Проблемы и вопросы уголовного права, уголовного процесса

УДК 343.9
ББК Х408.135
DOI: 10.14529/law210101

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ПРЕСТУПНОСТИ В ЦИФРОВОЙ СРЕДЕ

Ю. А. Воронин, И. М. Беляева, Т. В. Кухтина
Южно-Уральский государственный университет, г. Челябинск

Одной из важнейших задач криминологической науки и практики является комплексный анализ современных тенденций цифровой преступности и их классификация. При этом генеральной тенденцией, находящей свое отражение в более конкретных трендах, выступает использование в цифровой среде (или посредством использования цифровых технологий) специфических приемов и методов, открывающих новые возможности в криминальной деятельности. По сути, речь идет об активном применении преступниками цифровых технологий, электронно-вычислительной техники, телекоммуникационной связи. В статье подчеркивается, что неуклонно прогрессирующий уровень кибермошенничества, компьютерного шантажа и террористических угроз требует разработки и осуществления мер, направленных на эффективное противодействие развитию проанализированных авторами тенденций как в общеуголовной, так и в террористической цифровой преступности. Прежде всего очевидна необходимость усиления именно государственного контроля за использованием цифровой среды и средств коммуникации, в частности дальнейшая модернизация этого контроля.

Ключевые слова: цифровые технологии, тенденции цифровой преступности, преступления в сфере цифровой информации, кибермошенничество, террористическая цифровая преступность.

1. Достаточно устоявшейся в российской криминологии является трактовка цифровой преступности (информационно-цифровой преступности) как понятия и соответствующего явления, представляющего собой широкий круг общественно опасных деяний, совершенных в информационно-коммуникационной среде с использованием цифровой информации и информационно-телекоммуникационных технологий. В этой связи есть основание констатировать, что одной из важнейших задач криминологической науки и практики является комплексный анализ состояния и тенденций цифровой преступности, изучение обстоятельств, детерминирующих или стимулирующих ее рост, изменение и предположительное развитие в будущем, а также разработка проблем нейтрализации этих процессов и усиление контроля над цифровой преступностью на основе учета коренных закономерностей социального, политического и экономического развития общества [1, с. 76].

Существующее разнообразие преступных проявлений, связанных с информационно-цифровой средой (по предмету общественно опасных посягательств или способам их совершения), делает чрезвычайно сложным исчерпывающий обзор их состояния и современных тенденций их эволюции. Несмотря на это, с учетом степени распространенности, типичности, а также динамики проявлений таких общественно опасных деяний, попытки решения задачи их классификации и выделения тенденций их развития неоднократно предпринимались различными исследователями. Особенно плодотворным, на наш взгляд, явился подход к проблеме, предложенный российскими криминологами, в частности, В. С. Овчинским и рядом других отечественных специалистов [3]. Говоря о существовании наиболее заметных современных тенденций в информационно-цифровой преступности, на наш взгляд, есть основания диагностировать наличие целого ряда следующих, приобретающих все более заметное раз-

витие в криминальной среде, специфических характеристик, по сравнению с типичными, устоявшимися на протяжении многих десятилетий, чертами.

2. Так, анализ сложившейся сегодня криминогенной ситуации свидетельствует о том, что среди наиболее существенных факторов, оказывающих прямое воздействие на изменение характеристик преступных проявлений, в первую очередь следует назвать получение преступниками в результате информационно-цифрового бума возможности обладать чрезвычайно эффективными, не существовавшими ранее технологиями, методами и инструментами, открывающими новые перспективы и возможности при совершении преступлений. При этом информационно-цифровые средства расширили в первую очередь возможности именно организованных преступных сообществ, широко использующих сегодня высокие технологии во многих сферах криминальной деятельности. Речь, таким образом, идет прежде всего о развитии генеральной тенденции, а именно: о влиянии информационно-цифровой среды прежде всего на рост организованной преступности, активно использующей цифровые технологии, электронно-вычислительную технику. Совершенно очевидно, что в условиях цифровой экспансии во все сферы человеческого бытия всеобщая телекоммуникационная взаимосвязанность наложила заметный отпечаток и способствовала небывалому развитию именно высокотехнологичной (цифровой) транснациональной (территориально) и многонациональной (по своему составу) организованной преступности.

Указанная тенденция выразилась, во-первых, в ускорении динамики вовлечения в ряды транснациональных преступных сообществ этнических представителей самых разных стран, то есть в своеобразную «интернационализацию» состава этих преступных группировок. Достаточно сказать, что в транснациональной криминальной активности организованных преступных формирований с различным этническим составом сегодня принимают участие выходцы примерно из 80 % стран мирового сообщества. Характерным примером, в частности, явилась преступная деятельность группировки, базировавшейся в США. В июне 2020 года окружной федеральный суд в штате Вирджиния вынес приговор членам интернациональной ОПГ, действовавшим через форум «Direct Connection». По данным государственного обвинения, «элитные киберпреступники» на своем сайте «Cardplanet» продали на территории ряда государств украденные данные 150 тыс. банковских карт, покупали и продавали украденные товары и услуги, используя вредоносное программное обеспечение, оказывали услуги по отмыванию денег на десятки миллионов долларов.

Во-вторых, развитие анализируемой тенденции нашло отражение в усилении диверсификации криминальной активности организованных преступных сообществ именно на международном, транснациональном уровне, то есть на территории целого ряда государств. Высокотехнологичные транснациональные преступные группы стремительно расширяют свою специализацию и демонстрируют все более высокие «показатели экономической эффективности». Так, в своем релизе Министерство юстиции США в июне 2020 года сообщало об осуждении окружным судом штата Невада лидеров транснациональной преступной группы Infraud Organization. Организация занималась крупномасштабным приобретением, продажей и распространением похищенных идентификационных данных, скомпрометированных дебетовых и кредитных карт, личной, финансовой и банковской информации, компьютерных вредоносных программ. Ущерб от ее деятельности оценивается более чем в 568 млн. долларов.

Еще одной из стремительно набирающих обороты тенденций развития цифровой преступности является активизация криминалитета в связи с операциями с использованием виртуальных денег, в том числе биткоинов. Подоплека сложившейся ситуации достаточно ясна. Во-первых, мафиозные структуры, широко используя квалифицированных программистов, хакеров, специалистов по видеонаблюдению, манипуляторов с виртуальной валютой, «зарабатывают» на этом огромные суммы [2, с. 178–179]. Во-вторых, именно в силу «продвинутости» этой (в отличие от традиционных) сферы и способа мошеннических действий преступников подобная активность является такой эффективной. Наконец, в-третьих, она опять-таки чрезвычайно привлекательна из-за высокого уровня конспиративности и, следовательно, безнаказанности этого преступного бизнеса. Ведь в подобных случаях, несмотря на предпринимаемые усилия, спецслужбы обладают

сравнительно ограниченными возможностями для отслеживания денежных потоков нелегального характера, выявления и наказания подозреваемых в криминальных операциях лиц, хотя (время от времени) правоохранительным органам все же сопутствует успех. Так, по сообщению BBC Com от 20 июня 2020 г., ярким примером, отражающим указанную тенденцию, служит создание и использование криминальными структурами биржевых площадок, на которых – в обход норм национального и международного права – они занимаются кибермошенничеством, отмыванием денежных средств, в особенности биткоинов, новакоинов и других цифровых (виртуальных) валют. Речь, в частности, идет о деятельности крупнейшей криптобиржи BTC-e, а также целого ряда других организаций подобного типа, которые, в отличие от легальных биржевых площадок, просто не требовали от клиентов серьезной авторизации для осуществления торгов. Как следует из оценки неправительственной организации Global Witness, совокупный суточный оборот BTC-e превышал 66 млн. долларов, а с каждой сделки администраторы площадки получали 0,5 % комиссии. Причем никто из многочисленных «клиентов» (более 20 тыс. пользователей) не знал, кто владеет этим прибыльным полулегальным бизнесом, поскольку бенефициары BTC-e скрывались за сетью офшоров. По оценкам Департамента криминальных расследований Службы внутренних доходов США, их совокупные активы к 2020 году достигали 500 млн. долларов.

Но, пожалуй, наиболее динамичной и стремительно развивающейся в плане технической изощренности (несмотря на кажущуюся традиционность) является тенденция, характеризующаяся самым широким спектром преступных деяний именно с корыстной мотивацией, сопровождающихся использованием компьютерной техники, то есть по сути цифровых технологий. Речь идет о мошенничестве, связанном с применением компьютеров; подлоге, сопровождающемся использованием компьютерной техники; фишинге; краже персональных данных в корыстных целях; ином неправомерном использовании компьютерных устройств по корыстным мотивам.

В частности, как справедливо подчеркивается специалистами, одним из самых распространенных преступлений среди этого перечня прежде всего является компьютерное мошенничество в Интернете. Современная тенденция стремительного роста именно данной категории цифровой преступности не случайна. Интернет-технологии позволяют преступникам применять для сокрытия своих персональных данных автоматизацию и программные инструменты и в силу этого получать существенные преимущества при совершении преступлений. К наиболее популярным разновидностям мошеннических преступлений данной категории в настоящее время относятся компьютерные мошенничества с онлайновыми аукционами, получившими большую распространенность в ряду услуг электронной торговли. Мошенники, совершающие преступления на аукционных площадках, используют отсутствие личного контакта между продавцом и покупателем. В результате трудности, связанные с нахождением различия между настоящим пользователем и преступником, привели к тому, что мошенничество с аукционами стало одним из самых популярных видов киберпреступлений. Что же касается самых распространенных методов осуществления таких преступных деяний, то к ним относятся выставление на продажу несуществующих товаров и требований авансовой оплаты покупки до ее доставки, а также покупка товаров и просьба их доставить, но без реального намерения оплатить эти товары [4, с. 92].

Подлог, связанный с применением компьютеров и зачастую, основного составляющего элемента такого подлога – фишинга, – это также разновидность наиболее активно распространяющихся цифровых преступлений. Свидетельство тому – продолжающее увеличение объема и эффективность фишинговых компаний. Если раньше в основном их адресатами были отдельные граждане, то начиная с 2015–2016 гг. фишинговые атаки стали в больших масштабах осуществляться против частного и корпоративного секторов, особенно банков и других расчетных систем.

Подоплека такой широкой экспансии достаточно проста. Дело прежде всего в относительной простоте и результативности фишинговой технологии. Правонарушители разработали и используют методы, предотвращающие осознание конкретным пользователем того факта, что он введен в заблуждение. Злоумышленники приобретают набор уязвимых сайтов различной тематики, размещенных в Интернете. Обладая даже ограниченным доступом к данным сайтам, они могут изменять их таким образом, чтобы часть их посетите-

лей перенаправлялась на фишинговую страницу. Если пользователь зашел на «поломанный» сайт в результате поискового запроса в системах Google, Yandex, Bing, Rambler, Mail.ru, то его перенаправляют на фишинговый сайт. При этом переход жертвы может быть осуществлен на любую страницу «поломанного» сайта, кроме главной, иначе перенаправление на фишинговый сайт не осуществляется. Фишинговый сайт замаскирован, как правило, под акцию по розыгрышу призов и информирует потерпевшего о выигрыше денежного приза и возможности получить деньги. Но для этого злоумышленники просят указать реквизиты банковской карты. Как только личная информация владельца сайта раскрыта, правонарушители входят в учетные записи жертв и совершают преступления, такие как перевод денежных средств на новые счета и т.д. По мнению правоохранительных служб, рост числа успешных атак преступников демонстрирует довольно эффективный потенциал фишингового промысла.

Сродни фишингу выступает набирающее в России интенсивные обороты телефонное мошенничество с помощью роботов, при котором первоначальный «обзвон» потерпевших проводят автоматизированные центры. Злоумышленники могут звонить с поддельных номеров, используя сервисы IP-телефонии, Whats App, Vibet и т.д. О стремительности роста этой разновидности криминальных манипуляций свидетельствуют, в частности, данные ведомственной банковской статистики. Достаточно сказать, что только в течение 2020 года службами безопасности Сбербанка зарегистрировано более трех миллионов попыток телефонного мошенничества в отношении его клиентов. И это вдвое больше, чем за 2019 год.

Ко всему сказанному уместно добавить, что помимо упомянутых, многие из уже существовавших тенденций корыстной цифровой преступности не остаются стабильно неизменными. Это, в частности, относится к кибервымогательству, мелким хищениям с помощью вредоносного «софта», использованию банковских троянов. Против ожиданий, перечисленные виды относительно незамысловатой корыстной цифровой киберпреступности не растворились в высокотехнологичном цифровом криминале, а продолжают стабильно нарастать по объемам.

В целом же, по оценкам экспертов, мировой ущерб от всех рассмотренных разновидностей цифровых преступлений с корыстной мотивацией в годовом исчислении составляет примерно 600 миллиардов долларов – при росте на десятки процентов ежегодно [5, с. 1, 3–7]. Представляется, что эта ситуация будет сохраняться достаточно долго, будучи очевидно «востребованной» преступным рынком.

3. Наконец, было бы ошибкой игнорировать особенно опасную специфическую составляющую среди тенденций цифровой преступности: заметным трендом двух минувших десятилетий стало достаточно частое осуществление экстремистских и террористических преступлений с использованием компьютерных инструментов, масштабных и изощренных DDoSатак в комбинации с сетевыми атаками по выведению из строя систем информационной безопасности.

Прежде всего следует упомянуть об использовании террористами Интернета, «облачных» технологий для кибератак на важнейшие оборонные объекты, объекты энергетической, промышленной инфраструктуры и другие важнейшие системы жизнеобеспечения населения, применении вредоносных программ для цифровых диверсий. Важнейшей составляющей анализируемой тенденции является также проникновение террористов в веб-сайты финансовых структур, получение информации о кредитных картах частных лиц с последующим изъятием денежных средств.

Наконец, существенным элементом тенденции криминального использования террористами и экстремистами цифровой сферы является идеологическая обработка и вербовка контингента лиц для совершения насильственных действий на основе экстремистских идеологий или в террористических целях. Этот процесс включает использование пропаганды, которая на протяжении длительного времени ведется посредством Интернета. Обычно такие пропагандистские материалы имеют форму мультимедийных коммуникаций и содержат идеологические или практические разъяснения, рекомендации или рекламу террористической, экстремистской деятельности. Сюда относятся виртуальные сообщения, презентации, журналы, теоретические работы, аудио- и видеофайлы, разрабатываемые террористическими, экстремистскими организациями.

Поощрение насилия, как уже отмечалось, является центральной темой этой пропаганды.

Специалисты отмечают, что широкая область влияния распространяемой через Интернет информации в геометрической прогрессии увеличивает аудиторию, на которую она может воздействовать. Интернет-пропаганда также может включать такой контент, как видеосюжеты о насильственных, террористических актах или создаваемые террористическими организациями видеоигры, имитирующие акты терроризма и побуждающие пользователей участвовать в ролевой игре, выступая в роли виртуального террориста [3, с. 71–72]. Как это ни прискорбно констатировать, таким образом, оборотной стороной технологического прогресса явилось получение террористами, а также экстремистки настроенными лицами и организациями разнообразного арсенала цифровых средств и методов для использования их в противоправных целях.

В заключение краткого анализа современных тенденций цифровой преступности следует подчеркнуть, что неуклонно прогрессирующий уровень кибермошенничества, компьютерного шантажа и террористических угроз требует разработки и практического осуществления мер, направленных на эффективное противодействие дальнейшему развитию этих тенденций как в общеуголовной, так и в террористической цифровой преступности, а значит – диктует необходимость усиления государственного контроля над состоянием информационно-цифровой среды.

Литература

1. Воронин, Ю. А. Преступления в сфере обращения цифровой информации и их детерминанты / Ю. А. Воронин // Научно-практический журнал «Виктимология». – 2020. – № 1 (23). – С. 74–83.

2. Воронин, Ю. А. Криминогенные факторы в информационно-цифровой среде: сб. научных статей «Smart Law for Smart Industry» / Ю. А. Воронин // М.: Изд-во «Проспект», 2020. – 320 с.

3. Овчинский, В. С. Цифровое общество: преступление и наказание: интервью в интернет-портале «Лица» / В. С. Овчинский. URL: http//2035.media/2018/01/30ovchinskiy-interviiew/.

4. Овчинский, В. С. Криминология цифрового мира: учебник / В. С. Овчинский. – М.: Норма: ИНФРА-М, 2018. – 352 с.

5. Сюнтюренко, О. В. Цифровая среда: тренды и риски развития / О. В. Сюнтеренко // Научно-техн. информация. Серия 1. Организация и методика информационной работы. – М.: ВИНИТИ РАН. – 2015. – № 2. – С. 1–7.

Воронин Юрий Александрович – доктор юридических наук, профессор кафедры уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: voroninya@yandex.ru.

Беляева Ирина Михайловна – кандидат юридических наук, доцент, заведующий кафедрой уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: beliaevaim@susu.ru.

Кухтина Татьяна Владимировна – старший преподаватель кафедры уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: upiuip@mail.ru.

Статья поступила в редакцию 30 ноября 2020 г.

DOI: 10.14529/law210101

CONTEMPORARY CRIME TRENDS IN THE DIGITAL ENVIRONMENT

Yu. A. Voronin, I. M. Belyeva, T. V. Kukhtina
South Ural State University, Chelyabinsk, Russian Federation

One of the most important tasks of criminological science and practice is a comprehensive analysis of modern trends in digital crime and their classification. At the same time, the general trend, which is reflected in more specific trends, is the use in the digital environment (or through the use of digital technologies) of specific techniques and methods that open up new opportunities in criminal activity. In fact, it is about the active use by criminals of digital technologies, electronic computing technologies, telecommunications. The article emphasizes that the steadily progressing level of cyberfraud, computer blackmail and terrorist threats requires the development and implementation of measures aimed at effectively countering the development of the trends analyzed by the authors in both general criminal and terrorist digital crime. First of all, the need to strengthen the state control over the use of the digital environment and means of communication is obvious, in particular, the further modernization of this control.

Keywords: digital technologies, digital crime trends, crimes in the sphere of digital information, cyber fraud, terrorist digital crime.

References

1. Voronin Yu. A. [Crimes in the sphere of digital information circulation and their determinants]. *Nauchno-prakticheskiy zhurnal «Viktimologiya» [Scientific and practical journal "Victimology"]*, 2020, no.1 (23), pp. 74–83. (in Russ.)

2. Voronin Yu. A. *Kriminogennyye faktory v informatsionno-tsifrovoy srede. Sb. nauchnykh statey «Smart Law for Smart Industry»* [Criminogenic factors in the information and digital environment. Collection of scientific articles "Smart Law for Smart Industry"]. Moscow, 2020, 320 p.

3. Ovchinskiy V. S. Tsifrovoye obshchestvo: prestupleniye i nakazaniye: in-terv'yu v internet-portale «Litsa» [Digital society: crime and punishment: interview in the Internet portal "Persons"]. Available at: http//2035.media/2018/01/30ovchinskiy-interviiew/.

4. Ovchinskiy V. S. *Kriminologiya tsifrovogo mira: uchebnik* [Criminology of the digital world]. Moscow, 2018, 352 p.

5. Syuntyurenko O. V. [Digital environment: trends and risks of development]. *Nauchno-tekhnicheskaya informatsiya. Seriya 1. Organizatsiya i metodika informatsionnoy raboty [Scientific and technical information. Series 1. Organization and methods of outreach]*. Moscow, 2015, no. 2, pp. 1–7. (in Russ.)

Yuri Alexandrovich Voronin – Doctor of Sciences (Law), Professor of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russian Federation. E-mail: voroninya@yandex.ru.

Irina Mihailovna Beliaeva – Candidate of Sciences (Law), associate, Head Professor of Criminal and Criminal-Executive Law, Criminology, Chelyabinsk, Russian Federation. E-mail: beliaevaim@susu.ru.

Tatyana Vladimirovna Kukhtina – senior lecturer of Criminal and Criminal-Executive Law, Criminology, South Ural state University, Chelyabinsk, Russian Federation. E-mail: upiuip@mail.ru.

Received 30 November 2020.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Воронин, Ю. А. Современные тенденции преступности в цифровой среде / Ю. А. Воронин, И. М. Беляева, Т. В. Кухтина // Вестник ЮУрГУ. Серия «Право». – 2021. – Т. 21, № 1. – С. 7–12. DOI: 10.14529/law210101.

FOR CITATION

Voronin YU. A., Belyeva I. M., Kukhtina T. V. Contemporary crime trends in the digital environment. *Bulletin of the South Ural State University. Ser. Law,* 2021, vol. 21, no. 1, pp. 7–12. (in Russ.) DOI: 10.14529/law210101.