем плане. Вместе с тем, анализ судебной практики свидетельствует о том, что законодатель квалифицируют создание Интернет-магазина, который осуществляет сбыт

наркотиков в качестве совершения преступления организованной группой. Вместе с тем, данный подход нельзя считать правильным, так как Интернет-магазин может создать один человек и привлекать случайных лиц к установлению закладок на протяжении не продолжительного времени. Приведем пример из судебной практики. П. был привлечен к уголовной ответственности за покушение на незаконный сбыт наркотических средств, с использованием информационно-телекоммуникационных сетей, в том числе Интернет, организованной группой в крупном размере. Рассматривая материалы дела, судья установил, что П. в процессе поиска работы увидел в Интернете объявление о том, что требуется курьер для перевоза ювелирных изделий. Откликнувшись на объявление, П. узнал, что ему нужно перевезти пакет и кинуть его в почтовый ящик. Пакет П. должен был забрать в установленном заказчиком месте. Оплата за выполненную работу осуществлялась посредством осуществления перевода денежных средств через кошелек Qiwi. П. получил доступ к данным Интернет-магазина Prestigo, где якобы продавалось золото. В результате осуществления оперативно-розыскной деятельности П. был задержан рядом с почтовым ящиком. Пакет был изъят, в результате проведения экспертизы было установлено, что в нем содержалось наркотическое средство (соединение MMB(N)-BZ-F), массой не менее 205,012 г. Суд, рассматривая материалы дела, указал, что, несмотря на отсутствие определения роли всех участников организованной группы, степени их участия в организации и осуществления сбыта наркотиков посредством организации интернет-магазина, осведомленности П. об участии в данной схеме, действия П. следует квалифицировать как исполнителя и не имеет значения, было ли известно П. о всех особенностях сбыта наркотиков или нет, видах и размерах наркотиков, способе их реализации. При этом суд обратил внимание на некоторую законодательную неопределенность в данном вопросе [13].

Однако, существует и иная практика, когда суд, признавая, что подсудимый не осведомлен о том, что наркотические средства сбываются через Интернет-магазин, квалифицирует его действия исключительно как покушение на сбыт наркотических средств по ч. 1 ст. 208.1 УК РФ. Суд обратил внимание на то, что отсутствуют основные признаки организованной группы [14]. Анализ правовой литературе позволяет установить, что в качестве признаков организованной группы выступают:

1. Устойчивость и сплоченность. В частности, в организованной группе, занимающейся хищениями, признак устойчивости чаще всего характеризуется длительностью существования преступной группы; разделом сфер деятельности с другими подобными группами, жесткой внутренней дисциплиной, планированием преступной деятельности в целом, на определенный промежуток времени, и на совершение каждого конкретного преступления [15, с. 28].

2. Четкое распределение ролей и функций каждого участника группы, наличием лидера (организатора), который непосредственно руководит действиями группы и отвечает за все действия других участников, даже в том случае, если лично не участвует в совершении деяния. При этом, как правило, лидерство обу-

словлено авторитетом в преступном мире или личностными качествами, внушающими остальным участникам необходимость подчинения под страхом наступления возможных негативных последствий (физического, психического насилия, материальных санкций) [16, с. 37]. В данном случае П. являлся курьером, т. е. исполнителем. Однако, не являлся частью организованной группы.

Следовательно, отсутствует законодательная определенность в установлении ответственность за сбыт наркотиков через Интернет-магазин.

Это лишь некоторые проблемы, связанные с квалификацией преступлений по п. «б» ч. 2 ст. 228.1 УК РФ, и связаны они с тем, что недостаточно конкретно определена объективная сторона подобных деяний, не конкретизирована (индивидуализирована) ответственность лица за создание Интернет-магазина или приложения, посредством чего осуществляется сбыт наркотических веществ.

Список литературы

1. Состояние преступности. МВД России. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics.

2. Уголовный кодекс Российской Федерации // СПС «КонсультантПлюс».

3. Постановление Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» (ред. от 16.05.2017) // СПС «КонсультантПлюс».

4. Апелляционное определение Верховного Суда Российской Федерации от 28 ноября 2019 г. Дело № 3-АПУ19-12.

5. ГОСТ Р 53732-2009. Национальный стандарт Российской Федерации. Качество услуг сотовой связи. Показатели качества.

6. Ярцева А. В. Использование в доказывании информации, передаваемой по техническим каналам связи: правовые и тактико-криминалистические аспекты : автореф. дис. ... канд. юрид. наук. Ростов н/Д., 2012. С. 25.

7. Апелляционное определение Верховного Суда Российской Федерации от 5 февраля 2019 г. по делу № 3-10/2017.

8. Медведев С. С. Мошенничество в сфере высоких технологий : дис. ... канд. юрид. наук. Краснодар, 2008. С. 145–146.

9. Агибалов В. Ю. Виртуальные следы в криминалистике и в уголовном процессе : автореф. дис. … канд. юрид. наук. Воронеж, 2010. С. 7.

10. Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки : автореф. дис. … д-ра юрид. наук. Волгоград, 2008. С. 28–29.

11. Россинская Е. Р., Шамаев Г. П. Криминалистическое исследование компьютерных средств и систем как новый раздел криминалистической техники // Уголовно-процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства. 2014. С. 317–318.

12. Яджин Н. В., Егоров В. А. Некоторые элементы криминалистической характеристики преступлений, совершаемых с использованием средств сотовой связи // Концепт. 2017. № 29. С. 27.

13. Апелляционное определение Верховного Суда Российской Федерации от 15 октября 2019 г. по делу № 67-АПУ19-16.

14. Апелляционное определение Верховного Суда Российской Федерации от 3 сентября 2019 г. по делу № 2-26-2019.

15. Попов В. А. Группа лиц, группа лиц по предварительному сговору, организованная группа и преступное сообщество: соотношение понятий // Электронное приложение к Российскому юридическому журналу. 2016. Т. 35. № 3 (35). С. 28.

16. Пудовочкин Ю. Е. Учение о преступлении и о составе преступления. М. : Российский государственный университет правосудия, 2017. С. 37.

Черепенников Р. В.[1],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук

АНАЛИЗ РЕАЛИЗАЦИИ В НАЦИОНАЛЬНОМ ЗАКОНОДАТЕЛЬСТВЕ НОРМ МОДЕЛЬНОГО УГОЛОВНОГО КОДЕКСА СНГ, ПРЕДУСМАТРИВАЮЩИХ ОТВЕТСТВЕННОСТЬ ЗА СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Распад Союза Советских Социалистических Республик (СССР) и образование Содружества Независимых Государств (далее – СНГ; Содружество) 8 декабря 1991 г. поставили перед бывшими союзными республиками вопросы взаимодействия на межгосударственном уровне в различных областях внешней и внутренней политики.

С целью сближения правового регулирования однородных сфер общественных отношений в государствах Содружества в г. Санкт-Петербурге 17 февраля 1996 г. Постановлением № 7-5 на 7-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ был принят «Модельный уголовный кодекс для государств – участников Содружества Независимых Государств. Рекомендательный законодательный акт» (далее – Модельный УК СНГ).

Унификация уголовного законодательства государств – участников СНГ направлена на решение задач интеграционного развития Содружества, а также на формирование и осуществление согласованной законодательной деятельности государств – участников СНГ по вопросам, представляющим общий интерес в регулировании уголовно-правовых отношений [9, с. 295–307].

Реализация поставленных целей требует от государств – участников СНГ внесения изменений, которые бы в максимально возможном варианте сблизили структуру и содержание правовых норм, составляющих уголовно-правовые отрасли национального законодательства.

В период с 17 февраля 1996 г., т. е. с момента принятия Модельного УК СНГ, по настоящее время в него был внесен ряд изменений.

Последние изменения в Модельный УК СНГ были внесены постановлениями Межпарламентской Ассамблеи государств – участников СНГ от 27 ноября 2015 г. № 43-15 и № 43-16.

По своей структуре Модельный УК СНГ традиционно для государств – участников СНГ разделен на две относительно самостоятельные части: Общую, состоящую из пяти разделов, включающих 16 глав, которые содержат статьи с первой по 102; и Особенную, насчитывающую восемь разделов и включающих 18 глав, которые объединяют статьи с 103 по 341.

---

[1] © Черепенников Р. В., 2022.

В 2015 г. постановлениями Межпарламентской Ассамблеи государств – участников СНГ от 27 ноября 2015 г. № 43-15 и № 43-16 в Модельный УК СНГ были внесены существенные изменения, которые в большинстве случаев коснулись норм главы 29 «Преступления против порядка осуществления предпринимательской и иной экономической деятельности», где из 33, ранее входивших в данную главу уголовно-правовых норм, 11 были изменены, в том числе с введением квалифицированных видов преступлений и ужесточением ответственности, добавлены две нормы (ст. 271.1 «Посредничество в коммерческом подкупе» и ст. 265.1 «Принуждение к совершению сделки или к отказу от ее совершения»). В главе 30 «Преступления против информационной безопасности» подверглись изменению все входящие в данную главу нормы. Изменения коснулись и норм главы 23 «Преступления против общественной безопасности», предусматривающих ответственность за преступления террористической и экстремистской направленности, касающиеся как дополнения квалифицирующими признаками (ч. 3 ст. 177.1 «Склонение, вербовка или иное вовлечение в совершение преступлений террористического характера либо иное содействие осуществлению террористической деятельности, совершенные с использованием компьютерных устройств, системы или их сети»), так и уточнения отдельных конструктивных признаков (ч. 2 ст. 177.3 «Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма, совершенные с использованием средств массовой информации или компьютерной сети»).

В **Азербайджанской Республике** отношения, возникающие по поводу совершения преступления, регулируются нормами уголовного кодекса. На это прямо указывают чч. 1.1 и 1.3 ст. 1 Уголовного кодекса Азербайджанской Республики [2] (далее – УК Азербайджанской Республики), которые определяют, что «Уголовный закон Азербайджанской Республики состоит из настоящего Кодекса», «Законы, устанавливающие уголовную ответственность и предусматривающие наказание лица, совершившего преступление, подлежат применению только после включения в настоящий Кодекс». Такое положение соответствует Модельному УК СНГ. УК Азербайджанской Республики содержит гл. 30 «Киберпреступления», название которой, текст, содержание (частично), структура и количество норм не соответствуют главе 30 «Преступления против информационной безопасности» Модельного УК СНГ.

Между Модельным УК СНГ и УК Азербайджанской Республики нет единообразия в применении понятий. Так, в главе 30 «Киберпреступления» УК Азербайджанской Республики используются термины, не соответствующие Модельному УК СНГ: «компьютерная информация» вместо рекомендованного термина «компьютерные данные», «компьютерная система» вместо «компьютерного устройства».

Уголовный кодекс Республики Беларусь [3] содержит главу 31 «Преступления против компьютерной безопасности», название которой, текст, содержание (частично), структура и количество норм не соответствуют главе 30 «Преступления против информационной безопасности» Модельного УК СНГ. Наряду с этим, в УК Республики Беларусь последние изменения Модельного УК СНГ

(примечания 1 и 2 к ст. 286), связанные с дополнением норм гл. 30 «Преступления против информационной безопасности» примечаниями с конкретизацией понятий «компьютерные данные» и «компьютерное устройство», не учтены, лишь в ч. 18 ст. 4 УК Республики Беларусь содержится понятие «компьютерной информации».

Часть 1 ст. 1 Уголовного кодекса Республики Казахстан [4] (далее – УК Республики Казахстан), определяет, что «Уголовное законодательство Республики Казахстан состоит из настоящего Уголовного кодекса Республики Казахстан. Иные законы, предусматривающие уголовную ответственность, подлежат применению только после их включения в настоящий Кодекс». В целом такое положение соответствует Модельному УК СНГ. Наряду с этим, УК Республики Казахстан содержит главу 7 «Уголовные правонарушения в сфере информатизации и связи», название которой, текст, содержание (частично), структура и количество норм не соответствуют главе 30 «Преступления против информационной безопасности» Модельного УК СНГ. В статьях УК Республики Казахстан не реализованы последние изменения Модельного УК СНГ (примечания 1 и 2 к ст. 286), связанные с дополнением норм главы 30 «Преступления против информационной безопасности» примечаниями с конкретизацией понятий «компьютерные данные» и «компьютерное устройство».

Уголовный кодекс Кыргызской Республики [5] содержит главу 40 «Преступления против кибер-безопасности», название которой, текст, содержание (частично), структура и количество норм не соответствуют главе 30 «Преступления против информационной безопасности» Модельного УК СНГ. Однако, в статьях УК Кыргызской Республики не реализованы последние изменения Модельного УК СНГ (примечания 1 и 2 к ст. 286), связанные с дополнением норм гл. 30 «Преступления против информационной безопасности» примечаниями с конкретизацией понятий «компьютерные данные» и «компьютерное устройство».

Указанные изменения также не реализованы в: Уголовном кодекс Республики Молдова [6], хотя в нем выделена глава XI «Информационные преступления и преступления в области электросвязи», название которой, структура и количество норм не соответствуют гл. 30 «Преступления против информационной безопасности» Модельного УК СНГ; Уголовный кодекс Российской Федерации, где имеется гл. 28 «Преступления в сфере компьютерной информации», и где отсутствуют определения таких понятий «компьютерные данные» и «компьютерное устройство»; Уголовный кодекс Республики Таджикистан [7], в которой имеется гл. 28 «Преступления против информационной безопасности», и отсутствуют определения указанных понятий; Уголовный кодекс Республики Узбекистан [8], содержащий гл. XX-1 «Преступления в сфере информационных технологий», но не раскрывающий многие понятия данного раздела. В ст. 278-2 «Незаконный (несанкционированный) доступ к компьютерной информации» Уголовного кодекса Республики Узбекистан используются понятия «компьютерная информация» и «электронно-вычислительная машина». Причем понятие «компьютерная информация» раскрывается по тексту статьи, а не в виде примечания.

Вывод. Ни в одном из уголовных законов государств – участников СНГ не реализованы в полном объеме изменения Модельного УК СНГ.

Наиболее частые отступления в национальном уголовном законодательстве от Модельного УК СНГ допускаются: в структуре уголовного закона; использовании разных терминов при названии одного и того же явления в уголовно-правовых нормах; совокупности признаков уголовно-правовых норм, отражающих то или иное уголовно-правовое явление; отнесении преступлений к рекомендуемой категории; системе и видах наказаний.

Ни в одном уголовном законе государств – участников СНГ не воспроизводятся дословно нормы главы 30 «Преступления против информационной безопасности» Модельного УК СНГ.

В большей мере приближены к тексту, содержанию, структуре и количеству норм главы 30 «Преступления против информационной безопасности» Модельного УК СНГ уголовно-правовые нормы Уголовного кодекса Республики Таджикистан.

Такие разные подходы могут приводить к трудностям в межгосударственном уголовно-процессуальном взаимодействии. На наш взгляд, в целях более эффективного противодействия указанным преступлениям требуется унификация законодательства государств СНГ.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 22.08.2021).

2. Уголовный кодекс Азербайджанской Республики (утвержден законом Азербайджанской Республики от 30 декабря 1999 г. № 787-IQ «Об утверждении, вступлении в силу Уголовного кодекса Азербайджанской Республики и связанных с этих вопросов правового регулирования» // ИС «Континент». URL: http://continent-online.com/.

3. Уголовный кодекс Республики Беларусь (принят Палатой представителей 2 июня 1999 г. Одобрен Советом Республики 24 июня 1999 г.) // ИС «Континент». URL: http://continent-online.com/.

4. Уголовный кодекс Республики Казахстан (введен в действие с 1 января 2015 г.) // ИС «Континент». URL: http://continent-online.com/.

5. Уголовный кодекс Кыргызской Республики (введен в действие законом Кыргызской Республики от 28 октября 2021 г. № 126 «О введении в действие Уголовного кодекса Кыргызской Республики, Уголовно-процессуального кодекса Кыргызской Республики, Кодекса Кыргызской Республики о правонарушениях и внесении изменений в некоторые законодательные акты Кыргызской Республики» // ИС «Континент». URL: http://continent-online.com/.

6. Уголовный кодекс Республики Молдова (введен в действие законом Республики Молдова от 21 июня 2002 г. № 1160-XV «О введении в действие Уголовного кодекса Республики Молдова» (с изменениями и дополнениями по состоянию на 11.11.2021) // ИС «Континент». URL: http://continent-online.com/.

7. Уголовный кодекс Республики Таджикистан (принят Законом Республики Таджикистан от 21 мая 1998 г. № 574, введен в действие постановлением Маджлиси Оли Республики Таджикистан от 21 мая 1998 г. № 575) // ИС «Континент». URL: http://continent-online.com/.

8. Уголовный кодекс Республики Узбекистан (утвержден Законом Республики Узбекистан от 22 сентября 1994 г. № 2012-XII) (с изменениями и дополнениями по состоянию на 15.02.2022) // ИС «Континент». URL: http://continent-online.com/.

9. Положение о разработке модельных законодательных актов и рекомендаций Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств (принято в г. Санкт-Петербурге 14.04.2005 Постановлением 25-8 на 25-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (с изм. и доп. от 23.11.2012) // Информационный бюллетень Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств (Информационный бюллетень МПА). 2013. № 57. Ч. 2. С. 295–307.

Калининская Я. С.[1],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук

Бойцова Ж. А.[2],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук

О НЕКОТОРЫХ ПРОБЛЕМАХ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ ПРОТИВ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Согласно «Концепции общественной безопасности в Российской Федерации» под общественной безопасностью понимается состояние защищенности человека и гражданина, материальных и духовных ценностей общества от преступных и иных противоправных посягательств, социальных и межнациональных конфликтов, а также от чрезвычайных ситуаций природного и техногенного характера [1]. Данное определение фактически охватывает все те блага, которые включил законодатель в качестве объекта посягательства преступлений против общественной безопасности и общественного порядка: общественную безопасность в узком смысле слова, здоровье населения и общественную нравственность, экологию, безопасность дорожного движения и эксплуатации транспорта и сферу компьютерной информации.

Преступные посягательства на общественную безопасность представляют собой довольно обширную группу деяний, направленных на дестабилизацию нормального устройства общества и государства в целом, а также на возможность беспрепятственно реализовывать свои функции каждым конкретным человеком.

Достижение целей обеспечения государственной и общественной безопасности осуществляется путем реализации проводимой государством политики, направленной на решение перечисленных в Указе Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» задач, в число которых входит: предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе легализации преступных доходов, финансирования терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использования в противоправных целях цифровых валют [2].

---

[1] © Калининская Я. С., 2022.
[2] © Бойцова Ж. А., 2022.

Представляется необходимым отметить, что согласно статистическим сведениям, каждое четвертое преступление совершается с использованием информационно-телекоммуникационных технологий [3]. При этом, если в 2020 г. число таких преступлений возросло на 73,4 % (с использованием сети Интернет на 91,3 %) [4], то в 2021 г. темп прироста уменьшился (произошло его увеличение на 1,4 %). В январе–феврале 2022 г. выявлено снижение количества совершенных преступлений на 2,2 % по сравнению с аналогичным отрезком времени 2021 г. [3].

Использование сети Интернет стало одним из распространенных способов совершения публичных призывов к осуществлению террористической деятельности, публичного оправдания терроризма или пропаганды терроризма. Эти и иные противоправные действия, направленные против интересов Российской Федерации и ее граждан, совершаемые с использованием социальных сетей, мессенджеров и сервисов видеосообщений, приобрели такой масштаб, что помимо привлечения к ответственности пользователей, органами государственной власти принимаются решения, ограничивающие деятельность самих компаний, обладающих социальными сетями, мессенджерами и сервисами видеосообщений. Например, в отношении компании Meta Тверским районным судом было вынесено решение о запрете ее деятельности, связанной с реализацией продуктов Facebook и Instagram на территории Российской Федерации в связи с осуществлением экстремистской деятельности [5]. Необходимо отметить, что такое решение заслуживает одобрения, поскольку социальные сети, оказывающие огромное влияние на пользователей, формирование ими мировоззрения, точек зрения относительно происходящих в мире событий, (особенно среди несовершеннолетних и молодых людей), должны осуществлять свою деятельность в рамках правового поля и не допускать распространения информации, порочащей честь и достоинство граждан, содержащей угрозы различного характера в их адрес, а также подрывающих авторитет органов государственной власти и Российской Федерации в целом.

Оценивая деятельность пользователей в сети Интернет на предмет совершения ими противоправных деяний (административных правонарушений или преступлений, в частности, совершения публичных призывов к осуществлению террористической деятельности, публичного оправдания терроризма или пропаганды терроризма), необходимо заострять внимание на ряд характерных черт, позволяющих выявить преступные намерения и отличить их от «случайных» действий. К числу таких факторов можно отнести выявление признаков, характеризующих адресатов рассылаемых сообщений и публикуемых в аккаунтах сведениях. В некоторых случаях получателями информации, содержащей призывы к осуществлению террористической деятельности, сведения, оправдывающие терроризм или пропагандирующие терроризм, могут быть лица, уже разделяющие идеологию и практику терроризма. Образуют ли такие действия состав преступления, предусмотренного ст. 205^2 Уголовного кодекса Российской Федерации? Полагаем, что если речь идет о призывах к осуществлению терро-

ристической деятельности и оправданию терроризма, то лицо подлежит ответственности. Примером этому может послужить следующее: признавая Х. виновным в пропаганде терроризма с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет, суд исходил из того, что осужденный распространял среди четырех лиц, в том числе А., материалы и информацию, направленные на формирование у названных лиц идеологии терроризма, убежденности в ее привлекательности и представления о допустимости осуществления террористической деятельности. Публичность для привлечения к ответственности за пропаганду терроризма не требует установления. Поведение лица, имеющее своей целью внедрить идеологию терроризма хотя бы одному человеку, должно подлежать оценке как уголовно наказуемое. Если же такие действия направлены в адрес того, кому уже близки идеи терроризма, они не порождают юридического факта. Так, судом был исключен эпизод в отношении А., который разделял идеи терроризма, независимо от действий Х. [6].

Действия, образующие состав преступления, предусмотренного ст. 205² Уголовного кодекса Российской Федерации, имеют альтернативный способ описания в законе, при котором совершение как любого из названных действий, так и нескольких из них являются основанием для уголовной ответственности. Нередкими оказываются случаи, когда действия совершаются лицами систематично. В этой связи возникает вопрос, каким же образом надлежит квалифицировать действия лица, состоящие из публичных призывов к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганду терроризма, которые осуществлены одним и тем же лицом в разное время? Образуется ли в такой ситуации совокупность преступлений или это необходимо расценивать как сложное единое преступление?

В доктрине уголовного права этот вопрос решается, исходя из направленности умысла лица, совершающего деяние. В случаях, когда единый умысел отсутствует, содеянное подлежит квалификации как множественность преступлений (в форме совокупности). Проиллюстрировать это можно следующим: Х. признан виновным и осужден за совершение двух преступлений, предусмотренных ч. 2 ст. 205² Уголовного кодекса Российской Федерации (14 августа 2019 г. в г. Сарани Республики Казахстан и 23 октября 2019 г. в г. Калининграде). При рассмотрении дела принято во внимание, что при совершении публичного оправдания и пропаганды терроризма с использованием информационно-телекоммуникационной сети Интернет преступление считается оконченным с момента размещения информации в указанной сети общего пользования. Анализ и основанная на законе оценка совокупности исследованных в судебном заседании доказательств позволили суду правильно установить фактические обстоятельства содеянного Х. и верно квалифицировать его действия по совокупности двух преступлений, предусмотренных ч. 2 ст. 205² Уголовного кодекса Российской Федерации [7].

Иначе были оценены действия А. Суд установил, что 8 октября и 19 ноября 2020 г. А., являясь сторонником радикальных течений ислама, находясь в г. Норильске Красноярского края, с использованием своего мобильного телефона разместил в информационно-телекоммуникационной сети Интернет на своей персональной странице в социальной сети «ВКонтакте» изображения, отражающие деятельность радикальных течений ислама, а 18 октября и 19 ноября 2020 г. на той же странице опубликовал к ним свои комментарии с положительной оценкой деятельности террористической организации. Тем самым с использованием информационно-телекоммуникационной сети Интернет он совершил публичные призывы к осуществлению террористической деятельности, публичное оправдание и пропаганду терроризма [8]. То есть в данном случае действия виновного были охвачены единым умыслом, в связи с чем, квалифицированы как единичное продолжаемое преступление. Единый умысел в преступлениях рассматриваемого вида направлен на возбуждение желания осуществлять террористическую деятельность, на обоснование и (или) оправдание идеологии терроризма, пропаганду терроризма.

В свете решения вопроса о наличии совокупности преступлений или единого сложного преступления существенное значение имеет и момент окончания преступного деяния. Верховным Судом Российской Федерации применительно к ч. 2 ст. 205² и ч.2 ст. 280 Уголовного кодекса Российской Федерации он определен как момент размещения обращений в указанных сетях общего пользования (например, на сайтах, форумах или в блогах), отправления сообщений другим лицам [9].

Обобщая изложенное выше, отметим, что судебная практика применения нормы, предусматривающей ответственность за публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганду терроризма, не лишена некоторой неоднородности и неоднозначности. Устранению этих моментов может способствовать боле точное законодательное решение или оптимальное судебное толкование.

Список литературы

1. Концепция общественной безопасности в Российской Федерации (утв. Президентом Российской Федерации 14 ноября 2013 г. № Пр-2685) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_154602.

2. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_389271/?.

3. Краткая характеристика состояния преступности в Российской Федерации за январь–февраль 2022 г. URL: https://мвд.рф/reports/item/29152810/?ysclid=-l3iflsr96d.

4. Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2020 г. URL: https://мвд.рф/reports/item/22678184/?ysclid=-l3ifjdrzgh.

5. Признание Meta* экстремистской организацией: что нужно знать маркетологам компаний? URL: https://www.garant.ru/news/1535358/?.

6. Обзор судебной практики Верховного Суда Российской Федерации № 3 (2019) (утв. Президиумом Верховного Суда Российской Федерации 27 ноября 2019 г.) // СПС «КонсультантПлюс». URL: https://online11.consultant.ru.

7. Кассационное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 8 июля 2021 г. № 222-УД21-25-А6 // СПС «КонсультантПлюс». URL: https://online11.consultant.ru/.

8. Кассационное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 14 апреля 2022 г. № 225-УД22-3-А6 Приговор: по ч. 2 ст. 205.2 УК РФ за публичные призывы к осуществлению террористической деятельности, публичное оправдание и пропаганду терроризма, совершенные с использованием информационно-телекоммуникационной сети Интернет. Определение Верховного Суда Российской Федерации: Приговор оставлен без изменения // СПС «КонсультантПлюс». URL: https://online11.-consultant.ru/.

9. Постановление Пленума Верховного Суда Российской Федерации от 28.06.2011 № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (ред. от 20.09.2018) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_115712/ ; постановление Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» (ред. от 03.11.2016) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_125957/.

Нестерович С. А.[1],
доцент кафедры информационных технологий
и организации расследования киберпреступлений
Московской академии
Следственного комитета Российской Федерации

Купцова Ю. И.[2],
ассистент кафедры информационных технологий
и организации расследования киберпреступлений
Московской академии
Следственного комитета Российской Федерации

ФИШИНГОВЫЕ АТАКИ НА МОБИЛЬНЫЕ ТЕЛЕФОНЫ С ОПЕРАЦИОННОЙ СИСТЕМОЙ ANDROID

По данным информационного-аналитического сайта Statcounter.com, Android – наиболее популярная операционная система для мобильных устройств на сегодняшний день в мире. На долю устройств с iOS приходится лишь 28,53 %, тогда как Android установлен на 70,75 % мобильных устройств [2].

Чем же принципиально отличаются друг от друга iOS и Android? iOs – это операционная система, созданная исключительно для «яблочных» устройств компанией Apple, с закрытым исходным кодом, который не могут модифицировать сторонние разработчики, в то время как операционная система Android создана для огромного большинства мобильных устройств производства самых разных компаний по всему миру, она не «привязана» к конкретному производителю, а универсальна, исходный код Android – открытый, и исходные коды Android публикуются специально созданной компанией Android Open Source Project (AOSP).

С открытостью исходного кода Android связаны два важных момента.

Во-первых, именно поэтому в мобильных устройствах с Android гораздо проще технически получить root-права – режим расширенных настроек, то есть возможности разработчика, или суперюзера. Суперюзер – это «расширенные настройки» означают снятие заводских ограничений, которые устанавливает производитель смартфона или планшета, чтобы защитить устройство от установки потенциально опасных программ из непроверенных источников.

Во-вторых, из-за открытости исходного кода Android искать, находить и использовать уязвимости этой операционной системы может абсолютно любой человек, который этого захочет. Достаточно, чтобы у него было желание, компьютер или планшет и доступ к Интернету, где, к сожалению, океан информации на эту тему – специализированные журналы, форумы, видеоролики и подробные инструкции от «энтузиастов».

Казалось бы, Apple-устройства стоят дороже, а на счетах их обладателей, добраться до которых мечтают мошенники, больше денег, чем на счетах среднего

[1] © Нестерович С. А., 2022.
[2] © Купцова И. Ю., 2022.

пользователя Android-устройства. Но дело в том, что если iOs в плане безопасности похожа на тщательно охраняемый неприступный дворец (да, с богатыми подвалами, но под охраной), то Android – на проходной двор с дверями нараспашку, в который может заходить кто хочет и брать что хочет (и в нем, как правило, кое-что лежит).

А что нужно мошеннику, чтобы забрать деньги владельца смартфона или планшета? Знать персональные данные хозяина устройства, по которым его идентифицируют банки и другие финансовые системы, а также его друзья и знакомые: логины, пароли, ФИО, дату рождения, возможно, номера кредитных карточек и банковских счетов, кодовые слова, и т. д., и т. п.

Как мошенник собирается выудить эти данные из владельца смартфона на Android? Как рыбак выуживает рыбку из воды: на наживку. Поэтому этот процесс и называется «фишинг» (англ. «fishing» – «рыбалка»). Несложно догадаться, что самое «рыбное» место – именно устройства на Android, потому что, во-первых, они не защищены, а во-вторых, их более 70 % от всех, имеющихся в мире [3].

Способы фишинга – отдельная интереснейшая тема, поистине неисчерпаемая. Арсенал «наживок» сопоставим с разнообразием аксессуаров для рыбной ловли в магазине «охота и рыбалка», но, разумеется, значительно его превышает (люди «ловятся» на гораздо более изощренные приманки, кликая на пересланные или попавшиеся в Интернете статьи, ссылки, фото и посты, затрагивающие их эмоции и инстинкты, азарт, убеждения или любопытство, открывают письма, якобы от знакомого или партнера, и кликают на ссылки, в которых им обещают «золотые горы» или пишут, что именно они – те самые «миллионные пользователи», которые выиграли главный приз в конкурсе, в котором не участвовали). Наверняка в наше время не осталось пользователей гаджетов, кому хоть раз бы не пришло на почту или не попалось на глаза нечто подобное. На своих форумах злоумышленники называют все это не аферизмом, а «социальной инженерией», и обмениваются способами добычи конфиденциальных данных ничего не подозревающих законопослушных граждан.

В Российской Федерации самыми популярными «удочками» для фишинга раньше считались почта mail.ru и yandex.ru, а также социальные сети Одноклассники и VKontakte. Сейчас бесспорные «хедлайнеры» фишинга – это WhatsApp (83 %), Viber (10 %) и Telegram (7 %) хотя, при желании, для фишинга можно использовать что угодно, хоть почту, хоть Facebook, хоть Instagram, главное, чтобы пользователь кликнул по ссылке или изображению либо перешел по ссылке и заполнил своими данными форму на фишинговом сайте [1, с. 12].

Согласно статистике банка ВТБ, в первом полугодии 2020 г. наблюдался активный рост числа кибератак злоумышленников (доля сторонних сайтов выросла почти в два раза и составляла 17 %) [4]. За это же время в Telegram стало в 15 раз больше фишинговых страниц, что дало основания говорить о гораздо больших объемах и скорости роста «промысла» мошенников в данном мессенджере.

С появлением QR-кодов, к уже имевшимся на начало 2021 г. способам узнать конфиденциальные данные пользователей Android добавился еще один. Злоумышленники сообщали своему «клиенту» о блокировке банковского счета и предлагали решить этот вопрос при помощи мобильного приложения – отсканировать QR-код. Если жертва сканировала его, мошенники получали доступ к ее персональным данным, банковской информации, с карты или счета могла списаться сумма денег, и т. п. [5].

Как правило, примитивные фишинговые инструменты для смартфонов созданы с целью доступа к счетам и платежным данным для кражи денег; такие «удочки с приманками» («clickbait» – дословно переводится с английского как «кликни по наживке») аналогичны тем, что используются и для кражи информации с компьютеров. Однако возможности смартфона намного шире, так как он используется и как устройство связи, и как хранилище информации, и как устройство выхода в Интернет, и как банк фото, музыки, база контактов из телефонной книги и в различных социальных сетях и содержание их общения, и т. п., а также постоянно находится рядом с владельцем, что позволяет определить местоположение объекта слежки и превращает гаджет при желании и определенных технических навыках в полноценное шпионское устройство. Также, благодаря встроенной видеокамере, за объектом можно наблюдать, делать скриншоты экрана его телефона в фоновом режиме незаметно для него и практически полностью контролировать его жизнь.

Для этого создано множество программ с различным функционалом, например, Cocospy, Spyzie, VKur.se, Cell Phone Spy PRO+, Talklog, TrackView, FlexiSpy или Remote Administration Tool (в переводе с английского языка – «удаленное администрирование»).

Каковы возможности этих и других подобных программ? Прежде всего, как уже говорилось, это полноценный физический и информационный шпионаж. Действуя незаметно для жертвы, в фоновом режиме, программа позволяет злоумышленнику получать, копировать, хранить и делиться всей информацией, как находящейся на целевом смартфоне, так и проходящей через него, а именно, делает возможными:

– просмотр списка контактов, журналов входящих и исходящих вызовов смартфона, просмотр журнала SMS-сообщений и их чтение;

– прослушку и запись совершаемых разговоров;

– сохранения различных файлов (фото, видео, и т.д) на внешнее устройство или в облачное хранилище;

– определение местоположения и перемещений жертвы по сигналам вышек сотовой связи, GPS и/или Wi-Fi;

– использование смартфона в качестве устройства для скрытной аудио- и/или видеозаписи;

– сбор данных о посещенных страницах браузеров;

– отслеживание в реальном времени и архивирование переписки в почтовых программах, социальных сетях, мессенджерах;

– скриншоты экрана с заданной периодичностью;

– просмотр списка установленных программ, а также установка и удаление программ на смартфон;

– и многое другое (функционал перечисленных программ варьируется в зависимости от задач и возможностей).

Таким образом, смартфон заражается вреодоносным програмным обеспечением после прохождения по фишинговой ссылке и превращается в устройство слежения за своим пользьзователем. Это становится возможным за счет того, что посредством внедрения вредоносной программы на смартфон мошенник присваивает расширенные (root) права по управлению им, т. е. в конечном счете из-за уязвимостей операционной системы Android, обусловленных открытостью и общедоступностью ее исходного кода.

Приведем в таблице 1 некоторые разрешения, которыми пользуются вредоносные программы в операционной системе Android.

Таблица 1

№ п/п	Используемые расширения	Результат выполнения
1	adroid.permission.CHANGE_NETWORK_STATE	изменение подключения к сети
2	android.permission.DISABLE_KEYGUARD	отключение блокировки клавиатуры
3	android.permission.USE_CREDENTIALS	использование учетных записей
4	android.permission.READ_CALENDAR	чтение мероприятий в календаре
5	android.permission.CALL_PRIVILEGED	совершение вызовов на любые телефонные номера
6	android.permission.CALL_PRIVILEGED	совершение вызовов на любые телефонные номера
7	android.permission.ACCESS_FINE_LOCATION	доступ к данным GPS
8	android.permission.WRITE_SMS	редактирование SMS или MMS
9	android.permission.DELETE_PACKAGES	удаление приложений
10	android.permission.STATUS_BAR	(отключение или изменение строки состояния
11	com.android.browser.permission.READ_HISTORY_BOOKMARKS	чтение истории браузера и закладок
12	adroid.permission.WRITE_EXTERNAL_STORAGE	изменить/удалить содержимое SD-карты

Обычно управляемые вредоносные программы состоят из двух основных частей: это серверная часть (далее – «сервер»), которая отвечает за обработку поступающей информации, и клиентская часть (далее – «клиент»), которую устанавливают на целевой телефон.

С точки зрения законодательства (ст. 273 Уголовного кодекса Российской Федерации), вредоносным является именно клиент, потому что эта часть программы имеет все признаки нарушения закона, упомянутые в данной статье. Клиент запускается автоматически одновременно с включением смартфона и все время, пока гаджет работает, собирает и передает на сервер информацию, указанную злоумышленником в параметрах. Настройки удаленного сервера указываются в программе-клиенте, благодаря чему раскрывать такие преступления становится легче.

Поскольку программа-шпион, установленная на смартфон, работает скрытно, никак не давая владельцу устройства заметить себя, обнаружить и обезвредить ее можно только при помощи специальных программ.

По данным экспертов компании ESET (создателя антивирусного программного обеспечения NOD), в 2021 г. в период с января по июль более 150000 копий вируса FakeAdBlocker было загружено мошенниками на устройства с Android. Россия оказалась среди первых стран по числу тех, кто пострадал от вируса [6]. Причиной массового заражения стали переходы пользователей смартфонов по фишинговым ссылкам из сервисов сокращения ссылок. Попадая в операционную систему смартфона, FakeAdBlocker незаметно устанавливает Cerberus, Ginp, TeaBot (трояны, ворующие пароли и банковские данные) и запускает в фоновом режиме разнообразные процессы.

Некоторые специализированные разновидности вредоносных программ позволяют наблюдать за информацией и управлять программой через другое мобильное приложение, установленное на смартфон мошенника. Тогда обе части приложения – и сервер, и клиент – воспринимают смартфон злоумышленника как сервер.

Для примера, приведем анализ сетевого взаимодействия программы слежки за смартфоном (рис. 1).

Анализ сетевого трафика программы выявил обращение к ресурсам, с которыми программа в скрытом от пользователя режиме, осуществляет обмен информацией.

```
HTTP/1.1 403 Forbidden Server
158.187   открытие      217.172.190.216          12379
164.186   запись        217.172.190.216          12379
.
164.187   запись        217.172.190.216          12379

164.187   запись        217.172.190.216          12379
<.
164.187   запись        217.172.190.216          12379
....[
165.187   запись        217.172.190.216          12379
<.
165.200   чтение        217.172.190.216          12379
P:...PHONE:UNKNOWN PHONE
167.200   чтение        217.172.190.216          12379
PHONE:UNKNOWN PHONE
209.184   открытие      localhost                123
209.184   запись        localhost                123
```

Рис. 1. Фрагмент анализа сетевого трафика программы

Соответственно, при внимательном изучении обнаруженного экземпляра программы-вируса технически вполне возможно обнаружить местонахождение серверов управления и архивирования (рис. 2).

Рис. 2. Анализ сетевого трафика вредоносной программы

В заключение, вот несколько советов, которые помогут защититься от фишинга владельцам Android-смартфонов:

1. Если нужны приложения, скачивайте их только с Google Play. Apk-файлы, размещенные на других сайтах небезопасны и могут навредить вам.

2. Внимательно следите, какие разрешения есть у каких приложений, к чему они имеют доступ и соответствует ли уровень доступа их задачам.

3. Логины и пароли можно вводить только после того, как вы убедились, что соединение защищено – перед адресом сайта должно быть написано https (где «s» переводится как «secure» – «безопасное»).

4. Любые ссылки в почте, даже если письмо пришло с адреса кого-то из знакомых, нужно проверять не менее тщательно, чем если бы их прислал незнакомый человек. К сожалению, наших друзей, родных и коллег также могут взломать, от этого никто не застрахован, и тогда у злоумышленника окажется их почта и множество электронных адресов их контактов, среди которых будет и ваш.

5. Одна из самых распространенных уловок в фишинге – сделать сайт, полностью повторяющий сайт банка, платежной системы, Интернет-магазина. Цель – предложить вам форму для ввода ваших платежных данных. Защититься можно, не спеша, не поддаваясь сиюминутным порывам, а критически анализируя доменные имена. У поддельных сайтов они будут или с ошибкой, или вовсе не похожи на оригинал.

6. Можно поставить злоумышленникам заслон на пути к перехвату вашей информации, хранящейся на SD-карте, зашифровав ее. Защитить свою частную жизнь (фото, видео, книги, музыку, приложения и многое другое) можно так: Настройки – Безопасность – Зашифровать телефон – поставить галочку «Шифровать SD-карту».

7. Если вы хотите скрыть свое местонахождение, реальный ip-адрес, опасаетесь, что к вашему смартфону или планшету могут несанкционированно подключиться через уязвимости интернет-соединения – используйте VPN! Эта технология не только обеспечит приватность, но и поможет воспользоваться интернет-ресурсами, заблокированными в вашей стране.

8. Не выпускайте телефон из поля зрения, не давайте в руки знакомым и незнакомым людям (они могут сделать с ним многое: украсть, установить фишинговую программу, значок которой сразу же спрячется и станет необнаружим без специального софта, отправить на любой номер деньги с вашей сим-карты при помощи SMS на короткий номер сотового оператора и многое другое. Также старайтесь не пользоваться уведомлениями от приложений в режиме ожидания, чтобы их коды, приходящие на экран смартфона, не стали известны мошенникам.

Список литературы

1. Тресков В. И. Осторожно: мошенничество! Как защитить себя и своих близких (выпуск 8) // Российская газета. 2018. С. 60.

2. Доля рынка мобильных операционных систем по всему миру. URL: https://gs.statcounter.com/os-market-share/mobile/worldwide.

3. Доля фишинга в мошеннических. URL: https://tass.ru/ekonomika/12386337.

4. Доля фишинга в мошеннических. URL: https://tass.ru/ekonomika/12386337.

5. Спам и фишинг в I квартале 2021 г. URL: https://securelist.ru/spam-and-phishing-in-q1-2021/101270.

6. Разработчик антивирусов ESET сообщил о всплеске в России мошенничеств через короткие ссылки. URL: https://www.tinkoff.ru/invest/news/639847/.

Зиберова О. С.[1],
доцент кафедры криминалистики
Калининградского филиала
Санкт-Петербургского университета МВД России,
кандидат юридических наук

ПУТИ МОДЕРНИЗАЦИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАМКАХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ

Роль информационного обеспечения органов внутренних дел заключается в возможности максимально продуктивно использовать информацию в оперативно-служебной деятельности в целом и в противодействии преступности в частности. Мир интенсивно меняется, подстраиваясь под информационные преобразования общества, и преступники активно используют эти перемены в целях достижения преступного результата. Информационные технологии вплетаются в профессиональную деятельность органов внутренних дел, интегрируются и развиваются, с 2021 г. реализуется ведомственная программа цифровой трансформации [1].

Информационную трансформацию претерпевают многие сферы, затрагивают они и области противодействия преступности, в структуре которой за последние годы произошли существенные изменения. Так, по итогам 2021 г. количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий, продолжает расти: число тяжких и особо тяжких преступлений из их числа выросло на 7,7 %, совершенных посредством сети Интернет – на 17 %, мошенничеств – на 13,3 %, публичных призывов к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма – на 35,8 %, публичных призывов к осуществлению экстремистской деятельности – на 33,8 %, неправомерных доступов к компьютерной информации – на 55,7 % [2, с. 2–4, 30–32.].

Вокресенский Г. М. [3, с. 22] указывает, что под информационным обеспечением следует понимать деятельность, связанную с разработкой, функционированием, а также с развитием информационных систем, необходимых для достижения поставленных задач. Полагаем, успешность профессиональной деятельности органов внутренних дел в сфере противодействия преступности напрямую зависит от качественного информационного обеспечения.

Информационные технологии – это совокупность высокоэффективных средств и методов, направленных на сбор, обработку, анализ, систематизацию, а также накопление и последующее использование информации. Информационные технологии в органах внутренних дел – система средств, приемов и методов накопления, систематизации, анализа и применения информации в оперативно-служебных целях, в том числе в целях профилактики преступлений и правонарушений.

---

[1] © Зиберова О. С., 2022.

Обозначим направления развития информационных технологий в сфере противодействия преступности.

Важнейшим направлением видится развитие систем мониторинга текущего состояния программного обеспечения органов внутренних дел.

Целесообразным выглядит инициирование разработки мобильного приложения «Полиция» на примере банковских сервисов с возможностью обратной связи, централизованного оповещения населения на случай возможной чрезвычайной ситуации, доведения до населения ориентировок на разыскиваемых лиц и пропавших вез вести и пр. В этой связи С. А. Качанов, С. Н. Нехорошев, А. П. Попов [4] предлагают разрабатывать межведомственные комплексы программно-технических средств, позволяющие в максимально короткие сроки оповещать население о возникновении опасной ситуации, например, в случае возникновения террористической угрозы, техногенной или природной катастрофы, действиях особо опасных преступников.

В последние годы большое внимание уделяется личной безопасности сотрудников органов внутренних дел, а также автоматизации процессов, обеспечивающих поддержание правопорядка и общественной безопасности. В США роботы принимают участие в патрулировании улиц, а в 2023 г. в Дубае откроется полицейский участок, на службе в котором будут состоять только роботы. Сейчас Дубай является одним из самых безопасных мест в мире, а уровень роботизации там один из самых высоких. В Российской Федерации зарегистрировано порядка 5 тыс. роботов, в странах Евросоюза – свыше 400000, в Японии – свыше 600000, в Китае – около 500000 [5, с. 70–75].

Развитие и совершенствование «умных» систем видеонаблюдения, которые являются мерой профилактики преступлений и правонарушений, например, «Безопасный город», также представляется достаточно актуальным. На сегодняшний день свыше 70 % преступлений в столичном регионе страны раскрывается благодаря большому покрытию камерами зон слежения [6]. Ежегодная раскрываемость преступлений при помощи системы «Безопасный город» растет [7, с.4–56]. Одним из самых перспективных направлений видится развитие искусственного интеллекта, расширение его возможностей для оптимизации деятельности сотрудников органов внутренних дел в рамках противодействия преступлений.

Немаловажным представляется развитие компьютерных технологий с интегрированными системами мониторинга криминогенной обстановки. Эти технологии во многих странах давно перестали быть новинкой. Так, в Великобритании и США внедрена система прогнозирования совершения преступлений и правонарушений – «NDAS» («Национальное решение анализа данных»), основанная на оценке текущего состояния оперативной обстановки онлайн, а также с учетом накопленной статистики. Система способна спрогнозировать вероятность возникновения беспорядков и правонарушений и предложить оптимальное решение по их профилактике (оптимизировать распределение сил и средств полиции). Полагаем, разработка и внедрение аналогичной системы для отечественных орга-

нов внутренних дел, в том числе с возможностями статистического прогнозирования [8, с. 16–21], будет способствовать повышению качества работы органов внутренних дел в сфере противодействия преступности;

На современном этапе развития информатизации общества назрел вопрос о развитии полицейских чат-ботов – голосовых помощников. Такая система успешно применяется во многих сферах современной жизни, особенно при передаче и запросе данных с помощью мобильной связи и мессенджеров. Усовершенствованные полицейские чат-боты могут вывести на новый уровень работу полиции по противодействию преступности, поднять правовую грамотность граждан, разгрузить полицию от звонков, не связанных с преступлениями и правонарушениями. Таким образом граждане смогут получать адресную юридическую консультацию, узнать, в каком ведомстве и подразделении может быть решена их проблема, пользоваться предложенными рекомендациями и автоматическими алгоритмами действий. Кроме того, чат-боты могут быть единой службой доверия, принимая сообщения от населения, систематизируя их и направляя по подведомственности. Большие возможности открывают служебные чат-боты перед самими сотрудниками органов внутренних дел.

Важным направлением можно назвать и общетехнологическое совершенствование информационных технологий органов внутренних дел – повышение уровня технической обеспеченности деятельности правоохранительных органов.

Перспективы развития информационных технологий по противодействию преступности в органах внутренних дел многогранны и определяются не только потребностями стражей правопорядка, но и реалиями общества и мира.

Список литературы

1. Распоряжение МВД России от 29 декабря 2020 г. № 1/15065 «Об утверждении ведомственной программы цифровой трансформации МВД России на 2021–2023 гг.» (ред. от 08.09.2021). URL: //https://rulaws.ru/acts/Rasporyazhenie-MVD-Rossii-ot-29.12.2020-N-1_15065/.

2. Состояние преступности в России за январь–декабрь 2021 г. М., 2022. С. 2–4, 30–32.

3. Воскресенский Г. М. Теория и практика информационного обеспечения в органах внутренних дел. М. : Академия МВД СССР, 1985. С. 22.

4. Качанов С. А., Нехорошев С. Н., Попов А. П. Информатизационные технологии поддержки принятия решений в чрезвычайных ситуациях // Автоматизированная информационно-управляющая система Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций: вчера, сегодня, завтра. М. : Деловой экспресс, 2011.

5. Кокоркин В. М. Внедрение искусственного интеллекта и роботизация в деятельности полиции // Перспективы государственно-правового развития России в XXI веке : сборник статей / отв. ред. К. А. Плясов. 2018. С. 70–75.

6. Камеры видеонаблюдения в Москве задействованы в расследовании 70 % преступлений. URL: https://tass.ru/moskva/3177373/.

7. Обеспечение общественного порядка и противодействие преступности. Годовой отчет о ходе реализации и оценке эффективности государственной программы за 2019 г. М., 2020. С. 4–56.

8. Терехин В. И., Чернышов В. В. Статистический анализ и прогнозирование рецидивных преступлений // Человек: преступление и наказание. 2016. № 2 (93). С. 16–21.

Посельская Л. Н.[1],
доцент кафедры криминалистики
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук, доцент

ПРОБЛЕМЫ ВЫЯВЛЕНИЯ ПРИЗНАКОВ ЭКСТРЕМИЗМА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-ТЕХНОЛОГИЙ

В последнее десятилетие актуализировались различные проявления экстремистской деятельности, формирующей, в том числе идеологическую платформу для существования названных преступлений. Развитие и доступность интернет-технологий создает возможности для появления новых способов совершения преступлений экстремистской направленности.

В современной социотехнической среде для формирования экстремистских групп, сообществ и более организованных форм, идеологической обработки граждан и воздействия на массовое сознание активно используются Интернет и мобильная связь. Предпринимаются попытки восполнить пробелы в формировании мировоззрения представителей молодежной среды экстремистской пропагандой, создавая группировки по национальному, религиозному и даже расовому признаку.

Проведенные нами исследования свидетельствуют о тенденции роста преступлений данной категории, совершенных на территории Российской Федерации. В период с января по декабрь 2021 г. зарегистрировано 1057 преступлений экстремистской направленности, что больше на 26,9 % по сравнению с аналогичным периодом 2020 г. В суд направлено 606 уголовных дел [1].

Вместе с этим следует отметить, что сложность выявления в действиях, высказываниях, лозунгах и печатных изданиях признаков экстремизма, свидетельствует о латентности подобных деяний, с другой стороны, нежелании вникать в тонкости квалификации преступлений экстремистской направленности.

По Шанхайской Конвенции от 15 июня 2001 г. Россия признала «экстремизм одной из угроз международному миру и безопасности, развитию дружественных отношений между государствами, а также осуществлению основных прав и свобод человека. Как подчеркивается в данной конвенции, экстремизм, терроризм и сепаратизм серьезно угрожают территориальной целостности и безопасности государств, а также их политической, экономической и социальной стабильности» [2].

Современное законодательство использует категории «экстремистская деятельность», «экстремизм». Эти понятия были определены в Федеральном законе от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской

---

[1] © Посельская Л. Н., 2022.

деятельности» [3]. В данном документе рассматриваются понятия «экстремизм», «экстремистская деятельность», с 2021 г. введено понятие экстремистская организация, кроме этого, дана правовая характеристика и содержание понятий «экстремистские материалы» и «экстремистская символика».

В своем исследовании А. И. Долгова отмечала, что активными формами проявления экстремизма являются «пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходной с нацистской атрибутикой или символикой до степени смешения; публичные призывы к осуществлению указанной деятельности, а также публичные призывы и выступления, побуждающие к осуществлению указанной деятельности, обосновывающие либо оправдывающие совершение деяний, указанных в настоящей статье, финансирование указанной деятельности» [4]. Кашепов В. А. выделяет «наличие общего криминалистического признака – мотива антиобщественного поведения преступника-экстремиста, основанного на ненависти или вражде по отношению к иной (социальной, национальной, расовой, религиозной и др.) группе людей» [5].

Одним из необходимых для установления элементов экстремистской деятельности является цель и мотив, без выявления и оценки которых невозможно правильно оценить исходную информацию о рассматриваемом преступлении. Необходимо учитывать при этом сложность формирования и существования мотивов поведения.

Хлебушкин А. Г. и другие авторы предлагают определять экстремизм «как противоправную деятельность, осуществление которой причиняет, или может причинить существенный вред основам конституционного строя или конституционным основам межличностных отношений» [6].

Введение в соответствующие статьи понятий «экстремизм» и «экстремистская деятельность», позволяет более определенно отличать данные преступные деяния от других преступных проявлений. Но проблема не в восприятии и толковании правовых норм, а в терминах и символах, используемых экстремистами, что существенно влияет на правовую оценку деяния. При изучении практики выявления экстремизма при проверке информации и сообщений о преступлениях основным критерием оценки собранных материалов является лингвистическая экспертиза текстов, эмблем, нашивок, плакатов, видеоматериалов и других объектов, содержащих информацию. Выявлению признаков преступлений экстремистской направленности способствует более точное установление мотивации, оказывающей побудительное воздействие на поведение лица, совершающего экстремистские преступления.

Проведенное исследование по материалам территориальных подразделений по противодействию экстремизму практики расследования в Центральном Федеральном округе, где в период с января 2019 г. по декабрь 2021 г. выделены следующие доминирующие мотивы поведения лиц, совершивших преступления экстремистского характера, которые нашли свое отражение в изъятых материалах и документах экстремистского толка. Политические мотивы составили 45,8 % от числа регистрируемых преступлений; соответственно

националистические и религиозные мотивы составляют 48,1 %; экстремистские проявления с корыстной мотивацией 6,1 % [7]. Содержание и специфика такой деятельности предопределяют выбор способа совершения преступления и остальных его элементов, таких как время, место, средства и орудия.

В последнее время отмечается вовлеченность значительного количества молодых людей совершать преступления или иные действия экстремистской направленности в составе группы. И этому есть свое объяснение. С одной стороны, как отмечает К. Ю. Королева и другие авторы, «молодежи свойственна психология максимализма и подражания, что в условиях деформации социальной и культурной жизни общества является почвой для групповой агрессивности. Многочисленные неформальные группы, в основе которых зачастую лежат концепции того или иного вида деструктивной субкультуры, достаточно часто превращаются в молодежные группировки экстремистской направленности» [8].

С другой стороны, экстремизм развивается в привычной для них интернет – среде. Современный способ экстремистской деятельности активизировался с распространением по всей территории России сети Интернет, доступности для граждан разных возрастов компьютерных и телефонных технологий. Эти ресурсы активно используются различными экстремистскими организациями, в том числе леворадикального толка.

Результаты использования Интернета и его сайтов, социальных сетей таких как «В Контакте», Twitter, Facebook, и других позволяют выделить все разнообразие способов действий. Доступность социальных сетей для создания и распространения сайтов с соответствующей идеологической направленностью значительно расширяет круг пользователей информационных ресурсов, создает основу для распространения и тиражирования информационных блоков для распространения идеологии экстремизма. Следующим способом является изготовление и публикация различных мультимедийных аудио и видео материалов. Экстремистами стала активно использоваться так называемая «блог сфера», где активно пропагандируется дискриминация отдельных групп граждан по национальному, языковому и религиозному признаку.

В последнее время значительное место в сетевых ресурсах занимает «пропаганда и демонстрация нацистской и иной экстремистской символики. Через те же социальные сети осуществляется организация интернет – продаж и специфического форменного обмундирования – 23,6 %» [9]. Например, символика леворадикалов. Данный тип противоправной деятельности обусловливает неконтролируемое массовое распространение методических материалов и информации экстремистского толка, с последующим формирование интернет-сообществ и групп, и вовлечением в них новых сторонников и единомышленников.

Через социальные сети интернета осуществляется интерактивный обмен противоправной информацией по подготовке, планированию и проведению различных акций и преступлений экстремистской направленности. Для вовлекаемой молодежи используется игровой контент, с помощью которого

осуществляется маскировка информации о планируемых действиях и акциях, что привлекательно для несовершеннолетних и молодежи в возрасте до 18–20 лет. Использование игровых платформ позволяет лидерам экстремистских сообществ осуществлять размещение интерактивных инструкций и обучающих материалов. Как и другие преступные организации, экстремистские группы и сообщества не могут существовать без финансовой поддержки. Кроме сбора пожертвований через платежные платформы, например QIWI–кошелек, Яндекс-Деньги и др., через те же социальные сети осуществляется продажа символики принадлежности той или иной экстремистской группировке, футболок с изображением соответствующих логотипов, различных красочно оформленных и изданных брошюр и другой печатной продукции.

Для обеспечения длительного существования преступных объединений экстремистского направления используется отработанный способ преступления, включающий в себя элементы подготовки и сокрытия. Кроме собственных компьютерных и иных технических средств отрабатывается возможность использования электронно-вычислительной техники, через которую возможен анонимный доступ к ресурсам компьютерных сетей, используя программы – анонимизаторы, либо вредоносные программы, обеспечивающие удаленный доступ. В последнее время экстремистские организации привлекают специалистов в сфере IT-технологий для создания специального программного обеспечения для получения кодов доступа и другой частной конфиденциальной информации, выявляются наиболее уязвимые места в информационных системах.

Одновременно отрабатываются и способы сокрытия. Традиционно к таким способам относят уничтожение следов доступа к компьютерной технике, удаление log-файлов, содержащих информацию о пользователях и времени их работы в системе и reg-файлов, перечень команд и набор символов, несущих сведения об использовании специального, либо не стандартного программного обеспечения.

В настоящее время осуществляется лингвистическая маскировка текстовых файлов под общепринятые речевые конструкции, и используемую в гражданском обороте символику, что порождает определенные трудности в однозначной экспертной оценке содержания текстовых файлов, назначения символики, и издаваемой печатной продукции как объектов экстремистской направленности. Символика и скрытые в позитивных лозунгах смыслы в ряде случаев ведут к разночтению среди экспертов в оценке смысловых конструкций, направленности и целей деятельности экстремистских организаций.

Проблема выявления и исследования признаков экстремизма представляет научный интерес для дальнейшей разработки информационного и методического обеспечения организации раскрытия и расследования преступлений экстремистской направленности, формирования научно-обоснованных рекомендаций по анализу и систематизации криминалистической и иной значимой информации, используемой в оценке признаков преступного деяния. В целях однозначного восприятия электронной и печатной информации как

экстремистской полагаем, что необходимо сформировать правовую идеологическую основу для правильного и однозначного понимания и оценки лексических и грамматических средств в опубликованных текстах, электронных ресурсах на сайтах, содержащих мировоззренческую и целевую установку.

Список литературы

1. Сведения МВД России о состоянии преступности за 2021 г. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552

2. Шанхайская Конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом (Шанхай, 15 июня 2001 г.) // Собрание законодательства Российской Федерации. 2003. № 41. Ст. 3947.

3. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (в ред. от 01.07.2021 г. № 280-ФЗ) // Собрание законодательства Российской Федерации. 2002. № 30. Ст. 3031.

4. Долгова А. И., Гуськов А. Я., Чуганов Е. Г. Проблемы правового регулирования борьбы с экстремизмом и правоприменительной практики. М. : Норма, 2010. С. 140.

5. Кашепов В. А. Квалификация преступлений экстремистской направленности // Уголовное право. 2007. № 3. С. 33.

6. Хлебушкин А. Г. Экстремизм: уголовно-правовой и уголовно-политический анализ : монография. Саратов : Саратовское изд-во, 2007. С. 34.

7. Краткая характеристика состояния преступности в Российской Федерации за январь–октябрь 2019 г. URL: https://xn--b1aew.xn--p1ai/reports/item/19007735/ ; сведения МВД России о состоянии преступности за 2021 г. URL: https://xn--b1aew.xn--p1ai/reports/item/28021552.

8. Королева К. Ю., Борисова О. С., Ерохина Ю. В. Молодежь в виртуальных «сетях» экстремизма: социокультурный аспект // Наука. Искусство. Культура. 2013. № 2.

9. Самойлов С. Ф., Некрасова А. В., Шандакова А. С. Символика российских леворадикальных организаций: методические рекомендации. Краснодар : Краснодарский университет МВД России, 2021.

Никулина В. А.[1]**,**
доцент кафедры конституционного
и административного права
Санкт-Петербургского филиала
НИУ «Высшая школа экономики»,
кандидат юридических наук, доцент

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ЦИФРОВОГО ОБРАЗА ЛИЧНОСТИ

На XIV Конгрессе ООН по предупреждению преступности и уголовному правосудию вопросам использования информационно-коммуникационных технологий в преступных целях был посвящен отдельный семинар-практикум, на котором, в частности, обозначены следующие тематические области такого использования: рынок криптовалют, незаконный оборот наркотиков и огнестрельного оружия, торговля людьми и незаконная миграция, надругательства над детьми и эксплуатация детей [1, с. 51–54].

Охрана неприкосновенности «оцифрованной» частной жизни, злоупотребления в этой сфере, на первый взгляд, по характеру и степени общественной опасности, выпадают из этого списка. Однако отдельные события, такие как скандал с проектом «Pegasus» в 2021 г. [2], падение акций Twitter на фоне заявления Илона Маска проверить реальное число фейковых аккаунтов («спам-ботов») в социальной сети [3], хотя и не попадают в орбиту уголовно-правового регулирования, наглядно свидетельствуют о потенциально высоких рисках в этой области. Не случайно, в 2022 г. Роскомнадзор внес предложение о введении уголовной ответственности за торговлю утекшими персональными данными россиян [4].

В российском правопорядке уже стал традиционным такой термин, как «цифровой профиль гражданина», под которым понимается совокупность цифровых записей о гражданине, содержащихся в информационных системах государственных органов и организаций [5, с. 7]. Схожим образом его содержание раскрыто в законопроекте «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» [6]. В юридической же науке цифровой профиль лица определяется как «уникальная база данных, включающая совокупность идентификаторов и иных конфиденциальных и общедоступных сведений, отражающих различные аспекты частной и общественной жизни человека» [7, с. 141]. Таким образом, легальное определение значительно у́же и проводится через призму находящихся на официальных ресурсах конкретных, четко определенных данных о гражданине (не личности) – данных, позволяющих идентифицировать индивида в системе государственных органов [8]. Подобный подход обусловлен целями и задачами разрабатываемой государством концепции цифрового профиля, определившей его публично-правовой характер.

---

[1] © Никулина В. А., 2022.

Несмотря на некоторую дискуссионность данного понятия, очевидно, что независимо от его интерпретации, первоосновой существования человека в цифровой среде (в том числе и цифрового профиля) выступает информация. Но она не вся связана с объектом уголовно-правовой охраны, а только та ее часть, которая имеет режим ограниченного доступа. Поскольку, как справедливо указывают цивилисты, информация находит свое воплощение в других поименованных законодателем объектах гражданских прав: от исключительных (имущественных) прав до нематериальных благ [9, с. 37–39], значит, она может выступать предметом самых разнородных преступлений. Для правильной квалификации таких противоправных деяний необходимо четко разграничивать информационные ресурсы «с тем, чтобы увязать правовой режим защиты информации с ее правовым статусом, во многом определяемом уровнем ее доступности» [10, с. 119]. При этом сама по себе цифровизация информации представляет собой лишь определенный способ ее фиксации – с помощью цифрового кода или обозначения.

Закономерно возникает вопрос о соотношении данных цифрового профиля и охраняемой уголовным законом информации. Если под «цифровым профилем» понимать все зафиксированные в информационно-телекоммуникационной сети сведения о лице имущественного и неимущественного характера (персональные данные, сообщения личного и общедоступного характера, фотоснимки, аудио- и видеозаписи, результаты мониторинга Интернет-траффика лица: поисковые запросы и посещаемые веб-сайты и т. д.), то совпадение по содержанию и по объему цифрового профиля с уголовно-охраняемой информацией будет частичным. Но и при ограничительном толковании понятия цифрового профиля, не все сведения, составляющие его содержание, как представляется, будут подлежать уголовно-правовой защите. В частности, речь идет о персональных данных – основной составляющей цифрового профиля. Несмотря на то, что судебная практика нередко отождествляет эти данные с личной тайной или с охраняемой законом компьютерной информации в контексте ст. 272 Уголовного кодекса Российской Федерации, персональные данные не во всех случаях подпадают под режим охраны неприкосновенности частной жизни [11, с. 42–43]. Конституционный Суд Российской Федерации еще в 2012 г. в своем Определении № 1253-О «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав ст. 137 УК РФ» указал, что «в понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и *не подлежит контролю со стороны общества и государства* (курсив мой – В.Н.), если носит не противоправный характер» [12]. Поэтому созданные, в первую очередь, для регулирования публичных правоотношении между государством и индивидом, персональные данные, составляющие ядро цифрового профиля лица в узком понимании этого термина, только частично могут пересекаться с понятием «частной жизни». Что же касается возможности применения ст. 272 Уголовного кодекса Российской Федерации, то опять-таки режим общедоступности ряда сведений, составляющих содержание персональных данных, не дает оснований для

их отнесения к охраняемой законом компьютерной информации, и потому исключает уголовную ответственность.

Таким образом, цифровой профиль в настоящее время не только не выступает самостоятельным предметом уголовно-правовой охраны, но и не встречается в правоприменительной практике по уголовным делам, что вполне закономерно, учитывая его неопределенность в отечественной нормативно-правовой системе.

Практика оперирует таким понятием как аккаунт в социальной сети, которое, правда, также не имеет однозначного определения в правовой науке [13, с. 44]. Очевидно, что персональный аккаунт можно считать составной частью цифрового профиля, поэтому и режим его охраны необходимо определять соответствующим образом.

Дискуссионным представляется мнение, что лицо, создающее аккаунт другого человека без его согласия, не может быть привлечено к уголовной ответственности, поскольку такое деяние образует неправомерное использование персональных данных, не наказуемое в соответствии с действующим уголовным законом [8]. В подобной ситуации акцент должен быть уделен не персональным данным и аккаунту в социальной сети как составным частям цифрового профиля лица, а скорее – цифровому образу личности, который здесь выступает отдельным объектом уголовно-правовой охраны.

Если Гражданский кодекс Российской Федерации сперва (в 2006 г.) признал необходимость защиты изображения гражданина (ст. 152.1), а затем (в 2013 г.) конкретизировал охрану частной жизни (ст. 152.2), то представляется закономерным продолжением данного тренда появление в ближайшей перспективе цифрового образа личности как особого объекта. Попытка нормативного закрепления данного понятия уже предпринималась в связи с идентификацией, то есть, по сути, как аналог цифрового профиля (в программе «Цифровая экономика Российской Федерации», утвержденной Распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-р, хотя утратившей силу в настоящее время).

Однако цифровой образ, как представляется, шире профиля и включает помимо него данные расшифровки генома конкретного человека (образующие личную тайну), а также размещаемые, создаваемые им самим или с его участием сведения о частной жизни (виртуальный образ). При этом виртуальный образ может как являться цифровым слепком с личности (в этом случае его уголовно-правовая защита осуществляется в основном также, как охраняется частная жизнь, честь и достоинство в обычных правоотношениях), так и создавать самостоятельный имидж (по аналогии со сценическим образом актера или псевдонимом писателя). В первом случае он может выступать объектом правовой охраны в соответствии со ст. 23 Конституции Российской Федерации. Во втором случае угроза потенциального вреда порождается раскрытием подлинных сведений о бенефициаре этого персонального бренда (что при определенных обстоятельствах можно квалифицировать по ст. 137 Уголовного кодекса Российской Федерации) либо, напротив, распространением ложных сведений о нем (что образует

признаки клеветы). Наконец, неправомерное получение доступа к аккаунту, закрепляющему виртуальный образ, или противоправная модификация его может являться признаком компьютерного преступления (ст.ст. 272, 273 Уголовного кодекса Российской Федерации).

Создаваемый на основе цифрового профиля, цифровой образ личности может приобретать самостоятельное значение и даже выходить за рамки цифровой платформы. Загружая в цифровую среду свои персональные данные и другие сведения, «присутствуя» в сети, коммуницируя с другими авторами в виртуальном мире, человек не может не создавать соответствующий виртуальный образ, который «сочетает внешнюю предъявленность и частную субъективность, и сопровождает созданный индивидом профиль, автопроект, наделенный биографией и желаемыми личностными характеристиками» [14, с. 55]. И если цифровой профиль в основном создаваем сознательными усилиями самого индивида, то складывающий на его основе образ не всегда может поддаваться такому целенаправленному контролю и управлению, он может носить непредсказуемый характер, поскольку в его формировании задействованы и другие участники информационной среды (комментаторы, подписчики и т. д.). Цифровой образ, связанный с конкретной личностью, интегрирует в себе такие категории как честь, достоинство, доброе имя и репутацию этого лица. Усилиями индивида его образ может быть, как приближен к реальному, так и быть абсолютно вымышленным, искусственно сконструированным.

Также следует учитывать, что цифровой образ личности сохраняется даже после смерти. В этом случае появляется опасность подмены владельца (после взлома аккаунта) и также необходима охрана достоинства создателя образа.

Таким образом, цифровой образ личности подлежит самостоятельной уголовно-правовой охране, причем даже без введения новых запретов. С учетом его специфики и несовпадения с цифровым профилем необходима дальнейшая разработка правил квалификации как общеуголовных, так и компьютерных преступлений, совершаемых в отношении цифрового образа.

Список литературы

1. Материалы XIV Конгресса ООН по предупреждению преступности и уголовному правосудию. Руководство для дискуссий. URL: https://www.-unodc.org/documents/congress/Documentation_14th_Congress/DiscussionGuide/A_-CONF234_PM1_r_V1806331.pdf.

2. URL: https://iz.ru/1195409/2021-07-20/snouden-vystupil-za-zapret-programm-shpionov-posle-skandala-s-pegasus.

3. URL: https://tass.ru/ekonomika/14618285?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru.

4. РКН предложил ввести уголовное наказание за торговлю утекшими персональными данными. URL: https://www.interfax.ru/digital/841810.

5. Сценарии использования инфраструктуры Цифрового профиля. URL: https://digital.gov.ru/uploaded/presentations/stsenariiispolzovaniyatspv10-2.pdf.

6. Законопроект № 747513-7 «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)». URL: https://sozd.duma.gov.ru/bill/747513-7.

7. Наумов В. Б. Информационно-правовые вопросы идентификации при использовании цифрового профиля // Аграрное и земельное право. 2020. № 6 (186). С. 137–141.

8. Аналитические материалы членов Союза: Е. А. Русскевич о цифровом профиле как предмете преступлений. URL: http://crimescience.ru/?p=39598 .

9. Аюшева И. З. Цифровые объекты гражданских прав // *Lex russica* (Русский закон). 2021. № 7. С. 32–43.

10. Бойцов А. И. Преступления против собственности. СПб. : Издательство «Юридический центр Пресс», 2002.

11. Филатова М. А. Персональные данные как предмет преступного посягательства // Уголовное право. 2021. № 11 (135). С. 35–43.

12. URL: http://doc.ksrf.ru/decision/KSRFDecision105722.pdf.

13. Кирсанова Е. Е. Аккаунт как объект гражданских прав // Вестник арбитражной практики. 2020. № 2 (87). С. 44–48.

14. Соловьева Л. Н. Цифровая идентичность как феномен информационной современности // Общество: философия, история, культура. 2020. № 12 (80). С. 53–56.

Реутская Е. А.[1],
доцент кафедры уголовного права
учреждения образования
«Академия Министерства внутренних дел
Республики Беларусь»,
кандидат юридических наук

ОБ ОПРЕДЕЛЕНИИ ОБЪЕКТА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, С УЧЕТОМ НОВЕЛЛ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ БЕЛАРУСЬ

Тенденции развития общественных отношений свидетельствуют о повсеместном проникновении информационных технологий в жизнь каждого индивида, общества и государства. Современное общество по праву может называться информационным, что позволяет констатировать факт формирования и развития нового этапа цивилизации, основой которого являются информационные технологии и искусственный интеллект. Развитие информационного общества предопределило и законодательное урегулирование информационных правоотношений, которые основываются на принципах свободы поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией при одновременном соблюдении требований охранительного характера. Так, в соответствии со ст. 4 Закона Республики Беларусь «Об информации, информатизации и защите информации» свобода пользования и распространения информации ограничивается в целях защиты информации о частной жизни физического лица и персональных данных, а также обеспечения безопасности личности, общества и государства при пользовании информацией и применении информационных технологий [1]. Подобное положение было закреплено в законодательстве, так как с одной стороны информационные технологии способствуют более эффективной реализации гражданами своих прав и свобод, но с другой – наоборот могут оказывать негативное воздействие на правоотношения в масштабах целого региона или страны, когда, например, ведется «информационная» война. Как показал опыт последних лет, развитие информационных технологий и коммуникативных платформ (социальные сети, мессенджеры, облачные ресурсы), позволяет в кратчайшие сроки передавать любому количеству адресатов большие объемы информации.

Новые технологии позволяют распространять информацию (в том числе и так называемые «фейковые новости»), направленную на разжигание вражды или розни, не только в рамках одной или нескольких социальных групп, как это было раньше, а среди большей части населения в рамках целой страны. Указанные

[1] © Реутская Е. А., 2022.

проблемы актуальны в настоящее как для Республики Беларусь, так и для Российской Федерации. Для защиты прав и свобод граждан в информационной сфере необходимо на регулярной основе проводить комплексное научные исследования в указанной сфере с целью разработки на этой основе положений, оптимизирующих законодательство и правоприменительную практику. Как российский, так и белорусский законодатели успешно справляются с задачей постоянной актуализацией законодательства в сфере защиты информационной безопасности, одним из основных направлений которой является компьютерная безопасность.

На четкость квалификации преступлений в информационной сфере первую очередь влияет правильное определение объекта посягательства. Именно объект является основой систематизации норм уголовного законодательства: когда в обществе возникает потребность в криминализации определенного деяния с последующим его отнесением в определенную группу общественных отношений, законодатель сначала определяет родовой и видовой объект. Кроме этого, объект позволяет систематизировать нормы об ответственности за преступления внутри конкретной группы общественных отношений путем расположения от более опасных к менее опасным.

Обращаясь к анализу раздела XII главы 31 Уголовного кодекса Республики Беларусь (далее – УК) «Преступления против компьютерной безопасности», отметим, что название указанных раздела и главы УК до 2021 г. было иным – «Преступления против информационной безопасности» (изменения были внесены 26 мая 2021 г. Законом Республики Беларусь № 112-З) [2]. Изменение названия разделов и глав всегда влечет и изменение родового и видового объектов, сужая или наоборот расширяя сферу действия уголовного закона. В связи с этим, обратимся в первую очередь к анализу основных понятий, которые изменились в рамках гл. 31 УК в 2021 г.

Как было отмечено выше, первоначальное название объекта уголовно-правовой охраны в рамках разд. XII гл. 31 включало термин «информационная безопасность». Под информационной безопасностью, согласно п. 8 Концепции информационной безопасности Республики Беларусь, понимается *состояние защищенности* личности, общества и государства *от* внутренних и внешних *угроз в информационной сфере*, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность, оборона и безопасность государства. *Информационная сфера* представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом в информационном пространстве общественных отношений. *Информационное пространство* включает любую область деятельности, связанную с созданием, преобразованием, передачей, использованием, хранением информации, оказывающую воздействие, в том числе, на индивидуальное и общественное сознание и, собственно, на саму информацию [3].

В отличие от термина «информационная безопасность», понятие «компьютерной безопасности» в законодательстве Республики Беларусь не приводится. Анализ научной литературы позволяет систематизировать научные подходы и привести наиболее широкое определение. Так, под компьютерной безопасностью предлагается понимать *состояние защищенности* компьютерных *программ* и *данных* в средствах вычислительной техники, в каналах связи, в автоматизированных системах и других компьютеризированных изделиях, при котором обеспечивается конфиденциальность, целостность и доступность компьютерных программ и данных, а также обеспечивается выполнение компьютеризированными изделиями предписанных функций [4, с. 106]. Указанное определение представляется удачным, так как максимально учитывает особенности объекта и увеличивает круг предметов, водящих в состав компьютерных преступлений, закрепленных в главе 31 УК.

Из приведенных выше определений явно следует, что понятие «информационная безопасность» гораздо шире по кругу охватываемых общественных отношений, чем новое для УК понятие «компьютерная безопасность». Полагаем обоснованным изменение названия разд. XII гл. 31 УК, что привело к сужению тех общественных отношений, которые охраняются в рамках гл. 31 УК. В том время, как «информационная безопасность» помимо самих общественных отношений по поводу обеспечения защищенности компьютерных программ и данных, хранящихся в различных компьютеризированных изделиях, включает любое преступление, расположенное в Особенной части УК, совершенное с применением информационно-коммуникационных технологий (ст.ст. 130^2, 188, 2012, 216, 361, 367, 369^1 и ряд др.).

Одним из основных факторов, способствующих эффективной борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, является интеграция Республики Беларусь в систему международной информационной безопасности, синхронизации целей и задач национальной системы обеспечения информационной безопасности с корреспондирующей системой Российской Федерации, что предполагает анализ российского уголовного законодательства в целях заимствования положительного опыта конструирования норм в сфере борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий.

В Уголовном кодексе Российской Федерации (далее – УК РФ) содержится глава, аналогичная главе 31 УК РБ – глава 28 «Преступления в сфере компьютерной информации». В соответствии с примечанием к ст. 272 УК РФ, под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [5]. Сведения могут быть определены как познания в какой-либо области, либо как знание, представление о чем-либо [6, с. 698]. Сообщение представляет собой известие или саму информацию [6, с. 746]. Под данными понимают сведения, необходимые для какого-либо вывода, решения [6, с. 155]. В юридической литературе законодательно закрепленное понятие

компьютерной информации вызывает критику ввиду своей узости. Так, например, А. Н. Попов утверждает, что «в современных технологиях могут использоваться для передачи компьютерной информации самые различные по своей природе каналы связи. … световой луч, … инфракрасное излучение или лазер». Указанный автор предлагает помимо формы представления компьютерной информации заложить в определение и иные критерии компьютерной информации как предмета преступлений, предусмотренных нормами главы 28 Уголовного кодекса Российской Федерации [7, с. 23].

На основании анализа категориально-понятийного аппарата преступлений в сфере информационной безопасности можно сделать вывод о том, что изменения в названии раздела XII и главы 31 УК являются необходимыми и соответствующими современным подходам и тенденциям. Термин «компьютерная безопасность» обоснованно сужает круг общественных отношений, регулируемых гл. 31 УК. В свете последних изменений в гл. 31 УК, российское и белорусское определение объекта преступлений, совершаемых с использованием информационно-коммуникационных технологий, можно признать схожим. Под компьютерной безопасностью следует понимать состояние защищенности компьютерных программ и данных в компьютеризированных изделиях, целостность и доступность компьютерных программ и данных.

Список литературы

1. Об информации, информатизации и защите информации: Закон Республики Беларусь от 10 ноября 2008 г. № 455-З: принят Палатой представителей 9 октября 2008 г.; одобрен Советом Республики 22 октября 2008 г.: текст с изм. и доп. на 24 мая 2021 г. // Нац. реестр правовых актов Республики Беларусь. 2008. № 279. 2/1552.

2. Уголовный кодекс Республики Беларусь: Закон Республики Беларусь от 9 июля1999 г. № 275-З : принят Палатой представителей 2 июня 1999 г. ; одобрен Советом Республики 24 июня 1999 г.: текст с изм. и доп. на 5 января 2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2022.

3. О Концепции информационной безопасности Республики Беларусь : постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 // Нац. реестр правовых актов Республики Беларусь. 2019. 7/4227.

4. Забегалин Е. В. Определение термина «компьютерная безопасность» // Системы управления, связи и безопасности. 2017. № 4. С. 102–110.

5. Уголовный кодекс Российской Федерации: Федеральный закон от 15 апреля 1998 г. № 66-ФЗ : принят Государственной думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г. : текст с изм. и доп. на 24 февраля 2022 г. // СПС «КонсультантПлюс». М., 2022.

6. Ожегов С. И. Словарь русского языка / под ред. Н. Ю. Шведовой. М. : Русский язык, 1990.

7. Попов А. Н. Преступления в сфере компьютерной информации : учебное пособие. СПб. : Санкт-Петербургский юридический институт (ф-л) прокуратуры Российской Федерации, 2018.

Кравец Е. Г.[1],
кафедры предварительного расследования
учебно-научного комплекса по предварительному следствию
в органах внутренних дел
Волгоградской академии МВД России,
кандидат юридических наук, доцент

Евлушина Д. Н.[2],
старший преподаватель кафедры предварительного расследования
учебно-научного комплекса по предварительному следствию
в органах внутренних дел
Волгоградской академии МВД России,
кандидат юридических наук

КОМПЕТЕНТНОСТНЫЙ ИНСТРУМЕНТАРИЙ СПЕЦИАЛИСТА, ИСПОЛЬЗУЕМЫЙ ПРИ РАССЛЕДОВАНИИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

В нашей статье мы будем использовать некоторые повторяющиеся выражения, обороты и массивы понятий, для которых позволим себе ввести некоторые условные сокращения:

– персональные ЭВМ во всем многообразии (персональный компьютер, планшет, ноутбук, смартфон, иные устройства) – *пользовательские устройства или ПУ*;

– хищения с использованием компьютерных вредоносных программ – применим международную терминологию, основанную на буквальном переводе с английского языка – *ME* (malware embezzlement).

Анализируемый тип расследования преступлений предполагает высокую степень вовлеченности специалистов в области компьютерной техники. Потребуются они и при осмотре ПУ, принадлежащего потерпевшему. При принятии решения об оформлении результатов следственного действия правоприменителю предстоит сделать выбор между осмотром предметов и осмотром места происшествия. Мы рекомендуем остановиться на последнем варианте, так как он логичнее подчеркивает информационную интегрированность ПУ в механизм преступления расширяет процедурные возможности следователя.

Изучение следственных и судебных материалов явственно обнажает существенные технические и организационные проблемы, возникающие на пути следователей при принятии и реализации решения о подобном осмотре. Корни этих затруднений – прежде всего, в дефиците компетентности лиц, которым надлежит осуществить осмотр ПУ [1, с. 26].

---

[1] © Кравец Е. Г., 2022.
[2] © Евлушина Д. Н., 2022.

Именно доказательное документирование самого факта задействования вредоносных компьютерных программ, установление механизма и способа совершения МЕ – ключевая задача первоначального этапа раскрытия данного типа хищений. Для ее решения крайне важно правильно – как технически, так и юридически – произвести осмотр ПУ, которым пользовался потерпевший. От этого зависит последующая квалификация преступного деяния и содержание работы следователя, планирование дальнейших следственных действий [2, с. 7].

Требуемыми знаниями и навыками следователь (а равно дознаватель, если он при процессуальной проверке выполняет неотложные следственные действия), конечно, не обладает. Важно осознать это, не отказываться самонадеянно от квалифицированной помощи. Для точной и достаточной фиксации как доказательственной, так и ориентирующей информации, предположительно сохраненной в ПУ, требуется привлечь специалиста, компетентного в сфере технического оснащения мобильных терминалов. Это лицо, кроме того, должно на экспертном уровне разбираться в особенностях вредоносных компьютерных программ, созданных для похищения средств с платежных карт клиентов финансово-кредитных учреждений, их алгоритмах функционирования.

Лучше всего было бы включать в число участников осмотра в данной роли сотрудников регионального экспертно-криминалистического центра из профильного подразделения, проводящего компьютерно-технические исследования. У них точно будет соответствующий допуск, они регулярно подтверждают и повышают свою квалификацию в рамках выстроенной системы кадрового обеспечения ведомства. Однако, данный вариант, который можно было бы признать идеальным, затруднен из-за небольшой штатной численности таких отделов (чаще – отделений) и их существенной загруженности.

Если таких сотрудников пригласить не удается, следователь может обратиться за содействием в региональное управление Роскомнадзора, в одну из научно-исследовательских лабораторий судебных экспертиз системы соответствующих учреждений Министерства юстиции Российской Федерации, в Бюро специальных технических мероприятий и другие госструктуры. Альтернатива – технические работники IT-компаний, операторов сотовой связи, интернет-провайдеров. Они также проходят государственную и корпоративную сертификацию. Конечно, следователю предварительно нужно будет ознакомиться с дипломами, сертификатами и удостоверениями, подтверждающими компетентность специалиста. И подробно ознакомить его с режимом ограничения циркуляции материалов расследования [3, с. 79].

Первостепенное значение при осмотре ПУ потерпевшего имеет поиск и закрепление убедительных данных, подтверждающих нахождение на устройстве вредоносной программы либо следов ее применения.

Производственный принцип программного обеспечения, ориентирующегося на получение доступа к активам, помещенным на счета в банках и аналогичных структурах, следует признать вполне типическим: вирусное ПО (обычно – троянская программа семейства «Android.BankBot»), инсталлируемое преступни-

ками на пользовательское устройство, предназначено для аккумулирования значимых данных и дистанционного управления операциями с банковским счетом, прежде всего, для безакцептного перевода накоплений потерпевшего. Похитители считывают входящие на ПУ сообщения (в том числе сугубо технические, не анализируемые человеком), а также получают ключевое преимущество – возможность отправлять сообщения, будучи авторизованными от имени потерпевшего в любых системах, к которым он имел доступ, включая банковские базы. Собственник об таких сообщениях ничего при этом не знает.

Для уяснения механизма преступления важно понимать, что вредоносные программные средства не нуждаются в постоянном контроле со стороны злоумышленников – это действующие автономно боты с четко прописанным алгоритмом. Причем не требуется их вмешательства и при широкомасштабных множественных атаках на ПУ. Заметным явлением последнего времени стал лавинообразный рост МЕ со счетов клиентов крупнейших банков, использующих на своих мобильных устройствах программное приложение «Мобильный банк». Троянская программа мимикрировала под обновление приложения, хакеры на своем сервере накапливали данные о применении программы для дистанционного банковского обслуживания (ДБО), в том числе о привязанной к приложению банковской карте. Администрируя мобильное устройство потерпевшего дистанционно, используя функционал сервиса «Мобильный банк», похитители инициировали отправку коротких сообщений от имени авторизованного собственника средств с командой о переводе денег с его карты. Входящие сообщения из банка, запрашивающие пароли и подтверждения операции, перехватываются тем же вирусным ПО, что позволяет избегать внимания к происходящему со стороны потерпевшего. Троянская программа сама «отвечала» коротким сообщением на такие запросы с подтверждением проведения платежа, в том числе вводя одноразовый код подтверждения, если он требовался [4, с. 89].

Таким образом, на стадии осмотра целью привлечения специалиста являются обнаружение, установление типа вредоносной программы, принципа ее функционирования, фиксации следов ее использования.

Действия специалиста при осмотре компьютерного устройства заключаются в следующем:

– определение внешних признаков устройства, его размеров, модели, а для терминалов сотовой связи (планшетов, смартфонов) – сведений об IMEI-номере, используемых на момент осмотра абонентском номере и сим-карте;

– определение системных параметров устройства – установленные операционное система, программные приложения, параметры быстродействия (процессор, оперативная память и т. д.). Особое внимание на данном этапе уделяется наличию/отсутствию установленных программных приложений дистанционного банковского обслуживания (далее по тексту – ДБО), а также антивирусных программ. Необходимо отразить свойства данных приложений, даты и время установки и последнего использования;

– непосредственное обнаружение на компьютерном устройстве вредоносной программы либо следов ее применения, документирование факта осуществления

несанкционированных платежей. Для этого проводится изучение журнала работы программ ДБО, а также антивирусного программного обеспечения. В первом случае фиксируются сведения обо всех проведенных платежах за интересуемый период (дата, время, адресат денежного перевода и другие). Во втором случае необходимо отразить информацию обо всех обнаруженных угрозах и предупреждениях. Также в ходе осмотра целесообразно провести дополнительное сканирование системы на предмет обнаружения вредоносных программ. При этом крайне важно предварительно выставить правильные настройки сканирования (без опции удаления и других мер к обнаруженным угрозам), чтобы по неосторожности не удалить сами вредоносные программы, а также следы их функционирования;

– при осмотре сотовых терминалов (планшетов, смартфонов) необходимо изучение и фиксация журнала SMS-сообщений и телефонных соединений за период, в который осуществлено хищение денежных средств (проведены несанкционированные транзакции со счета потерпевшего). Подробно описывается и фиксируется каждое входящее и исходящее SMS-сообщение (время, дата, адресат отправки, полный текст сообщения, а также время, дата и адресаты входящих/исходящих телефонных звонков) [5, с. 97].

Все приведенные выше манипуляции важно фотографировать, это обеспечит возможность анализировать результаты осмотра на последующих этапах. А еще предпочтительнее использовать видеозапись, особенно прогнозируя высокую вероятность обнаружения самого вредоносного ПО или его следов.

Снова хочется акцентировать внимание: проведенный анализ следственной практики позволяет проследить прямую зависимость между самим фактом привлечения специалиста к осмотрам анализируемого типа, его компетентностью и эффективность следственного действия, его доказательственной ценностью. То есть применение качественных программно-технических знаний – безальтернативный фундамент профессионального расследования МЕ.

Список литературы

1. Хаскина В. Ю. Основные направления работы со следами, изъятыми при осмотре места происшествия // Судебная экспертиза. 2018. № 4 (56). С. 26.

2. Аминев Ф. Г. Проблемные вопросы, возникающие при назначении новых родов и видов судебных экспертиз // Судебная экспертиза. 2018. № 2 (54) С. 7.

3. Австрийсков А. В. Ретроспектива использования технических средств оперативно-разыскного назначения при раскрытии и расследовании преступлений в России // Вестник Волгоградской академии МВД России. 2019. № 1 (48). С. 79.

4. Еремин С. Г., Домовец С. С. Способы совершения преступлений в сфере дистанционно-банковского обслуживания и следы-признаки их образования // Вестник Волгоградской академии МВД России. 2018. № 2 (45). С. 89.

5. Желудков М. А., Попов А. М., Дубровина М. М. Проблемы правового обеспечения противодействия киберпреступности в России и зарубежных странах // Вестник Волгоградской академии МВД России. 2018. № 3 (46). С. 97.

Пикта В. И.[1],
старший преподаватель
кафедры информационного права
факультета криминальной милиции
Академии МВД Республики Беларусь

ОСОБЕННОСТИ СЛЕДООБРАЗОВАНИЯ ПРИ РАСПРОСТРАНЕНИИ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Вредоносное программное обеспечение – это любое программное обеспечение, которое негативным образом влияет на работу персонального компьютера или радиоэлектронного устройства. Вредоносное программное обеспечение может быть представлено в виде всплывающего окна, которое не позволяет пользователю получить доступ к основному функционалу интернет-ресурса или к программному обеспечению, копирующему финансовую информацию с компьютера жертвы.

Согласно исследованиям «Лаборатории Касперского», в последние годы число новых семейств и разновидностей вредоносного программного обеспечения стремительно растет. «Лаборатория Касперского» ежедневно выявляет около 325000 уникальных образцов вредоносных программ. Под угрозой находятся как домашние пользователи, так и крупные компании, банки, критическая инфраструктура, государственные организации, промышленные предприятия, использующие Автоматизированные системы управления технологическими процессами [1, с. 8].

Среди огромного ландшафта угроз в сфере распространения вредоносного программного обеспечения, одним из лидеров выступают программы-вымогатели (шифровальщики). Данная угроза свойственна всем сферам функционирования информационных систем государственного и частного сектора. По статистическим сведениям за 2020 г. мировой ущерб от распространения программ-вымогателей составляет около сорока миллиардов долларов США в связи с выплатой выкупов вымогателям и простоями [2].

Программа-вымогатель (от англ. «*ransomware»* – компиляция слов «*ransom»* – выкуп и «*software»* – программное обеспечение) – является разновидностью вредоносного программного обеспечения, предназначенного для блокирования доступа к компьютерным системам или предотвращения считывания компьютерной информации (преимущественно с использованием методов шифрования), после чего от жертвы за дешифрование информации требуется выплатить денежные средства [3].

В зарубежной литературе программы-вымогатели определяются как тип вредоносного программного обеспечения, которое поражает компьютерные системы, ограничивая доступ пользователей к данным, хранящимся в скомпрометированных системах [4]. Восстановление измененной информации является трудоемким процессом, и многие жертвы выплачивают выкуп в целях получения

[1] © Пикта В. И., 2022.

ключей дешифрования. Однако выплата выкупа не гарантирует, что файлы будут дешифрованы или программа-вымогатель будет отключена или удалена для предотвращения повторения заражения информационных систем в будущем.

Угрозы, исходящие от программ-вымогателей, зависят от типа вируса, в следствии чего, представляется возможным выделить две основные категории указанных программ: программы-блокировщики и программы-шифровальщики.

Программа-блокировщик – тип программ-вымогателей, предназначение которого блокировать работу персонального компьютера или мобильного устройства, с целью последующего требования выкупа. В отличие от программ-шифровальщиков, блокировщик не шифрует компьютерную информацию, а блокирует доступ к основному функционалу компьютерной системы. Предметом посягательства данного вида программ-вымогателей может выступать как устройство в целом, так и отдельное программное обеспечение – например, веб-браузер.

Программа-шифровальщик – тип программ-вымогателей, которая модифицирует пользовательские данные, путем использования различных алгоритмов и техник шифрования. После кодирования информации вредоносное программное обеспечение инициирует подключение к удаленному рабочему столу и пересылает информацию об идентификаторе зашифрованного устройства, для последующего восстановления модифицированной компьютерной информации.

Указанные типы вредоносного программного обеспечения может распространяться по следующим векторам:

- перенаправление трафика;
- вложения электронной почты;
- ботнеты.

Перенаправление траффика. Данный вектор является наиболее распространенным способом побудить пользователя перейти по ссылке на вредоносную рекламу или перенаправить веб-трафик пользователя на другой интернет-ресурс, на котором размещено вредоносное программное обеспечение в виде набора различных эксплоитов. Чаще всего это встречается на интернет-ресурсах с порнографическим содержимым, пользователя с указанных сайтов перенаправляют на портал, предлагающий бесплатные игры или обновления для пользовательских приложений. При загрузке указанного контента, вредоносное программное обеспечение использует уязвимости устройства пользователя, что приводит к блокировке либо шифрованию пользовательской информации.

Механизм проникновения и функционирования вредоносного программного обеспечения при данном виде атак, представляется возможным определить посредством исследования следов, оставленных зловредным программным обеспечением в компьютерной системе или сети:

1. Во-первых, необходимо проанализировать историю посещенных интернет-ресурсов пользователя, исследование которых выполняется двумя способами: либо непосредственное изучение клиентского приложения (например, веб-браузера), посредством которого осуществлялся переход по вредоносным ссылкам, либо использование специализированного программного обеспечения для

исследования следов активности пользователи в сети. К специализированному программному обеспечению предназначенного для анализа следов активности можно отнести свободно распространяемый программный комплекс «Нирсофт», среди компонентов которого есть утилита BrowsingHistoryView, позволяющая собрать информацию из всех веб-браузеров, установленных на персональном компьютере жертвы.

2. Во-вторых, в связи с тем, что программа-вымогатель может быть замаскирована под обычное браузерное расширение, немаловажным аспектом является необходимость анализа установленных дополнений для клиентских приложений.

3. В-третьих, необходимо изучить загруженные пользователем исполняемые файлы, которые необходимо проверить лицензированным программным обеспечением на предмет наличия вредоносного кода в программе.

4. В-четвертых, важным аспектом является изучение записей, оставленных программой-вымогателем в системном реестре операционной системы, которая является иерархически построенной базой данных параметров и настроек операционной системы.

Для изучения параметров системного реестра необходимо воспользоваться встроенным функционалом операционной системы. На примере операционной системы Microsoft Windows используется встроенный в систему редактор реестра, в параметрах которого можно установить:

– в ключе UserAssist записываются параметры каждой запущенной GUI-программы;

– в параметрах работы службы BAM, представляется возможным изучить информацию о запуске исполняемых файлов, работающих в фоновом режим, среди информации, полученной из данных параметров, можно установить: полный путь к исполняемому файлу, дату и время последнего исполнения;

– в ключе RecentApps отображаются записи запуска последних программ.

Как видим, следовая картина при перенаправлении трафика оставляемая функционированием вредоносного программного обеспечения достаточно обширна и выполнение указанных действий позволит определить механизм заражения и работы программ-вымогателей в компьютерной системе или сети.

Вложения электронной почты. Электронные письма с вложениями или ссылками побуждают пользователей открывать и получать доступ к веб-ресурсам, содержащим программу-вымогатель. На первый взгляд жертве кажется, что электронное письмо отправлено подлинным корреспондентом, так как вложения могут содержать электронный счет за потребляемую электроэнергию, налоговую или юридическую документацию, или даже содержат информацию от лиц, ищущих работу с просьбой открыть вложение или перейти по ссылке, чтобы актуализировать информацию о пользователе.

Для получения значимой информации при данном виде атак, необходимо:

1. Осмотреть электронный почтовый адрес жертвы на предмет установления электронного письма, содержащего вредоносное вложение. При установлении такового письма необходимо осмотреть служебные заголовки электронного

письма, в которых содержится информации об отправителе письма, времени отправления и доставке конечному пользователю письма. В случае отправки злоумышленником электронного письма с корпоративной электронной почты, в служебных заголовках может содержаться IP-адрес устройства, с которого отправлено электронное письмо.

2. Следующим шагом необходимо проанализировать загруженные жертвой файлы из вложений электронных писем. Особый интерес представляют файлы для обработки текстовыми процессорами и имеющими расширения .doc (-x), а также файлы для обработки табличными процессорами и имеющими расширения .xls (-x), так как данные файлы могут содержать встроенные макросы – небольшие программы, которые исполняются прямо внутри файлов. Вместе с тем необходимо обратить внимание на ZIP- и RAR-архивы, файлы PDF и образы дисков ISO и IMG [6].

Последующие этапы определения механизма заражения компьютерной системы или сети вредоносным программным обеспечением идентичны, как и при перенаправлении трафика.

Ботнеты. В последние годы особую популярность приобрел данный вид вредоносного программного обеспечения, так злоумышленники стремятся взять под контроль миллионы устройств по всему миру и таким образом управлять огромной сетью устройств, которые можно использовать для осуществления атак типа «отказ в обслуживании» (DDoS), тем самым блокирую доступ к информационным системам. Распространяется данный вид вредоносного программного обеспечения при помощи загрузчиков путем компрометации пользовательских компьютерных систем и сетей, после чего загружается вредоносное программное обеспечение в качестве второго шага. Загрузчики представляют собой легальное программное обеспечение, такое как бесплатные игры и инструменты, которые не содержат вредоносного кода, а загружает его позже.

В данной ситуации, для получения необходимой информации о распространителе вредоносного программного обеспечения важно проанализировать данные, хранящиеся в журналах обращений к сетевому оборудованию, либо оперативного взаимодействия с организациями, представляющих услуги в качестве хостинг- и интернет-провайдера.

Данный перечень угроз не является исчерпывающим. Преступный мир не ограничивается существующими решениями, а постоянно совершенствует инструменты для проведения кибератак с целью заражения компьютерных систем и сетей. Указанные векторы атак активно сочетаются с методами социальной инженерии, которые вызывают у пользователей чувство эйфории, чрезвычайной заинтересованности, ответственности или тревоги. Например, злоумышленники при отправке электронного письма в адрес коммерческих организаций от имени налоговых органов указывают на необходимость срочного исполнения требований документа, находящегося во вложении электронного письма.

Подводя итог изложенному в настоящей статье, хотелось бы особо отметить необходимость в разработке научно-методических и научно-практических рекомендаций для сотрудников правоохранительных органов по грамотному и эффективному извлечению следов активности программ-вымогателей, и сохранению данных следов для последующего изучения и использования в суде в качестве доказательства.

Список литературы

1. Руководство по реагированию на инциденты информационной безопасности // Kaspersky ICS CERT. Текст: электронный. 2022. URL: http://surl.li/bzpyh.

2. Шифровальщики – это не про вас. Текст: электронный // Лаборатория Касперского: [сайт]. 2022. URL: https://noransom.kaspersky.ru/.

3. Программа-вымогатель, программа-шантажист. Текст: электронный // ВикипедияURL: https://ru.wikipedia.org/wiki/Программа-вымогатель.

4. B. Cromis: Ransomware, a system centric detection approach // Master's theses submitted to the Graduate School by Ball State University master's degree candidates in partial fulfillment of degree requirements. Текст: электронный // Department of Computer Science. 2017. URL: https://cardinalscholar.bsu.edu/handle/123456789/-200699.

5. Россинская Е. Р., Рядовский И. А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования // Всероссийский криминологический журнал. 2020. Т. 14. № 5. С. 699–709.

6. Топ-4 самых опасных типа вложенных файлов. Текст: электронный // Kaspersky.ru : [сайт] 2019. 27 мая. URL: https://www.kaspersky.ru/blog/top4-dangerous-attachments-2019/22767.

Лутцева К. В.[1],
преподаватель кафедры уголовного процесса
Рязанского филиала
Московского университета МВД России
имени В.Я. Кикотя

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ДОПРОСА ПОТЕРПЕВШЕГО ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В Российской Федерации в последние годы наблюдается устойчивая тенденция роста преступлений, совершаемых путем хищения чужого имущества с использованием средств мобильной связи. Рост информационных технологий обусловил расширение сфер применения мобильной связи, мобильных приложений, с помощью которых осуществляется большинство банковских платежей по безналичному списанию денежных средств граждан как с подтверждением транзакций через СМС-уведомления, так и без таковых. Быстрое развитие таких информационных технологий создает предпосылки для их использования в преступных целях, что влияет на ежегодное увеличение уровня регистрируемых преступлений против собственности граждан.

Наиболее распространенными способами совершения преступлений данной категории являются:

– хищения денежных средств с использованием компьютерных технологий (кражи с электронных кошельков, с банковских счетов физических и юридических лиц);

– неправомерный доступ к охраняемой законом компьютерной информации;

– применение вредоносных программ;

– хищения путем заражения систем дистанционного банковского обслуживания.

Расследование указанных видов преступлений возложено на органы предварительного следствия, правомочные проводить следственные действия согласно требованиям уголовно-процессуального законодательства.

В последнее время научным сообществом, а также практическими сотрудниками уделяется большое внимание вопросам, связанным с организацией расследования указанных видов преступлений, тактике производства отдельных следственных действий. Однако остаются сложности в расследовании таких преступлений.

Данные сложности обусловлены:

– во-первых, недостаточной профессиональной подготовленностью сотрудников, осуществляющих борьбу с данными видами преступлений, их методико-криминалистическим обеспечением;

---

[1] © Лутцева К. В., 2022.

– во-вторых, механизмом преступления, так как средства и методы, применяемые злоумышленниками, постоянно меняются в условиях быстро развивающихся технических возможностей использования информационно - телекоммуникационных технологий;

– в-третьих, несвоевременным принятием органами дознания, следователями мер, в том числе оперативно-розыскных, на этапе проверки сообщения о совершенном преступлении в порядке ст.ст. 144–145 Уголовно-процессуального кодекса Российской Федерации (далее по тексту – УПК РФ), направленных на установление обстоятельств произошедшего, механизма хищения денежных средств, принадлежащих потерпевшему, изобличение виновного лица, а также установление местонахождения похищенных денежных средств.

Одним из важнейших условий раскрытия в короткие сроки хищения денежных средств гражданина с принадлежащего ему банковского счета, совершенного с использованием мобильных средств связи, является допрос потерпевшего, который должен быть проведен своевременно после принятия следователем решения о возбуждении уголовного дела. В данном случае своевременность, полнота отраженных в протоколе допроса потерпевшего сведений имеет решающее значение при определении перечня следственных действий, а также последовательности, в которой их необходимо провести следователю.

Тактические особенности производства следственных действий при расследовании указанной категории преступлений обусловлены способом хищения денежных средств потерпевших. Из вышеперечисленных способов хищения наиболее распространенным является хищение денежных средств с банковских счетов с использованием средств мобильной связи при отсутствии вербального контакта потерпевшего со злоумышленником, в результате которого хищение денежных средств осуществляется путем использования мобильных онлайн приложений. Указанный способ хищения денежных средств значительно затрудняет деятельность сотрудников следственных подразделений, направленную на установление личности злоумышленника, так как потерпевший фактически не обладает какой-либо значимой для предварительного следствия информацией о преступнике, кроме как об особенностях его речи, голоса. В связи с чем, правильно выбранная сотрудниками следственных подразделений тактика проведения допроса потерпевшего, с учетом особенностей его личности, позволяет установить все обстоятельства произошедшего, выполнить следственные действия, направленные на раскрытие и расследование преступления.

Как правило, лица, ставшие жертвами хищения денежных средств с принадлежащих им банковских счетов, под воздействием обмана со стороны якобы банковских сотрудников, сотрудников иных государственных учреждений имеют определенные виктимные свойства личности, которые под воздействием внешних факторов обостряются. Указанные обстоятельства необходимо учитывать в ходе проведения допроса потерпевшего, так как в силу имеющейся эмоциональной предрасположенности в ходе следственного действия может проявляться импульсивность, нетерпеливость, отсутствовать внимание к мелочам,

присутствовать плохая концентрация внимания при ответе на задаваемые следователем вопросы по обстоятельствам произошедшего. Указанные поведенческие особенности потерпевшего отражаются на установлении объективной картины произошедшего.

Так, при допросе потерпевшего в первую очередь необходимо обратить внимание на следующие обстоятельства, подлежащие установлению следователем.

Во-первых, установить: наиболее точную дату, время списания либо перевода самим потерпевшим денежных средств с принадлежащего ему банковского счета, время и дату телефонных звонков, поступивших потерпевшему от злоумышленника (в зависимости от временного интервала между совершенным хищением принадлежащих ему денежных средств и обращением с заявлением в органы внутренних дел).

В ходе допроса потерпевшего правильно установленные следователем дата, время хищения (незаконного списания) денежных средств и телефонных звонков злоумышленника на первоначальном этапе расследования позволят установить иные обстоятельства совершенного преступления. Ошибки при установлении указанных данных, неточное их отражение в протоколе допроса потерпевшего либо указание слишком длинного временного промежутка, в течение которого было совершено хищение денежных средств потерпевшего, в дальнейшем приводит к истребованию в банковских организациях ненужной следователю информации о движении денежных средств по банковскому счету потерпевшего, а также получению не представляющих интерес для следствия сведений у операторов мобильной связи. Данные обстоятельства приводят к нарушению разумных сроков уголовного судопроизводства, принятию органами предварительного следствия промежуточных решений в порядке ст. 208 УПК РФ, не соблюдению принципа неотвратимости уголовного наказания.

Кроме того, необходимо учитывать, что в связи с ежегодным ростом преступности в сфере информационно - телекоммуникационных технологий возросла загруженность работников банковской сферы, а также операторов услуг мобильной связи по представлению сведений о движении денежных средств по банковским счетам граждан, а также сведений о соединениях между абонентами и абонентскими устройствами, что напрямую также влияет на процессуальные сроки по уголовному делу.

Таким образом, следователь в ходе допроса потерпевшего должен обратить особое внимание на данные обстоятельства, которые подлежат доказыванию по уголовному делу в порядке ст. 73 УПК РФ, так как не во все случаях при возбуждении уголовного дела, а также на первоначальном этапе расследования у потерпевшего имеются при себе расширенные банковские выписки о движении денежных средств по его банковским счетам, а также не по всем операциям по списанию денежных средств с его счета, зачастую не сохраняются сведения о телефонных разговорах со злоумышленником, что не позволяет своевременно направить соответствующие запросы операторам сотовой связи.

Во-вторых, немаловажным аспектом при проведении допроса потерпевшего по указанной категории уголовных дел является установление способа хищения

принадлежащих потерпевшему денежных средств. В зависимости от обстоятельств совершенного преступления следователь должен определить перечень вопросов, которые подлежат выяснению, а именно: установить механизм хищения денежных средств потерпевшего, используемые злоумышленником в целях хищения компьютерные программы, абонентские номера, особенности речи злоумышленника (лингвистические особенности, акцент), установить длительность общения потерпевшего со злоумышленником, уточнить какие сведения о банковском счете и банковской карте сообщал потерпевший, совершал ли он какие-либо действия с находящимся в его пользовании банковским счетом с использованием мобильных приложений по просьбе злоумышленника. В силу существующего множества способов хищения денежных средств с банковских счетов потерпевших сотрудникам следственных подразделений необходимо обратить внимание на возможность привлечения специалистов в сфере информационных - телекоммуникационных технологий, знания которых помогут более правильно изложить в протоколе допроса потерпевшего весь алгоритм действий потерпевшего по переводу им денежных средств злоумышленнику.

На практике сотрудники следственных подразделений зачастую не привлекают специалиста при проведении такого следственного действия как допрос потерпевшего, что в свою очередь влияет на полноту и нередко правильность отраженных в процессуальном документе сведений.

В-третьих, при проведении следственных действий с участием потерпевшего необходимо обратить внимание на своевременность производства выемки мобильного устройства, с помощью которого потерпевший общался со злоумышленником, сим - карты с абонентским номером, а также иных документов, содержащих сведения о движении денежных средств по его банковскому счету, имеющихся при нем. Своевременное изъятие указанных предметов, документов способствует фиксации, закреплению следов преступления. В данном случае мобильное устройство, принадлежащее потерпевшему, с находящийся внутри него сим-картой, с помощью которого он общался со злоумышленником, использовал находящиеся на нем приложения для осуществления операций по перечислению принадлежащих ему денежных средств будет служить средством для обнаружения преступления и установления обстоятельств уголовного дела согласно положениям ст. 81 УПК РФ.

В связи с чем, сотрудникам следственных органов необходимо обратить внимание на своевременное проведение с участием потерпевшего данного следственного действия в целях предупреждения утраты вещественных доказательств, своевременного осмотра, фиксации сведений о перечислении денежных средств, о соединениях с абонентским номером злоумышленника, находящихся на мобильном устройстве. При необходимости, с учетом полученных сведений с мобильного устройства потерпевшего, следователь должен назначить компьютерную судебную экспертизу, для разрешения ряда вопросов, связанных с поиском на носителе информации, сведений о действиях пользователя (процессах обработки файлов, работе в сетях передачи данных и др.).

Рассмотренный перечень обстоятельств, подлежащих установлению следователем в ходе допроса потерпевшего, при расследовании преступлений, связанных с хищением денежных средств с банковских счетов, совершенных с использованием средств мобильной связи, обращает внимание на базовые ошибки, которые могут быть допущены.

Принимая во внимание ежегодный рост количества преступлений в рассматриваемой сфере, ущерб, причиняемый потерпевшим действиями злоумышленников, небольшое количество раскрытых преступлений относительно регистрируемых, своевременная и полная фиксация сотрудниками следственных подразделений обстоятельств произошедшего в ходе допроса потерпевшего, служит основой для проведения последующих следственных действий, направленных на сбор доказательственной базы по уголовному делу.

Мурадян С. В.[1],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук

Альховская А. В.[2],
курсант международно-правового факультета
Московского университета МВД России
имени В.Я. Кикотя

К ВОПРОСУ О ПОСЯГАТЕЛЬСТВАХ НА ЧАСТНУЮ ЖИЗНЬ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Постепенная трансформация всех сфер жизни общества и государства ввиду процесса цифровизации автоматически влечет за собой внедрение в повседневную жизнь передовых достижений науки и техники. С одной стороны, это существенно оптимизирует и повышает эффективность различных сфер жизни общества, а, с другой стороны, обуславливает необходимость постоянного совершенствования средств и мер по обеспечению информационной безопасности в соответствии с актуальными тенденциями развития новых технологий и применения их на практике. Так, «Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг.» закрепляет необходимость защиты данных посредством обеспечения баланса в вопросах применения современных технологий обработки данных и защите прав граждан [1].

В настоящее время возрастает число посягательств на конституционные права граждан, совершаемые с использованием информационно-телекоммуникационных технологий. Провозглашенное в ст. 23 Конституции Российской Федерации [2] право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений рассматривается как составной элемент неприкосновенности частной жизни в целом, реализация которого крайне важна в контексте обеспечения правопорядка и безопасности в государстве. Данное право распространяется не только на сведения, передаваемые на бумажном носителе, но и представленные в цифровой форме (например, сообщения в социальных сетях и мессенджерах, личные данные, необходимые для использования системы дистанционного банковского обслуживания и т. д.).

Положения в области охраны тайны переписки детализированы в Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3] и в Федеральном законе № 126-ФЗ «О связи» [4]. Ключевым нормативным правовым актом, конкретизирующим положения указанной статьи Конституции Российской Федерации в сфере защиты конфиденциальной информации, является Федеральный закон №152-ФЗ «О персональных данных» [5], целью которого является обеспечение и реализация прав и свобод субъектов

[1] © Мурадян С. В., 2022.
[2] © Альховская А. В., 2022.

информационного взаимодействия на неприкосновенность частной жизни и тайну переписки. Закрепление данного права является следствием реализации общедемократических тенденций развития законодательства и гарантией независимости частной жизни от государства и общества.

Неприкосновенность частной жизни в современном мире может быть нарушена посредством совершения преступлений, предусмотренных ст.ст. 137, 138 Уголовного кодекса Российской Федерации (далее – УК РФ) [6]. Разница между этими составами состоит в том, что предметом преступления, предусмотренного ст. 137 УК РФ могут быть любые сведения о частной жизни лица, а по ст. 138 УК РФ только те, которые перечислены в диспозиции нормы. Статья 138 УК РФ не содержит прямого указания на необходимость квалифицировать по данной статье случаи нарушения указанных прав в цифровой сфере, однако согласно постановлению Пленума Верховного Суда Российской Федерации от 25 декабря 2018 г. № 46 [7] под «иными сообщениями» следует понимать сведения, передаваемые посредством телетайпа, сети Интернет, СМС- и ММС-сообщений, а также следует учитывать электронные письма, IP-телефонию, сервисы видеосообщений типа Skype, Viber. Причем согласно тому же постановлению Пленума Верховного Суда Российской Федерации № 46 [7], ответственность по ст. 138 УК РФ наступает независимо от того, составляют передаваемые в переписке, переговорах, сообщениях сведения личную или семейную тайну гражданина или нет.

При собирании таких сведений возможна идеальная совокупность преступлений, предусмотренных ст.ст. 137, 138–139 либо 272 УК РФ.

Так, согласно приговору Савеловского районного суда г. Москвы частный детектив Л. был признан виновным в совершении преступлений, предусмотренных ч.1 ст.137, ч.1 ст.138, ч.1 ст.203 УК РФ. Незаконным способом гражданин Л. получил от оператора сотовой связи сведения о телефонных соединениях потерпевшей У. Полученную из переписки У. информацию Л. в дальнейшем распространил с целью получения денежных средств [8].

Корыстный мотив в преступлениях, предусмотренных ст. 138 УК РФ, нивелирует возможности оценки его, как малозначительного деяний.

Так, Ф., незаконно изъяв адресованное Л. письмо, ознакомился с его содержимым и передал его участковому уполномоченному полиции. При этом Ф. действовал преднамеренно, с целью использования имеющейся в письме информации в своих корыстных целях, в связи с чем, по мнению Калужского областного суда, нельзя говорить о малозначительности его действий [9].

При распространении лицо, о котором сообщаются те или иные сведения, должно быть индивидуально конкретизировано до степени его узнаваемости третьим лицом.

Законодатель устанавливает правовые гарантии для субъектов цифрового информационного пространства, поскольку данная среда наравне с преимуществами ее использования несет в себе и угрозы обеспечения защиты данных.

Неоднократно поднимался вопрос о правомерности доступа Федеральной службы по надзору в сфере связи к перепискам интернет-пользователей. Однако

Роскомнадзор осуществляет свою деятельность в соответствии с Федеральным законом № 144-ФЗ «Об оперативно-розыскной деятельности» [10] и на основании судебного решения. То есть, охрана права на неприкосновенность частной жизни перестает действовать в случаях, указанных в ст. 9 данного Федерального закона. Подобная ситуация складывается и в отношении ограничения конституционного права на тайну переписки и переговоров в интересах следствия, когда правоохранительным органам в случаях, не терпящих отлагательств, предоставляется возможность провести любое мероприятие без судебного решения, но с последующим уведомлением суда.

Использование информационно-телекоммуникационных сетей при посягательстве на частную жизнь часто сопряжено с использованием вредоносного программного обеспечения и специальных технических средств, основное назначение которых – негласное несанкционированное получение информации, что само по себе образует состав преступления, предусмотренный ст.ст. 138[1] и 273 УК РФ. Например, Феодосийским городским судом Республики Крым П. был признан виновным в совершении преступлений, предусмотренных ч. 1 ст. 137 и ст. 138[1] УК РФ. Так П., проживая совместно с А., преследуя мотив незаконного получения информации, составляющей тайну ее личной жизни, умышленно приобрел смарт-часы и произвел их существенное конструктивное изменение для возможности тайного размещения в предметах, используемых А. Вшив часы с установленной сим-картой в личную сумку А., П. при необходимости совершал соединения с электронными часами с микрофоном со встроенным GSM-модулем, в ходе чего тайно получал информацию о месте нахождения А. и происходящих событиях, составляющих сведения о ее частной жизни [11].

А нарушение тайны переписки в информационно-телекоммуникационных сетях сопряжено с получением несанкционированного доступа к компьютерной информации, который влечет за собой наступление последствий в виде различного рода модификаций такой информации. Так, Кировский районный суд г. Ярославля признал виновным гражданина К. в совершении преступлений, предусмотренных ч. 2 ст. 138, ч. 3 ст. 272 УК РФ, то есть в нарушении тайны переписки, а также неправомерном доступе к охраняемой законом компьютерной информации. Реализуя преступный умысел, гражданин К. получил доступ к персональной странице гражданки Ф. в социальной сети «ВКонтакте», вступил в переписку от имени потерпевшей с иными лицами, после чего изменил необходимый для входа в сеть пароль, что повлекло изменение личной информации гражданки Ф. [12].

Следует отметить, что в случае согласия хотя бы одного из участников тайны на ознакомление третьих лиц с содержанием переписки указанное право граждан не нарушается, поскольку каждый из субъектов информационного обмена является носителем не только права на неприкосновенность общения, но и на разглашение сведений. Верховный Суд Российской Федерации уточняет, что уголовная ответственность наступает только в том случае, если умыслом преступника охватывается тот факт, что разглашаемые конфиденциальные сведения лица хранятся им в тайне [7].

Не является нарушением права на тайну переписки обращение законных представителей к операторам связи и Интернет-провайдерам за детализацией информации об отправленных и полученных сообщениях несовершеннолетними. Однако А. Н. Изотова считает, что это может ущемлять права детей ввиду того, что они обладают равным с совершеннолетними лицами правами [13].

Определенные сложности в процессе квалификации преступлений, посягающих на неприкосновенность частной жизни, обусловлены групповым характером переписки. Ключевым вопросом является определение лица, подлежащего ответственности за нарушение рассматриваемого конституционного права. В таких случаях практически невозможно установить источник утечки информации ввиду многочисленности участников.

Еще одной особенностью рассматриваемого вида преступлений является проблема установления места совершения преступного посягательства, связанная с реализацией его в киберпространстве. В результате проведенного исследования, С. В. Баринов пришел к выводу, что в большинстве случаев местом фактического нарушения тайны переписки является не сетевой адрес, а расположение помещения, из которого, посредством технических устройств, осуществлялся доступ в информационно-телекоммуникационную сеть [14].

Специалисты «Лаборатории Касперского» указывают на рост числа вредоносных рассылок, получаемых отдельными гражданами и организациями. Злоумышленники преследуют главную цель – распространение вредоносов, влекущее заражение персональных компьютеров и сетей для получения доступа к охраняемой законом информации. Согласно сведениям, предоставленным экспертами, количество таких рассылок с начала 2022 г. возросло в 10 раз и составило более 30 тыс. случаев [15].

Механизм функционирования таких атак выглядит следующим образом: пользователи глобальной цифровой сети получают электронные письма в, как правило, уже имеющейся переписке, в корне которых содержится ссылка с информацией по самым популярным запросам или платежными формами. При переходе по данной ссылке на устройство сети из облачного хранилища и загружается троянская вирусная программа.

Посредством загружаемого на персональный компьютер вредоносного программного обеспечения правонарушители получают доступ не только к персональным данным, но и электронным сообщениям, письмам, а также приобретают возможность контролировать деятельность зараженного устройства.

В настоящее время эксперты в области информационной безопасности разработали комплекс мер, направленных на защиту охраняемой законом информации и предупреждение несанкционированного доступа к устройствам. Однако ввиду постоянно развивающейся информационно-телекоммуникационной сферы необходимо уделить особое внимание совершенствованию методов защиты от возникающих в киберпространстве угроз.

Отметим и тот факт, что функциональные возможности большинства мессенджеров, социальных сетей и интернет-платформ создают благоприятную среду для совершения преступных посягательств на тайну переписки. Так, например,

в чатах участникам предоставляется возможность пересылки сообщений, копирования текста, фото-, видеоматериалов, аудиосообщений. Наибольшая степень защиты конфиденциальной информации реализована в Российском мессенджере «Телеграм». Пользователям представлены опции создания «Секретных чатов», установления запрета на пересылку сообщений, ограничение создание скриншотов. Однако и в этом случае посягательство на тайну переписки может быть осуществлено путем непосредственного фотографирования экрана с другого устройства.

В рамках проведенного исследования судебной практики по вопросам посягательств на частную жизнь лиц Группа компаний «InfoWacth» опубликовал статистику за 2019–2020 гг. В 2020 г. количество уголовных дел, рассмотренных судами первой инстанции по исследуемым составам преступлений, увеличилось на 18 %. Большая часть преступлений связана с нарушениями должностных лиц (более 70 %). Самый распространенный способ нарушения права на тайну переписки – получение сведений об общении в мессенджерах, а также посредством электронной почты. Реже всего использовались бумажные носители информации [16].

Спектр проблем, связанных с обеспечением конституционного права на конфиденциальность сведений, составляющих частную жизнь лиц в условиях цифровизации, связан в том числе с большим количеством устройств, которые являются предметом такой охраны (базы данных/сервера, рабочие станции сотрудников, облака, мобильные устройства, ноутбуки, сетевые папки и бизнес-приложения). Кроме того, такого рода преступления обладают вполне закономерным высоким уровнем латентности, обусловленным либо невозможностью установления самого факта нарушения данного права, либо субъекта, совершившего преступное посягательство.

Стоит отметить, что наличие технической подготовки у потенциальных и реальных преступников, занимающихся противоправной деятельностью в данной области, существенно осложняет работу по выявлению и пресечению преступлений данной категории. И это обстоятельство выдвигает определенные требования к сотрудникам правоохранительных органов по наличию у них специальных знаний, умений и навыков, а также поднимает вопросы, связанные с оснащением рабочих мест сотрудников прикладным программным обеспечением, необходимым для осуществления документирования и дальнейшего расследования преступлений в цифровой среде.

Нередки случаи отсутствия технической возможности установления отдельных признаков объективной стороны преступления, поскольку злоумышленники используют при осуществлении преступных посягательств различные VPN и proxy- сервисы, значительно затрудняющие расследование преступлений.

На сегодняшний день обеспечить конституционное право на тайну переписки в киберпространстве в полном объеме не представляется возможным. Цифровая информация ежедневно подвергается новым по своей природе видам угроз и атак. Злоумышленники получают несанкционированный доступ к охраняемой законом информации посредством вредоносного программного обеспечения

и технических средств, предназначенных для негласного получения данных, осуществляя посягательства на конфиденциальные сведения. Правовое регулирование обеспечения неприкосновенности частной жизни, в том числе тайны связи отстает от сложных технологий. Ввиду этого необходимо совершенствование оборота цифровых сведений в информационно-телекоммуникационной сфере на законодательном уровне, развитие методов и способов защиты информации от неправомерного доступа, разработка инновационных мер, соответствующего материально- технического обеспечения для эффективного предупреждения, пресечения, раскрытия, и расследования преступлений, в сфере информационно-телекоммуникационных технологий, посягающих на неприкосновенность частной жизни.

Список литературы

1. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.» // СПС «КонсультантПлюс».

2. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г., с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // СПС «КонсультантПлюс».

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 30.12.2021) // СПС «КонсультантПлюс».

4. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (ред. от 30.12.2021) // СПС «КонсультантПлюс».

5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 02.07.2021) // СПС «КонсультантПлюс».

6. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 22.08.2021) // СПС «Консультант Плюс».

7. Постановления Пленума Верховного Суда Российской Федерации от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138^1, 139, 144^1, 145, 145^1) Уголовного кодекса Российской Федерации» // СПС «КонсультантПлюс».

8. Приговор Савеловского районного суда г. Москвы от 4 апреля 2019 г. по уголовному делу № 1-138/19. URL: https://vk.com/away.php?to=https-%3A%2F%2Fmos-gorsud.ru%2Frs%2Fsa vyolovskij%2Fcases%2Fdocs%2Fcontent%2Fd58bde2d-098a-4b84-aa0b-cc965f07a8b5&cc_key=.

9. Апелляционное постановление Калужского областного суда от 22 сентября 2017 г. по делу № УК-22-1308/2017 // СПС «КонсультантПлюс».

10. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (ред. от 01.04.2022) // СПС «КонсультантПлюс».

11. Постановление Феодосийского городского суда Республики Крым от 5 февраля 2020 г. по делу № 1-64/2020 // СПС «КонсультантПлюс».

12. Приговор Кировского районного суда г. Ярославля по уголовному делу № 1-59/2021 от 11 мая 2021 г. URL: https://sudact.ru/regular/doc/0xb0QKWbvjrbL/.

13. Изотова А. Н. Право на тайну связи абонента и пользователя // Юридическая наука. 2020. № 9. URL: https://cyberleninka.ru/article/n/pravo-na-taynu-svyazi-abonenta-i-polzovatelya.

14. Баринов С. В. Некоторые особенности преступных нарушений тайны переписки и иных сообщений, совершаемых в киберпространстве // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 2 (10). URL: https://cyberleninka.ru/article/n/nekotorye-osobennosti-prestupnyh-narusheniy-tayny-perepiski-i-inyh-soobscheniy-sovershaemyh-v-kiberprostranstve.

15. Васин М. «Лаборатория Касперского» обнаружила массовую вредоносную рассылку на крупные компании по всему миру. URL: https://www.kaspersky.-ru/about/press-releases/2022_laboratoriya-kasperskogo-obnaruzhila-massovuyu-vredonosnuyu-rassylku-na-krupnye-kompanii-po-vsemu-miru.

16. В России по статье 137 УК РФ чаще штрафуют / Официальный сайт ГК «InfoWacth». URL: https://www.infowatch.ru/company/ presscenter/news/v-rossii-po-state-137-uk-rf-chasche-shtrafuyut.

Семочкина А. А.[1],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук

Вильмс А. А.[2],
курсант 591 учебного взвода
международно-правового факультета
Московского университета МВД России
имени В.Я. Кикотя

К ВОПРОСУ ОБ УГОЛОВНО-ПРАВОВОМ ПРОТИВОДЕЙСТВИИ КИБЕРБУЛЛИНГУ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Стремительно развивающийся век информационных технологий так или иначе предполагает масштабное использование социальных сетей и различных мессенджеров. Появление большого количества средств коммуникации посредством сети Интернет послужили началом развития нового места совершения преступлений. Огромное число деяний зафиксировано именно с использованием Всемирной паутины. При этом наряду с достаточно большим количеством преступлений в сфере экономики, возрос объем общественно опасных деяний против личности.

Одним из распространенных видов преступлений, затрагивающих интересы личности во всех ее проявлениях, является оскорбление в интернете. В связи с этим, для обозначения таких деяний обострилась необходимость принятия термина «кибербуллинг», который в полной мере описывает признаки совершенного деяния.

Впервые данная формулировка была предложена, а затем и введена в использование Биллом Белсеем, который определил ее как использование информационных или коммуникационных технологий для преднамеренного, повторяющегося и враждебного поведения, намеревающегося нанести вред другим [3]. При этом происходило уточнение и дополнение данного понятия.

Существует множество подходов к определению кибербуллинга. Например, А. В. Путинцева определяет данную дефиницию как психологическое насилие в сети [4, с. 52]. При этом автор подчеркивает, само понятие происходит от английского слова – «буллинг», которое один из иностранных словарей определяет, как насилие, запугивание, направленное на то, чтобы вызвать у жертвы страх и тем самым подчинить себе [1].

В свою очередь Н. Ю. Федунина определяет данное понятие как способ травли человека через сообщения в сети Интернет, содержащие негативные оценки, оскорбления, угрозы [5, с. 11].

---

[1] © Семочкина А. А., 2022.
[2] © Вильмс А. А., 2022.

Российский исследователь С. И. Анохин под кибербуллингом понимает целенаправленные агрессивные умышленные действия, совершаемые группой лиц или одним лицом с использованием электронных форм воздействия в отношении жертвы, которая не может себя защитить.

В настоящее время живое общение стремительно уходит на второй план. Первое место среди способов коммуникации, особенно между подростками, является Интернет. Многообразие социальных сетей и платформ предоставляет широкий выбор ресурсов для изменения не только своей внешности, но и личностных характеристик. Происходит стирание собственного «Я». Дети и подростки получили возможность выбрать характер и манеру общения, т. е. в виртуальном пространстве появляется возможность создания альтернативного «собственного образа». Одни используют виртуальную среду для поддержания дружественного общения, иные применяют для вымещения своей агрессии и надеются избежать ответственности за свои действия. Развитие интернет-переписки привело к появлению различных форм интернет-травли. Например, Н. С. Бобровникова видит такие виды кибербуллинга:

1. Перепалки, или флейминг – обмен короткими эмоциональными репликами между двумя и более людьми, разворачивается обычно в публичных местах Сети.

2. Нападки, постоянные изнурительные атаки – повторяющиеся оскорбительные сообщения, направленные на жертву.

3. Клевета – распространение оскорбительной и неправдивой информации. Текстовые сообщения, фото, песни, которые часто имеют сексуальный характер.

4. Самозванство, перевоплощение в определенное лицо – преследователь позиционирует себя как жертву, используя ее пароль доступа к аккаунту в социальных сетях, в блоге, почте, системе мгновенных сообщений, либо создает свой аккаунт с аналогичным никнеймом и осуществляет от имени жертвы негативную коммуникацию.

5. Надувательство, выманивание конфиденциальной информации и ее распространение – получение персональной информации и публикация ее в интернете или передача тем, кому она не предназначалась.

6. Отчуждение (остракизм, изоляция). Любому человеку присуще желание быть включенным в группу. Исключение же из группы воспринимается как социальная смерть. Чем в большей степени человек исключается из взаимодействия, тем хуже он себя чувствует, и тем больше падает его самооценка.

7. Киберпреследование – скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т. д.

8. Хеппислепинг – название происходит от случаев в английском метро, где подростки избивали прохожих, тогда как другие записывали это на камеру мобильного телефона. Сейчас это название закрепилось за любыми видеороликами с записями реальных сцен насилия [2, с. 6–9].

Активное развитие данного термина на практике связано, как нами уже отмечалось ранее, с появлением Интернета, с его многообразием социальных сетей,

как одного из способов коммуникаций. При этом наиболее широкое использование мессенджеров для распространения своих негативных мыслей было отмечено среди молодых людей, в частности – в кругу подростков. Наряду с этим не многие из них задумываются, что такой способ выплескивания своей агрессии часто носят достаточно тяжелые последствия как для объекта травли и издевательств, так и для самого совершающего данные действия человека. Нельзя не сказать и о том, что не всегда такие общественно-опасные деяния не подразумевают под собой никакой ответственности.

Приведенное Н. С. Боровиковой исследование подтверждает необходимость реформирования законодательной базы Российской Федерации. Несмотря на то, что действующий закон не содержит статьи, предусматривающей ответственности за кибербуллинг, необходимо отметить, что совершение данного акта не будет оставаться безнаказанным. При этом подобные деяния будут урегулированы действующими на данный момент общими правилами.

В виду наличия различных форм интернет-травли, уже высказанных автором, нельзя сказать, что список является исчерпывающим. Осваивая интернет-платформу с развитием нормы административной ответственности, они не затрагивают вопроса интернет-травли на прямую. Одними из самых распространенных видов кибербуллинга являются оскорбления. В виду того, что ст. 130 УК РФ утратила силу в виду принятия Федерального закона от 7 декабря 2011 г. № 420-ФЗ, ответственность наступает по ст. 5.61 КоАП РФ.

Независимо от того, что нормы УК РФ также не предусматривают наказания за общие средства кибербуллинга, во многих диспозициях находят свое отражение его некоторые формы. Опираясь на действующие уголовно-правовые принципы, с точки зрения преступности будут рассмотрены только те деяния, которые повлекли существенные последствия не только для самого потерпевшего, но и для охраняемых законом интересов общества.

Например, достаточно распространенными в практике являются действия, направленные на распространение порочащих сведений о человеке с использованием информационно-телекоммуникационных сетей. Законодатель, применяя ст. 128^1 УК РФ, преследует свою главную задачу – защиту законных прав и интересов другого лица от посягательства, порочащего его честь и достоинство, а также подрывающего его репутацию. Частной ситуацией является создание специальной группы в одной из социальных сетей, задачей которой является распространение заведомо ложной информации, носящей в большинстве случаев оскорбительный характер. Важная особенность применения данной статьи – наличие у выкладываемой информации признака заведомости для субъекта преступления.

Нередко интернет-травля может быть осуществлена с угрозой для потерпевшей стороны. Высказывая свое намерение о причинении тяжкого вреда здоровью или о убийстве, субъект будет нести ответственность по ст. 119 УК РФ только в том случае, если пострадавший действительно будет опасаться угроз.

Всеобщую огласку получила быстро распространившаяся в 2016 г. среди подростков «игра» в сети Интернет – «Синий кит». До сих пор доподлинно не известно о количестве ее жертв. Безусловно, нельзя сказать о прямой форме кибербуллинга, поскольку главной целью и последним заданием являлось самоубийство ребенка. Однако наличие умысла у субъекта нанести вред жертве, вызвать у нее страх и опасение за свою жизнь также является одним из признаков интернет-травли. Первоначально такие действия квалифицировались по ст. 110 УК РФ, однако в виду распространенности «игры» Федеральным законом от 7 июня 2017 г. № 120-ФЗ была введена ст. 110[1] УК РФ. Действия близких людей подростков и социальных служб с плотным сотрудничеством с правоохранительными органами позволили снизить популярность «игры смерти» среди несовершеннолетних, однако, не исключили их создание полностью.

Нельзя не сказать о еще одной форме кибербуллинга, непосредственно связанной с Интернетом. В виду распространения средств связи среди огромного количества разных профессий, допустимо говорить о том, что отсутствие личной электронной почты является редким явлением. Такие уголовно-правовые нормы, как, например, ст.ст. 138 и 272 УК РФ – следствие стремительного увеличения случаев взломов аккаунтов на различных платформах.

В связи распространением мнения о равенстве людей независимо от их расы, нации, социальной группы или от иного признака, Российская Федерация не стала исключением. Статья 282 УК РФ предусматривает защиту от одной из наиболее агрессивных форм кибербуллинга – возбуждения ненависти или вражды только к определенной группе людей.

Бесспорно, появление Интернета в жизни людей облегчила осуществление различных сфер жизни, и при этом, в свою очередь повлекла за собой наличие определенной угрозы. В первую очередь, уменьшение личного, «живого» общения между людьми, приводит к устареванию непосредственной коммуникации, поскольку написать сообщение намного проще. Однако не менее важной проблемой стало распространение агрессии посредством социальных сетей с целью избегания реального наказания. Наличие большого количества запретной информации, анонимность в общении усложняют работу правоохранительных органов.

Анализируя существующие административно-правовые и уголовно-правовые нормы, необходимо сделать вывод о недостаточной защите прав и законных интересов личности и общества. Как и в случае с административной ответственностью возраст привлечения к уголовной ответственности по подавляющему большинству составов преступлений составляет 16 лет. При этом сами средства кибербуллинга, основываясь на теории его стремительного распространения и модификации, являются феноменом среди способов коммуникации. Речь идет именно об интернет-травле, как об одном из видов простого психологического буллинга, совершающегося с использованием всего многообразия телекоммуникационных технологий.

В связи с этим считаем необходимым рассмотрение и последующее принятие на законодательном уровне нормы, непосредственно затрагивающей возможные

формы кибербуллинга, что незамедлительно приведет к повышению уровня защиты населения в интернет-среде.

Список литературы

1. Англо-русский словарь общей лексики «Lingvo Universal». URL: https://dic.1963.ru/121.

2. Бобровникова Н. С. Опасность интернета-кибербуллинг / Н. С. Бобровникова // Восточно-Европейский научный вестник. 2015. № 1 (1). С. 6–9.

3. Belsey B. Cyberbullying: An emerging threat to the «always on» generation. URL:http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf.

4. Путинцева А. В. Развитие феномена «Кибербуллинг»: анализ подходов к определению // Вестник УЮИ. 2020. №3 (89). С. 52.

5. Федунина Н. Ю. Представления о триаде «преследователь–жертва–наблюдатель» в кибербуллинге в англоязычной литературе // Психологические исследования. 2015. Т. 8. № 41. С. 11.

Густова Э. В.[1],
доцент кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук

Хисматова А. Р.[2],
курсант 4 курса Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

ТОЛКОВАНИЕ ПРИЗНАКА ПУБЛИЧНОСТИ В ПРЕСТУПЛЕНИЯХ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИННЫХ СЕТЕЙ

Современное общество стремительно развивается и вместе с ним совершенствуются технологии в информационной сфере. На сегодняшний день можно с уверенностью утверждать, что мы живем в эпоху информационно-технологической революции, достижения и разработки которой проникают во все сферы человеческой жизни. Мало кто из людей может представить свою повседневную жизнь без использования информационно-телекоммуникационных технологий, в особенности – сети Интернет. Глобальная сеть стала местом скопления информации различной направленности, доступ к которой может получить каждый желающий. О широте распространения сети Интернет в России и мире свидетельствуют различные источники, в частности Global Digital в ежегодном отчете за 2021 г. приводит данные об использовании сети Интернет 4,66 млрд человек, что соответствует 60 % всего населения. При этом количество пользователей ежегодно растет – за 2021 г. их число увеличилось на 7,3 % [13].

Одновременно и преступный мир все шире использует потенциал информационно-телекоммуникационных сетей для совершения преступлений.

В последнее время в Уголовный кодекс Российской Федерации (далее – УК РФ) вносится большое количество изменений, касающихся дополнений ряда статей квалифицирующим признаком «с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет», а также введения самостоятельных составов преступлений, где важным признаком объективной стороны является «публичность» действий. Так, в качестве основного признака «публичность» предусмотрена в 16 составах преступлений (ч. 1 ст. 137; ч. 1 ст. 148; ч. 1 ст. 197; ч. 1 ст. 205.2; ч. 1 ст. 207.1; ч. 1 ст. 207.2; ч. 1 ст. 207.3; ч. 1 ст. 242; ч .1 ст. 242.1; ч. 1 ст. 280; ч. 1 ст. 280.1; ч. 1 ст. 280.3; ч. 1 ст. 282; ст. 319; ч. 1 ст. 354; ч. 1 ст. 354.1). В качестве квалифицированного – 9 (п. «д» ч. 2 ст. 110; ч. 2 ст. 110.2; ч. 2 ст.128.1; п. «в» ч. 2 ст. 151.2; ч. 2 ст.242; п. «г» ч. 2 ст. 245; п. «в» ч. 2 ст. 258.1; ч. 2 ст. 280.3; ч. 2 ст. 282). В качестве особо квалифицированного – 3 (п. «д» ч. 3 ст. 110.1; ч. 3 ст. 137; ч. 3 ст. 354.1). При этом в ст.ст. 137,

[1] © Густова Э. В., 2022.
[2] © Хисматова А. Р., 2022.

242, 280.3, 282, 354.1 – встречается и в основном, и в квалифицированном составах.

В результате чего в уголовно-правовой науке и судебной практике происходит поэтапное слияние понятий публичности совершенного преступного деяния и факта использования сети Интернет при его совершении. В первую очередь это связано с тем, что в конструкции большинства составов, закрепляющих данный признак, законодатель изложил его в формулировке: совершенное в «публичном выступлении, публично демонстрирующемся произведении, в СМИ или информационно-телекоммуникационных сетях (включая сеть Интернет). И если в случаях публичного выступления, совершения преступления посредством его публичной демонстрации в виде различных материальных предметов (произведений) или афишировании в средствах массовой информации не возникает вопроса относительно наличия признака публичности, то относительно использования информационно-телекоммуникационных сетей – сложно дать однозначный ответ.

Отождествление признака публичности совершения деяния и использования информационно-телекоммуникационных сетей при его совершении может привести к случаям привлечения лиц к уголовной ответственности, совершивших преступление в сети Интернет по статьям, где обязательным признаком выступает публичность совершения преступления, что является недопустимым с учетом положений принципов справедливости и гуманизма. Ввиду чего актуальным представляется рассмотрение целесообразности применения признака публичности к деяниям, совершенным в сети Интернет, а также разграничение данных понятий.

По исследованиям Н. В. Артеменко, А. М. Разогреевой и А. А. Чутченко, в судебной практике по уголовным делам данной категории суды не обращают внимание, были ли посетители у Интернет-ресурсов, просматривалась ли кем-либо размещенная информация и иные факторы, ввиду чего усматриваются элементы объективного вменения [2, с. 32].

Рассмотрение данной темы актуализируется в связи с отсутствием легального толкования термина «публичность». Согласно словарю С. И. Ожегова и Н. Ю. Шведовой понятие «публичность» олицетворяется с выступлением, исполнением, игрой перед публикой, речами и высказываниями [8, с. 652]. По мнению Ш. З. Маталаева, законодатель использует понятие публичности, прежде всего, в значении принадлежности к государству в широком смысле, включающем все, что относится к государству, гласности, открытости правосудия и т. д. [6, с. 240].

Некоторое аспекты толкования признака публичности разъясняются Верховным Судом Российской Федерации в Обзоре по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции [7], в котором под публичностью распространения информации предлагается понимать такое распространение информации, когда «она

адресована группе или неограниченному кругу лиц и выражена в любой доступной форме, а именно: устной, письменной, с использованием технических средств». Кроме того, обращено внимание на факт возможности наличия признака публичности при совершении деяния с использованием СМИ, информационно-телекоммуникационных сетей и мессенджеров, путем рассылки электронных сообщений.

Обращаясь к частным случаям урегулирования признака публичности некоторых составов Особенной части УК РФ, Верховный Суд Российской Федерации разъясняет отдельные моменты. Например, в п. 6.1 постановления Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 1 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» указывается, что моментом окончания преступления признается момент размещения обращений в сетях общего пользования (например, на сайтах, форумах или в блогах), отправления сообщений другим лицам. Аналогичным примером может служить п. 3 постановления Пленума Верховного Суда Российской Федерации от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (ст.ст. 137, 138, 138.1, 139, 144.1, 145, 145.1 УК РФ)», закрепляющий положение, что распространение сведений о частной жизни может быть совершено путем передачи их одному или нескольким лицам в том числе путем передачи материалов или размещения информации с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет.

Данные положения применимы к конкретным статьям, однако в судебной практике они активно применяются и к иным нормам УК РФ, примером чего может служить постановление от 7 июля 2020 г. по делу № 1-90/2020 Михайловского районного суда Амурской области, в котором судьей было удовлетворено ходатайство следователя о признании лица виновным в совершении преступления, предусмотренного п «г» ч. 2 ст. 245 УК РФ. При этом в качестве признака «публичности демонстрации» суд признал отправку видео в «группе» в мессенджере WhatsApp [9].

Общеизвестным является факт, что указанная платформа не содержит тематических групп «по интересам», как, к примеру, социальная сеть «ВКонтакте» или платформа «Telegram», в «WhatsApp» может быть создан лишь групповой чат, при этом групповым он становится при наличии уже трех участников, включая самого публикующего пользователя. Так как в соответствующем постановлении не отражено количество участников данного группового чата, можно предполагать, что вменение лицу п «г» ч. 2 указанной статьи было не обоснованным. Аналогичная ситуация встречается и в иных примерах судебной практики.

Опираясь на изложенные выше факты, на наш взгляд, деяние следует признавать публичным, когда оно направлено на определенную аудиторию лиц, однако, как уже отмечалось выше, из-за отсутствия толкования термина «публичность» неразрешенным остается и вопрос – начиная от какого минимального количества людей деяние стоит признавать публичным? Необходимость урегулирования

данного вопроса обусловлена тем, что при совершении преступления в сети Интернет не всегда доступ к ней получает неограниченный круг лиц, примером чего может служить распространение информации на так называемых «закрытых станицах» и «профилях с ограниченным количеством подписчиков» или, как приводилось в примере выше, в групповых чатах, состоящих из малого количества человек. Аналогично этому сложно говорить о публичности совершения преступления, когда информация распространяется в личных сообщениях между пользователями.

Так, к примеру, можно ли признать публичным преступление, совершенное на личной страничке пользователя социальной сети «ВКонтакте» у которого всего пять/десять/сто подписчиков? На наш взгляд, в данной ситуации целесообразность вменения данного признака спорна, так как не все подписчики ежедневно переходят на личные страницы для просмотра опубликованной информации. При этом, считаем, что при проведении предварительного расследования по данным уголовным делам, логичным выступает учет количества просмотров опубликованного поста, а не количество общих пользователей группы или подписчиков страницы. В поддержку данного положения приведем следующий пример: так, информация может быть размещена, к примеру, на страничке группы в социальной сети «ВКонтакте», у которой 500 подписчиков. Однако, из этих 500 пользователей часть уже не используют свои страницы, еще часть страниц – это, так называемые, боты или пустые страницы, созданные для увеличения числа подписчиков и придания «статуса» группе, еще часть не заходит в группу, так как давно потеряла к ней интерес, а кто-то просто «пролистает» данную запись в общем массиве опубликованной в ленте информации, даже не прочитав. Таким образом, из теоретического распространения информации на аудиторию в 500 человек, фактически доступ к ней получат максимум несколько десятков. При этом, не каждый пользователь дочитает до конца или решит изучить подробнее, так как данная информация не будет для него интересна. Представляется ли возможным вменить в данной ситуации признак публичности совершения деяния? Например, выступление в аудитории, на сцене, симпозиумах, собраниях, митингах, где присутствует аналогичная аудитория в 500 человек признак публичности будет налицо, в сравнении с предыдущим примером. Ведь очевидна разница в количестве лиц, получивших доступ и реально воспринявших данную информацию. Из чего следует вывод, что не всегда использование сети Интернет делает деяние публичным или может способствовать распространению информации на более широкий круг лиц.

Кроме того, важным моментом определения публичности является фактор субъективного восприятия информации: лицо, увидев опубликованную запись, внимательно ее прочло и переслало кому-либо еще, тем самым распространив или просто «пролистало» в общем массиве новостной ленты.

Значительным плюсом социальных сетей и мессенджеров выступает тот факт, что в них можно отследить, какому именно количеству пользователей данная информация была распространена – путем рассылки сообщения или «репостом» записи.

Проблемой изучения количественного показателя признака публичности занимались многие ученые, в числе которых Ю. М. Ткачевский, отмечавший, что двух-трех лиц недостаточно для признания публичности, в то время как публичное выступление перед группой из пяти-шести человек, к примеру, на митинге, при собрании и т. д. – уже можно признать таковым [10, с. 69]. По мнению В. И. Шмарион, для признания публичности достаточно уже трех человек, если они могут способствовать дальнейшему распространению информации [11, с. 123]. Практически аналогичного мнения – достаточности трех человек, придерживался и А. А. Арямов, но оговаривал тот факт, что лицом планировалось выступление на большую аудиторию, однако фактически она составила всего три человека [12, с. 521]. Д. А. Бажин выражает мнение, что понятия «неопределенный круг лиц» и «широкий круг лиц», применимые к признаку публичности, указывают на количество существенно больше, чем два человека [3, с. 163]. Однако большинство ученых апеллируют неопределенными понятиями – «многим лицам», «широкому кругу лиц», «широкой аудитории» и иными [4; 5].

При изучении судебной практики по данной категории уголовных дел, нами было отмечено, что в подавляющем большинстве приведенных актов реальное количество аудитории, которым стала доступна данная информация скрыто или не приведено, что с одной стороны, можно объяснить отсутствием официально закрепленного минимального количества людей, чтоб признать деяние публичным. С другой – может свидетельствовать об ошибочном вменении данного состава лицам, совершившим преступление при малой аудитории пользователей.

Подводя итог всему вышеизложенному, отметим, что признание публичным деяния, совершенного в сети Интернет или разграничение данных признаков – одна из первоочередных задач, стоящих перед законодателем ввиду того, что сложившаяся в судебной практике тенденция постепенного слияния данных понятий может привести к нарушению основных принципов уголовного права.

На данный момент необходимым является легальное толкование признака публичности и определение минимального количества человек, при которых данный признак будет признаваться действительным. Также, должно быть унифицировано включение данного признака в нормы Особенной части УК РФ, так как, как отмечал Р. Н. Алмакаев – интерпретации данного термина могут кардинально поменять объективную сторону преступлений, в то время как правила законодательной техники требуют единого подхода [1, с. 336].

На наш взгляд, на данный момент, однозначно совершенным публично в сети Интернет должны признаваться деяния, совершенные:

1. На интернет-ресурсах, зарегистрированных в качестве средств массовой информации.

2. На интернет-сайтах, доступ к которым имеет неограниченное количество человек и которые, хоть и не являются СМИ, однако обладают огромной аудиторией пользователей, посещающих их ежедневно. К примеру, интернет-энциклопедия «Википедия».

Спорным же является совершение публичных преступлений на интернет-сайтах «закрытого типа», на личных страница пользователей, не обладающих большим количеством подписчиках, в групповых чатах и личных сообщениях. В данных случаях, органам предварительного расследования и судам, на наш взгляд, следует исходить из количества «репостов» и реальных просмотров опубликованных записей или числа разосланных сообщений.

Публичность – это обязательное условие привлечения к уголовной ответственности. Полагаем, что кроме легального и судебного толкования данного признака, необходимо создание медиаэкспертизы. Она должна изучать не только содержание материала, но и направленность действий лица – продвигал ли он запрещенный контент или публикация является единичной и случайной на его странице.

Список литературы

1. Алмакаев Р. Н. Признак публичности в уголовном законодательстве: краткий анализ // Молодой ученый. 2017. № 11 (145). С. 335–338.

2. Артеменко Н. В., Разогреева А. М., Чутченко А. А. Клевета в Сети и в отношении индивидуально не определенного круга лиц: границы ответственности // Уголовный процесс. 2021. № 9. С. 32–37.

3. Бажин Д. А. К вопросу о понимании публичности в уголовном праве // Российский юридический журнал. 2011. № 2. С. 162–168.

4. Комментарий к Уголовному кодексу Российской Федерации. 7-е изд., перераб. и доп. / отв. ред. В. М. Лебедев. М., 2007.

5. Комментарий к Уголовному кодексу Российской Федерации. 2-е изд., перераб. и доп. / отв. ред. В. И. Радченко. М., 2008.

6. Маталаев Ш. З. Признак публичности и некоторые вопросы квалификации преступлений // Образование и право. 2017. №4. С. 240–244.

7. Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2 : утвержден Президиумом Верховного Суда Российской Федерации 30 апреля 2020 г. // СПС «КонсультантПлюс».

8. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. 4-е изд., доп. М. : ИТИ Технологии, 2006.

9. Постановление от 7 июля 2020 г. № 1-90/2020 // Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/regular/doc/mCT4myCgBTN1/.

10. Ткачевский Ю. М. Уголовная ответственность за клевету // Законодательство. 1999. № 11. С. 62–70.

11. Шмарион В. И. Ответственность за преступления против чести и достоинства личности по российскому уголовному законодательству : дис. ... канд. юрид. наук. Ростов-на-Дону, 2001.

12. Энциклопедия уголовного права. Т. 14. Преступления против свободы, чести и достоинства личности. СПб. : ГКА, 2010.

13. Digital 2021: главная статистика по России и всему миру // Spark.ru. URL: https://spark.ru/user/115680/blog/74085/digital-2021-glavnaya-statistika-po-rossii-i-vsemu-miru.

Шемчук С. Ю.[1],
командир отделения 191 учебного взвода
Московского областного филиала
Московского университета МВД России
имени В.Я. Кикотя

Раненкова Е. А.[2],
старший преподаватель
кафедры уголовного права и криминологии
Московского областного филиала
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук

К ВОПРОСУ ПРАВОВОЙ ОЦЕНКИ ДЕЯТЕЛЬНОСТИ ЛИЦ, ВОВЛЕЧЕННЫХ В ДВИЖЕНИЕ «КОЛУМБАЙН (СКУЛШУТИНГ)»

В конце мая 2022 г. совершено самое крупное массовое убийство в Соединенных Штатах Америки за последние десять лет – в штате Техас местный житель открыл стрельбу по ученикам начальной школы. В списке погибших 21 человек, большинство – маленькие дети. Вооруженное нападение совершил 18-летний юноша С. Рамос [1]. В России за последнее время известны случаи нападения на школу в Бурятии, в Отрадном, на колледж Благовещенска, а также массовые убийства «Керченского» и «Ивантеевского» стрелков. Это лишь самые громкие примеры явления, которое в средствах массовой информации (далее – СМИ) получило название «Скулшутинг» или «Колумбайн», в России принято называть его «стрельбой в образовательных учреждениях» [2]. В данной статье нами одинаково будут использоваться три этих термина.

Обозначим наиболее характерные черты стрельбы в образовательных организациях, чтобы раскрыть сущность этого феномена:

1. В отличие от убийств в рамках межличностного конфликта «Скулшутинг» – неперсофиницированный акт насилия, т. е. стрелок конкретных жертв не выбирает, хотя какая-либо личность все-таки может быть в его списке, в частности, речь идет о мотиве мести за предшествующие данному деянию издевательства со стороны жертвы и прочее [3].

2. «Колумбайн» – это не серийные убийства, так как представляет собой единичный акт, осуществляющийся в рамках определенного периода. Он реализуется по шаблону, то есть осуществляется в определенной одежде, в определенном порядке и с некой наигранностью в целях «пиара» самого стрелка, пусть даже посмертно. Важно отметить, «Скулшутинг», как правило, оканчивается суицидом стрелка, то есть стрелки, никогда не планируют отступление, они не ду-

[1] © Шемчук С. Ю., 2022.
[2] © Раненкова Е. А., 2022.

мают о том, как будут скрываться от правоохранительных органов, а прямо заявляют о самоубийстве, но уйти из жизни им хочется максимально громко, забрав с собой наибольшее количество жертв.

3. Современные информационные технологии – основной канал вовлечения несовершеннолетних в «Скулшутинг», который на данный момент изучен недостаточно и контролируется в малой степени. К каналам передачи информации о данной криминальной субкультуре можно отнести: мессенджеры WhatsApp, Viber, Skype, Telegram, Facebook, Messenger и другие; социальные сети: «Вконтакте», «Одноклассники», а также видеохостинг: «YouTube», что свидетельствует о масштабном овладении деструктивной субкультурой как реального, так и виртуального пространства. Так, нами был осуществлен поиск в социальной сети «Вконтакте» по наиболее простому запросу в рамках идеологии стрельбы в образовательных учреждениях «Клиборд» и «Харрис». Результаты поиска: «Клиболд» – 98 пользователей, использующих в качестве никнейма (от англ. «*nickname*» – сетевое имя, используемое в сети Интернет) данную фамилию, «Эрик Харрис» – восемь пользователей и по запросу «Харрис» – более 40 тыс. человек (однако в это число входят пользователи, реальное имя которых поисковик посчитал за фамилию известного стрелка) [4].

Важно подчеркнуть, именно посредством интернет-пространства школьные стрелки «предупреждают» о своих намерениях и «делятся» задуманным с подписчиками. Возьмем хотя бы крайний случай «Скулшутинга» – ранее упомянутый нами Техасский колумбайнер С. Рамос. За несколько дней до убийства он опубликовал фото винтовки на своем аккаунте (от англ. «*account*» – учетная запись или профиль пользователя в социальной сети) в Instagram (запрещен в Российской Федерации (далее – РФ)), а также персонально отправил данную публикацию одному из одноклассников. И это далеко не исключение, подобным образом поступали стрелки из России (Росляков, Галявиев и др.) [5].

Обозначенные характерные черты отражают высокую степень общественной опасности вооруженных нападений на образовательные учреждения в России. Именно поэтому, для правоохранительных органов, равно как и для самих учебных заведений, сокращение количества случаев «Скулшутинга» является первоочередной задачей. К тому же еще не сложилась в достаточной мере система превентивных мер противодействия данному социальному феномену, а в науке отсутствует единый подход разъяснения проблемных вопросов.

Более того, 2 февраля 2022 г. Верховный Суд Российской Федерации (далее – ВС РФ) признал молодежное движение «Колумбайн (Скулшутинг)» террористической организацией, что в свою очередь автоматически привело к пополнению единого списка террористических организаций, признанных такими на территории нашего государства [6]. Данные законодательные новшества, на наш взгляд, не в полной мере внесли ясность в решение спорных моментов по проблеме противодействия стрельбе в образовательных организациях. Так, не совсем понятно, какую именно организацию ВС РФ признал террористической, ведь «Колумбайн» – это идеология, под влиянием которой стрелки-одиночки совершают нападения на образовательные учреждения. Характерной уголовно-правовой

чертой понятия «преступная организация» является ее структурная составляющая: некая совокупность людей, объединяющихся под эгидой единой цели, осуществляющих свою совместную преступную деятельность для достижения единого результата.

Стрельба в образовательных организациях осуществляется, как правило, одним лицом. Исключение, когда стрелков несколько, примером чего является нападение Эрика Харриса и Дилана Клиболда 20 апреля 1999 г. на школу в штате Колорадо [7]. Однако М. А. Стародубцева, А. П. Пинчук и А. В. Кулаевский полагают: «Рост предотвращенных террористических актов и актов кибертерроризма, всплеск случаев «Скулшутинга», активизация националистских и террористических организаций – все это звенья одной цепи. В деструктивные организации сейчас вербуют не религиозных фанатиков, а подростков, легко поддающихся влиянию кураторов в социальных сетях [8].

Следующий проблемный аспект, который отмечается нами на теоретическом уровне – отсутствие законодательного закрепления термина «Скулшутинг» или «Колумбайн». Безусловно, в научных кругах предпринимаются попытки дать собственное определение этому феномену, однако большое множество подходов не позволяет выработать единое понятие [9]. Представляется, что официальное закрепление понятия термина «Колумбайн» смогло бы разрешить противоречия, которые возникают вокруг данного явления, однозначно определить его криминологические и уголовно-правовые аспекты, а, следовательно, разработать пути для снижения масштабов его проявления.

Цель террористической деятельности и стрельбы в образовательной организации не в полном объеме совпадает – это еще одна проблема правовой оценки деятельности лиц, вовлеченных в молодежное движение «Колумбайн». Террористическим актом согласно ч. 1 ст. 205 Уголовного кодекса Российской Федерации (далее – ч. 1 ст. 205 УК РФ) признается: «Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений…», а действия стрелка направлены на устрашение населения, вызов общественного резонанса, а также месть и поиск личной славы. Для него нападение представляет собой некое театральное действие, в ходе которого он выражает свое недовольство обществом, системой, образованием.

Возвращаясь к рассмотренным выше проблемным аспектам, предлагаем внесение изменений в законодательство Российской Федерации в части дополнения понятийного аппарата термином «Колумбайн (Скулшутинг)» и даем авторское определение: «малопрогнозируемый противоправный акт, выражающийся в вооруженном нападении (с применением любого вида оружия; предметов, используемых в качестве оружия; а также различных взрывчатых веществ) лица (лиц) на образовательные организации, с целью причинения вреда жизни и здоровью неопределенному количеству лиц».

С учетом признания молодежного движения «Колумбайн (Скулшутинг)» террористической организацией, в целях привлечения к ответственности лиц, организующих деятельность таких террористических сообществ и участвующих в подобной деятельности, предлагаем внести изменения в определение понятия «террористический акт», а именно в ч. 1 ст. 205 УК РФ и изложить его в следующей редакции: «Совершение взрыва, поджога, вооруженного нападения или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а равно в целях дестабилизации функционирования организаций, осуществляющих образовательную деятельность путем реализации масштабных насильственных акций, а также угроза совершения указанных действий». Таким образом, субъективная сторона преступления, предусмотренного ч. 1 ст. 205 УК РФ, будет охватывать цель, преследуемую скулшутером в рамках реализации своего преступного намерения.

Подводя итог, следует отметить, что проблема вооруженных нападений на образовательные учреждения не теряет своей актуальности. В целях ограничения распространения идеологии «Колумбайн», в том числе и посредством сети Интернет, внесены изменения в законодательство, согласно которым международное движение «Колумбайн (Скулшутинг)» признано террористической организацией, запрещенной на территории России. Однако субъективная сторона состава преступления, предусмотренного ст. 205 УК РФ в действующей редакции, не в полной мере соответствует составу общественно опасного деяния, совершаемого в рамках «Скулшутинга». В статье нами был предложен один из возможных путей решения данного противоречия.

Список литературы

1. URL: tass.ru›Происшествия›14718423.

2. Шемчук С. Ю. От травли до расстрела: как предотвратить насилие в образовательных организациях // Уголовное судопроизводство по делам несовершеннолетних и ювенальная юстиция: проблемы и перспективы развития (правовые, социальные и психолого-педагогические аспекты) : сборник статей. Руза : ИП «Коняхин Александр Викторович», 2021. С. 187.

3. Раненкова Е. А., Шемчук С. Ю. К вопросу защиты жизни детей в российских школах // Уголовно-правовая охрана конституционных прав и свобод граждан, суверенитета и территориальной целостности Российской Федерации : сборник научных трудов. М. : Московский университет МВД России имени В.Я. Кикотя, 2021. С. 274.

4. Российская социальная сеть «ВКонтакте». URL: https://vk.com/.

5. «Круто было бы устроить бойню»: керченский стрелок рассказывал друзьям о своих планах атаки на колледж. URL: https://www.kp.ru/-daily/26896/3940895/ ; «Я как Бог». 19-летний стрелок из Казани опубликовал

«манифест» в интернете. URL: https://anews.com/136497213-ja-kak-bog-19-letnij-strelok-iz-kazani-opublikoval-manifest-v-internete.html.

6. Верховный Суд Российской Федерации признал «Колумбайн» террористической организацией. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=70034347 ; Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими. URL: http://-www.fsb.ru/fsb/npd/terror.htm.

7. URL: ru.wikipedia.org›Массовое убийство в школе «Колумбайн».

8. Стародубцева М. А., Пинчук А. П., Кулаевский А. В. Кибертерроризм как фактор угрозы национальной безопасности России // Юридическая наука. 2022. № 3. URL: https://cyberleninka.ru/article/n/kiberterrorizm-kak-faktor-ugrozy-natsionalnoy-bezopasnosti-rossii.

9. Пучнин А. В., Пучнина М. Ю. Идеология «колумбайн» как экстремистская и террористическая угроза национальной безопасности Российской Федерации // Общество и право. 2021. № 2 (76) ; Чунин А. С. Феномен скулшутинга в современной России. Правовой аспект // Обзор. НЦПТИ. 2020. № 3 (22).

Мухамеджанова А. Д.[1]*,*
научный сотрудник Центра по исследованию
проблем уголовной политики и профилактики преступности
НИИ Карагандинской академии
МВД Республики Казахстан
имени Б. Бейсенова,
магистр юридических наук

ОНЛАЙН-КРЕДИТОВАНИЕ КАК ЧАСТНЫЙ СЛУЧАЙ ИНТЕРНЕТ-МОШЕННИЧЕСТВА В РЕСПУБЛИКЕ КАЗАХСТАН

Мошенники – элита криминального мира, цель которых завладеть чужим имуществом обманным путем, не прибегая к использованию насилия, угроз и оружия против жертвы. Обманутая жертва сама передает свое имущество или права на него мошенникам, не подозревая о совершении противоправных деяний против нее [1].

Однако такие обстоятельства совершения мошенничества присущи классической форме мошенничества, когда злоумышленник вступает в прямой контакт с потерпевшим. Современные реалии таковы, что с развитием информационных технологий мошенничество плавно перетекло в сеть Интернет, где не только не требуется наличие прямого контакта с потерпевшим, но и возможно причинение материального ущерба путем обмана третьих лиц, не являющихся ни собственниками, ни иными владельцами имущества.

К такому виду интернет-мошенничеств относятся преступные действия по незаконному оформлению онлайн-кредитов. В последние годы, проблемы предупреждения, квалификации и расследования данных фактов все чаще освещаются многими учеными [2; 3; 4; 5], что, несомненно, подтверждает актуальность данной тематики.

В виду повсеместной цифровизации, внедрения мобильных приложений для совершения оплаты, а также в связи со сложившейся эпидемиологической ситуацией в мире (распространение COVID-19), в последние годы стали набирать обороты финансовые онлайн-операции. При этом большинство сайтов и приложений, на которых пользователи производят оплату, являются небезопасными. К примеру, не так давно, было совершено преступное посягательство на персональные данные пользователей интернет-магазина WILDBERRIES [6], который хранит не только анкетные данные покупателей, но также их адреса проживания, мобильные телефоны, номера платежных карт и т. д.

Несмотря на то, что повсеместно принимаемые на постоянной основе организационные меры, направленные на борьбу с киберпреступлениями, совершенствуются из года в год [7], ориентируясь на каждый новый способ совершения кибер-мошенничества, на наш взгляд, уголовное законодательство, регламенти-

[1] © Мухамеджанова А. Д., 2022.

рующее ответственность за совершение того или иного вида интернет-мошенничества, также должно соответствовать современным реалиям и отвечать нуждам правоприменительной практики.

Вместе с тем, анализ уголовного законодательства Республики Казахстан позволил выявить некоторые пробелы, касающиеся привлечения к ответственности лиц, совершающих хищения денежных средств посредством использования сети интернет, путем незаконного оформления онлайн-кредитов на третьих лиц.

Следует отметить, что ответственность за мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы, предусмотрена в п. 4 ч. 2 ст. 190 Уголовного кодекса Республики Казахстан (далее – УК РК) [8]. Однако, на наш взгляд, обман, составляющий объективную сторону рассматриваемого деяния, с учетом действующих реалий, должен толковаться немного иначе в случаях применения его с целью незаконного оформления онлайн-кредитов.

Таким образом, в целях обоснования авторской позиции, необходимо рассмотреть особенности интернет-мошенничеств, связанных с незаконным оформлением онлайн-кредитов.

Первой особенностью рассматриваемых деяний является то, что имущество, на которое посягает мошенник, является собственностью банка или кредитной организации, выдающей кредит. Денежные средства не принадлежат лицу, на которого мошенник оформляет онлайн-кредит, они являются собственностью юридического лица, а значит в данном случае, обман всегда производится в отношении лица, не являющегося собственником или владельцем имущества. Обман в данном случае может быть направлен:

1) на лицо, выступающее кредитополучателем, чьи анкетные данные используются для оформления онлайн-кредита;

2) на сотрудника банка, осуществляющего определенный ряд действий в интернет-системе банкинга для оформления кредита;

3) на программу интернет-банкинга, без какого-либо контакта с физическими лицами (путем взлома системы, ее обмана путем введения ложных или недостоверных сведений и т. д.).

Вместе с тем, в Нормативном постановлении Верховного Суда Республики Казахстан «О судебной практике по делам о мошенничестве» (далее – НПВС) указывается, что обман должен быть направлен на собственника или иного владельца имущества [9], что не подпадает под признаки объективной стороны интернет-мошенничеств, связанных с оформлением онлайн-кредитов.

Также в НПВС содержится оговорка, что в исключительных случаях обман может быть направлен на лицо, не являющее собственником или иным владельцем имущества, к примеру – он может быть направлен на сотрудника банка, но лишь в случае безвозмездного обращения лицом в свою пользу или в пользу других лиц денежных средств, находящихся на счетах в банках (п. 13). Данный

случай также не подпадает под признаки рассматриваемых видов интернет-мошенничеств, но доказывает, что при мошенничестве обман может быть направлен не только на собственника или иного владельца имущества.

Вторая особенность рассматриваемых деяний заключается в том, что в случаях обмана представителя банка или кредитной организации, или в случаях обмана самой системы, с точки зрения положений УК РК и НПВС, деяние (незаконное оформление онлайн-кредита) нельзя квалифицировать как интернет-мошенничество, поскольку диспозиция п. 4 ч. 2 ст. 190 УК РК и п. 9 НПВС четко обозначают, что обман должен быть направлен на пользователя информационной системы, который является собственником или владельцем имущества. Кроме того, в п. 9 НПВС обозначается способ действий интернет-мошенника, а именно - деяние должно совершаться путем размещения в информационной системе заведомо недостоверных сведений или программ. В случае незаконного оформления онлайн-кредита, интернет-мошенник не размещает в информационной системе никаких недостоверных сведений или программ, а просто использует персональную информацию кредитополучателя или же использует специальные программы для взлома приложений интернет-банкинга.

Таким образом, рассмотренные выше особенности незаконного оформления онлайн-кредита показывают, что в такого рода мошеннических действиях обман имеет совершенно иные признаки, отличающиеся от традиционного обмана, применяемого в традиционных видах мошенничества [10; 11], а лицо, в отношении которого совершается обман не всегда является пользователем информационной системы и одновременно владельцем или собственником имущества.

Все вышеуказанные действия мошенника осуществляются посредством использования возможностей сети интернет, но такие действия, к сожалению, не подпадают под объективную сторону деяния, предусмотренного п. 4 ч. 2 ст. 190 УК РК, что может вызвать трудности при квалификации рассматриваемых деяний.

Согласно действующему уголовному законодательству, если рассмотренные факты не подпадают под объективную сторону деяния, предусмотренного п. 4 ч. 2 ст. 190 УК РК, то их следует квалифицировать по совокупности ст.ст. 190, 205 УК РК. Однако, следует отметить, что в таком случае правоприменительная практика лишится необходимых показателей, учитываемых при оценке оперативной обстановки по делам об интернет-мошенничествах. В этой связи, необходимость совершенствования п. 4 ч. 2 ст. 190 УК РК обусловлена несколькими обстоятельствами:

1. Все данные о мошенничествах, совершенных с использованием сети-интернет формируются в единую статистику, с целью изучения причин и условий их совершения, выработки единых мер профилактики и предупреждения.

2. Исходя из данных правовой статистики, для оценки оперативной обстановки в области совершения интернет-мошенничеств, используется отдельная графа, введенная для расчета в 2018 г. Данная графа позволяет не только анализировать криминологический портрет интернет-мошенника, но

и сравнивать отдельно ущерб, причиненный традиционными видами мошенничеств и интернет-мошенничествами, причины прекращения и прерывания сроков досудебных расследований и т. д.

В этой связи, совершенствование пункта 4 ч. 2 ст. 190 УК РК с учетом указанных выше обстоятельств, позволит минимизировать факты неверной квалификации интернет-мошенничеств, совершаемых путем оформления онлайн-кредитов и позволит анализировать данные деяния с другими интернет-мошенничествами в единой статистике. Изучение причин совершения всех способов интернет-мошенничеств отдельно от традиционных видов мошенничеств представляется не только целесообразным, но и более значимым не только для организации профилактической деятельности, но и в целом для правоприменительной практики.

На основании вышеизложенного, возникает необходимость совершенствования уголовного законодательства с целью предоставления возможности своевременного реагирования на вновь возникающие преступные схемы интернет-мошенничеств.

Так, предлагаем признавать интернет-мошенничеством не только мошенничество, осуществляемое посредством обмана пользователя информационной системы, или осуществляемое путем размещения в информационной системе заведомо недостоверных сведений или программ, но и в целом совершение обманных действий с использованием сети интернет и информационных технологий (компьютера, компьютерных программ, мобильных приложений, сотового телефона и т. п.).

Также необходимо внести изменения в НПВС, относительно направленности обмана при совершении интернет-мошенничеств, связанных с оформлением онлайн-кредита, а именно, следует учитывать, что при незаконном оформлении онлайн-кредита, обман может быть направлен как на кредитополучателя, так и на представителя банка или кредитной организации.

В этой связи, предлагаем следующее:

1. Пункт 4 ч. 2 ст. 190 УК РК изложить в следующей редакции: «путем обмана или злоупотребления доверием пользователя информационной системы или с использованием сети интернет и информационных технологий».

2. Пункт 9 НПВС изложить в следующей редакции: «под мошенничеством, совершенным путем обмана или злоупотребления доверием пользователя информационной системы или с использованием сети интернет и информационных технологий следует признавать действия виновного, направленные на завладение имуществом или правом на имущество пользователя информационной системы или на имущество юридического лица, совершенные с использованием сети интернет или посредством информационных технологий (компьютера, компьютерных программ, сотового телефона и т. п.), или путем размещения в информационной системе заведомо недостоверных сведений или программ, с целью реализации его преступного умысла на обман пользователя посредством Qiwi-кошелька, интернет-банкинга и т. д.

Таким образом, предложенные меры, на наш взгляд будут способствовать совершенствованию законодательства и правоприменительной практики в вопросах квалификации интернет-мошенничества, связанного с незаконным оформлением онлайн-кредитов, в результате чего с учетом специфики совершенного уголовного правонарушения, деяние получит должную правовую оценку, а назначенное наказание будет соответствовать принципу уголовного права – справедливости.

Список литературы

1. Юрочкин Н. С. Кибермошенничество: характеристика, приемы и методы его совершения // Таврический научный обозреватель. 2016. № 12-2 (17). С. 156–159.

2. Любивый Н. Ю. Кредитное мошенничество юридических лиц и меры противодействия // Проблемы анализа риска. 2013. Т. 10. № 3. С. 74–87.

3. Ивашкина Е. А. Динамика преступлений в финансово-кредитной сфере на примере мошенничества в сфере кредитования // Инновации. Наука. Образование. 2021. № 31. С. 707–711.

4. Колбаса Д. Ю. Предупреждение мошенничеств, совершаемых в сети интернет // Цифровые трансформации в развитии экономики и общества : сборник статей. В 4-х т. Воронеж, 2021. С. 277–281.

5. Романов А. А., Машлякевич В. А. О современных способах мошенничеств, совершаемых с использованием средств мобильной связи // Евразийский юридический журнал. 2021. № 10 (161). С. 254–255.

6. Информационный интернет-ресурс «АСТВ.РУ». URL: https://astv.ru/news/-society/2022-03-16-sboj-v-wildberries-chto-na-samom-dele-proizoshlo-i-kogda-vse-zarabotaet.

7. Информационный интернет-ресурс «КазИнформ». URL: https://www.inform.kz/ru/kakie-mery-predprinimayutsya-v-kazahstane-po-bor-be-s-kiberprestupnost-yu_a3865334.

8. Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V (с изменениями и дополнениями по состоянию на 02.03.2022)// Опубликован: «Казахстанская правда» от 9 июля 2014 г. № 132 (27753). URL: https://online.zakon.kz/document/?doc_id=31575252#sub_id=0.

9. Нормативное постановление Верховного Суда Республики Казахстан от 29 июня 2017 г. № 6 «О судебной практике по делам о мошенничестве» // Казахстанская правда. 2017 № 142 (28521). 27 июля. URL: https://adilet.zan.kz/rus/-docs/P170000006S.

10. Овсюков Д. А. Электронная форма совершения обмана при посягательствах на собственность с использованием информационно телекоммуникационных сетей // Вестник современных исследований. 2018. № 10.4 (25). С. 26–28.

11. Капустина Е. Мошенничество в сфере денежного обращения, кредита и банковской деятельности: современное состояние и квалификация // Вестник Тамбовского университета. 2009. № 8 (76). С. 401–404.

Молбасин С. И.[1],
научный сотрудник Центра по исследованию
проблем уголовной политики и профилактики преступности
НИИ Карагандинской академии
МВД Республики Казахстан
имени Б. Бейсенова,
магистр юридических наук

К ВОПРОСУ ОБ ОПРЕДЕЛЕНИИ ТЕРРИТОРИАЛЬНОЙ ПОДСЛЕДСТВЕННОСТИ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ДЕЛ О МОШЕННИЧЕСТВАХ, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, В РЕСПУБЛИКЕ КАЗАХСТАН

Информационные технологии, мобильные коммуникации, онлайн-сервисы глубоко внедряются во все сферы социальной деятельности, экономики, производства, здравоохранения, образования.

Преступность как социальное явление не остается в стороне. В последние годы наблюдается ее глубокая трансформация. Резко увеличилось количество преступлений, совершаемых с использованием цифровых технологий.

Согласно официальным статистическим данным по мошенничествам, совершенным путем обмана или злоупотребления доверием пользователя информационной системы (п. 4 ч. 2 ст. 190 Уголовного кодекса Республики Казахстан), в 2019 г. в Казахстане зарегистрировано 7769 преступлений. В 2020 г. этот показатель составил 14155 преступлений, что на 1,8 раза больше прошлогоднего показателя. В 2021 г. совершено 21405 мошенничеств с применением информационно-коммуникационных технологий (на 1,5 раза больше по сравнение с прошлогодними показателями). За 4 месяца 2022 г. уже совершено 6256 преступлений [1].

Таблица 1

	2019	2020	2021	за 4 месяца 2022 г.
Мошенничество путем обмана или злоупотребления доверием пользователя информационной системы (п. 4 ч. 2 ст.190 УК РК)	7769	14155	21405	6256

Цифровая преступность сегодня, ее масштабы и темпы распространения – это глобальный вызов безопасности наших государств и всего международного сообщества.

[1] © Молбасин С. И., 2022.

Специфика данного вида преступности создает определенные сложности при их расследовании. Так, одним актуальных в теории и практике расследования преступлений, связанных с мошенничествами, совершаемыми с применением информационно-коммуникационных технологий, является вопрос о территориальной подследственности уголовных дел по ним. Данная проблема присуще для уголовного судопроизводства многих государств. В силу особенностей совершения данных мошенничеств – а именно способа их совершения (с использованием интернета), нахождения потерпевшего и подозреваемого в разных городах или государствах, вопрос об определении территориальной подследственности уголовных дел по рассматриваемой категории мошенничеств стал объектом обсуждения ученых и практических работников.

В целом в уголовно-процессуальной науке вопросам правильного определения подследственности уделяется особое внимание. Так, А. А. Савина и В. В. Торопова отмечают, что определение территориальной подследственности уголовных дел играет значимую роль в расследовании преступлений [2, с. 119–122]. По мнению Н. В. Ковалевской, соблюдение правил, установленных действующим уголовно-процессуальным законодательством о подследственности, повышает качество расследования уголовных дел [3, с. 25].

Неоднозначность практики в данном вопросе приводит к затягиванию сроков досудебного производства, порой передача уголовных дел по подследственности с одного территориального подразделения органов внутренних дел в другой может занять значительное времени. Как отмечает С. В. Ревякин, «вопрос об определении места производства предварительного расследования по уголовным делам о телефонных мошенничествах не получил однозначного понимания в практике органов внутренних дел…». Автор указывает, что это положение привело к необоснованному неоднократному направлению соответствующих доследственных материалов из одного территориального подразделения органов внутренних дел в другое, что, в свою очередь, затягивает сроки проверки, приводит к утрате следов преступления и позволяет виновным уйти [4, с. 29].

В научной литературе приводятся различные мнения по поводу определения территориальной подследственности данной категории уголовных правонарушений. К примеру, Р. Р. Хасанов, анализируя правоприменительную практику следственных подразделений органов внутренних дел, особо акцентирует внимание на вопросе об определении территориальной подследственности в зависимости от места окончания преступления. При этом, учитывая специфику интернет-мошенничеств (нахождение потерпевшего и преступника в разных местах), автор рассматривает несколько вариантов места окончания данного преступления:

1) по месту нахождения потерпевшего;

2) по месту нахождения преступника;

3) по месту нахождения отдела полиции, куда обратится потерпевший;

4) по месту нахождения оборудования, с которого преступник имеет доступ к электронному счету;

5) по месту регистрации электронного счета;

6) по месту, где были обналичены похищенные денежные средства [5, с. 151].

Российские исследователи А. А. Ларинков и В. А. Шиплюк, на основе мнения ряда ученых-процессуалистов, также приводят разные версии определения территориальной подследственности преступлений, совершенных с применением информационно-коммуникационных технологий [6, с. 145–146]. Так, согласно их исследованиям, существуют следующие научные версии определения данного вопроса:

1. Местом окончания мошенничества является то место, из которого перечислены денежные средства потерпевшим, так как именно в этом месте для него наступили вредные последствия… [7, с. 51–53]. Иными словами, это место нахождения потерпевшего.

2. При определении места производства предварительного расследования следует исходить из принципа целесообразности, поэтому преступления с материальным составом вполне допустимо расследовать в том субъекте Российской Федерации (или районе, муниципальном образовании и т. д.), где непосредственно совершались действия, вне зависимости от того, что последствия наступили в другом месте. Если же место совершения преступления установить не представляется возможным, то предварительное расследование должно производиться по месту непосредственного обнаружения преступления или по месту наступления последствий уголовно наказуемого деяния [8, с. 37–39].

3. Решение вопроса о возбуждении уголовного дела территориальным органом, принявшим заявление. При установлении в ходе производства предварительного расследования точного места совершения преступления за пределами подведомственной территории (после производства неотложных следственных действий) необходимо направить уголовное дело (но не материалы доследственной проверки, как это часто практикуется) по подследственности в порядке, установленном ст. 152 УПК РФ [9, с. 51–53].

4. Обман доверчивого гражданина происходит во время телефонного разговора злоумышленника с потерпевшим, местом совершения этого преступления, а, следовательно, и местом предварительного расследования, является место нахождения злоумышленника независимо от места перечисления пострадавшим денежных средств и места зачисления их на счет виновного (завладения ими злоумышленником) [10, с. 43–44].

Таким образом, мы видим, что вариантов определения места окончания мошенничеств, совершаемых с применением информационно-коммуникационных технологий, в уголовно-процессуальной науке великое множество. Безусловно, такое разнообразие мнений порождает неопределенность в вопросе определения территориальной подследственности по уголовным делам данной категории.

Указанная проблема характерна и для досудебного производства Казахстана. Действующее законодательство не дает четкого определения по вопросу регламентации территориальной подследственности уголовных дел по указанному виду мошенничеств. Так, п. 1 ст. 188 УПК РК устанавливает, что досудебное расследование должно производиться в том районе (области, городе республиканского значения, столице), где совершено уголовное правонарушение. Кроме

того, п. 2 указанной статьи устанавливает возможность производить расследование по месту обнаружения уголовного правонарушения, а также по месту нахождения подозреваемого или большинства свидетелей. Таким образом, законодатель предусмотрел три варианта расследования уголовных дел по территориальности:

- место совершения правонарушения;
- место обнаружения правонарушения;
- место нахождения подозреваемого и свидетелей.

В случае определения территориальной последственности данных уголовных правонарушений по месту их совершения, возникает логический вопрос «где данное преступление считается оконченным?». Касательно этого вопроса в п. 14 Нормативного постановления Верховного Суда Республики Казахстан от 29 июня 2017 г. № 6 «О судебной практике по делам о мошенничестве» [11], указано, что «с момента зачисления денег на банковский счет в результате мошенничества лицо приобретает возможность распоряжаться ими, и преступление следует считать оконченным с момента зачисления этих средств на его счет». Исходя из данного положения, сложно установить место совершения преступления, так как в нем говорится лишь о моменте окончания преступления. Так как деньги перечисляются в виртуальной среде сложно определить, где было окончено преступление – по месту перечисления денежных средств (место нахождения потерпевшего) или по месту нахождения подозреваемого. В практической деятельности органов досудебного расследования сложилось правило признания местом окончания преступления место снятия денежных средств, добытых преступным путем. К такому выводу мы пришли на основе изучения материалов уголовных дел, находящихся в производстве в следственных подразделениях органов внутренних дел Республики Казахстан.

Как показывает практика, в основном преступники обналичивают денежные средства по месту своего проживания. Соответственно досудебное расследование проводится по указанной геолокации. При этом нередки случаи, когда расследование проводится и по месту жительства потерпевшего, по которому они обратился в полицию с заявлением.

При расследовании мошенничества, совершенного с применением информационно-коммуникационных технологий, по месту нахождения потерпевшего есть ряд преимуществ. Во-первых, сложно представить расследование данного преступления по месту снятия денежных средств, в случаях их перевода в зарубежный банк. Во-вторых, расследование по месту нахождения потерпевшего удобно для него самого. В данном случае его интересы полностью учитываются, потерпевший имеет возможность непосредственно участвовать в досудебном производстве. К примеру, в производстве Следственного отдела Управления полиции г. Караганды находилось уголовное дело по п. 4 ч. 2 ст. 190 УК РК в отношении гр. М, жителя г. Костанай, совершившего мошеннические действия с использованием информационных систем в отношении гр. К, жителя г. Караганды. Подозреваемый гр. М на момент задержания находился в г. Алма-Аты, где и успел обналичить денежные средства, добытые преступным путем. В данном случае расследование было начато в г. Караганды по месту подачи заявления.

С точки зрения вышеперечисленных преимуществ расследование данного уголовного дела в указанном городе вполне логично. Однако при изучении приведенного примере выяснились некоторые дополнительные обстоятельства. Как оказалось, подозреваемый гр. М наряду с этим совершил мошеннические действия и в отношении жителей других городов Казахстана. Соответственно все эти уголовные дела согласно ст. 43 УПК Республики Казахстан подлежат соединению в одно производство. В связи с этим возникает вопрос, где в данной ситуации должно расследоваться соединенное уголовное дело – по месту, где было подано заявление и начато досудебное производство (г. Караганды) или по месту нахождения подозреваемого при его задержании (г. Алма-Аты).

Как следует из приведенного примера, в практической деятельности органов досудебного расследования могут возникнуть разные ситуации при расследовании мошенничеств, совершенных с применением информационно-коммуникационных технологий. Анализ правоприменительной практики органов досудебного расследования показал, что по вопросу об определении территориальной подследственности этого вида мошенничеств нет единой практики, рассматриваемый вопрос может решаться исходя из конкретной ситуации.

На основании анализа научной литературы, действующего законодательства Республики Казахстан и сложившейся правоприменительной практики предлагается унифицировать порядок определения территориальной подследственности расследования уголовных дел по мошенничествам, совершенных с применением информационно-коммуникационных технологий и включить п. 14-1 в Нормативное постановление Верховного Суда Республики Казахстан от 29 июня 2017 г. № 6 «О судебной практике по делам о мошенничестве» в следующей редакции:

«14-1. В случае, если потерпевший по уголовному делу о мошенничестве с использованием информационных систем один или потерпевших несколько и все они находятся в одном регионе (городе) – расследование следует производить по месту нахождения потерпевшего (потерпевших) или по месту его (их) обращения в полицию.

В случае, если потерпевших по уголовному делу о мошенничествах с использованием информационных систем, несколько и их преимущественное большинство находится в одном регионе (городе) – расследование следует производить по месту нахождения большинства потерпевших или по месту их обращения в полицию.

В случае, если потерпевших по уголовному делу о мошенничествах с использованием информационных систем, несколько и они находятся в разных регионах (городах) – расследование следует производить по месту нахождения или задержания подозреваемого».

Полагаем, что данная мера позволит четко регламентировать вопрос о территориальной подследственности при расследовании уголовных дел о мошенничествах, совершенных с применением информационно-коммуникационных технологий, в Республике Казахстан. В свою очередь единообразная регламентация данного вопроса позволит исключить случаи необоснованного

неоднократного направления материалов уголовных дел из одного территориального подразделения органов внутренних дел в другое. На наш взгляд – это обстоятельство повысить качество расследования уголовных дел рассматриваемой категории и обеспечить защиту прав и свобод потерпевших.

Список литературы

1. Форма отчета № 1-М «О зарегистрированных уголовных правонарушениях» за 2019-2022 гг. Информационный сервис Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан // URL: https://qamqor.gov.kz/crimestat/statistics.

2. Савина А. А., Торопова В. В. Проблема определения территориальной подследственности уголовных дел // Новая наука: история становления, современное состояние, перспективы развития : сборник статей. Уфа : ООО «Аэтерна», 2019. С. 119–122.

3. Ковалевская Н. В. Соблюдение правил подследственности уголовных дел // Вестник ОГУ. 2014. № 3 (164). С. 24–28.

4. Ревякин С. В. Проблемы раскрытия хищений, совершаемых посредством современных электронных средств коммуникации // Правопорядок: история, теория, практика. 2018. № 3 (18). С. 27–32.

5. Хасанов Р. Р. Определение территориальной подследственности по уголовным делам о мошенничествах в социальной сфере: проблемы практики // Вестник экономики, права и социологии. 2015, № 1. С. 151–154.

6. Ларинков А. А., Шиплюк В. А. Проблемы определения места производства предварительного расследования преступлений, совершаемых с использованием сети Интернет, средств сотовой связи и систем дистанционного банковского обслуживания // Российский журнал правовых исследований. 2017. № 2 (11). С. 144–150.

7. Фрост С., Федосов А. Проблемы определения места расследования мошенничества с использованием электронных форм платежей // Законность. 2015. № 1. С. 51–53.

8. Тимошенко Ю. А. Место совершения преступления: уголовно-правовой и процессуальный аспекты // Законность. 2015. № 7. С. 37–39.

9. Францифиров Ю. В. Определение места совершения телефонного мошенничества // Законность. 2016. № 2. С. 51–53.

10. Лукинов А. Место расследования телефонного мошенничества // Законность. 2014. № 9. С. 43–44.

11. Нормативное постановление Верховного Суда Республики Казахстан от 29 июня 2017 г. № 6 «О судебной практике по делам о мошенничестве». URL: //https://adilet.zan.kz/rus/docs/P170000006S.

Копаева Ю. Ю.[1],
следователь по особо важным делам
второго отдела по расследованию особо важных дел
(о преступлениях против государственной власти
и в сфере экономики)
следственного управления
Следственного комитета Российской Федерации
по Тамбовской области

ПРОБЛЕМЫ КВАЛИФИКАЦИИ И ДОКАЗЫВАНИЯ ИСТЯЗАНИЙ НЕСОВЕРШЕННОЛЕТНИХ С ПРИЧИНЕНИЕМ ПСИХИЧЕСКИХ СТРАДАНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Семья – это основная сфера жизни и развития любого ребенка. Атмосфера в семье напрямую влияет на мироощущение, самооценку, реакцию детей на все, что происходит с ними ежедневно, именно в семье формируется мировосприятие каждого конкретного нового члена социума, в связи с чем можно сделать вывод, что от внутреннего семейного климата зависит вся его дальнейшая жизнь, в том числе и в период, когда он станет взрослым и самостоятельным участником общественных отношений.

В данной статье особое внимание уделено ответственности за совершение истязаний несовершеннолетних с причинением им психических страданий, так как данный вид преступлений обладает высоким уровнем латентности, что, в свою очередь, порождает множество различных проблем как в квалификации преступного деяния, так и в доказывании его события. Особе внимание уделено видам истязаний несовершеннолетних, которые совершаются с использованием информационно-телекоммуникационной сети Интернет, когда и родитель, и ребенок уже на момент совершения преступлений являются активными пользователями различных социальных сетей и мессенджеров, посредством которых также поддерживают коммуникацию, несмотря на «удаленный» характер общения.

Диспозиция п. «г» ч. 2 ст. 117 Уголовного кодекса Российской Федерации предусматривает уголовную ответственность за причинение физических или психических страданий путем систематического нанесения побоев либо иными насильственными действиями, если это не повлекло последствий, указанных в ст.ст. 111, 112 УК РФ, совершенное в отношении заведомо несовершеннолетнего или лица, заведомо для виновного находящегося в беспомощном состоянии либо в материальной или иной зависимости от виновного [1].

Из вышеизложенного следует, что законодатель прямо определяет обязательное наличие в действиях виновного такого признака, как нанесение

[1] © Копаева Ю. Ю., 2022.

побоев или иных насильственных действий, то есть наличие непосредственного физического контакта с потерпевшим, а также такого признака, как «систематичность».

Однако, изучение множества уголовных дел о преступлениях, предусмотренных п. «г» ч. 2 ст. 117 УК РФ, показало, что под иными насильственными действиями могут пониматься не только длительное причинение боли щипанием, сечением, причинением множественных, в том числе небольших, повреждений тупыми или острыми предметами, воздействием термических факторов и другими аналогичными действиями, а также иные действия, направленные на причинение потерпевшему психических страданий.

Так, Ставропольским краевым судом по поручению Верховного Суда Российской Федерации проведено изучение судебной практики рассмотрения уголовных дел по вопросам квалификации преступлений, совершенных с применением насилия или угрозой его применения, по результатам которого установлено, что понятием «иные насильственные действия» может охватываться не только физическое или иное воздействие на тело потерпевшего, но и информационное воздействие на его психику, носящее характер насилия, например систематические угрозы, оскорбления, травля, если они отражают умысел виновного на причинение жертве психических страданий [2].

Из вышеизложенного можно сделать вывод о том, что истязания могут выражаться как в причинении несовершеннолетнему побоев или иных телесных повреждений, так и в причинении психических страданий в виде эмоционального насилия, и, в случае установления указанных фактов, необходимо рассматривать вопрос о квалификации совершенного деяния по п. «г» ч. 2 ст. 117 УК РФ.

По мнению специалистов, эмоциональное насилие может выражаться в постоянном или периодическом оскорблении ребенка, в обвинениях в его адрес (брань, крики), в виде угроз со стороны родителей или лиц, их заменяющих, в принижении его успехов, в унижении его человеческого достоинства, в запугивании ребенка, а также в иных действиях [3]. Применение в отношении несовершеннолетнего эмоционального насилия, как уже отмечалось ранее, может быть, как в «очной» форме, так и путем систематического общения родителя или лица, его заменяющего, с ребенком в социальных сетях или мессенджерах (сервисах мгновенного обмена сообщениями) в информационно-телекоммуникационной сети Интерне».

Совершение истязания с причинением психических страданий с применением информационно-коммуникационных технологий может восприниматься правоприменителями с отрицательной стороны, так как отсутствуют материальные следы совершения преступления, например, телесные повреждения, позволяющие определить степень общественной опасности совершенного деяния, однако, причинение психических страданий и эмоциональное насилие если не больше, но, как минимум, в той же степени имеет отражение в окружающей обстановке и влекут последствия, которые по своей степени опасности не уступают физическому насилию.

В первую очередь, при поступлении сообщения о совершении истязания с причинением психических страданий необходимо уделить внимание на беседу с несовершеннолетним потерпевшим. Как правило, потерпевший находится в социальной и материальной зависимости от виновного, в связи с чем давать в отношении члена своей семьи показания и изобличать его в совершении преступления ему будет психологически сложно, также рассказу о преступлении несовершеннолетнему может мешать чувство вины, ведь дети, неоднократно подвергающиеся эмоциональному насилию, на подсознательном уровне обвиняют в истязаниях себя, что именно он ведет себя неправильно, что влечет за собой соответствующее к нему отношение. В данном случае необходимо установить психологический контакт с несовершеннолетним, сообщить ему о необходимости рассказать органу предварительного следствия о произошедшем, а также дать возможность осознать, что в совершении истязаний виноват лишь тот, кто применял эмоциональное насилие, но никак не тот, кто является жертвой преступления. Также в период беседы с потерпевшим необходимо точно установить способы совершения преступления в случае, если сообщения с признаками эмоционального насилия поступали несовершеннолетнему через определенные мессенджеры, необходимо отразить это в соответствующих процессуальных документах

После получения необходимых от несовершеннолетнего сведений, следователь в безотлагательном порядке производит ряд следственных и процессуальных действий, направленных на «закрепление» имеющейся информации. Если ребенок на постоянной основе использует мобильный телефон для общения с близкими, друзьями и виновным в совершении истязания лицом, необходимо изъять указанный объект и осмотреть его с участием потерпевшего. Данные действия позволят оперативно получить значимую для расследования информацию, которая впоследствии станет доказательством по уголовному делу. Также имеет важную практическую цель получение сведений из социальных сетей, например, из ООО «Вконтакте», так как указанное Общество хранит на своих серверах все имеющиеся чаты и сообщения, в том числе удаленные пользователем, что позволит восполнить недостающие элементы и установить полную хронологическую картину произошедшего.

После принятия решения о возбуждении уголовного дела необходимо назначить и провести в отношении потерпевшего амбулаторную комплексную психолого-психиатрическую экспертизу, которая позволит органу предварительного следствия определить наличие последствий от совершенного преступления, установить уровень психологического риска, а также получить необходимые сведения о личности потерпевшего, которые впоследствии он может использовать для работы с ним, обеспечить правильный психологический климат при работе с несовершеннолетним по уголовному делу, так как следственные и процессуальные действия, производимые в рамках расследования также несут большую психологическую нагрузку на потерпевшего, которому из раза в раз приходится активизировать неприятные для него

воспоминания, проговаривать их вслух в присутствии незнакомых ему людей (следователей, психологов, членов экспертной комиссии).

Само по себе совершение истязаний воспринимается лицом, его совершившим, как нечто незначительное, не являющееся уголовно наказуемым деянием. В его понимании, эмоциональное насилие таковым не является, а все его действия представляются как элементы воспитания несовершеннолетнего, необходимые для становления ребенка как личности и как будущего участника общественных отношений, в связи с чем в большей степени привлекаемые в качестве подозреваемых и обвиняемых в совершении данной категории преступлений лица отрицают свою вину и в процессе всего расследования оказывают противодействие, находятся в конфликтной ситуации и обвиняют сотрудников правоохранительных органов и системы профилактики в незаконном привлечении его к ответственности, в связи с чем следователю всегда нужно быть готовым к принятию мер по устранению внутреннего конфликта и обеспечению полноты осуществляемых следственных и процессуальных действий с его участием.

Кроме того, совершение истязаний с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, представляют собой некий эфемерный вид, т. е. лицом, его совершившим, не воспринимается как четкое совершение определенных действий и практически не закрепляется в памяти ввиду отсутствия физического воздействия на потерпевшего, что, в свою очередь, создает еще большую опасность для ребенка, находящегося в положении потерпевшего и лишает виновного критического мышления относительно совершаемых им действий.

При расследовании указанной категории уголовных дел следователю нужно быть готовым к острой и быстрой реакции на все поступающие по нему сведения, своевременно и полно осуществлять сбор доказательств, которые впоследствии позволят привлечь виновное лицо к уголовной ответственности.

Список литературы

1. Уголовный кодекс Российской Федерации // СПП «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699/b57dd2d1f388b4e1dd1d92556d43d3fcb202f2da/.

2. Официальный сайт Ставропольского краевого суда. URL: http://kraevoy.-stv.sudrf.ru/modules.php?name=docum_sud&id=119/.

3. Проблемы насилия над детьми и пути их преодоления / под. ред. Е. Н. Волковой. СПб. : Питер, 2008.

Григорьев Д. А.[1]*,*
заведующий лабораторией
«Криминалистика и специальная техника»
кафедры государственно-правовых
и уголовно-правовых дисциплин
Российского экономического университета
имени Г.В. Плеханова,
кандидат юридических наук

Басина А. С.[2]*,*
следователь Следственного управления
Управления Министерства внутренних дел
по Ленинскому городскому округу
Московской области

ОБ ОТДЕЛЬНЫХ ПРОБЛЕМАХ ДОСУДЕБНОГО ПРОИЗВОДСТВА ПО ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Одним из основных назначений МВД России в настоящее время является деятельность, направленная на раскрытие и расследование хищений, совершенных с использованием информационно-телекоммуникационных технологий (далее – ИТТ). Общепринятым названием данной категории преступлений является «дистанционное» мошенничество, при этом не все хищения среди преступлений имущественного характера совершаются в указанной форме.

Прилагаемые усилия, направленный на пресечение совершения дистанционных хищений, с учетом применения правоохранительными органами специального комплекса мероприятий, результаты противодействия преступникам остаются малоэффективными.

Так, по итогам 2021 г. зарегистрировано 517,7 тыс. преступлений, совершенных с использованием ИТТ, что значительно больше, чем число зарегистрированных преступлений указанной категории в 2020 г. [9].

Увеличение числа совершенных преступлений обусловлен рядом факторов, к числу которых относятся: низкая цифровая грамотность населения, заключающаяся в отсутствии достаточных знаний в области информации в сфере финансов, деятельности банковских служб, служб кредитования и иных сервисов, реализующих имущественные права граждан с применением сети Интернет. Кроме того, на увеличение числа совершенных преступлений в сфере «дистанционных» хищений оказывает активное распространение программных средств аноними-

[1] © Григорьев Д. А., 2022.
[2] © Басина А. С., 2022.

зации личности, обеспечивающих сокрытие информации о совершившем преступлении лице, распространение программ для мобильных устройств, позволяющих расшифровывать имена и пароли пользователей. Для граждан порядок функционирования данных программ незнаком, сведений о их существовании и работоспособности в настоящее время недостаточно, несмотря на активизацию деятельности правоохранительных органов Российской Федерации, направленной на повышение уровня осведомленности граждан о способах хищений, используемых преступниками для совершения хищений с использованием информационно-телекоммуникационных технологий. Данный перечень условий, обуславливающий увеличение количества совершенных преступлений указанной категории, не является исчерпывающим. Среди данных причин неотъемлемую часть составляет отсутствие должного уровня социальной пропаганды противодействия хищениям, совершаемым с использованием компьютерных технологий среди граждан.

Общепринятым в практической деятельности является деление на типичные виды совершения «дистанционных» преступлений, а именно: роуминговое мошенничество [1, с. 154]; звонки от «сотрудника техподдержки» [2, с. 67]; «пенсионного фонда», «службы безопасности банка» [3, с. 228]; мошенничество с помощью звонка или SMS-сообщения [4, с. 38]; а также тайное хищение (кража) с банковского счета.

Стоит отметить, что возложенные на правоохранительные органы Российской Федерации обязанности по предотвращению и предупреждению преступлений не исчерпываются лишь профилактической работой, не мало важной составляющей остается досудебное производство. На основе существующих методик, разработанных как теоретическими, так и практическими сотрудниками, выработан общий перечень следственных ситуаций, сведений, необходимых для установления обстоятельств совершения преступления и личности преступника.

Наличие указанных методик, содержанием которых является плановое и поэтапное расследование указанной категории уголовных дел, основной задачей которых является получение информации, имеющей значение для расследования, позволяет следователю, в том числе, не специализирующемся на расследовании указанной категории уголовных дел, изначально определить ход расследования, его этапы, спланировать работу, определить сроки, фактически исключив ошибки.

С учетом данных следственной практики были разработаны и выработаны типичные следственные ситуации, которые возникают при расследовании уголовных дел по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, в том числе определен перечень необходимых следственных действий, проводимых на каждом этапе расследования. Несмотря на то, что данные методики существуют, указанный в них перечень следственных и процессуальных действий является исчерпывающим, при расследовании конкретного уголовного дела стоит принимать во внимание и фактические данные совершенного преступления.

Зачастую, используя формальной подход к расследованию преступлений, следователями допускается утрата информации, имеющей доказательственное значение. Так, полагая, что данный вид преступлений совершается лицами, ведущими антиобщественный образ жизни, злоупотребляющих алкоголем, употребляющих наркотические средства и пр., лицо, в действительности совершившее вышеуказанные преступления, может скрыться от органов следствия или продолжить заниматься преступной деятельностью. В практической деятельности злоумышленники могут лишь использовать указанные категории лиц, за незначительное вознаграждение, например, для оформления на них расчетных (дебетовых) карт, которые, в свою очередь, впоследствии используются для обналичивания денежных средств, поступивших со счетов потерпевших.

Грамотное планирование, исходя из складывающейся по ходу следственной ситуации, проведение комплекса следственных действий как на первоначальном, так и на последующем этапах расследования позволит установить лицо (лиц), совершившее преступление, в полной мере собрать доказательства вины и как итог, достигнуть основных целей уголовного судопроизводства.

Первоначальные следственные действия, процедура их производства во многом зависят от того, удалось ли на момент возбуждения уголовного дела установить лицо, подозреваемое в совершении преступления данной категории. На момент поступления заявления, в большинстве случаев неизвестно, кто совершил преступление. Успех раскрытия и расследования такого преступления определяет тесный контакт следователя с сотрудниками, производящими оперативно-розыскные и технические мероприятия.

Кроме того, стоит отметить, что отсутствие единого подхода к применению уголовных норм, регламентирующих ответственность за совершение преступлений, порождает возникновение правовых коллизий, которые возникают в ходе осуществления досудебного производства в практической деятельности следователя.

Законодатель предусмотрел ответственность за хищение электронных денежных средств, совершенное путем кражи (п. «г» ч. 3 ст. 158 УК РФ). Однако в практической деятельности возникают проблемы, связанные с разграничением указанного преступления и иных хищений, что существенно осложняет возможность применения данной нормы.

Данная ситуация была разрешена при введении в действие Федерального закона от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации». В практической судебно-следственной деятельности выработано два подхода к толкованию данной нормы. Первый подход заключается в том, что данный особо квалифицированный вид кражи имеет место не во всех случаях хищения денежных средств с банковского счета потерпевшего, а только при хищении безналичных и электронных денежных средств путем их перевода в рамках применяемых форм безналичных расчетов и порядке, регламентированном ст. 5 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе».

Второй подход заключается в том, что тайное хищение безналичных денежных средств с банковского счета потерпевшего, без вмешательства в функционирование сервисов дистанционного банковского обслуживания необходимо квалифицировать по ч. 1 ст. 158 УК РФ [5].

Ранее, до появления разъяснений Пленума Верховного Суда Российской Федерации (постановление от 30 ноября 2017 г. № 48), суд квалифицировал действия лиц, использующих чужую банковскую карту, снабженную функцией «ПайПасс», как мошенничество с использованием электронных средств платежа, а не как кражу с банковского счета [6]. Данный вид совершения хищения указанным способом в практической деятельности широко распространен, что в очередной раз указывает на необходимость существования единого подхода к применению норм уголовного закона.

Судебная коллегия по уголовным делам Верховного Суда Российской Федерации, в своем постановлении от 29 сентября 2020 г., разрешила данную проблему, указав, что совершая хищение указанным способом, а именно: оплачивая товары бесконтактным способом, без совершения обмана или злоупотребления доверием работников торговых организаций, не сообщая ложные сведения о принадлежности карты сотрудникам торговой организации, в обязанности которых не входит обязанность идентификации держателя карты по документам, удостоверяющим личность, не возлагается, содеянное надлежит квалифицировать как тайное хищение [7].

Также был разрешен вопрос о квалификации преступного деяния, исходя из суммы причиненного ущерба. Ранее, до внесения изменений 29.06.2021 в постановление Пленума Верховного суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое», к уголовной ответственности за совершение вышеуказанной категории преступлений привлекались лица, причинившие материальный ущерб на сумму ниже 2500 руб. Так, по приговору Видновского городского суда Московской области по делу от 29.01.2021 № 1-100/21 осуждена У., которая совершила тайное хищение электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ), причинив своими действиями Д. материальный ущерб на общую сумму 595 руб. 28 коп. [8]. В настоящее время в виду малозначительности деяния в возбуждении уголовного дела будет отказано.

Еще одной из животрепещущих проблем досудебного производства по анализируемым нами преступлениям является то, что уровень знаний сотрудниками оперативных и следственных подразделений в сфере информационно-телекоммуникационных технологий пока явно не соответствуют тем требованиям, которые необходимы для успешной борьбы с этими преступлениями.

Все это стало основанием формирования в учебных заведениях МВД России, Следственного комитета России, в ряде высших учебных заведений Министерства науки и высшего образования Российской Федерации, Министерства цифрового развития, связи и массовых коммуникаций

Российской Федерации специальных дисциплин для курсантов и студентов по рассматриваемой теме, в рамках курсов повышения квалификаций для сотрудников правоохранительных органов.

Так, к примеру, с 2019 г. Научно-исследовательский университет «Московский институт электронной техники» готовит специалистов по направлению «Правовое обеспечение национальной безопасности». Основная концепция образовательной программы «Расследование киберпреступлений».

Таким образом, учитывая вышеизложенное, можно утверждать, что эти проблемы можно решить только в комплексе: путем усовершенствования действующего законодательства; подготовки курсантов и слушателей ВУЗов правоохранительных органов по новым учебным дисциплинам. Знания последних должны стать основой для противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий. Большим подспорьем будет и регулярная переподготовка следователей, дознавателей, экспертов-криминалистов в рамках дополнительного профессионального образования.

Список литературы

1. Парфенов А. В., Кокуйский О. В., Мошенничества с использованием сотовой связи // Закон и право. 2019. № 6. С. 154.

2. Михнев И. П. Информационная безопасность на просторах мобильного интернета // образовательные ресурсы и технологии. 2015. № 4. С. 165.

3. Гумаров И. А., Саетгараев И. А. Некоторые проблемы организации работы оперативных подразделений органов внутренних дел по противодействию мошенничествам общеуголовной направленности // Вестник Казанского юридического института МВД России. 2018. № 2. С. 228.

4. Долинин В. Н. Классификация способов совершения мошенничества в отношении имущества физических лиц // Российское право. 2017. № 1. С. 38.

5. Апелляционное определение Кемеровского областного суда от 20 февраля 2019 г. по делу № 22-455/2019.

6. Приговор Ново-Савинского районного суда г. Казани от 16 ноября 2018 г. по делу № 1-525/2018.

7. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29 сентября 2020 г. № 12-УДП20-5-К6.

8. Приговор Видновского городского суда Московской области от 29 января 2021 г. по делу № 1-100/21.

9. Состояние преступности в России за январь–декабрь 2021 г. URL: https://-мвд.рф/reports/item/28021552.

Корниенкова М. Р.[1],
преподаватель кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук

Дякина С. Н.[2],
курсант 193 учебного взвода ФПСОПП
Московского университета МВД России имени В.Я. Кикотя

К ВОПРОСУ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Сегодня сделки, которые заключаются между сторонами, нередко оплачиваются с помощью кредитных и депозитных пластиковых карт либо при помощи мобильного устройства бесконтактным способом. Ввиду этого, учащаются случаи мошенничества, совершенные с использованием электронных средств платежа. На этой уголовно-правовой проблеме мы бы и хотели остановиться подробнее.

В России официально уголовная ответственность за мошенничество с использованием электронных средств платежа была установлена в ноябре 2012 г. путем принятия Федерального закона от 29 ноября 2012 г. «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [1]. Однако изначально данную норму назвали «Мошенничеством с использованием платежных карт».

Отметим, что информационные технологии в настоящее время затронули практически все сферы общественной жизни, а также отрасли экономики. Не является исключением финансовая сфера, где внедрение новых информационных технологий является частью эволюционного процесса развития и совершенствования различных финансовых продуктов, а также способов совершения финансовых операций. С каждым годом бумажные деньги теряют свою актуальность, а большинство граждан предпочитает безналичное способы осуществления оплаты. При этом для организаций законодательством в императивном порядке ограничены операции с бумажными денежными средствами. Безналичные платежи характеризуется удобством использования, а также возможностью осуществления контроля над финансовыми операциями со стороны государства и финансовых учреждений.

Нами были опрошены сто двадцать респондентов из разных возрастных групп: от 18 до 30 лет, от 31 до 45 лет и от 46 лет. Участникам опроса предлагалось ответить «да» или «нет» на два следующих вопроса: «Поступал ли вам звонок от мошенников, которые представлялись сотрудниками банка?», «Становились ли вы жертвой такого мошенничества?». По первому вопросу

[1] © Корниенкова М. Р., 2022.
[2] © Дякина С. Н., 2022.

респондентами от 18 до 30 лет ответы «да» были даны тридцатью семью участниками опроса. Электронные денежные средства были похищены с банковских карт десяти человек, что в процентном соотношении составляет 27 %. Также тридцать семь респондентов в возрасте от 31 до 45 лет утверждают, что им поступал такой звонок, а с банковских карт двадцати из них были похищены денежные средства. В процентах это составляет 54,1 %. Из третьей группы опрашиваемых – от 46 лет, на первый вопрос ответ «да» дали тридцать восемь человек, из которых жертвами «телефонного» мошенничества стали тридцать респондентов, что выражается в 78,9 %. Изучив получившиеся результаты опроса, мы можем объяснить сложившуюся ситуацию качеством осведомленности граждан о «телефонном» мошенничестве, исходя из возрастного фактора. Данные опроса демонстрируют и подкрепляют актуальность выбранной нами темы и свидетельствуют о необходимости более тщательных исследований.

Однако на сегодняшний день не исключены трудности при разграничении составов преступлений, предусмотренных п. «г» ч. 3 ст. 158, ст. 159.3, ст. 159.6 УК РФ [2]. Возможно, это обусловлено тем, что правоприменитель сталкивается с обозначенными нами в последующем трудностями при толковании объективных сторон вышеуказанных преступлений.

Приобретение права на чужое имущество подразумевает под собой исполнение обязательств, связанных с условиями передачи лицу такового или права на его приобретение. Соответственно, неисполнение этого обязательства причиняет материальный ущерб потерпевшему лицу, вследствие чего совершенное деяние квалифицируют как мошенничество. Обратим внимание на то, что у виновного подобный умысел зарождается до завладения чужим имуществом или получения права на его приобретение. Следовательно, судам необходимо установить тот факт, что виновный заведомо не намеревался исполнять обязательства.

Наличные денежные средства заменяются электронными, которые помогают осуществить платеж путем перевода определенной суммы непосредственно на электронное устройство торговой организации. Понятие «электронного средства платежа» устанавливается Федеральным законом от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» (последняя редакция) [4]. Так, под электронным средством платежа, согласно п. 19 ст. 3, понимают «средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств» [4].

Интерпретация данного понятия указывает на то, что электронные денежные средства носят безналичный характер, и отмечает появление эквайринга. Под эквайрингом принято понимать объективную возможность торговой организации принимать безналичную оплату товаров и услуг при помощи пластиковых карт. Законодатель предпринимает попытку разграничить два смежных состава преступления – мошенничество с использованием электронных средств платежа и

кражу с банковского счета, а равно в отношении электронных денежных средств. Такие средства платежа используются для создания и отправления банку поручения о переводе электронных денежных средств.

Особенность преступления, предусмотренного ст. 159.3 УК РФ, заключается в том, что доступ к банковским картам и счетам осуществляется путем использования различных технических средств и платежных карт, а это, в свою очередь, позволяет преступнику оставаться анонимным, что затрудняет его розыск и привлечение к уголовной ответственности. Когда предметом хищения были признаны безналичные денежные средства, в том числе электронные денежные средства, появилось соответствующее разъяснение [3], из которого следует, что мошенничество с использованием электронных средств платежа считается оконченным с момента изъятия этих средств с банковского счета владельца.

Проанализировав диспозицию ч. 1 ст. 159.3 УК РФ, целесообразно заключить, что предметом мошенничества выступают находящиеся на банковском счете потерпевшего электронные денежные средства. В таком случае можно сформулировать определение мошенничества с использованием электронных средств платежа следующим образом: – это противоправное безвозмездное изъятие денежных средств с банковского счета их владельца, совершенное путем обмана как способа совершения хищения или злоупотребления доверием, причинившее материальный ущерб владельцу банковского счета.

Состав данного преступления по конструкции является материальным. Соответственно, объективная сторона включает в себя:

– общественно-опасное деяние в форме действия, выраженное в хищении чужого имущества или приобретении права на него с использованием электронных средств платежа;

– общественно-опасные последствия в виде причиненного потерпевшему материального ущерба;

– причинно-следственную связь между хищением чужого имущества или приобретением права не него и наступившим вследствие этого материальным ущербом.

Обязательными признаками выступают использование электронных средств платежа и способ, заключающийся в обмане либо злоупотреблении доверием владельца банковского счета или иного лица для завладения имуществом. Причем обман состоит как в сообщении ложных сведений о находящейся у виновного банковской карте (активный обман), так и в умолчании об ее истинном владельце (пассивный обман). Думается, что нельзя квалифицировать деяние как мошенничество с использованием электронных средств платежа, если обман направлен лишь на облегчение доступа к предмету посягательства.

Для субъективной стороны рассматриваемого преступления свойственен исключительно прямой умысел. Лицо, виновное в совершении преступления, осознает общественную опасность деяния, выраженную в хищении чужого имущества или приобретении права на него с использованием электронных средств платежа путем обмана или злоупотребления доверием потерпевшего или иных

лиц, предвидит наступление общественно-опасных последствий, а именно причинение материального ущерба владельцу банковского счета, и желает их наступления.

Субъект преступления – общий. Это значит, что согласно ст. 20 УК РФ, к уголовной ответственности может быть привлечено такое физическое лицо, которое ко времени совершения преступления достигло шестнадцати лет, и является вменяемым.

Следует отметить, что создание видимости законной передачи имущества и имущественных прав требует от исполнителя определенных навыков и умений, в этой связи справедливо считается, что мошенничество выступает одним из наиболее высокопрофессиональных корыстных преступлений, поскольку его совершение с точки зрения криминального мастерства значительно сложнее кражи, грабежа или разбоя.

Мошенничество с объективной точки зрения проявляется путем применения разнообразных способов совершения преступления, которые безусловно, необходимо учитывать.

Вместе с тем, на практике встречаются и спорные ситуации квалификации хищения денежных средств с использованием электронных средств платежа.

Так, постановленным в особом порядке судебного разбирательства в соответствии с глава 40 Уголовно-процессуального кодекса Российской Федерации [6] приговором Йошкар-Олинского городского суда республики Марий Эл от 28 октября 2019 г. К. осужден по ч. 3 ст. 30 п. «г» ч. 3 ст. 158 УК РФ – покушение на кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств, к одному году девяти месяцам лишения свободы. Виновный, осознавая общественно-опасный характер своих действий, 13 мая 2019 г. пытался потратить денежные средства с банковской карты, обнаруженной им во дворе жилого дома, но не смог довести преступление до конца, поскольку владелец банковской карты обнаружил пропажу и заблокировал ее. Суд апелляционной инстанции принял такое же решение. Кассационной суд общей юрисдикции переквалифицировал совершенное деяние на ч. 3 ст. 30 ч. 1 ст. 159.3 УК РФ: покушение на мошенничество с использованием электронных средств платежа. Судебная коллегия по уголовным делам Верховного Суда Российской Федерации 29 сентября 2020 г. отменила кассационное определение и направила дело на новое рассмотрение в суд кассационной инстанции [5]. Принятие такого решения обосновывается тремя составляющими, которые, на наш взгляд, заслуживают особого внимания.

Во-первых, осуществление изъятия денежных средств путем обмана или злоупотребления доверием их владельца либо иного лица по смыслу уголовного закона образует состав преступления, установленного ч. 1 ст. 159.3 УК РФ, а именно: хищение денежных средств, совершенное с использованием виновным электронного средства платежа. Так, К. нашел банковскую карту, принадлежащую потерпевшему, во дворе жилого дома. После чего, у виновного возник умысел на удовлетворение своих желаний противоправным способом. Точнее говоря, К. за приобретаемые им товары расплачивался найденной картой,

воспользовавшись бесконтактным способом оплаты. Важно отметить, что при выполнении виновным объективной стороны такого мошенничества работники торговых организаций никакого-либо участия в осуществлении операций по списанию денежных средств с банковского счета не принимали. Это означает, что виновный не вводил в заблуждение работников, а также не сообщал последним ложных сведений об истинной принадлежности банковской карты, служащей средством оплаты.

Во-вторых, необходимо отметить, что в обязанности работников торговых организаций не входит идентификация гражданина-держателя, предоставляющего карту для оплаты товаров и услуг, что находит подтверждение в действующих нормативных актах.

В-третьих, Судебная коллегия по уголовным делам Верховного Суда Российской Федерации признала необоснованной отсылку суда кассационной инстанции на п. 17 постановления Пленума Верховного Суда Российской Федерации, так как содержащиеся в нем разъяснения были даны к ранее действующей редакции ст. 159.3 Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 19.02.2018, с изм. от 25.04.2018). В нынешней же редакции диспозиция вышеуказанной статьи сформулирована крайне расплывчато и обширно, если читать ее без привязки к п. «г» ч. 3 ст. 158 УК РФ и сравнения с предыдущей редакцией. Нет никаких оснований полагать, что законодатель, принимая Федеральный закон от 23.04.2018 № 111-ФЗ [7], всецело изменил объем деяний, подпадающих под ст. 159.3 УК РФ. Напротив, был расширен перечень средств, при помощи которых совершается преступление. Отсюда следует вывод, что данная норма не отражает реальное положение вещей, связанное с такими формами хищения.

Вышеуказанный Федеральный закон при формулировке понятия «кражи с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ)» определил деяние так, что в конечном счете п. «г» ч. 3 ст. 158 и ст. 159.3 УК РФ конкурируют между собой как общая и специальная норма соответственно, то есть одни и те же уголовно-правовые отношения регулируются двумя нормами, из которых имеет место применение лишь одной из них. Как определено в ч. 3 ст. 17 УК РФ, при наличии такой конкуренции, применяется специальная норма – в исследуемом нами моменте это ст. 159.3 УК РФ. Выходит, что действия, подпадающие под ст. 159.3 УК РФ, выступают частным случаем кражи? Отвечая на поставленный вопрос, мы согласны с позицией П. С. Яни: «Этот «гордиев узел» может разрубить только законотворец путем совершенствования уголовного законодательства» [8].

Важно то, что в деянии, совершенном К., обман не выступает способом изъятия имущества. В данном случае целесообразно говорить об обмане как способе облегчить получение доступа к денежным средствам, находящимся на банковском счете потерпевшего. Мы приходим к выводу, что невозможно противостоять позиции кассационного суда. Так и Верховный Суд Российской Федерации

в третьем абзаце п. 2 постановления Пленума от 30 ноября 2017 г. № 48 [3] закрепляет, что в тех случаях, когда обман не направлен на завладение чужим имуществом, а лишь служит облегчением доступа к нему, то действия виновного образуют состав преступления, именуемого кражей либо грабежом в зависимости от способа хищения.

Таким образом, можно заключить, что в современной действительности ввод ПИН-кодов как таковой (то есть непосредственный обман представителей торговых организаций) не реализуется. Здесь имеет место тайное хищение электронных денежных средств со счета владельца банковской карты. Так как система не запрашивает ввод ПИН-кода, и, следовательно, квалифицировать совершенное деяние как мошенничество с использованием электронных средств платежа, на наш взгляд, неправомерно, потому что обман направлен исключительно на облегчение доступа к этим средствам.

Вышеизложенные нами обстоятельства не способствуют принятию правомерных решений при уголовно-правовой оценке подобных ситуаций. Для разрешения сложившейся уголовно-правовой проблемы, исходя из особенностей объективной и субъективной сторон исследуемого деяния, а также учитывая наступление века цифровизации, считаем необходимым:

1. Наиболее масштабно (на региональном уровне) и эффективно произвести обобщение судебной практики по уголовным делам, квалифицированным по ст. 159.3 УК.

2. Проанализировав результаты обобщения, конкретизировать, каким именно способом совершается деяние в рассматриваемой нами статье, выделить особенности его совершения и отличия от других видов хищений.

3. На основании соблюдения предыдущих пунктов внести изменения в действующее постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» в части разъяснений применения норм, затрагивающих п. «г» ч. 3 ст. 158, ст. 159.3 и ст. 159.6 УК РФ.

Список литературы

1. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 29 ноября 2012 г. // Российская газета. 2012. 3 дек.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 22.08.2021).

3. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате».

4.Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» (последняя редакция).

5. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29 сентября 2020 г. № 12-УДП20-5-К6.

6. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 01.07.2021, с изм. от 23.09.2021).

7. Федеральный закон от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации».

8. Квалификация хищений, совершаемых с использованием банковских карт. URL: https://www.youtube.com/watch?v=N_4bxfEr21o.

Алференок Е. А.[1],
преподаватель кафедры уголовного права
Московского университета МВД России
имени В.Я. Кикотя,
кандидат юридических наук

Бандурович А. Б.[2],
слушатель 171 учебного взвода 5 «О» курса
факультета подготовки сотрудников
для оперативных подразделений полиции
Московского университета МВД России
имени В.Я. Кикотя

К ВОПРОСУ О СОЦИАЛЬНОЙ ОБУСЛОВЛЕННОСТИ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

С момента появления первой гражданской электронно-вычислительной машины прошло уже более 90 лет. За такой период развития компьютерной техники, информационно-коммуникационных технологий и распространения информации, преодолевая некоторые технические трудности, важно понять значение существующих системных связей. Эти связи представляют собой колоссальную всемирную паутину (англ. – «World Wide Web»), позволяющую нам сегодня увидеть человека, находящегося от нас за тысячи километров, через экран монитора, передать ему любую информацию, а также перевести денежные средства с минимальными временными затратами.

Цифровизация экономики, сопряженная с переходом в виртуальную среду, позволяет приобретать или продавать товар из одной точки мира в другую, даже не общаясь с владельцем этого товара. Мировые гиганты реселлинга позволяют совершать различные сделки посредством нажатия клавиш «принять условия договора» и «оплатить», в результате чего человек вступает в гражданско-правовые отношения без подписания огромного количества бумаг и личного присутствия.

Интернет, являясь крупнейшим хранилищем информации, занимает важнейшую часть современной жизни любого человека. К сожалению, высокие темпы научно-технического прогресса порождают все больший интерес и для преступного мира. Существует огромное количество схем для хищения денежных средств у граждан, организаций, международных корпораций и государства.

Мошенники по всему миру под видом благотворительности ради собственной наживы используют ситуации с заболеванием детей, локальными, региональными и межрегиональными происшествиями, завладевая путем обмана или злоупотребления доверием крупными денежными суммами, которые складываются из переводов обманутых граждан. Интересным примером выступает слу-

[1] © Алференок Е. А., 2022.
[2] © Бандурович А. Б., 2022.

чай, приведенный В. А. Лещенко: «Известно, что буквально через несколько часов после трагедии на Гаити, в адрес интернет-пользователей поступали сообщения с просьбами о пожертвовании денег для людей, пострадавших от землетрясения, тогда власти официально обратились с просьбой критически реагировать на данные призывы и высокой доли вероятности мошенничества» [5].

Кроме того, практически каждому человеку, имеющему сегодня сотовый телефон и зарегистрированному в социальных сетях, известны случаи взлома аккаунтов друзей или коллег, в результате чего мошенник под видом знакомого или близкого человека обманным путем просит перевести денежные средства. В 2018 г. МВД России был представлен «Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития» [4, с. 44–46]. В указанном сборнике имеется информация о неуклонном росте количества преступлений, предусмотренных ст. 159.6 УК РФ с 2013 по 2017 гг. Так, если в 2013 г. их было совершено только 693, то в 2015 г. – 5442. Данные 2018 г. свидетельствуют об удвоении числа кибератак, в результате которых доходы хакеров составили более 2 млрд руб. [4, с. 44–46].

Рассматривая дальнейшее состояние преступности, отметим тенденцию на спад количества зарегистрированных мошенничеств в сфере компьютерной информации. В 2019 г. их было 687, в 2020 г. – 761, а в 2021 г. – всего 431 [6]. Несмотря на это, нельзя не согласиться с точкой зрения О. С. Гузеевой, что «главенствующее место среди преступлений, совершаемых в российском сегменте сети Интернет, занимает мошенничество» [3].

Российская Федерация, являясь одним из лидеров мировой арены и не отставая от всемирных тенденций, приняла Стратегию развития информационного общества на 2017–2030 гг., определив главные направления, среди которых развитие информационного общества, обеспечение безопасности граждан и государства, способствование укреплению государственного управления, развитие и формирование цифровой экономики [8]. В указанной стратегии употребляются следующие термины: «информационное общество», «информационное пространство». Именно безопасность информационного пространства, согласно указанной стратегии, является одной из приоритетных задач нашей страны. Однако скоротечность протекания операций по переводам и обналичиванию денежных средств, добытых преступных путем, в том числе посредством мошенничества в сфере компьютерной информации, не позволяет столь же оперативно реагировать и предупреждать преступления правоохранительными органами. Имеющиеся сегодня разъяснения, объявления по радио, в СМИ и общественном транспорте, профилактические беседы не оказывают должного результата по профилактике и предупреждению указанных деяний.

Также одним из факторов, способствующих совершению указанных преступлений, выступает их высокая латентность. По данным зарубежных специалистов, огромная часть указанных преступлений даже не расследуется, поскольку потерпевшие стыдятся собственной глупости, наивности и жадности [7].

Стоит согласиться с Д. А. Грибом, что на территории Российской Федерации отсутствуют единые разъяснения высшего судебного органа по вопросам юридической оценки рассматриваемого преступления, что сохраняет условия, способствующие дальнейшей криминализации виртуального пространства [с. 23].

На сегодняшний день, ни одна страна мира не имеет глобального, затрагивающего все из возможных совершаемых преступлений в сфере компьютерной информации, законодательства. Этот и множество иных факторов свидетельствуют о социальной обусловленности и значимости установления уголовной ответственности за мошенничество в сфере компьютерной информации.

К сожалению, рассматривая складывающиеся мировые тенденции и темпы роста преступности с использованием компьютерной информации, к числу которых относится и состав преступления, предусмотренный ст. 159.6 УК РФ, можно спрогнозировать и дальнейший значительный рост совершения запрещенных деяний с использованием информационно-телекоммуникационных технологий, что свидетельствует об актуальности и необходимости криминализации указанного вида хищений. Кроме того, отметим, что наличествующие сегодня средства и способы борьбы с преступлениями и преступностью в исследуемой сфере, действия, направленные на профилактику совершения указанных преступлений, являются недостаточными или полностью не выполняют возложенные на них задачи.

Обезличенность и анонимность мошенников, возможность совершать преступления из любой точки мира, где может быть осуществлено подключение к сети Интернет, также влияет на проблемы, связанные с привлечением указанных лиц к уголовной ответственности.

Следовательно, криминализация, то есть введение уголовной ответственности за совершение определенных действий, – мошенничества с использованием информационно-телекоммуникационных сетей или компьютерной информации обусловлена, в первую очередь, возросшей общественной опасностью совершаемых деяний указанными способами и средствами, а также размерами причиняемого имущественного ущерба. Также нельзя не согласиться с точкой зрения Д. В. Гриба о том, что, с одной стороны, широкое распространение мошенничества, совершаемого путем использования информационных технологий, обусловлено тем, что при помощи глобальной сети «Интернет» преступник обладает возможностью доступа к потенциальным потерпевшим, а также доступом к информационным ресурсам компаний, банковским учреждениям; с другой стороны, санкции за своего рода «традиционное» мошенничество и мошенничество в сфере компьютерной информации, которые предусмотрены ст.ст. 159, 159.6 УК РФ, в большинстве своем совпадают [1], что не соответствует принципам дифференциации уголовной ответственности.

Учитывая, что одним из основных критериев криминализации того или иного деяния выступает общественная опасность, нельзя не отметить, что такой признак присущ и исследуемому составу мошенничества в сфере компьютерной информации, что соответствует ст. 14 УК РФ. Налицо угроза отношениям права

собственности, являющимся объектом уголовно-правовой охраны, в которых участвуют все без исключения люди.

Следующим критерием можно выделить противоречие нормам морали и взглядам подавляющего большинства членов общества. Само по себе хищение имущества признается аморальным и противоправным еще с времен Древнего Рима и Законов XII таблиц [9, с. 21–33]. Использование компьютерной информации представляет собой наличие особого способа хищения, присущего развитию современного общества и складывающихся внутри него правоотношений.

Противодействие указанным общественно опасным деяниям возможно исключительно с помощью привлечения к уголовной ответственности, поскольку иные виды ответственности (в том числе и административная ответственность) не позволят в полной мере противодействовать таким противоправным проявлениям. Кроме того, приведенные нами выше темпы роста показателей преступности по данному составу преступления свидетельствуют не только о наличии угрозы правоотношениям в сфере обеспечения права собственности, но и о недостаточных мерах реализации уголовной политики в данной области. То есть, даже наличие уголовного наказания за мошенничество в сфере компьютерной информации не в полной мере выполняет превентивную функцию.

Таким образом, подводя итог социальной обусловленности уголовной ответственности за мошенничество в сфере компьютерной информации, можно сделать следующие выводы:

1. Уголовная ответственность за мошенничество в сфере компьютерной информации является социально обусловленной, поскольку соответствует научно-обоснованным критериям криминализации общественно-опасных деяний. Названное преступление представляет собой резко негативное явление, проявляемое ввиду скоротечного развития научно-технического прогресса, характеризуемое быстрыми темпами роста.

2. Складывающиеся как в Российской Федерации, так и на мировой арене, тенденции по росту преступлений указанной категории требуют совершенствования уголовно-правовых мер по противодействию им, поскольку имеющиеся на сегодняшний день инструменты не позволяют в полной мере противостоять подобного рода деяниям.

Список литературы

1. Гриб Д. В. Социальная обусловленность норм уголовного законодательства Российской Федерации и Республики Беларусь, предусматривающих ответственность за хищения, совершаемые с использованием информационных технологий // Евразийская адвокатура. 2019. № 2 (39). С. 74–78.

2. Гриб Д. В. Уголовная ответственность за хищение, совершаемое путем использования информационных технологий по законодательству Республики Беларусь и Российской Федерации : дис. … канд. юрид. наук : 12.00.08. М. : Московский университет МВД России имени В.Я. Кикотя, 2021.

3. Гузеева О. С. Квалификация мошенничества в российском сегменте сети Интернет // Законность. 2013. № 3. С. 21–24.

4. Комплексный анализ состояния преступности в Российской Федерации по итогам 2018 г. и ожидаемые тенденции ее развития / [М. В. Гончарова и др.]. М. : ВНИИ МВД России, 2019. 56 с.

5. Лещенко В. П. Социально-правовая обусловленность уголовной ответственности за мошенничество с использованием средств электронного платежа, совершенного в сети «интернет» // Наука. Образование. Современность. 2020. № 3. С. 43–46.

6. Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/folder/101762.

7. Петров С. А. Способ мошенничества – пассивный обман // Уголовное право. 2016. № 5. С. 57–62.

8. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс».

9. Хрестоматия по истории Древнего мира. Т. III. Рим / под ред. В. В. Струве. М., 1953.

Котова А. А.[1],
адъюнкт факультета подготовки
научно-педагогических и научных кадров
Московского университета МВД России
имени В.Я. Кикотя

К ВОПРОСУ О РОЛИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В ПРОТИВОДЕЙСТВИИ НЕЗАКОННОМУ ОБОРОТУ ДРАГОЦЕННЫХ МЕТАЛЛОВ И КАМНЕЙ

Известно, что национальная безопасность Российской Федерации включает в себя рад важнейших составляющих, в числе которых обеспечение социально-экономического развития страны. При этом в качестве приоритетных задач в сфере обеспечения экономической безопасности Президент Российской Федерации установил «создание стратегических резервов минерально-сырьевых ресурсов, достаточных для гарантированного обеспечения мобилизационных нужд Российской Федерации и потребностей экономики страны на долгосрочную перспективу» [7]. К таким ресурсам относятся, в первую очередь, драгоценные металлы и камни, которые обладают исключительной редкостью, уникальностью и высокой экономической стоимостью.

Ученые отмечают, что от объема запасов золота зависит устойчивость финансовой системы государства, а также развитие экономики. В частности, Н. А. Пучков пишет, что «золотой запас – это символ экономического и валютного могущества, показатель роли и места, занимаемого данной страной в мировом хозяйстве» [6, с. 5].

Вышеназванное указывает на исключительную важность драгоценных металлов и камней для экономики Российской Федерации и обуславливает установление в отношении незаконного оборота данных ценностей наиболее строгой ответственности. Так, в соответствии со ст.191 УК РФ преступлением признается совершение сделок с драгоценными металлами и камнями в нарушение правил, установленных законодательством Российской Федерации, их незаконное хранение, перевозка или пересылка. Также уголовно-наказуемым является нарушение правил сдачи государству драгоценных металлов и драгоценных камней (ст. 192 УК РФ).

Согласно статистике Судебного департамента, при Верховном Суде Российской Федерации, в 2021 г. всего по ст. 191 УК РФ было осуждено 47 человек, в 2020 г. по статье 191 УК РФ было привлечено к ответственности 28 человек. По ст. 192 УК РФ за два года никто не был привлечен к уголовной ответственности [4].

По оценкам специалистов, преступления в сфере оборота драгоценных металлов и камней характеризуются высокой латентностью, обусловленной профессионализмом преступников, сложным механизмом совершения преступлений, участием значительного круга лиц, сложностями в квалификации преступлений

[1] © Котова А. А., 2022.

и другими факторами [3, с. 3]. Из этого следует, что одной из существенных проблем применения указанных уголовно-правовых норм являются трудности выявления рассматриваемых преступлений. Принимая во внимание положительные аспекты цифровизации государственных услуг, полагаем, что решению обозначенной проблемы может способствовать использование современных информационных технологий в рассматриваемой области.

Руководитель Федеральной пробирной палаты Ю. И. Зубарев обозначил ряд негативных фактов, показывающих необходимость совершенствования правового регулирования сферы оборота драгоценных металлов и камней: «теневой сектор составил около 50 % рынка ювелирных изделий, стоимость нелегально ввезенных драгоценных камней более чем в 80 раз превысила стоимость драгоценных камней, законно используемых в производстве ювелирных изделий. Как следствие – бюджет недосчитался десятков миллиардов рублей налогов от операций с золотом на рынке» [2, с. 42–45]. Вместе с тем, руководитель федеральной службы отметил в качестве приоритетной задачи ведомства внедрение современных информационных систем в сферу оборота драгоценных металлов и камней. Следует отметить, что данная задача постепенно реализуется.

Например, 26 февраля 2021 г. постановлением Правительства Российской Федерации № 270 были утверждены Правила введения государственной интегрированной информационной системы в сфере контроля за оборотом драгоценных металлов, драгоценных камней и изделий из них на всех этапах этого оборота (ГИИС ДМДК) (далее – Правила функционирования ГИИС ДМДК) [5]. Цели создания системы – «обеспечение прослеживаемости (учета) драгоценных металлов, драгоценных камней и изделий из них в целях осуществления контроля за обращением драгоценных металлов и драгоценных камней, а также подтверждения их подлинности и легальности происхождения» и др. [8]. Цели создания ГИИС ДМДК, а также основные положения о функционировании данной системы нашли свое отражение в Федеральном законе «О драгоценных металлах и камнях» (ст. 12.2).

Новая система контроля за оборотом драгоценных металлов и камней предполагает присвоение каждому драгоценному металлу, камню или изделию из них уникального идентификационного номера (УИН) с последующим внесением в систему отметок о всех операциях с данными предметами. Таким образом, государство стремится обеспечить учет всех ценностей на территории Российской Федерации и установить прозрачность всех операций с ними.

Оценить эффективность действия данной информационной системы в данный момент не представляется возможным, так как в настоящее время происходит постепенное введение ее в эксплуатацию. Полагаем, что одним и результатов работы ГИИС ДМДК в будущем станет повышение эффективности выявления преступлений в сфере оборота драгоценных металлов и камней, а также борьбы с данным негативным явлением.

При рассмотрении вопроса следует сказать об ответственности за невнесение данных в ГИИС ДМДК и совершение операций с драгоценными металлами

и камнями в нарушение Правил функционирования ГИИС ДМДК. В п. 50 указанных Правил установлено, что «ответственность за полноту, достоверность, и своевременность направляемых сведений (информации) несут участники оборота» [5]. В данном нормативном акте не конкретизируется, к какому виду ответственности привлекаются обозначенные лица в случае совершения соответствующих нарушений.

По мнению специалистов, лица, не выполняющие рассматриваемые предписания законодательства, могут быть привлечены к административной ответственности по ст.ст. 15.43, 15.46 и 15.47 КоАП РФ [1].

На наш взгляд, при совершении нарушений, связанных с учетом и хранением драгоценных металлов и камней, а также совершением сделок с данными ценностями в нарушение законодательства о функционировании ГИИС ДМДК в крупном размере, не исключена уголовная ответственность по ст. 191 УК РФ. Обозначенная уголовно-правовая норма характеризуется особой бланкетностью. Более того, в настоящее время отсутствуют акты судебного толкования, разъясняющие, какие сделки с драгоценными металлами и камнями признаются сделками, совершенными в нарушение законодательства о драгоценных металлах и камнях, а также другие вопросы применения статьи 191 УК РФ. Вместе с тем, справедливо утверждение Н. Г. Кадникова о том, что «одной из основных задач уголовного права является точное и четкое определение того, какие из конфликтов между личностью и обществом представляют повышенную опасность и требуют применения уголовно-правовых мер» [9, с. 25].

Основываясь на юридическом анализе нормы, а также на существующих доктринальных разъяснениях, полагаем, что оборот драгоценных металлов и камней, сопряженный с несоблюдением положений ст. 12.2 Федерального закона «О драгоценных металлах и камнях», а также Правил функционирования ГИИС ДМДК, составляет признаки объективной стороны состава преступления, предусмотренного ст. 191 УК РФ.

Таким образом, в настоящее время происходит совершенствование системы контроля за оборотом драгоценных металлов и драгоценных камней, неотъемлемой частью которого является создание государственной интегрированной информационной системы в сфере контроля за оборотом драгоценных металлов, драгоценных камней и изделий из них на всех этапах этого оборота (ГИИС ДМДК). Полагаем, данная система позволит повысить эффективность борьбы с преступлениями в рассматриваемой области. Вместе с тем, несоблюдение требований о внесении установленной законодательством информации в ГИИС ДМДК фактически может повлечь административную или уголовную ответственность по ст.ст. 15.43, 15.46, 15,47 КоАП РФ и ст. 191 УК РФ соответственно.

Список литературы

1. Внедрение ГИИС ДМДК в ювелирной сфере: основные этапы и правовые основы // Ассоциация «Гильдия ювелиров России» URL: https://uvelir.info/news/-vnedrenie-giis-dmdk-v-yuvelirnoj-sfere-osnovnyie-etapyi-i-pravovyie-osnovyi/?.

2. Зубарев Ю. И. Вектор контроля – на нарушителя // Журнал Бюджет. 2020. № 9 (213). С. 42–45.

3. Никонович С. Л. Теория и практика расследования преступлений в сфере оборота драгоценных металлов и драгоценных камней : автореф. дис. … д-ра юрид. наук : 12.00.12. М. : Московский университет МВД России имени В.Я. Кикотя, 2015. С. 3.

4. Отчет о числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации и иных лиц, в отношении которых вынесены судебные акты по уголовным делам за 12 месяцев 2021 и 2020 года // Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. URL: http://www.cdep.ru/index.php?id=79&item=5669.

5. Постановление Правительства Российской Федерации от 26 февраля 2021 г. № 270 «О некоторых вопросах контроля за оборотом драгоценных металлов, драгоценных камней и изделий из них на всех этапах этого оборота и внесении изменений в некоторые акты Правительства Российской Федерации» (ред. от 02.04.2022) (вместе с «Правилами функционирования государственной интегрированной информационной системы в сфере контроля за оборотом драгоценных металлов, драгоценных камней и изделий из них на всех этапах этого оборота») // СПС «КонсультантПлюс».

6. Пучков Н. А. Проблемы становления и развития системы государственного регулирования добычи и производства золота в России: дис. … д-ра эконом. наук : 08.00.03. М., 2000. С. 5.

7. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Гарант.ру.

8. Федеральный закон от 26 марта 1998 г. № 41-ФЗ «О драгоценных металлах и драгоценных камнях» (ред. от 11.06.2021) // СПС «КонсультантПлюс».

9. Кадников Н. Г. Классификация преступлений по уголовному праву России : монография. М. : ИД «Юриспруденция», 2020. С. 25.

Ковригин В. С.[1],
адъюнкт факультета подготовки
научно-педагогических и научных кадров
Московского университета МВД России
имени В.Я. Кикотя

К ВОПРОСУ ОБ ИНОМ СПОСОБЕ ПРИВЕДЕНИЯ В НЕГОДНОСТЬ ОБЪЕКТОВ ЖИЗНЕОБЕСПЕЧЕНИЯ (СТ. 215² УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ)

Преступление, предусмотренное ст. 215[2] УК РФ, относится к числу деяний, посягающих на общественную безопасность. Диспозиция указанной нормы включает в себя определенный перечень альтернативных деяний, к которым относятся разрушение и повреждение объектов жизнеобеспечения. Кроме того, в этом перечне законодатель прямо указывает на «иной способ» совершения вышеуказанного преступления. Это совокупность иных действий, которые не охватываются первыми двумя вышеперечисленными, и законодатель не указал, какие действия имеются в виду, что не может не вызывать вопросов в научном сообществе.

В доктрине уголовного права большинство авторов [3; 10] под иным способом понимают совершение любых действий (бездействий), в результате которых объекты жизнеобеспечения приводятся в негодное для эксплуатации состояние, их нельзя использовать по своему назначению (к примеру, отключение подачи тепла зимой, в результате чего отопительная система жилого сектора была заморожена). А. И. Чучаев [8] понимает под этим способом невозможность использования объекта по целевому назначению: устройство препятствий к доступу объекта, замусоривание воды водозаборного участка и т. п. Под иным способом Е. Н. Туякина [7] понимает создание определенных условий, при которых объект не может использоваться по прямому назначению в течение некоторого промежутка времени. К примеру, изъятие детали, агрегата или узла из объекта жизнеобеспечения либо информационное изменение состояния технологических систем управления, что приводит к непригодности его эксплуатации, хотя качественных изменений конструктивной целостности может не происходить.

С мнением автора Е. Н. Туякиной расходятся материалы судебно-следственной практики, где имеется оправдательный приговор Ярославского областного суда [14]. Так, обвиняемый Б. осужден судом первой инстанции за приведение иным способом в негодное для эксплуатации состояние объекта жизнеобеспечения. По материалам дела Б., являясь директором организации, осуществляющей услуги по эксплуатации котельной, осуществил демонтаж оборудования котельной, без которого ее нормальное функционирование невозможно, остановив ее работу во время отопительного сезона, поставив под угрозу жизнь и здоровье граждан. В апелляционной инстанции суд установил, что под иным способом приведения объекта в негодное для эксплуатации состояние понимаются любые

[1] © Ковригин В. С., 2022.

действия (бездействия), в результате которых объект жизнеобеспечения нельзя использовать по своему назначению. Установлен факт невозможности использования котельной без указанного оборудования, однако, Б. быстро и без материальных затрат установил его обратно в тот же день. Фактически он остановил работу объекта жизнеобеспечения на непродолжительное время, то есть отключил его указанным способом, а не привел в негодность. В связи с вышеизложенным был вынесен оправдательный приговор.

Таким образом на приведение в негодность объектов жизнеобеспечения влияет обстоятельство, которое связано с временным интервалом не функционирования объекта. Кроме того, существующая практика применения данной нормы чревата возможностью уклонения виновных лиц от уголовной ответственности. В судебно-следственной практике нередки случаи, когда правоохранительными органами лицо задерживается непосредственно после совершения хищения на месте преступления при осуществлении демонтажа комплектующих частей трансформаторной станции. Если злоумышленник будет настаивать на том, что своими действиями он хотел отключить объект жизнеобеспечения на непродолжительное время, отрицая корыстный и хулиганский мотивы, то наверняка он избежит уголовной ответственности. Так, примером будет являться приговор Приозерского городского суда Ленинградской области [13], согласно которому Л. совершил покушение на кражу с незаконным проникновением в хранилище трансформаторной подстанции, где произвел разбор трансформатора, однако в ходе демонтажа получил травму и не смог продолжить свои действия. Можно сказать, что подсудимый, будучи юридически грамотным в области уголовного законодательства, мог в свою очередь избежать уголовной ответственности.

В качестве иных способов некоторые авторы [9] выделяют устройство препятствий в виде завалов или затопления, нарушение работы лифтового транспорта, радиоактивное, химическое или бактериологическое заражение, создающее препятствие для эксплуатации объекта и т. д. Хочется обратить внимание, что данные действия больше напоминают и подходят к другим смежным составам преступлений, таким как диверсия или террористический акт, где степень общественной опасности намного выше и преследуются более весомые цели и мотивы (дезорганизация органов государственной власти, подрыв экономической безопасности и обороноспособности государства).

Часть авторов [6; 7] допускают в качестве одного из способов пассивное поведение виновного, например, при неосуществлении ответственным лицом в течение длительного промежутка времени должного технического обслуживания объекта, что привело к отрицательным негативным последствиям в виде замораживания систем отопления и водоснабжения, засорения, затопления и прочее, препятствующее дальнейшей эксплуатации объекта в соответствии с целевым назначением. То есть данные действия связаны с нарушением специально закрепленных на данном объекте правил, связанных с безопасностью объекта и его функционированием. Негодность объекта наступает в результате нарушения ли-

цом специально предусмотренных правил безопасности, в основном, технологических (производственных), что приводит к остановке производственного процесса жизнеобеспечения.

Как справедливо отмечено И. И. Бикеевым, отличительной особенностью иных способов заключается в том, что в результате совершения вышеуказанных преступных действий объект жизнеобеспечения сохраняет свою первоначальную целостность, не получает каких-либо механических повреждений [1], т. е. временно выходит из эксплуатации соответствующая инфраструктура объекта жизнеобеспечения, а не сам объект. К ним можно отнести: разукомплектование узлов, деталей, агрегатов, их отсоединение, выключение, деформацию, выведение из строя, изъятие и прочее.

Наряду с физическим уничтожением и повреждением объектов жизнеобеспечения вполне допустимо отнести к числу иного способа совершения преступления с использованием информационно-коммуникационных систем, при этом объект жизнеобеспечения должен быть приведен в негодное для эксплуатации состояние [2]. Этот качественно новый вид деяния в области IT-технологий, с использованием современных компьютерных систем. Применительно к ст. 215^2 УК РФ детальное его рассмотрение в литературе не освещено.

В современное время компьютерные технологии активно включаются практически во все сферы человеческой жизни. Поэтому киберпреступность также достигает определенных успехов и наращивает преступные позиции, охватывая также сферу объектов жизнеобеспечения. В качестве иного способа совершения вышеуказанного преступления киберпреступление достаточно актуально, так как целенаправленные хакерские атаки с использованием различных вирусных программ находят свое отражение и в нашей стране. По словам заместителя секретаря Совета Безопасности Российской Федерации, в 2018 г. число опасных кибератак на критическую инфраструктуру страны выросло до 17 тыс. [15].

Данные кибератаки приводят к удалению, блокированию, изменению или иным негативным воздействиям в работе соответствующих программ, отвечающих за эксплуатацию объектов жизнеобеспечения, создающих неисправности в их функционировании, в сбоях, а также в приостановлении деятельности. Сам объект жизнеобеспечения остается статичным и внешне не изменяется, т. е. целостность объекта не нарушается, качественная сторона объекта не изменяется, но программный сбой, вызванный внешним вмешательством в функционирование объекта, приводит к его непригодности для дальнейшей эксплуатации. Одним из последних резонансных случаев в нашей стране стала хакерская кибератака на объекты жизнеобеспечения, произошедшая в мае 2017 г., когда объектами атаки стали структурные подразделения МВД России, Министерства здравоохранения Российской Федерации, банковской сферы, в результате использования злоумышленниками так называемого вируса «WannaCry» [16], в результате чего была парализована деятельность экстренных служб по всей стране. От распространения вируса «WannaCry» пострадали 74 страны. Некоторые авторы [5] называют этот вид актом кибертерроризма, который обладает не меньшей общественной опасностью по сравнению с «традиционными» способами,

помимо всего прочего обладающий своими специфическими особенностями, набирающий обороты не только в нашей стране, но и по всему миру. В 2018 г. зарегистрировано 121 тыс. киберпреступлений, наблюдается стремительный рост на 8,1 % по сравнению с 2017 г. (90 тыс.).

В теории уголовного права дискуссионным остается вопрос о правильности используемой законодательной терминологии в контексте употребления термина «способ» в диспозиции рассматриваемой статьи. Во-первых, в диспозиции статьи указаны именно альтернативные действия виновного – разрушение, повреждение, приведение иным способом в негодность. Определенная неточность понятий прослеживается и здесь, где общественно опасное деяние отождествляются со способом и наоборот. Правильно отмечено автором Р. В. Закомолдиным [4], что в этом контексте законодателю в целях устранения противоречивости и двусмысленности толкования диспозиции нормы правильнее было бы использовать формулировку термина «иное приведение».

Как показало проведенное исследование, в правоприменительной практике приведение в негодность иным способом наблюдается в 5 % случаев. Как правило, иной способ сопряжен с повреждением объектов жизнеобеспечения, а как единственный вариант преступного посягательства еще более редкое явление. Так, согласно приговору Заводского районного суда, г. Кемерово [11], подсудимый привел в негодное для эксплуатации состояние объект электросвязи, путем отсоединения проводов от коммутатора и последующего его хищения, в результате чего лишил ПАО (данные изъяты) возможности использовать объект по его целевому назначению.

Важно понимать, что применение виновным лицом иного способа включает также позволяет говорить о причинении вреда как о последствии преступления и наличии прямой причинно-следственной связи между действиями и наступившим вредом. В случае, если в ходе расследования уголовного дела данное обстоятельство должным образом не подтверждено, можно утверждать, что в действиях виновного лица отсутствует состав преступления. Так, согласно приговору Новочеркасского городского суда Ростовской области [12] подсудимыми похищены аккумуляторные батареи из базовых станций. Суд признал, что аккумуляторные батареи служат альтернативным источником питания и необходимы для обеспечения бесперебойной работы базовой станции, в частности, в случаях отключения основного питания. В случае же отключения основного питания и отсутствия при этом аккумуляторных батарей, базовая станция прекращает свою работу. Однако, изъятие аккумулятора при наличии штатного внешнего питания, не повлияет на работу базовой станции. Суд пришел к выводу, что изъятие аккумуляторных батарей из базовых станций охватывалось умыслом подсудимых только на совершение кражи, исключив излишнюю квалификацию по ст. 215^2 УК РФ.

Таким образом, законодательная формулировка термина «иной способ» в контексте ст. 215^2 УК РФ очень сложна и противоречива, требующая более детального и глубокого научного осмысления, и последующей редакционной корректировки действующей нормы.

Список литературы

1. Бикеев И. И. Ответственность за преступление против общественной безопасности, связанные с незаконным обращением с материальными объектами повышенной опасности: вопросы теории и практики : дис. ... д-ра юрид. наук. Казань, 2008. С. 274.

2. Габдрахманов Р. Л. Преступления против общественной безопасности : учебное пособие. М. : Московский университет МВД России, 2003. С. 57.

3. Диваева И. Р. Преступления против общественной безопасности : учебное пособие. Уфа: Уфимский юридический институт МВД России, 2011. С. 83–84.

4. Закомолдин Р. В. Преступные нарушения специальных правил и требований безопасности : монография // СПС «КонсультантПлюс».

5. Костенко Н. И. Уголовно-правовые и криминологические проблемы борьбы с компьютерными преступлениями : монография. М. : Юрлитинформ, 2020. С. 143, 283–285.

6. Ростокинский А. В. Преступления против общественной безопасности: современное состояние и развитие законодательного регулирования. Саратов : Изд-во «Саратовский источник», 2012. С. 243.

7. Туякина Е. Н. Уголовная ответственность за приведение в негодность объектов жизнеобеспечения : дис. ... канд. юрид. наук. Рязань, 2011. С. 67–68.

8. Комментарий к Уголовному кодексу Российской Федерации (научно-практический) / под ред. А. И. Чучаева. М. : Проспект, 2021. С. 990–991.

9. Курс уголовного права. Особенная часть. Том 4 : учебник для вузов / под ред. Г. Н. Борзенкова, В. С. Комиссарова. М. : ИКД «Зерцало-М», 2002. С. 312.

10. Уголовно-правовой аспект борьбы с преступлениями против общественной безопасности : монография / [В. Е. Степенко и др.] ; под ред. В. Е. Степенко. Хабаровск : Изд-во Тихоокеанского государственного университета, 2017. С. 115.

11. Приговор Заводского районного суда города Кемерово от 9 сентября 2021 г. по делу № 1-592/2021 // СПС «КонсультантПлюс».

12. Приговор Новочеркасского городского суда Ростовской области от 7 июня 2021 г. по делу № 1-147/2021 // СПС «КонсультантПлюс».

13. Приговор Приозерского городского суда Ленинградской области от 24 июня 2019 г. по делу № 1-131/2019 // СПС «КонсультантПлюс».

14. Приговор Ярославского областного суда от 7 октября 2016 г. по делу № 22-1408/2016 // СПС «КонсультантПлюс».

15. Сайт Совета Безопасности Российской Федерации. URL: http://www.-scrf.gov.ru/news/allnews/2629/.

16. Сайт «Лаборатории Касперского». URL: https://www.kaspersky.ru/blog/-wannacry-ransomware/16147/.

Юдина У. С.[1],
адъюнкт факультета подготовки
научно-педагогических и научных кадров
Московского университета МВД России
имени В.Я. Кикотя

К ВОПРОСУ ОБ УМЫШЛЕННЫХ УНИЧТОЖЕНИИ ИЛИ ПОВРЕЖДЕНИИ ЧУЖОГО ИМУЩЕСТВА, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В настоящее время актуальной является проблема развития информационно-коммуникационных технологий, которая исследуется многими учеными [3; 1]. В эпоху цифровизации большое количество преступлений совершается с использованием указанных технологий ввиду их стремительного развития. Не являются исключением и преступление, предусмотренное ст. 167 (умышленное уничтожение или повреждение чужого имущества) УК РФ.

Непосредственным объектом преступления, предусмотренного ст. 167 УК РФ, являются общественные отношения по поводу правомочий конкретного собственника (физического или юридического лица), который владеть, пользоваться и распоряжаться принадлежащим ему имуществом [8, с. 151]. По мнению Н. Г. Кадникова, предметом указанного преступления является чужое имущество, а именно: вещи и объекты материального мира, имеющие стоимостный эквивалент [2, с. 130]. Полагаем, что таковым выступает имущество, которое не является собственностью виновного, повреждение или уничтожение которого влечет причинение значительного ущерба, за исключением имущества, относящегося к предмету составов преступлений, ответственность за которые предусмотрена так называемыми специальными нормами в иных главах Особенной части УК РФ.

Умышленные уничтожение или повреждение чужого имущества могут совершаться различными способами, которые повышают степень опасности деяния. Следует обратить внимание на элементы и признаки квалифицированного состава преступления, закрепленного в диспозиции ч. 2 ст. 167 УК РФ. Для его конструирования законодателем использованы следующие квалифицирующие признаки: мотив – хулиганские побуждения; способ совершения деяний в виде поджога, взрыва или иной общеопасный способ; дополнительные тяжкие последствия деяний в виде неосторожного причинения человеку смерти или иных тяжких последствий. Однако, на наш взгляд, стоит подробнее рассмотреть вопрос и о «новых» возможных способах совершения указанных деяний.

Согласно данным официальной статистики, за 2019 г. было зарегистрировано более 294 тыс. преступлений, совершенных с использованием информационно-коммуникационных технологий, что почти на 70 % больше, чем за 2018 г.

[1] © Юдина У. С., 2022.

В 2020 г. количество таких преступлений возросло на 73,4 %, в том числе с использованием сети Интернет – на 91,3 %. В 2021 г. количество преступлений увеличилось на 1,4 %. Кроме того, каждое четвертое преступление совершается с использованием IT-технологий [9].

Характерны следующие примеры. Существует версия о произошедшем в 1982 г. взрыве на заводе «Автоваз». С помощью использования логической бомбы в компьютерной программе злоумышленники остановили процесс работы сборочного конвейера [10]. В 2018 г. в Тюменском федеральном центре нейрохирургии проводилась сложнейшая операция на головном мозге несовершеннолетней девочки, во время которой посредством кибератаки с использованием вируса Purgen было выведено из строя используемое врачами медицинское оборудование. Однако, благодаря высокому профессионализму последних, операция была успешно завершена без показаний приборов. Было установлено, что таким образом виновные пытались вымогать денежные средства [11]. В настоящее время число подобных случаев стремительно увеличивается [12; 13;14].

Специалисты «Лаборатории Касперского» отмечают, что злоумышленники могут удаленно взломать коробку передач автомобиля, тем самым перехватив управление, как это было сделано в США К. и Ч. в отношении автомобиля Jeep Cherokee, который передвигался со скоростью 110 км/ч [15]. Кроме того, специалисты указывают и на наличие уязвимости в инструменте мониторинга вождения Progressive Snapshot, предназначенного для наблюдения за стилем вождения водителей, с помощью которой лицо может взломать бортовую систему автомобиля [16]. С целью предупреждения подобных преступлений производителям необходимо принимать различные меры для защиты производимого ими оборудования, автомобилей и иной техники от кибератак.

Указанные примеры свидетельствуют о том, что уголовная ответственность, несомненно, выходит за рамки статей, предусматривающих ответственность за совершение компьютерных преступлений, в том числе при наступлении таких последствий, как причинение значительного ущерба собственнику или иному законному владельцу имущества.

Исходя из анализа вышеуказанных материалов, отметим, что в настоящее время для государства стоит важная задача – защитить жизнь и здоровье граждан, их имущество, необходимую инфраструктуру, объекты стратегического назначения, информацию в целом и другие объекты от кибератак.

В зарубежных странах долгое время не была установлена ответственность за совершение компьютерных преступлений, так как законодатель считал, что информатизация преступности и «виртуальные» способы совершения преступлений не мешают применять к виновным классические конструкции об уничтожении и повреждении имущества [7, с. 100]. Тем не менее, Е. А. Русскевич отмечает, что в настоящее время судам сложно дать юридическую оценку действиям лиц, использующих для совершения преступлений компьютерные системы. В качестве примера указанный автор приводит дело «Cox vs Rilley», согласно которому лицо вывело устройство из строя посредством уничтожения

информации с карты памяти. Несмотря на то, что физический облик карты сохранился, суд все же принял решение о применении нормы о повреждении чужого имущества [7, с. 100].

По мнению М. А. Простосердова, имеет место быть уничтожение или повреждение чужого имущества в киберпространстве в случае реального причинения ущерба, предметом которых являются чужие компьютер, мобильный телефон или иное высокотехнологичное электронное устройство. Указанный автор отмечает, что посредством использования вируса практически невозможно уничтожить устройство полностью, и в случае его отрицательного воздействия на программное обеспечение компьютера, деяние следует квалифицировать по ст. 273 УК РФ, однако с помощью вируса может быть уничтожен SSD-накопитель [6, с. 82–83]. На наш взгляд, в случае реального причинения ущерба общественная опасность подобных деяний намного выше, чем компьютерных преступлений.

В настоящее время достаточно распространено использование злоумышленниками такого устройства, как USB-killer, внешне похожего на USB-флеш-накопитель. С. Пескова отмечает, что оно может повреждать не только компьютеры или планшеты, но и любые другие устройства или приборы, имеющие USB Host интерфейс на борту, например, мультиметры, телевизоры, роутеры и иные. При этом автор указывает, что несмотря на вредоносные свойства USB-killer, пользователи активно приобретают его на различных площадках, включая Aliexpress и другие интернет-магазины, более того, его версии постоянно совершенствуются разработчиками [5, с. 102]. На наш взгляд, использование такого устройства злоумышленниками может привести к серьезным последствиям.

Учитывая вышеизложенное, считаем, что квалифицирующий признак умышленных уничтожения или повреждения чужого имущества, предполагающий их совершение с использованием информационно-коммуникационных технологий, в настоящее время будет излишен, однако судебное толкование в данном вопросе, определенно, необходимо. Например, по мнению Е. А. Русскевича, если виновный при использовании или распространении вредоносных программ совершает умышленные уничтожение или повреждение компьютерного оборудования с причинением значительного ущерба, то его деяние надлежит квалифицировать по совокупности преступлений, предусмотренных ст.ст. 167 и 273 УК РФ [4, с. 849]. Мы поддерживаем мнение автора, так как в подобных случаях речь идет о разных составах преступлений.

Таким образом, полагаем, что ввиду увеличения числа компьютерных преступлений в недалеком будущем в число квалифицирующих признаков уничтожения или повреждения имущества можно будет включить и искомый признак: «совершенные с использованием информационно-коммуникационных технологий».

Список литературы

1. Дмитренко А. П., Русскевич Е. А. О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий // Вестник Академии Генеральной прокуратуры Российской Федерации. 2017. № 5 (61). С. 18–22.

2. Кадников Н. Г. Квалификация преступлений и вопросы судебного толкования : монография. М. : ИД Юриспруденция, 2019.

3. Кадников Н. Г. Развитие информационных технологий как общественное благо и новая угроза охраняемым интересам граждан, общества и государства // Уголовное право и информатизация преступности: проблемы теории, практики и преподавания : сборник статей. М. :Издательский дом «Юриспруденция», 2018. С. 9–15.

4. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) / под ред. Н. Г. Кадникова. 6-е изд., перераб. и доп. М. : ИД «Юриспруденция», 2019.

5. Пескова С. Убить USB-киллера // Электроника: Наука, технология, бизнес. 2019. № 2 (183). С. 102–105.

6. Простосердов М. А. Экономические преступления, совершаемые в киберпространстве : монография. М. : Юрлитинформ, 2017.

7. Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. ... д-ра юрид. наук : 12.00.08. М., 2020.

8. Уголовное право России: учебник в 2 т. Т. 2: Особенная часть / под ред. Н. Г. Кадникова. М. : ИД «Юриспруденция», 2018.

9. Официальный интернет-сайт МВД России. URL: https://мвд.рф/reports/-item/27024130/.

10. В Тюмени хакеры атаковали центр нейрохирургии во время операции. URL: https://rg.ru/2018/07/06/reg-urfo/centr-nejrohirurgii-v-tiumeni-podvergsiahakerskojatake. html.

11. Глобальная хакерская атака затронула компьютеры российских телекоммуникационных компаний и силовых ведомств. URL: http://progressmedia.ru/news/interesnoe/globalnaya-hakerskaya-ataka-zatronula-kompyutery-rossijskih-telekommunikatsionnyh-kompanij-i-silovyh-vedomstv.php.

12. В 2020 г. российские больницы впервые подверглись хакерским атакам. URL: https://www.rbc.ru/rbcfreenews/601bb2ef9a7947fca439d624.

13. Больницы Забайкальского края подверглись хакерской атаке. URL: https://zab.ru/news/151572.

14. Сюрприз для водителя: несущийся по шоссе джип можно взломать удаленно. URL: https://www.kaspersky.ru/blog/remote-car-hack/8430/.

15. Progressive Snapshot открывает возможность взлома автомобиля. URL: https://www.kaspersky.ru/blog/progressive-snapshot-car-hacking/6761/.

Карпушкин А. В.[1],
адъюнкт факультета
научно-педагогических и научных кадров
Московского университета МВД России
имени В.Я. Кикотя

К ВОПРОСУ О ГРАНИЦАХ ПРАВОМЕРНОГО ПРИЧИНЕНИЯ ВРЕДА ПРИ ЗАДЕРЖАНИИ ЛИЦА, СОВЕРШИВШЕГО ПРЕСТУПЛЕНИЕ В ЦИФРОВОЙ СРЕДЕ

С момента появления первой гражданской электронно-вычислительной машины прошло уже более 90 лет. Цифровизация экономики, сопряженная с переходом в виртуальную среду, позволяет приобретать или продавать товар из одной точки мира в другую, даже не общаясь с владельцем этого товара. Мировые гиганты реселлинга позволяют совершать различные сделки посредством нажатия клавиш «принять условия договора» и «оплатить», в результате чего человек вступает в гражданско-правовые отношения без подписания огромного количества бумаг и личного присутствия.

Цифровая среда, являясь крупнейшим хранилищем информации, занимает важнейшую часть современной жизни любого человека. К сожалению, высокие темпы научно-технического прогресса порождают все больший интерес и для преступного мира.

В первую очередь, деятельность по выявлению, раскрытию, расследованию и пресечению преступлений, совершаемых в цифровой среде, а также с использованием информационно-телекоммуникационных технологий, а, следовательно, и задержанию лиц, их совершивших, осуществляется сотрудниками МВД России, ФСБ России и Федеральной службы войск национальной гвардии (Росгвардия) Российской Федерации. Физическое задержание виновных в подготовке и совершении названных преступлений является одной из ключевых составных частей борьбы с преступностью в целом. Но преступления, совершаемые с использованием информационно-телекоммуникационных технологий, имеют свои особенности, что необходимо учитывать при задержании виновных.

Однако, в первую очередь необходимо точно соблюдать общие требования закона. В ст. 38 УК РФ закреплено в качестве обстоятельства, исключающего преступность деяния, причинение вреда при задержании лица, совершившего преступление. Закон определяет критерии правомерности причинения вреда задерживаемому, а также и условия, при которых действия задерживающего признаются превышением мер, необходимых для задержания. В соответствии с ч. 2 ст. 38 УК РФ под превышением мер, необходимых для задержания, понимается их явное несоответствие характеру и степени общественной опасности совершенного задерживаемым лицом преступления и обстоятельствам задержания, когда лицу без необходимости причиняется явно чрезмерный, не вызываемый обстановкой вред.

---

[1] © Карпушкин А. В., 2022.

Весьма актуальной проблемой, которая стоит перед сотрудниками правоохранительных органов, осуществляющих задержание, является проблема применения физической силы, специальных средств и огнестрельного оружия [1].

Примечательно, что п. 4 ч. 1 ст. 23 Федерального закона «О полиции» допускает применение оружия для задержания лица, застигнутого при совершении деяния, содержащего признаки тяжкого или особо тяжкого преступления против жизни, здоровья или собственности, и пытающегося скрыться. Представляется, в названных условиях следует признавать правомерным производство выстрела для задержания лица, совершившего кражу с банковского счета, которое следует относить к компьютеризированным преступлениям и которое в соответствии со ст. 15 УК РФ относится к категории тяжких преступлений [2, с. 11–12].

Особый случай при задержании преступника – применение огнестрельного оружия, особенно при оценке действий как превышающих необходимые для задержания меры. Судебная практика предлагает рассматривать такие случаи в рамках ответственности по ст. 108 УК РФ.

В то же время недопустимо умалять опасность для жизни и здоровья сотрудников правоохранительных органов, осуществляющих физическое задержание. Так, «08 ноября 2021 г. в г. Санкт-Петербурге во время задержания лиц, подозреваемых в совершении «телефонного мошенничества» в результате умышленных действий задерживаемого, управляющего фургоном, вследствие наезда погиб 48-летний сотрудник СОБРа Росгвардии Евгений Захаров» [3].

Возникает закономерный вопрос об отсутствии единого подхода к определению границ правомерного причинения вреда при задержании лица, совершившего преступление. Напомним, что уголовный закон в ч. 2 ст. 38 содержит понятия оценочного характера, не подлежащие формализации и нормативному закреплению [4, с. 260]. Как результат, оценка правомерности таких действий реализуется усмотрением третьих лиц – представителями органов дознания, следствия и суда [5, с. 230]. Представляется неочевидным вопрос о мерах, необходимых для задержания лица, совершившего именно преступления в цифровой среде.

Проблемным выступает вопрос о правомерности причинения имущественного ущерба лицу, совершившему преступление, путем уничтожения, блокирования или модификации компьютерной информации, приведения в негодность его компьютерной техники, обусловленные необходимостью осуществления физического задержания. Разумеется, квалификация таких действий по ч. 2 ст.ст. 108 и 114 УК РФ в названных случаях недопустима, поскольку не причиняется вред охраняемым уголовным законом общественным отношениям, а именно жизни и здоровью человека. Более того, в Особенной части УК РФ не закреплено нормы о причинении имущественного ущерба в результате превышения мер, необходимых для задержания. Возможно, исключительные случаи, обусловленные причинением крупного имущественного ущерба, будут квалифицированы как превышение должностных полномочий (ст. 286 УК РФ), однако на сегодняшний день такая судебная практика отсутствует. Учитывая, что в современную эпоху, когда под влиянием цифровизации жизнедеятельности

происходит информационно-телекоммуникационная трансформация преступности, это проблема весьма актуальная и оценке значимости вреда при задержании лица, совершившего преступление.

Также следует задуматься и о возможности использования искусственного интеллекта при создании специальных средств, способствующих в том числе и задержанию лиц, совершивших преступления. К таковым, например, следует отнести пилотные проекты сервиса оперативного распознавания человеческой речи и семантического анализа текстов, интеллектуальной системы идентификации и маркировки граждан, причастных к совершению преступления, систем биометрической идентификации по изображению лица и многие другие.

В обозримом будущем нельзя исключать и вооружение сотрудников правоохранительных органов системами и средствами, предназначенными для воздействия на лиц, подлежащих физическому задержанию, на их компьютерную технику и иное имущество посредством электромагнитного, звукового или светового импульса. Разумеется, применение названных средств и систем возможно только после тщательного законодательного урегулирования. Нельзя забывать и о необходимости совершенствования уголовного закона в части оценки правомерности причинения вреда при задержании лица, совершившего преступление, обусловленного применением таких средств и систем, в том числе и в цифровой среде. По нашему мнению, должен быть единый подход в этой сфере, что подтверждается задачами и принципами уголовного закона (ст.ст. 2, 3 и 4 УК РФ).

При этом важно, чтобы законодательное регулирование и судебное толкование подобных случаев было более точное и конкретное, чтобы выдержать баланс между обеспечением и охраной прав, свобод и законных интересов граждан, полной и четкой реализацией всех функций правоохранительных органов и недопущением как превышения мер, необходимых для задержания, так и ущерба безопасности жизни и здоровья сотрудников правоохранительных органов.

Список литературы

1. Пункт «г» ст. 14.3 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности», п. «4» ч. 1 ст. 21 Федерального закона от 3 июля 2016 г. № 226-ФЗ «О войсках национальной гвардии Российской Федерации», п. «4» ч. 1 ст. 23 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции».

2. Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : автореф. дис. ... д-ра юрид. наук : 12.00.08. М., 2020. 52 с.

3. Лялин Р. «Раньше задерживал террористов» // Комсомольская Правда. URL: https://www.spb.kp.ru/daily/28354/4501316/.

4. Уголовное право России : учебник в 2 т. Т. 1: Общая часть / под ред. Н. Г. Кадникова. М. : ИД «Юриспруденция», 2018.

5. Дмитренко А. П. Обстоятельства, исключающие преступность деяния, в уголовном праве Российской Федерации. М. : Илекса, 2010.

Попов А. Ю.[1],
адъюнкт факультета
научно-педагогических и научных кадров
Московского университета МВД России
имени В.Я. Кикотя

К ВОПРОСУ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ В СФЕРЕ ОБОРОТА ОРУЖИЯ, ИЗГОТОВЛЕННОГО ПОСРЕДСТВОМ 3D-ПЕЧАТИ

Исходя из данных статистики МВД России за период с января 2019 г. по сентябрь 2021 г., видно, что идет тенденция к увеличению числа совершенных преступлений с использованием оружия. Ввиду нарастающей угрозы массового распространения оружия среди населения, следует предпринять ряд действенных мер, по ограничению его распространения и пресечения попыток незаконного оборота. Одним из актуальных направлений развития технологий настоящего времени является трехмерная печать. 3D-принтер предназначен для построения трехмерной формы объекта, заложенной программой модели изделия на компьютере. Эта технология позволяет напечатать самые разные изделия, начиная от обычных детских игрушек, заканчивая сложными механизмами жизнеобеспечения в медицине.

Вместе с тем доступность создания трехмерных цифровых объектов несет в себе серьезные угрозы для общественной безопасности, в том числе связанные с производством в домашних условиях прототипов огнестрельного оружия [1].

Так в 2013 г. техасский юрист Коди Уилсон приспособил технологию 3D- для создания трехмерных моделей действующих образцов оружия. Он создал сайт и программу с помощью которой стал выкладывать на сайт трехмерные чертежи различных образцов оружия и продавать любому, кто захочет их приобрести. Первые попытки органов государственной власти США остановить деятельность Уилсона были безуспешны, так как такая деятельность попадает под категорию научных изобретений и не может быть ограничена государством на права автора. По данному поводу в Конгрессе США разгорелись серьезные споры. Фактически Коди создал оружие, которое не попадает ни под один из действующих нормативно-правовых актов США, и его оборот не может быть законодательно урегулирован и ограничен. Особую озабоченность вызывает то обстоятельство, что изготовленное посредством трехмерной печати оружие является очень дешевым в производстве. По сути никаких сложных операций делать не приходится, нужно всего лишь скачать с сайта чертежи, загрузить их в принтер и дождаться распечатки готового изделия.

Сложившаяся ситуация вызывает серьезное опасение со стороны правоохранительных органов, в частности, такое оружие нельзя отследить с помощью имеющихся криминалистических методик идентификации, а обладателем такого

[1] © Попов А. Ю., 2022.

прототипа может стать совершенно любой человек, так как никаких специальных разрешений для его приобретения или производства не требуется.

Первые модели такого напечатанного оружия были одноразового действия. В частности, однозарядный пистолет Liberator.380 («Освободитель») был напечатан на принтере StratasysDimension SST, в его конструкции было 16 пластиковых деталей и металлический боек, функцию которого выполнял обычный, строительный гвоздь. Стрелял он штатным пистолетным боеприпасом НАТО 9х19 мм «Люгер». Стоимость этого образца составила 9 долл. США, произвести он мог лишь один или два выстрела, после чего ствол оплавлялся и приходил в негодность [2]. Связано это было с тем, что конструкция модели была совсем примитивной, не отвечала требованиям надежности, а материал применялся не самого лучшего качества. Но время не стоит на месте, и техническая мысль всегда развивается. За последние несколько лет Уилсон значительно усовершенствовал технологию производства своих изделий. Он стал дорабатывать чертежи моделей оружия и адаптировать их для печати по пластику, а также использовать в качестве основного материала ABS пластик.

Сегодня 3D-оружие уже может выдерживать до нескольких сотен выстрелов боевыми патронами со стальным сердечником и цельнометаллической оболочкой без смены пластикового ствола и замены частей ударно-спускового магазина. Но все осложняется тем, что данное новшество не попадает под категорию огнестрельного оружия в Российской Федерации. В Федеральном законе «Об оружии» (далее – ФЗ «Об оружии) [3] нет такого вида оружия, как изготовленного посредством 3D-печати, самого понятия и классификации. Это является отправной точкой для исследования данного вопроса, что очень актуально для быстроразвивающегося прогресса производства подобного вида оружия.

Основываясь на определенных в этом Федеральном законе видах оружия, правоохранительные органы осуществляют контроль и надзор за обладателями оружия, а также осуществляют выявление и пресечение преступлений, связанных с незаконным оборотом этого оружия. Но сложность и состоит в том, что действия с 3D-оружием не охватываются действием ст. 222 УК РФ, а также ст. 223 УК РФ. В ст. 1 ФЗ «Об оружии» огнестрельное оружие определяется как «оружие, предназначенное для механического поражения цели на расстоянии метаемым снаряжением, получающим направленное движение за счет энергии порохового или иного заряда» [4]. Исходя из этого определения, любой механизм, который конструктивно может быть приспособлен для производства выстрела, будет попадать под действие ФЗ «Об Оружии». В частности, «самопалы» и переделки из газового, травматического и охолощенного оружия. Но совсем иначе обстоит дело при производстве баллистической экспертизы 3D-оружия, когда необходимо установить, является ли это оружие огнестрельным, возможно ли из него произвести выстрел, и к какому классу оружия относится тот или иной образец. Тут и кроется самая главная проблема.

Согласно методике установления принадлежности объекта, к огнестрельному оружию [5], учитываются ряд признаков, предусмотренных п. 3 данной методики, при наличии которых устанавливается принадлежность конкретно исследуемого объекта к классу огнестрельного оружия, а именно:

– конструктивные;
– энергетические характеристики снаряда;
– надежность.

Интересующий нас для настоящего исследования признак «надежность» согласно п. 3.3, определяется как возможность производства неоднократных выстрелов без деформирования и разрушения исследуемого объекта и опасности для оператора, производящего выстрел. Затем, обращаясь к п. 6.9.1, становится понятно, что при изучении самодельно изготовленного оружия, обязательно устанавливается, обладает ли объект поражающим действием, прочностью конструкции и надежностью. Затем, формулируя выводы об относимости исследуемого объекта к классу огнестрельного оружия, эксперт будет основываться на п. 7.4, в котором четко закреплено, что «объект самодельного изготовления имеет комплекс конструктивных признаков, свойственных огнестрельному оружию, но не обладает достаточной поражающей способностью (особенности конструкции по каким-либо причинам не обеспечивают необходимой удельной кинетической энергии снаряда, конструкция разрушается при выстреле и не отвечает требованиям безопасности) [6].

Иными словами, оружие признается огнестрельным, если оно соответствует всем трем категориям признаков, и как следствие, если одна из групп критериев не будет иметь место у исследуемого образца, то к классу огнестрельное оружие данное изделие не может быть отнесено. Оценка 3D-оружия как класса оружия не может иметь смысл, так как отсутствуют критерии оценки данного оружия, и, кроме того, само подобное оружие не может быть отнесено к классу «огнестрельное оружие» только по одному критерию – критерию надежности [7], так как этот образец полностью изготовлен из полимерного пластика и при проведении экспертизы не сможет пройти неоднократный отстрел боеприпасами в силу своей хрупкости и малоустойчивой возможности к деформации. Все эти аспекты не позволяют трехмерному оружию попадать под юрисдикцию ФЗ «Об оружии».

Говоря о таком предмете преступления как трехмерное оружие, целесообразно обратиться к исследованию его понятия, особенностей и видам. Исследуя вопрос, касающийся этого вида оружия, становиться понятно, что в настоящее время общепризнанной, определенной терминологии, понятия, а также четкообозначенных видов подобного новшества просто нет, что является еще одним специфическим фактором исследования.

На сегодняшний день можно привести ряд примеров, прямо указывающих на угрозу, исходящую от бездействия властей некоторых стран по отношению к подобным новинкам. В частности, в Мьянме повстанцы начали производить на 3D-принтере карабин FGC-9. Это поддающийся 3D-печати полуавтоматический образец под пистолетный калибр 9х19 мм «Люгер», впервые спроектированный

в 2019 г. и напечатанный в начале 2020 г. Используя в качестве основы Shuty AP-9 фирмы Derwood [8].

В 2014 г. в Японии 28-летний Yoshitomo Imura вдохновившись идеями Уилсона скачал с сайта Defense Distributed несколько чертежей огнестрельного оружия и распечатал их на своем 3D-принтере, который приобрел задолго до этого за 600 долларов США. Чертежи обошлись ему в сумму 15 долл. за пару. Через несколько дней Imura снял подробный ролик-обзор своих прототипов и выложил его на свой YouTube-канал, где рассказал, как он увидел видео на YouTubeи и решил сделать тоже самое, в результате чего и получились пластиковые пистолеты конструкции Liberator.380 («освободитель»). Этим, весьма оперативно, заинтересовались правоохранительные органы Японии, так как своими действиями Yoshitomo Imura нарушил целый ряд законов, в результате чего он был осужден на два года тюремного заключения [9].

Для правильного понимания и простоты оценки при классификации, оружие, имеющее полное или частичное сходство с действующими образцами ранее разработанного вооружения, или принципиально новое изобретение, изготовленное из полимерных, композитных материалов, посредством трехмерного моделирования и печати на 3D-принтере можно определить, как *3D-оружие.*

Существуют следующие варианты 3D-оружия:

1. Изготовленное из полимерного пластика, путем полного или частичного копирования существующих образцов огнестрельного оружия.

2. Изготовленное из полимерного композитного сплава легких металлов, путем полного или частичного копирования существующих образцов огнестрельного оружия.

3. Имеющее в своей конструкции металлические элементы.

4. Не имеющее в своей конструкции металлических элементов.

Изучая проблему изготовления, распространения и использования 3D-оружия уже сейчас можно выделить несколько факторов опасности оборота подобных изделий. Самый опасный фактор этого оружия заключается в его неконтролируемом распространении, обусловленном отсутствием запретов к обороту в гражданском обращении, отсутствием современной нормативно-правовой базы, которая должна строго регулировать этот оборот. Кроме этого, есть еще ряд опасных факторов при незаконном использовании данных изделий.

Напечатанное из современных композитных материалов 3D-оружие не сможет обнаружить ни один из существующих металлодетекторов, в силу отсутствия в данных образцах металлических деталей. Кроме того, при необходимости его быстрой утилизации и сокрытии следов совершения преступления достаточно просто сжечь или растворить в кислоте использованный экземпляр.

Несмотря на все вышеперечисленные опасные факторы, в 2013 г. компанией «Solid Concepts», основанной в 1991 г. и специализирующейся на аддитивном производстве трехмерных моделей различного оборудования бизнес-продуктов, аэрокосмических, беспилотных систем, медицинского оборудования и устройств, литейных моделей, промышленного оборудования и дизайна, а также транспортных деталей создан «оружейный проект». Координатор проекта Эрик Матчлер

изготовил пробную партию моделей армейского пистолета Colt M1911 из металла, посредством его печати на трехмерном принтере из специального металлического сплава. Модель была кастомизирована (добавили современные средства обвеса оружия) и состояла из 35 деталей, изготавливаемых трехмерной печатью. Свое изделие Матчлер испытал в тактическом тире г. Лос-Анджелеса, где произвел его отстрел штатным для такой модели пистолета боеприпасом как 45ACP, который является одним из самых мощных пистолетных боеприпасов, что в переводе на российские обозначения калибров в мм составляет (11,43х23). Напечатанный пистолет выдержал более 1000 выстрелов без деформаций основных частей и опасности для стрелка. Сама по себе технология производства достаточно уникальна. Ее суть заключается в прямом лазерном спекании металла и придании ему необходимой формы с помощью заложенной программы, основанной на трехмерных чертежах модели пистолета. К слову Матчлер смог беспрепятственно, путем свободного, открытого доступа скачать эти чертежи с сайта проекта «Defense Distributed» о котором уже было сказано ранее. Изготовление пистолета происходит в течении 36 часов в зависимости от модели используемого принтера и исходного сырья. Но сам Матчлер пояснил, что произвести такой прототип в домашних условиях пока невозможно.

Вместе с тем, говоря о металлической трехмерной печати, можно смело утверждать, что данный тип должен подпадать под категорию огнестрельного оружия, что указано в ФЗ «Об оружии» и «Методических рекомендациях экспертам», как следствие и незаконные действия с таким оружием подлежат квалификации по ст.ст. 222 или 223 УК РФ, так как данные модели имеют все признаки огнестрельного оружия, в том числе и надежность, а незаконный их оборот будет соответствующим образом выявляться и пресекаться. Однако, в отношении изготовленных из ABS пластика изделия, возникает прямая необходимость в их экспертной оценке, которая в 100 % случаях даст заключение о невозможности признания такого пистолета огнестрельным оружием, что исключает привлечение к уголовной ответственности лиц, осуществляющих их незаконный оборот по статьям, предусмотренным действующим уголовным законодательством Российской Федерации.

В связи с этим целесообразно внести ряд определенных поправок в законодательство, а именно, в ФЗ «Об оружии», вводя в оборот понятие 3D-оружия как класса, в методику установления принадлежности объекта к огнестрельному оружию, обозначая новый п. 7.4.1, раскрывающий потенциал вводимого нового класса оружия, а также в ст. 223 УК РФ ввести в действие новую часть, обозначающую изготовление оружия посредством трехмерного моделирования и печати на 3D-принтере. Эти изменения смогут в полной мере предотвратить риск неконтролируемого распространения подобного новшества, снизить вероятность попыток его изготовления, а также обеспечить законное разрешение уголовных дел, связанных с этим новым видом оружия.

Список литературы

1. E-commerce и взаимосвязанные области (правовое регулирование) : сборник статей / [А. А. Богустов и др.]. М. : Статут, 2019.

2. Медведицкова Л. В., Кочерова Л. А., Неупокоева И. А., Нестеренко А. В. Технологии 3D-печати при изготовлении огнестрельного оружия. Проблемы в расследовании преступлений : диссертационные исследования // Закон и право. 2019. С. 4. URL: https://clck.ru/bVajC.

3. Федеральный закон № 150-ФЗ «Об оружии» : принят Государственной Думой 13 ноября 1996 г. : одобрен Советом Федерации 13 ноября 1996 г. // Собрание законодательства Российской Федерации. 1996. № 51. Ст. 5681.

4. Методика установления принадлежности объекта к огнестрельному оружию. М. : ГУ ЭКЦ МВД России, 2000. URL: https://clck.ru/bVakQ.

5. Пистолет из 3D-принтера: эволюция самодельного пластикового оружия. URL: https://clck.ru/bVamK.

6. Японца посадили на 2 года за распечатку пистолета на 3D принтере. URL: https://clck.ru/bVanE/.

7. Очумелые ручки: 3D-печать оружия в США может выйти из-под контроля. URL: https://clck.ru/bVane.

Меерсон В. Р.[1],
адъюнкт факультета подготовки
научно-педагогических и научных кадров
Московского университета МВД России
имени В.Я. Кикотя,
научно-педагогический факультет
УО «Академия МВД Республики Беларусь»

К ВОПРОСУ О ДЕЗОРГАНИЗАЦИИ ФУНКЦИОНИРОВАНИЯ УЧРЕЖДЕНИЯ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Современное состояние, а равно перспективное развитие современного общества требуют внесения определенных корректив в различных сферах деятельности личности. Социальное прогнозирование и непрекращающийся научный поиск решения ряда существующих проблем не может существовать в отрыве от окружающей реальности. Этот тезис в полной мере справедлив и к области юридической науки, которая напрямую взаимосвязана с развитием общественных отношений. Разумеется, далеко не все действующие нормативные правовые акты и содержащиеся в них правовые нормы являются в полной мере соответствующими текущему состоянию регулируемых (охраняемых) отношений. Это связано в первую очередь с определенными огрехами, возникающими в нормотворческом процессе, неучетом законодателем требующей внимания проблематики (а также актуальных в данной сфере научных изысканий), значительным объемом законодательных актов и т. д. В этой связи необходимо обратить внимание и на особенности науки юриспруденции, которая отчасти остается достаточно консервативной и под влиянием классической парадигмы не всегда приемлет какие-либо новые концептуальные (дискуссионные) положения. Вместе с тем, следует отметить позитивную динамику современных отраслевых юридических наук, которые под влиянием формирующейся правоприменительной практики достаточно эффективно реагируют на постоянно меняющуюся правовую реальность.

Не вызывает никаких сомнений факт того, что в настоящее время цивилизация вступила в эпоху колоссального проникновения технологий практически во все сферы жизни. В начале третьего десятилетия XXI в. уже достаточно сложно представить отдельные процессы без использования информационно-коммуникационных технологий (как в специализированных, так и в повседневных сферах человеческой деятельности). Вместе с тем, использование технических средств детерминирует прогресс и обуславливает также качественно иной уровень взаимодействия в социуме. Широкая распространенность и достаточно легкая доступность современных технических средств также способствует и значительному увеличению числа преступлений, сопряженных с их использованием.

[1] © Меерсон В. Р., 2022.

В настоящее время указанный признак, его значение при совершенствовании законодательства, а также квалификации преступлений является достаточно актуальной темой в современной уголовно-правовой науке.

Учитывая вышеизложенное, заслуживает внимания вопрос, касающийся совершения различных преступлений в контексте указанного способа. В настоящее время актуальной является область уголовно-правового исследования действий, дезорганизующих функционирование учреждений уголовно-исполнительной системы, в том числе и в рамках сравнительно-правового анализа законодательства союзных государств – Российской Федерации и Республики Беларусь. Обращая внимание на специфику конструкции объективной стороны рассматриваемых преступлений, содержащихся в национальном уголовном законодательстве, следует отметить определенную близость регламентации таковых. Однако это не исключает некоторых особенностей, которые в определенной мере взаимосвязаны с рассматриваемой темой.

Возвращаясь к распространению информационно-коммуникационных технологий следует обратить внимание, что на особенности исполнения и отбывания наказания также повлиял данный глобальный процесс. Исходя из специфики учреждений уголовно-исполнительной системы, в частности тех из них, которые обеспечивают изоляцию от общества, необходимо выделить серьезную проблему, которая касается нелегального проникновением вещей и предметов, которые лицам, содержащимся в указанных учреждениях, запрещается приобретать, изготавливать, иметь при себе, а также получать через разрешенные передачи либо входящие почтовые отправления. Указанные перечни запрещенных предметов регламентированы соответствующими подзаконными нормативными актами и сходны в Российской Федерации и Республике Беларусь. Наряду с колюще-режущими предметами, оружием и иными устоявшимися запрещенными предметами в указанные перечни с учетом динамичной цифровизации включены также электронно-вычислительные машины, носители информации, а также средства мобильной связи и коммуникации, либо комплектующие к ним. Важно подчеркнуть, что использование указанных предметов в первую очередь является нарушением установленных уголовно-исполнительным законодательством ограничений, связанных с особенностями отбывания наказания в виде лишения свободы (либо содержания под стражей). В то же время негласно доставленные в учреждение уголовно-исполнительной системы технические средства коммуникации активно используются содержащимися в данных учреждениях лицами для совершения новых преступлений.

Это относится к так называемому «телефонному мошенничеству», совершаемому осужденными (заключенными), что уже становилось предметом рассмотрения отдельными авторами [1, с. 24–30; 2, с. 103–105; 3, с. 215–219]. Как отмечают А. В. Акчурин и Г. Х. Шаутаева, подавляющая доля (85,6 %) из общего числа зарегистрированных мошеннических действий, совершаемых осужденными, осуществлялись с использованием средств мобильной связи [4, с. 59]. Стоит акцентировать внимание на указываемые авторами сведенья, которые сви-

детельствуют о существующем значительном «насыщении» средствами информационно-коммуникационных технологий мест отбывания наказаний (содержания под стражей).

Описываемые обстоятельства позволяют прийти к выводу о том, что наличие у содержащихся в учреждениях уголовно-исполнительной системы лиц технических средств коммуникации позволяют осуществлять преступную деятельность специфическим способом, в том числе и дезорганизацию функционирования указанных учреждений. Выражаться подобные преступные посягательства могут в угрозе применения насилия со стороны осужденных (заключенных), осуществляемой с использованием технических средств в отношении представителей администрации учреждений в связи с осуществлением ими служебной деятельности, либо их близких. Звонки (сообщения) с угрозами сотрудникам, обусловленные их служебной деятельностью, могут оказывать значительное влияние на процесс исполнения наказаний, пагубно отразиться на упорядоченном функционировании соответствующего пенитенциарного учреждения.

Следует отметить, что в аспекте указанного примера российским законодателем в ст. 321 УК РФ закреплена одна из форм дезорганизации выражающаяся в психическом насилии в отношении субъектов уголовно-исполнительной деятельности, что является позитивной особенностью в сравнении с аналогичной ст. 410 УК Республики Беларусь. Указанные в белорусской статье формы дезорганизации в виде «терроризирования осужденных» и «нападения на представителей администрации», достаточно расплывчатые по своему толкованию, и, исходя из сложившейся правоприменительной практики, заключаются только в физическом насилии. Поэтому данное обстоятельство требует изменения существующих подходов к регламентации рассматриваемого преступления и прямого указания в тексте белорусского уголовного закона на «насилие», а также «угрозу применения насилия» ориентируясь на положительный пример действующей конструкции соответствующей статьи российского УК.

Наряду с вышеуказанным, достаточно дискуссионным является само понятие «дезорганизации», в особенности в преломлении через призму использования информационно-коммуникационных технологий. Видится, что всеобъемлющая цифровизация функционирования учреждений уголовно-исполнительной системы детерминирует как и оптимизацию процессов, так и создает определенные условия для возникновения новых форм дезорганизации в перспективе. Например, преступник имея доступ к инфраструктуре, а также определенные знания, может, осуществив приготовительную деятельность (при наличие технических средств), нанести серьезный ущерб упорядоченной и стабильной деятельности пенитенциарного учреждения. Аналогичная по степени общественной опасности ситуация может возникнуть при использовании лицами, содержащимися в исправительных учреждениях, технических носителей информации, полученных по каналам поставки запрещенных предметов и содержащих вредоносные программы, которые могут быть загружены на персональные рабочие места сотрудников и распространены по всем служебным компьютерам. Указанное может

привезти к уничтожению, модификации служебных данных, несанкционированному доступу и ознакомлению с ними злоумышленников и т. п. В данных примерах определенным образом отражается использование в преступных целях технических средств, способное привезти к значительной дестабилизации работы исправительного учреждения сопряженной с достаточно вероятным наступлением тяжких последствий. Поэтому чем больше процессы исполнения наказания будут переходить на применение «высоких технологий», тем вероятнее будет множиться опасность возникновения угроз, обусловленных уязвимостями в любой компьютерной системе.

В завершении, необходимо отметить, несколько выводов. Во-первых, развитие и распространение информационно-коммуникационных технологий пронизывает все сферы общественных отношений. Не исключением в данном аспекте являются и относительно изолированные режимные учреждения, к которым непосредственно относятся учреждения уголовно-исполнительной системы. Во-вторых, действия, дезорганизующие функционирования учреждения уголовно-исполнительной системы, вполне могут осуществляться с использованием технических средств, оборот которых хоть и запрещен для лиц, содержащихся в данных учреждениях, однако, далеко не является еще решенной до конца проблемой в настоящее время. В-третьих, совершенствование уголовного законодательства, а также теоретических и практических подходов к пониманию сущности такого преступления как дезорганизация функционирования учреждения уголовно-исполнительной системы, позволит на перспективу успешнее бороться с соответствующими преступными посягательствами.

Поэтому следует дать новое концептуальное определение понятия «дезорганизация», позволяющее отойти от устоявшегося подхода, отождествляющего ее лишь как насилие в отношении субъектов уголовно-исполнительных правоотношений. Так, в контексте рассматриваемого преступления, проанализировав особенности содержания элементов и признаков в двух союзных государствах, под дезорганизацией учреждения уголовно-исполнительной системы (места содержания под стражей) следует понимать общественно опасные, виновные, противоправные, наказуемые действия лица, содержащегося в соответствующих учреждениях, в отношении субъектов уголовно-исполнительной деятельности (учреждения в целом), выражающиеся в различных альтернативных формах, препятствующие законодательно регламентированному функционированию учреждения, противодействующие достижению целей правосудия и реализации вынесенных управомоченными государственными органами актов в сфере исполнения и отбывания (в соответствии с установленным порядком) меры пресечения в виде заключения под стражу, уголовного наказания, либо иной меры государственного принуждения.

Список литературы

1. Грязева Н. В. Предупреждение мошенничеств, совершаемых осужденными, содержащимися в исправительных учреждениях, с использованием

средств мобильной связи: проблемы и пути их решения // Вестник Самарского юридического института. 2019. № 5 (36). С. 24–30.

2. Филипьев Р. А. Телефонное мошенничество в стенах пенитенциарных учреждениях ФСИН России // Вестник молодого ученого Кузбасского института : сборник научных статей / отв. ред. Н. Н. Ивашко. Новокузнецк : Кузбасский институт Федеральной службы исполнения наказаний, 2021. С. 103–105.

3. Ципилев С. Н. О телефонных мошенничествах, совершаемых осужденными, содержащимися в исправительных учреждениях уголовно-исполнительной системы // Актуальные вопросы права : сборник научных трудов / под общ. ред. В. Н. Некрасова. Вологда : Вологодский институт права и экономики Федеральной службы исполнения наказаний, 2020. С. 215–219.

4. Акчурин А. В., Шаутаева Г. Х. О некоторых обстоятельствах совершения мошенничества осужденными, отбывающими наказание в исправительных колониях // Вестник Нижегородской академии МВД России. 2017. № 2 (38). С. 58–63.

Виссаров В. А.[1],
адъюнкт факультета подготовки
научно-педагогических и научных кадров
Московского университета МВД России
имени В.Я. Кикотя

К ВОПРОСУ СОЦИАЛЬНОЙ ОБУСЛОВЛЕННОСТИ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НЕЗАКОННЫЙ ОБОРОТ АЛКОГОЛЬНОЙ ПРОДУКЦИИ, СОВЕРШАЕМЫЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В уголовно-правовой доктрине вопросы социальной обусловленности установления уголовной ответственности неразрывно связываются с определением критериев криминализации и декриминализации общественно-опасных деяний [1, с. 100]. Основополагающее значение при их анализе отводится отсутствию противоречий с существующими социально-правовыми отношениями.

Нарастающий процесс внедрения современных информационных технологий в экономику государства диктует необходимость постоянного обновления отраслевого законодательства. Так, в 2016 г. в сферу производства и оборота алкогольной продукции была введена единая государственная автоматизированная информационная система (ЕГАИС) целями функционирования которой является учет алкогольной продукции на всех этапах ее оборота, а также устранение и сокращение объема контрафактной продукции на потребительском рынке.

Вместе с тем ускоренная цифровизация предпринимательской деятельности порождает возможность причинения вреда общественным отношениям, в которых она функционирует. Как отмечает Н. Г. Кадников, одним из наиболее распространенных способов ответа на возникающие угрозы является отнесение определенных общественно опасных деяний к числу преступных путем закрепления признаков составов соответствующих преступлений в нормах Особенной части уголовного законодательства [5]. Следовательно, вышеуказанная возможность обуславливает появление уголовно-правовых норм, устанавливающих запрет на совершение некоторых общественно-опасных действий.

Уголовная политика последних лет наглядно демонстрирует повышенное внимание со стороны государства к противодействию незаконным проявлениям в сфере предпринимательской деятельности. Об этом свидетельствует, в частности, введение в Уголовный кодекс Российской Федерации (далее – УК РФ) ст. 171.3, предусматривающей ответственность за незаконные производство и оборот этилового спирта, алкогольной и спиртосодержащей продукции. Как указывает М. Г. Жилкин, незаконные действия в рассматриваемой сфере предпринимательской деятельности обладают значительной степенью общественной опасности [8]. В этой связи, установление уголовной ответственности за вышеперечисленные незаконные действия представляется нам социально обусловленным [4].

---

[1] © Виссаров В. А., 2022.

Введение ст. 171.3 УК РФ значительно расширило границы уголовно-правового регулирования производства и оборота алкогольной продукции. Так, наряду с запретом на осуществление незаконных производства и оборота алкогольной продукции (ст. 171.3 УК РФ); незаконной розничной продажи алкогольной и спиртосодержащей пищевой продукции (ст. 171.4 УК РФ), продолжают существовать нормы об ответственности за розничную продажу несовершеннолетним алкогольной продукции (ст. 151.1 УК РФ); производство, приобретение, хранение, перевозку в целях сбыта или продажу немаркированной алкогольной продукции (ст. 171.1 УК РФ); контрабанду алкогольной продукции и (или) табачных изделий (ст. 200.2 УК РФ); изготовление в целях сбыта или сбыт поддельных акцизных марок либо федеральных специальных марок для маркировки алкогольной продукции (ст. 327.1 УК РФ). Анализ положений отмеченных норм показывает, что дифференциация уголовной ответственности за их совершение произведена посредством таких признаков как: размер предмета преступления (ст.ст. 171.1, 171.3 200.2 УК РФ); способ его совершения (ст.ст. 171.4, 327.1 УК РФ); субъект преступления (ст. 151 УК РФ).

На доктринальном уровне превалирующей является точка зрения о том, что любая правотворческая деятельность состоит в анализе объективных общественных процессов (позитивных и негативных), а установление уголовной ответственности должно соответствовать уровню развития общественных отношений и их закономерностям [6, с. 114; 7]. Между тем, не всегда принимаемые законодательные решения в части изменения уголовного закона осуществляются с учетом принципов и тенденций эволюции уголовно-правовой науки и практики.

Так, несколько противоречивой представляется позиция законодателя в части оценки степени общественной опасности незаконного оборота алкогольной продукции, совершаемой с использованием информационных технологий. В пояснительной записке к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» он отмечает, что на долю реализации без соответствующей лицензии алкоголя с использованием сети Интернет, приходится от 50 до 70 % от объема продаваемого спиртного [9]. О высокой степени распространенности исследуемого деяния (до введения ст. 171.3 УК РФ), свидетельствует и проведенное автором выборочное изучение приговоров, в 40 % из которых отмечалось использование информационных технологий. Одним из многочисленных примеров является следующий случай. К. узнав о возможности приобретения алкоголя через Интернет, для пробы приобрел три бутылки водки, которая по мнению подсудимого оказалась качественной. После чего, К. приобрел большое количество спиртного и развез по двум арендованным им гаражам. В ходе проведения оперативно-следственных мероприятий К. задержали, а незаконно хранящуюся продукцию изъяли из незаконного оборота [10]. Однако, несмотря на указанные факты, действующая редакция ст. 171.3 УК РФ соответствующего квалифицирующего признака все же не содержит.

Проведенный анализ уголовных дел, возбужденных по фактам незаконного сбыта алкогольной продукции, показывает, что использование информационных

технологий является фактором, существенно затрудняющим выявление лиц, совершивших это преступление. Так, К. Н. Б. и К. Б. Ч., используя информационно-телекоммуникационную сеть Интернет осуществили незаконную закупку у неустановленного следствия лица этиловый спирт в крупном размере. Договорившись с неустановленным лицом о встрече на 1622 км трассы М5 «Москва – Челябинск», указанные лица перегрузили из его автомобиля этиловый спирт, расфасованный не менее чем в 266 емкостях объемами 10 и 21,5 литров каждая в собственные автомобили, после чего осуществляли его незаконное хранение на арендованном складе [11]. Лица, сбывшие эту продукцию, не установлены. Это объясняется тем, что имеющиеся в распоряжении преступников средства (специальное программное обеспечение VPN, использование прокси серверов и др.) позволяют скрыть следы противоправной деятельности задолго до начала проверочных мероприятий.

Характеризуя общественную опасность рассматриваемого способа преступления, стоит акцентировать внимание и на высокой степени его латентности.

Отмеченные обстоятельства свидетельствует о том, что незаконный оборот алкогольной продукции, совершенный с использованием информационных технологий, обладает более высокой общественной опасностью, что должно найти свое отражение в уголовном законе.

Разумеется, как отмечает С. Е. Вицин, иногда происходящие изменения бывают настолько существенными, что не только общественное мнение и обыденное правосознание, но и оценки специалистов не могут охватить их своим предвидением [3]. Тем не менее, до установления ответственности за незаконные производство и оборот алкогольной продукции, уголовный закон насчитывал значительное количество примеров своевременного реагирования на изменения, происходящие в общественных отношениях. Так, в ст. 228.1 УК РФ сбыт наркотических средств, психотропных веществ или их аналогов совершенный с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет), предусмотрен в качестве квалифицирующего признака. Иллюстрацией успешного принятия мер для борьбы с мошенничеством с использованием информационных технологий является и криминализация его специальных видов (ст.ст. 159–159.6 УК РФ). Появление указанных уголовно-правовых норм обусловлено тщательным теоретико-практическим анализом уровня развития общественных отношений, которые, по мнению Л. И. Спиридонова, определяют пределы их уголовно-правового регулирования [2, с. 76].

Таким образом, незаконный оборот этилового спирта, алкогольной и спиртосодержащей продукции с использованием информационных технологий обладает повышенной степенью общественной опасности и высокой степенью распространенности. Отсутствие противоречий действующему законодательству Российской Федерации и невозможность противодействия данному способу совершения преступления нормами иных отраслей права свидетельствуют о возможности выделения в ст. 171.3 УК РФ соответствующего квалифицирующего признака.

Список литературы

1. Кудрявцев В. Н. Закон, проступок, ответственность. М. : Наука, 1986.

2. Спиридонов Л. И. Социология уголовного права. М.: Юридическая литература, 1986.

3. Вицин С. Е. О научно-правовых предпосылках минимизации преступности как негативно отклоняющегося поведения // Вестник Академии права и управления. 2004. № 4. С. 33–38.

4. Виссаров В. А. Социальная обусловленность уголовной ответственности за незаконные производство и оборот алкогольной продукции // Вестник Российского университета кооперации. 2021. № 3 (45). С. 86–89.

5. Кадников Н. Г., Кадников Б. Н., Коробец Б. Н. К вопросу о новеллах уголовного закона в свете теории криминализации и декриминализации // Уголовная политика: теория и практика. Общество и право. 2015. № 3 (53). С. 60–62.

6. Кригер Г. А., Кузнецова Н. Ф. Проблемы социальной обусловленности уголовного закона // XXV Съезд КПСС и дальнейшее укрепление социалистической законности. М., 1977.

7. Кудрявцев В. Н. Криминализация: оптимальные модели // Уголовное право в борьбе с преступностью. М., 1995. С. 3–20.

8. Жилкин М. Г. Преступления в сфере предпринимательской деятельности: проблемы классификации и дифференциации ответственности : монография. М. : Юриспруденция, 2019 // СПС «КонсультантПлюс».

9. Пояснительная записка к проекту федерального закона / Паспорт проекта Федерального закона № 50030-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» (в части усиления уголовной ответственности за нелегальный оборот этилового спирта, алкогольной и спиртосодержащей продукции) (внесен членами Совета Федерации ФС РФ Е. В. Бушминым, С. Н. Рябухиным, В. Б. Шубой, депутатом Государственной Думы ФС РФ И. И. Гильмутдиновым) // «КонсультантПлюс».

10. Приговор Промышленного районного суда г. Самары от 16 ноября 2016 г. по делу № 1-651/2016. / Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/regular/doc/Nkc5e847AZWO/.

11. Приговор Усть-Катавского районного суда Челябинской области от 27 мая 2020 г. № 1-60/2020 // Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/regular/doc/QPuDHfTLnV5r/.

Христофорова С. А.[1],
адъюнкт факультета
научно-педагогических и научных кадров
Московского университета МВД России
имени В.Я. Кикотя

ПРИНУЖДЕНИЕ К ДАЧЕ ПОКАЗАНИЙ, СВЯЗАННОЕ С УГРОЗОЙ РАСПРОСТРАНЕНИЯ КОМПРОМИТИРУЮЩИХ СВЕДЕНИЙ В СЕТИ ИНТЕРНЕТ

Согласно Всеобщей декларации прав человека от 10 декабря 1948 г., каждый человек неприкосновенен и не может быть подвергнут пыткам или жестоким, бесчеловечным или унижающим достоинство обращениям [1]. Подобное законодательное требование содержится и в ч. 2 ст. 21 Конституции Российской Федерации [2].

С учетом такого представления, государство, выступая правовым рычагом защиты граждан, обязано исключить произвольное вмешательство в сферу личностной автономии при помощи нормативно-правовых запретов.

Так, например, одни из таких запретов регламентируется в нормах Уголовно-процессуального кодекса Российской Федерации. Согласно ч. 2 ст. 9 УПК РФ «Никто из участников уголовного судопроизводства не может подвергаться насилию, пыткам, другому жестокому или унижающему человеческое достоинство обращению» [3]. Другие – в нормах Уголовного Кодекса Российской Федерации, регламентирующих различные составы преступлений и предусматривающих уголовную ответственность за них [4].

Учитывая тематику данной статьи, представляется целесообразным остановиться на таком противоправном деянии, как принуждение к даче показаний, уголовная ответственность за которое предусмотрена ст. 302 УК РФ.

Актуальность изучения данной уголовно-правовой нормы, как верно в своих научных трудах отмечают И. Ю. Бунева [5], А. А. Калашникова [6], Ю. И. Кулешов [7], Е. А. Авдеева [8], В. Л. Кудрявцев [9], заключается в отсутствии практики ее применения. На данный факт указывает то обстоятельство, что распространенность этого противоправного явления явно не соответствует уровню регистрации преступлений указанной категории.

Подтверждением этому служат статистические данные Федерального казенного учреждения «Главный информационно-аналитический центр МВД России», анализ которых указывает на немногочисленность регистрации случаев совершения указанных преступлений. Так, в 2015 г. было зарегистрировано 4 преступления, в 2016–2017 гг. – 0 преступлений, в 2018 г. – 2 преступления, в 2019 г. – 0 преступлений, в 2020 г. – 2 преступления, в 2021 г. – 1 преступление [10]. И это, несмотря на то, что количество обращений граждан с жалобами на противоправные действия сотрудников правоохранительных органов, связанные

[1] © Христофорова С. А., 2022.

с принуждением к даче показаний, намного больше. По материалам рассмотрения таких обращений, как правило, выносятся постановления об отказе в возбуждении уголовного дела по основаниям, предусмотренным: п. 1 ч. 1 ст. 24 УПК РФ (отсутствие события преступления) и п. 2 ч. 1 ст. 24 УПК РФ (отсутствие в деянии состава преступления) [3]. Такой вывод следует исходя из анализа судебной практики рассмотрения заявлений граждан, связанных с обжалованием таких решений (постановлений об отказе в возбуждении уголовных дел), за период с 2015 г. по 2021 г. И, как правило, указанные заявления оставляются судами без удовлетворения по причине отсутствия в представленных материалах фактических данных, указывающих на необоснованность таких решений. Вследствие чего, у граждан возникает разочарование в правовой защищенности, а также рождается недоверие ко всей нашей системе правосудия.

Кроме того, в правоприменительной практике существуют сложности, связанные с расследованием уголовных дел данной категории. Такие сложности обусловлены различными причинами, среди которых целесообразно отметить: отсутствие или недостаточность доказательств, подтверждающих виновность лица; противодействие со стороны субъекта данного преступления, а также его защиты и т. д. Многие из таких дел не доходят до суда и прекращаются еще на стадии предварительного следствия по причине недоказанности вины потенциального субъекта преступления [3].

Поэтому неслучайно то обстоятельство, что количество уголовных дел указанной категории, направленных в суд с обвинительным заключением, единично. На это указывает анализ статистических данных, полученных из Федерального казенного учреждения «Главный информационно-аналитический центр МВД России». Так, в 2015 г. в суд было направлено только 1 уголовное дело, в 2016–2020 гг. – 0 уголовных дел, в 2021 г. – 3 уголовных дела [10].

Согласно обозначенной статистике можно заметить, что количество уголовных дел, направленных в суд в порядке ст. 222 УПК РФ [3], в период с 2015 г. по 2021 г., порядком меньше количества уголовных дел, возбужденных за этот же период времени.

Альтернативность способов совершения преступления, содержащихся в ст. 302 УК РФ, говорит о многогранности проявлений указанного противоправного деяния и в части первой рассматриваемой статьи, законодателем отражены такие как: угроза, шантаж и иные незаконные действия.

В рамках данной статьи остановимся на таком способе совершения указанного преступления, как шантаж.

В доктрине уголовного права существует плюрализм научных взглядов, касающихся определения понятия «шантаж», рассматриваемого в ч. 1 ст. 302 УК РФ. Так, например, ряд ученых, исследовавших уголовно-правовые и практические аспекты указанного деяния, полагают, что «шантаж» следует понимать, как:

– «разновидность угроз, состоящих в высказывании намерения разгласить позорящие лицо сведения. Эти сведения должны иметь такое содержание, которое потерпевший желает сохранить в тайне. Такие сведения могут быть правдивыми или ложными» [11];

– «способ принуждения к даче показаний потерпевшего, заключающийся в угрозе разоблачения, разглашения позорящих, сфабрикованных сведений с целью получения нужных материалов» [12];

– «угроза распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких» [13];

– «одна из форм угрозы, выражающаяся в запугивании чем-либо в целях создания обстановки, под влиянием которой указанные в законе лица вынуждаются к даче показаний или к даче заключения» [14];

– «угроза распространения позорящих, а равно иных сведений, оглашение которых может нанести ущерб чести, достоинству потерпевшего или его близких, независимо от того, являются ли они действительно таковыми для данного лица, соответствуют или нет истине» [15].

Проанализировав вышеизложенные мнения, можно резолютировать, что под принуждением к даче показаний или заключения путем шантажа следует понимать незаконные действия следователя или лица, производящего дознание, а равно другого лица с ведома или молчаливого согласия следователя или лица, производящего дознание, состоящие в угрозе распространения компрометирующих сведений (независимо от того, действительные ли они или ложные), и оглашение которых может нанести ущерб нематериальным благам (чести, достоинству или подрыв репутации) потерпевшего или его близких, целью которой является вынуждение лица, подвергнутого допросу или предоставлению заключения, дать те показания или то заключение, которые от него требуют, и не имеет значение, будут ли они правдивыми или нет.

К таким сведениям следует относить: факты биографии, сведения о заболеваниях, сведения о скрытых физических недостатках, сведения о совершенных поступках, сведения о привычках и увлечениях, сведения о нравственных, политических, сексуальных и религиозных пристрастиях и т. д.

Указанная информация может быть передана потерпевшим следователю или лицу, производящему дознание, добровольно, а также помимо воли. В последнем случае имеются в виду такие сведения о потерпевшем, которые стали известными следователю или лицу, производящему дознание, в ходе производства по уголовному делу, и разглашение которых, как известно, запрещено уголовно-процессуальным законодательством Российской Федерации (ст. 161 УПК РФ) [3].

Анализ изученных научных материалов в контексте ст. 302 УК РФ, позволяет указать на то, что до настоящего времени в науке уголовного права не рассматривался вопрос о принуждении к даче показаний, связанном с угрозой распространения сведений, компрометирующих потерпевшего или его близких в сети Интернета, и это, несмотря на то, что сфера информационно-коммуникационных технологий, на сегодняшний день, приобрела достаточно масштабный характер в жизнедеятельности всего общества. Интернет стал неотъемлемой частью жизни каждого человека. При этом, известен и тот факт, что нередко информационно-коммуникационные сети могут быть использованы для совершения различных правонарушений, посягающих на конституционные права и законные

интересы личности. К таким можно отнести нематериальные блага, присущие каждому человеку с рождения и являются неотчуждаемыми.

Так, ч. 1 ст. 23 Конституции Российской Федерации закреплено право на защиту чести и доброго имени [1]. Статьей 150 Гражданского кодекса Российской Федерации регламентировано право на защиту личного достоинства, чести и доброго имени, деловой репутации, неприкосновенности частной жизни, личной и семейной тайны, а также иных личных неимущественных прав [16]. Разумеется, такие законодательные положения применимы и к сети Интернета.

Обязанностью государства, в частности, правоохранительных органов, в силу выполнения ими своих профессиональных функций, является защита вышеуказанных естественных прав. Однако, как показывает практика, не исключаются случаи нарушения указанных прав самими правоохранителями. В данном контексте речь идет о том, когда следователь или лицо, производящее дознание, а равно другое лицо с ведома или молчаливого согласия следователя или лица, производящего дознание, угрожает потерпевшему распространением компрометирующих сведений о нем в информационно-телекоммуникационных сетях, включая сеть Интернет, с целью получить те или иные показания, либо заключение, которые требуются для «быстрого» и «нетрудоемкого» расследования уголовного дела.

Подобного рода угроза со стороны субъекта указанного преступления, заключается в намерении опубликовать компрометирующие сведения о потерпевшем через интернет сайты, а их, как известно, в настоящее время неограниченное количество.

В литературе нет единого мнения, касающегося определения понятия «сайт». Однако очевидно, что под данным понятием следует понимать сетевой информационный ресурс, оснащенный определенным режимом базы данных. В таком информационном ресурсе может храниться различная информация, в частности, сведения, относящиеся к компрометирующим. К числу такой информации можно отнести любые сведения о человеке, которые последний желает сохранить в тайне от иных лиц. Вместе с этим, не следует забывать и том, что размещаемая на такого рода ресурсах информация может абсолютно не соответствовать действительности и быть ложной.

В информационно-телекоммуникационных сетях существует большое многообразие сайтов, специализирующихся на распространении компрометирующей информации. Так, к примеру, до 2016 г., большой популярностью пользовался сайт «www.compromat.ru.». Указанный информационный ресурс был весьма обширного масштаба и достаточно известен. Он содержал в себе большую информационную библиотеку, которая систематизировалась по фигурантам. В нем размещались различные компрометирующие материалы, достоверность которых никаким образом не проверялись. Также на данном сайте имелся форум, где каждый желающий мог ознакомиться с теми или иными материалами, разместить там различную по своему характеру информацию, а также выразить, относительно нее, свое мнение. В настоящее время доступ к указанному ресурсу

заблокирован на основании Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [17].

Всем известно, что размещение тех или иных сведений на сайтах, в частности и на страницах анонимных сайтов, не составляет большого труда. Так, разместив соответствующие сведения на каком-либо сайте в сети Интернета, их будет читать и обсуждать неограниченный круг лиц, кроме того, на них будут ссылаться как на источник информации.

Таким образом, распространяется подобного рода дискредитирующая информация, достаточно быстро и масштабно. Отсюда вытекает и общественная опасность указанных действий, которая обусловлена своим воздействием на массовое сознание людей и общества в целом, а это влечет за собой значительное изменение общественной оценки личности компрометируемого.

Вместе с тем, подобные действия имеют и другое, не менее негативное последствие, которое заключается в том, что удалить, а также опровергнуть размещенные в сети Интернета сведения, которые были опубликованы в тех или иных информационных форматах, крайне сложно, а в некоторых случаях вообще невозможно. И эти обстоятельства вызывают еще более устрашающую реакцию у лиц, подвергнутых такой шантажной угрозе, что приводит их к вынужденному согласию дать «требуемые» показания или заключения, независимо от того являются ли они истинными или ложными.

Несомненно, указанные выше действия, заключающиеся в угрозе распространения компрометирующих сведений в сети Интернета, следует относить к одной из форм шантажа, рассматриваемого в контексте ст. 302 УК РФ. Однако, такая форма шантажа должна быть отграничена от шантажа, регламентированного ч. 1 ст. 302 УК РФ, в отдельный квалифицирующий признак, поскольку влечет за собой более тяжкие правовые последствия, заключающиеся в значительности причиняемого ущерба чести и достоинству потерпевшего или его близких.

Учитывая вышеизложенные обстоятельства, а также общественную опасность и тяжесть возможных последствий такого деяния, представляется целесообразным рассмотрение вопроса о внесении в ст. 302 УК РФ дополнительного квалифицирующего признака, предусматривающего уголовную ответственность за принуждение к даче показаний, связанное с угрозой распространения компрометирующих сведений в информационно-телекоммуникационных сетях, включая сеть Интернет.

В связи с чем, предлагается на рассмотрение следующая редакция указанного квалифицирующего признака в контексте исследуемой нормы:

«Принуждение подозреваемого, обвиняемого, потерпевшего, свидетеля к даче показаний либо эксперта, специалиста к даче заключения или показаний путем применения шантажа, содержащегося в угрозе распространения компрометирующих сведений в информационно-телекоммуникационных сетях, включая сеть Интернет, со стороны следователя или лица, производящего дознание, а равно другого лица с ведома или молчаливого согласия следователя или лица,

производящего дознание, – наказывается ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок».

А в случае же, если в ходе такого принуждения, все же было осуществлено фактическое распространение вышеуказанных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет, и если такие сведения являлись заведомо ложными, порочащими честь и достоинство лица или подрывающими его репутацию, то такие действия, следует квалифицировать по совокупности преступлений, предусмотренных соответствующей частью ст. 302 УК РФ и ч. 2 ст. 128.1. УК РФ.

Список литературы

1. Всеобщая декларация прав человека принята 10 декабря 1948 г. Генеральной Ассамблеей ООН // СПС «КонсультантПлюс».

2. Конституция Российской Федерации принята 12 декабря 1993 г. всенародным голосованием, с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. // СПС «КонсультантПлюс».

3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 25.03.2022, с изм. от 19.05.2022) // Собрание законодательства Российской Федерации // СПС «КонсультантПлюс».

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 28.01.2022) // Собрание законодательства Российской Федерации. 1996 // СПС «Консультант Плюс».

5. Бунева И. Ю. Уголовная ответственность за принуждение к даче показаний : автореф. дис. … канд. юрид. наук. Омск, 2000.

6. Калашникова А. А. Принуждение к даче показаний: Уголовно-правовой аспект : автореф. дис. … канд. юрид. наук. М., 2004.

7. Кулешов Ю. И. Преступления против правосудия: проблемы теории, законотворчества и правоприменения : автореф. дис. … д-ра юрид. наук. Владивосток, 2007.

8. Авдеева Е. А. Принуждение к даче показаний: причины и меры предупреждения : автореф. дис. … канд. юрид. наук. М., 2008.

9. Кудрявцев В. Л. Принуждение к даче показаний (состав преступления) как обстоятельство, исключающее допустимость доказательства (вопросы теории и практики) : монография. СПб. : Санкт-Петербургский институт (филиал) ВГУЮ (РПА Минюста России), 2018.

10. Сведения Федерального казенного учреждения «Главный информационно-аналитический центр МВД России».

11. Коробейников Б. В. Комментарий к статье 302 УК РФ // Комментарий к Уголовному кодексу Российской Федерации: научно-практический (постатейный) / под ред. С. В. Дьякова, Н. Г. Кадникова. 2-е изд., перераб. и доп. М. : Юриспруденция, 2013 // СПС «КонсультантПлюс».

12. Кузнецов А. П., Сидоров Б. В. Принуждение к даче показаний (ст. 302 УК РФ) // Конкретные виды преступлений против правосудия // Преступления

против правосудия // Уголовное право России. Особенная часть : учебник / под ред. Ф. Р. Сундурова, М. В. Талан. М. : Статут, 2012 // СПС «КонсультантПлюс».

13. Калашникова А. А. Принуждение к даче показаний (ст. 302 УК РФ) // Преступления против правосудия / под ред. А. В. Галаховой. М. : «Норма», 2005 // СПС «КонсультантПлюс».

14. Чучаев А. И. Комментарий к ст. 302 УК РФ // Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. И. Чучаева (испр., доп., перераб). М. : «КОНТРАКТ», 2013 // СПС «КонсультантПлюс».

15. Бриллиантов А. В., Косевич Н. Р. Комментарий к статье 302 УК РФ // Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2-х томах / [А. В. Бриллиантов и др.] ; под ред. А. В. Бриллиантова. 2-е изд., науч. Т. 2. М. : Проспект, 2015 // СПС «КонсультантПлюс».

16. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ (ред. от 25.02.2022) // СПС «КонсультантПлюс».

17. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

Гришин Н. С.[1],
адъюнкт факультета
научно-педагогических и научных кадров
Московского университета МВД России
имени В.Я. Кикотя

ОБОРОТ ТОВАРОВ, НЕ ОТВЕЧАЮЩИХ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ, С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Информационно-телекоммуникационные сети сегодня стали незаменимой частью жизни большинства населения планеты. В настоящее время достаточно трудно представить жизнь современного человека без интернета, мессенджеров, социальных сетей. Безусловно подобная тенденция оказывает влияние и на криминальную сферу: постоянно появляются новые формы преступной деятельности, в немалой части из которых активно используется информационное пространство.

Рынок товаров и услуг – важная часть существующих на сегодняшний день в государстве экономических процессов. Общество потребления – так достаточно часто в литературе и публицистике обозначается складывающаяся социальная действительность. Оборот товаров и услуг является обязательным атрибутом жизни любого человека, с помощью которого он может удовлетворять любые возникающие потребности, как материального, так и нематериального характера. Однако, люди всегда заинтересованы в предоставлении услуг и продукции высокого качества, которые бы соответствовали требованиям безопасности. Ведь именно от этого критерия зависит конструктивность самого процесса потребления – он не должен создавать угроз здоровью человека и гармоничному развитию его организма. К сожалению, далеко не все производители понимают данный аспект, ставя коммерческий интерес превыше общечеловеческих ценностей.

Пандемия коронавируса Covid-19, начавшаяся в 2020 г., и сопутствующие ей предупредительные меры: локдауны, санитарно-эпидемиологические ограничения – способствовали увеличению удельной доли сервисов, предлагающих онлайн продажу товаров и продукции, с последующей доставкой на дом. По данным аналитического агентства Data Insight, режим самоизоляции 2020 г. привлек в российскую онлайн торговлю более 10 млн новых пользователей, увеличив среднегодовой объем покупок с использованием сети Интернет в 4 раза [1]. Представляется, что немалая часть подобного рода новых покупателей остались пользователями сервисов онлайн-доставки уже после окончания действия ограничительных мер.

Оборот товаров и продукции, оказание услуг и выполнение работ, не отвечающих требованиям безопасности, остается одним из наиболее опасных составов преступлений против здоровья населения. Несмотря на то, что статистически

[1] © Гришин Н. С., 2022.

указанные общественно опасные деяния совершаются относительно нечасто – по данным Судебного департамента при Верховном Суде Российской Федерации, за 2021 г. по ст. 238 УК РФ было осуждено 815 человек, в 2020 г. – 780 человек – они могут приводить к тяжким последствиям и вызвать широкий социальный резонанс [2]. Например, в сентябре 2021 г. было возбуждено уголовное дело по факту отравления семьи из трех человек, купивших арбуз в магазине «Магнит». Следствием было установлено, что сотрудники организации, обрабатывавшей торговое помещение от насекомых, не соблюдали порядок обращения токсичного вещества – цигатрина, в результате чего, последнее попало на купленный товар, а потом и в организм потерпевших. В результате, двое из них – 61-летняя женщина и ее 15-летняя внучка скончались, а еще одна девушка получила тяжелое пищевое отравление [3]. 3 июня 2022 г. в г. Тольятти за сутки были госпитализированы более 30 человек, в их числе, четыре ребенка и беременная женщина. Причина – острое пищевое отравление. Следствием установлено, что все госпитализированные пользовались услугами доставки японской кухни. В настоящий момент решается вопрос о возбуждении уголовного дела по ст. 238 УК РФ [3].

Рост сферы онлайн-продаж товаров, продукции, услуг и работ в последнее десятилетие привлекает внимание ученых, исследующих проблемы привлечения к уголовной ответственности за оборот указанных предметов, не отвечающих требованиям безопасности. Так, И. А. Шеина указывает на то, что реализация такого рода товаров с использованием сети Интернет обладает повышенной степенью общественной опасности ввиду того, что значительно ослабляются контрольные полномочия правоохранительных органов по проверке качества объектов, вовлеченных в потребительский оборот [4, с. 137]. Кроме того, распространение товаров, не отвечающих требованиям безопасности, с использованием информационно-телекоммуникационных технологий, значительно затрудняет возможность установления и привлечения к уголовной ответственности виновных лиц. На основании этого, автор предлагает дополнить ч. 2 ст. 238 УК РФ новым квалифицирующим признаком: «использование сети Интернет».

Л. Ш. Бахаев в своем диссертационном исследовании поддерживает указанную позицию, однако, приводит иное обоснование. Исследователь указывает, что реализация товаров с использованием социальных сетей расширяет рынок сбыта продукции, не отвечающей требованиям безопасности, вовлекает в него дополнительный круг покупателей и, как следствие, увеличивает обороты самой общественно опасной деятельности, масштабируя угрозу причинения вреда жизни и здоровью потребителей [5, с. 124]. Таким образом, автор обосновывает необходимость введения квалифицированного состава преступления, предусмотренного ст. 238 УК РФ, связанного с применением сети Интернет.

Следует согласиться с тем, что современные возможности информационно-телекоммуникационных сетей создают условия для значительного расширения степени охвата потенциальных покупателей при реализации товаров и продукции: начиная от рекламных кампаний, заканчивая непосредственным соверше-

нием сделки купли-продажи. Однако, мы не поддерживаем приведенные позиции авторов относительно вопроса необходимости изменения уголовного законодательства, в части введения повышенной ответственности за оборот товаров и продукции, не отвечающих требованиям безопасности, с использованием сети Интернет.

Во-первых, по нашему мнению, информационно-телекоммуникационные технологии на современном этапе развития общества стали обыденностью. Это же можно сказать и об онлайн-продажах различных товаров и продукции. В подтверждение позиции можно вспомнить о таких крупнейших ритейлинговых интернет-площадках, как «Ozon», «Aliexpress», «Яндекс.Маркет», которые занимаются дистанционной продажей широкого круга объектов, в том числе продуктов питания, и имеют многомиллиардные обороты денежных средств. В этой связи, не следует противопоставлять розничную торговлю в магазинах и в информационном пространстве, ведь сегодня это звенья единого механизма оборота товаров и продукции для нужд потребителей.

Во-вторых, довод о том, что использование сети Интернет облегчает совершение преступлений, предусмотренных ст. 238 УК РФ, а также затрудняет деятельность правоохранительных органов, в современных реалиях кажется неубедительным. Роспотребнадзор, Роскомнадзор, подразделения экономической безопасности и иные контролирующие органы уже давно разработали эффективные механизмы противодействия правонарушениям, связанным с оборотом опасной и фальсифицированной продукции в информационно-телекоммуникационных сетях. В этой связи, деятельность продавцов, применяющих для ведения бизнеса возможности сети Интернет, наоборот, является более открытой для правоохранительных органов. Так, в марте 2020 г. была проведена совместная профилактическая операция МВД России, ФСБ России, Росздравнадзора и Роспотребнадзора «Пангея», в результате которой было выявлено более 2 тыс. сайтов, которые нелегально распространяли контрафактные лекарственные средства [6]. Если говорить о том, что оборот товаров, не отвечающих требованиям безопасности, с использованием сети Интернет, позволяет более быстро и эффективно вводить потребителя в заблуждение, здесь также складывается весьма противоречивая ситуация. Покупатели достаточно давно начали отходить от приверженности частным продавцам при покупке товаров и продукции в сети Интернет. В последнее время предпочтение отдается именно крупным платформам по продажам, где за проверку безопасности реализуемых объектов отвечает сам организатор информационного пространства. Если же покупатель, по каким-либо причинам, вступает в контакт с более мелкими интернет-ритейлерами, в большинстве случаев, проводится тщательное изучение отзывов о товаре, сертификатов качества и т. п. В этой связи, шанс осуществления покупки у сомнительного продавца в сети Интернет уменьшается в разы. Однако, в судебно-следственной практике появляются случаи, когда лица осуществляют оборот товаров и продукции, не отвечающих требования безопасности, получая данные о покупателях из баз данных легальных интернет-магазинов. Так, согласно приговору № 1-389/2017 Ленинского районного суда г. Ростова-на-Дону от 7 декабря 2017 г.,

по ч. 1 ст. 238 УК РФ был осужден гражданин П., который через сайт, специализирующийся на розничной продаже алкогольной продукции, договорился с одним из администраторов о том, что последний за денежное вознаграждение будет передавать номера клиентов из базы данных. Используя полученные сведения, гражданин П. совершил сбыт спиртосодержащей жидкости, изготовленной им кустарным способом, которая по своему химическому составу не соответствовала требованиям безопасности. [7] Здесь следует отметить, что использование сети Интернет вообще не будет охватываться объективной стороной самого преступления, а потому не может рассматриваться в качестве конструктивного признака.

Наконец, следует не согласиться с позицией И. А. Шеиной о том, что введение квалифицированного состава преступления, связанного с оборотом товаров и продукции, не отвечающих требованиям безопасности, с использованием сети «Интернет» будет логичным, поскольку законодатель уже ввел похожий квалифицирующий признак в ч. 2 ст. 228.1 УК РФ, которая расположена в той же главе Кодекса. Сбыт наркотических средств, психотропных веществ или их аналогов, сам по себе, является преступным. Именно поэтому обе стороны – сбывающая и получающая – заинтересованы в сокрытии факта передачи запрещенных к гражданскому обороту предметов. В этой связи, использование сети Интернет действительно может облегчать совершение самого преступления и затруднять возможность противодействия ему со стороны правоохранительных органов. Информационно-телекоммуникационные технологии дают возможность тайно договориться о месте и времени сбыта и даже осуществить его без прямого контакта участвующих лиц. В случае с составом преступления, предусмотренным ст. 238 УК РФ, ситуация диаметрально противоположная. Сам по себе, оборот товаров и продукции не является преступным, а потребитель всегда заинтересован в том, чтобы избежать приобретения опасного для жизни и здоровья объекта.

Таким образом, в современных реалиях рынок онлайн-продаж товаров и продукции стал весьма востребованным. Возрастает степень охвата потенциальных потребителей, заинтересованных в покупке необходимых им объектов материального мира, что повышает риск совершения в отношении таких субъектов преступлений, предусмотренных ст. 238 УК РФ. Однако, нами было установлено, что в настоящее время не существует объективной необходимости введения квалифицированного состава преступления, связанного с оборотом товаров и продукции, не отвечающих требованиям безопасности, с использованием сети Интернет.

Список литературы

1. Сайт информационного агентства «РБК». URL: https://www.rbc.ru.

2. Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. URL: https:// http://www.cdep.ru/.

3. Сайт информационного агентства «Газета.ru». URL: https:// https://www.-gazeta.ru.

4. Шеина И. А. Уголовно-правовые меры противодействия производству, хранению, перевозке либо сбыту товаров и продукции, выполнению работ или оказанию услуг, не отвечающих требованиям безопасности : дис. ... канд. юрид. наук : 12.00.08. М., 2016.

5. Бахаев Л. Ш. Уголовно-правовое и криминологическое противодействие преступлениям, совершаемым в сфере безопасности пищевых продуктов : дис. ... канд. юрид. наук : 12.00.08. М., 2019.

6. Официальный сайт МВД России. URL: https://мвд.рф/.

7. Приговор № 1-389/2017 Ленинского районного суда г. Ростова-на-Дону от 7 декабря 2017 г. URL: http://sud-praktika.ru.