ISSN 2500-4255

Научная статья
УДК 343.9
DOI 10.17150/2500-4255.2022.16(2).185-198

ЦИФРОВАЯ ПРЕСТУПНОСТЬ В УСЛОВИЯХ ПАНДЕМИИ: ОСНОВНЫЕ ТРЕНДЫ

З.И. Хисамова[1], И.Р. Бегишев[2]
[1] Краснодарский университет Министерства внутренних дел Российской Федерации, г. Краснодар, Российская Федерация
[2] Казанский инновационный университет имени В.Г. Тимирясова (ИЭУП), г. Казань, Российская Федерация

Информация о статье

Дата поступления
8 июня 2020 г.

Дата принятия в печать
5 мая 2022 г.

Дата онлайн-размещения
23 мая 2022 г.

Ключевые слова

COVID-19; Zoom; DarkNet; коронавирус; пандемия; цифровая преступность; кибербезопасность; киберкриминология; киберпреступность; кибератака; цифровые технологии; цифровая криминология; фишинг; социальная инженерия; онлайн-игра

Аннотация. 30 января 2020 г. группа экспертов Всемирной организации здравоохранения заявила о вспышке болезни COVID-19, вызванной коронавирусом SARS-CoV-2, а уже 11 марта 2020 г. было объявлено о пандемии новой коронавирусной инфекции. В этих условиях появилось множество новых векторов атак киберпреступников. Во время пандемии рекордное количество людей осуществляло работу из дома, многие пользовались разными онлайн-услугами и сервисами. При этом в большинстве случаев на домашних компьютерах граждан установлены устаревшие системы кибербезопасности либо они вовсе отсутствуют. Киберпреступники воспользовались открывшимися перед ними возможностями для совершения различных цифровых мошенничеств. Настоящее исследование содержит сведения из мировых отчетов и пресс-релизов о цифровых угрозах в период пандемии. В работе определены устойчивые тренды в динамике цифровой преступности в данный период, среди которых: 1) массовые кибератаки на недавно (и часто быстро) развернутую инфраструктуру удаленного доступа или удаленную рабочую инфраструктуру; 2) рост количества фишинговых атак и распространение вредоносных программ в связи с расширением цифровой аудитории; 3) адаптация классических схем мошенничества при помощи методов социальной инженерии; 4) атаки на цифровые платформы для коммуникации, их взлом («Zoombombing»); 5) рост числа криминальных проявлений в онлайн-играх; 6) повышение спроса на порнографические материалы и, как результат, их широкое распространение через социальные сети, зашифрованные приложения и в DarkNet. Предложен ряд профилактических мер по уменьшению воздействия цифровой преступности в период пандемии.

Original article

DIGITAL CRIME IN THE CONTEXT OF A PANDEMIC: MAIN TRENDS

Zarina I. Khisamova[1], Ildar R. Begishev[2]
[1] Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Krasnodar, the Russian Federation
[2] Kazan Innovative University named after V.G. Timiryasov (IEML), Kazan, the Russian Federation

Article info

Received
2020 June 8

Accepted
2022 May 5

Available online
2022 May 23

Keywords

COVID-19; Zoom; DarkNet; coronavirus; pandemic; digital crime; cybersecurity; cyber-criminology; cybercrime; cyberattack; digital technology; digital criminology; phishing; social engineering; online game

Abstract. On January 30, 2020, a group of experts from the world health organization announced an outbreak of SARS-CoV-2, which caused the coronavirus disease COVID-19. On March 11, 2020, the ongoing outbreak of coronavirus infection was declared a pandemic, which led to a huge number of new vectors of digital crime attacks. Cybercriminals did not shy away from the situation and used the pandemic to commit various digital scams and cyber-attacks. Due to the fact that a large number of people were working from home and using online services during the pandemic, the capacity of cybercriminals to exploit emerging opportunities and vulnerabilities increased significantly. In most cases, citizens have outdated cybersecurity systems in their homes, or they do not have them at all. Cybercriminals are preying on the opportunity to take advantage of this situation and are focusing even more on cybercrime activities. The study contains data from global reports and press releases on digital threats during the pandemic. The work identified sustainable trends in digital crime in the period of the pandemic, among them: 1) mass cyber-attacks on recently (and often quickly) deployed remote access infrastructure or remote work infrastructure; 2) the growth of phishing attacks and malware distribution due to the growth of the digital audience; 3) adaptation of «classic» fraud schemes using social engineer-

ISSN 2500-4255

ing methods; 4) attacks and hacking of digital communication platforms («Zoombombing»); 5) the growth of criminal phenomena in online games; 6) increased demand and distribution of pornographic materials through social networks, encrypted applications and the DarkNet. A number of preventive measures to reduce the impact of digital crime during the pandemic are proposed.

Карантин и «великий» локдаун спровоцировали в обществе экспоненциальный рост страха за здоровье свое и своих близких, сформировали предчувствие катастрофического развития событий. В совокупности с социальным дистанцированием и масштабным распространением фейковых новостей такой общественный настрой стал объектом пристального интереса со стороны как преступных сообществ, действующих в цифровой среде, так и отдельных киберпреступников.

В последнее время всплеск киберпреступности был обусловлен одной темой — пандемией COVID-19 [1]. Преступники быстро ухватились за возможность воспользоваться кризисом, адаптируя методы преступной деятельности под сложившиеся условия[1]. Страны по всему миру сообщают о росте киберпреступности во время пандемии [2]. В такой ситуации проблема обеспечения информационной безопасности приобретает еще большее значение, поскольку в период пандемии характер киберугроз сильно изменился [3].

По заявлению заместителя Генерального секретаря ООН и Высокого представителя по вопросам разоружения И. Накамицу, из разных точек мира поступают тревожные сообщения о кибератаках на организации здравоохранения и медицинские исследовательские учреждения. Атаки происходят каждые 39 секунд, а объем рассылок вредоносных электронных писем во время пандемии вырос на 600 %[2].

Уголовно наказуемые деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, характеризуются тенденцией к возрастанию их количества: так, в 2021 г. было зарегистрировано 517,7 тыс. подобных преступлений, что на 1,4 % больше, чем за аналогичный период прошлого года[3]. За тот же период было зарегистрировано 6 869 преступлений в сфере компьютерной информации, что в сравнении с предыдущим годом больше на 52,7 %. В общей структуре данной разновидности преступности выделяются деяния, связанные с неправомерным доступом к компьютерной информации, число которых увеличилось на 55,7 %[4].

На фоне продолжающейся пандемии появляется информация о различных цифровых преступлениях, приобретших в сложившихся реалиях новый формат. Отметим, однако, что динамично меняющиеся условия ограничивают нас в возможности каталогизировать либо иным образом систематизировать всю вредоносную киберактивность и преступные проявления. Тем не менее определенные тренды могут быть выделены уже сегодня.

Настоящая статья содержит прогнозную аналитику относительно того, какие направления преступной деятельности будут определяющими в период пандемии. Прогнозирование преступности и ее изучение представляют собой самостоятельный блок криминологической науки. Как справедливо отмечают Е.В. Герасимова, А.В. Миронов и А.Н. Рубищев, «в условиях мировой пандемии состояние преступности и ее динамика существенно изменились… В этой связи требуется изучение тенденций развития преступности в целях обеспечения криминологической обоснованности дальнейшего совершенствования законодательства» [4].

Как указывается в аналитических докладах, «на состояние и динамику преступности в течение прошедшего года наибольшее воздействие оказывали неблагоприятные социально-экономические условия, в первую очередь снижение уровня доходов населения и рост уровня безработицы. Большое влияние на криминальную ситуацию оказали и противоэпидемические меры, принятые в связи с необходимостью борьбы с пандемией» [там же].

[1] Preventing crime and protecting police: INTERPOL's COVID-19 global threat assessment // Interpol. URL: https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment.

[2] Briefing at the Security Council Virtual Arria-formula meeting on «Cyber Stability, Conflict Prevention and Capacity Building» // Front. URL: https://front.un-arm.org/wp-content/uploads/2020/05/UNSC-Arria-Formula-Meeting-on-Cybersecurity-HR-Remarks-22-May-2020.pdf.

[3] Состояние преступности в Российской Федерации за январь — декабрь 2021 года // Министерство внутренних дел РФ : офиц. сайт. URL: https://media.mvd.ru/files/application/2315310.

[4] Там же.

Представляется очевидным, что мировое развитие информационно-цифровой среды, являясь объективным, неизбежным процессом, не только приносит позитивные результаты, но и одновременно порождает сложные, в том числе негативные, социальные и правовые последствия [5].

Активизации цифровой преступности в условиях пандемии способствовали: высокий спрос на определенные товары, переход огромного количества компаний на удаленную работу, распространение СМИ информации о значительных мерах адресной поддержки государством населения в связи с пандемией, сокращение поставок некоторых незаконных товаров ввиду закрытия государственных границ.

Вышеописанные явления послужили причиной устойчивых трендов в динамике цифровой преступности в период пандемии. Рассмотрим их подробнее:

1. *Массовые кибератаки на (часто быстро) развернутую инфраструктуру удаленного доступа или удаленную рабочую инфраструктуру*.

Карантин выступил катализатором процесса цифровизации как в тех компаниях, которые начали внедрять новые технологии ранее, так и в тех, которые только задумались о предстоящей трансформации.

Цифровые технологии стали критически важными для поддержания социальных связей в обществе и обеспечения жизнеспособности бизнеса [6]. Организация рабочего процесса и бизнес-коммуникации посредством цифровых решений явилась причиной взрывного многократного роста количества кибератак [7], совершенных с целью хищения персональных данных и иной конфиденциальной цифровой информации [8], в том числе из объектов критической информационной инфраструктуры [9; 10].

Сайты сегодня стали ядром многих бизнесов и государственных сервисов. Ежедневно в мире взламывается более 150 тыс. сайтов. В кризисное время сайты интернет-магазинов и государственных органов — основная цель кибератак.

По мнению специалистов Group-IB, наблюдается рост числа кибератак на компьютеры, роутеры, видеокамеры и незащищенные домашние сети сотрудников компаний, которые из-за коронавируса перешли на удаленный режим работы. В группе риска находятся сотрудники финансовых учреждений, телеком-операторов и IT-компаний[5].

Указанные компании[6] и до пандемии наряду с государственными и медицинскими учреждениями, промышленными компаниями были в числе наиболее атакуемых [11]. Необходимо заметить, что выявленная в 2019 г. аналитиками Positive Technologies тенденция превалирования числа целевых атак[7] над массовыми (более 60 %) продолжится[8].

По подсчетам экспертов, злоумышленники уже сегодня могут получить доступ к каждому десятому открытому удаленному рабочему столу[9]. Кроме того, ряд экспертов, говоря о возрастающих угрозах для информационных систем организаций, отмечают прежде всего угрозу, исходящую от самих сотрудников, за которыми на дому будет отсутствовать контроль со стороны службы безопасности компаний [12].

Отдельной целью кибератак стали центры изучения новой коронавирусной инфекции. Выступая на онлайн-панели, организованной Институтом Аспена, заместитель помощника директора ФБР Т. Угорец сообщила о том, что количество сообщений о кибератаках увеличилось в 4 раза по сравнению со временем до пандемии. В дополнение к регулярным сообщениям о киберпреступности Бюро также осведомлено о нападениях, нацеленных на национальный сектор здравоохранения и исследовательский потенциал США по COVID-19 [13].

Отметим, что с точки зрения уголовного права указанные деяния в полном объеме охватываются ст. 272–274.1 УК РФ. Вопрос о содержательной стороне информации, доступ к которой образует состав преступления, предусмотренного ст. 272 УК РФ, продолжает вызывать научную дискуссию и трудности в правоприме-

[5] Group-IB ожидает роста числа кибератак на компьютеры сотрудников, работающих из дома // Kommersant.ru. URL: https://www.kommersant.ru/doc/4291700.

[6] Cybercriminals targeting critical healthcare institutions with ransomware // Interpol. URL: https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.

[7] Целевая атака — это непрерывный процесс несанкционированной активности в инфраструктуре атакуемой системы, удаленно управляемый в реальном времени вручную.

[8] Positive Technologies: в 2019 году 60 % кибератак имели целенаправленный характер // Ptsecurity. URL: https://www.ptsecurity.com/ru-ru/about/news/v-2019-godu-60-kiberatak-imeli-celenapravlennyy-harakter.

[9] Positive Technologies: злоумышленники могут получить доступ к каждому десятому открытому удаленному рабочему столу // Там же. URL: https://www.ptsecurity.com/ru-ru/about/news/zloumyshlenniki-mogut-poluchit-dostup-k-kazhdomu-desyatomu-otkrytomu-udalennomu-rabochemu-stolu.

нении. Длительное время научная доктрина и правоприменительная практика шли по пути признания неправомерным доступом к компьютерной информации «любого неправомерного обращения к информации вопреки воле ее владельца либо признания такой информации» [14], «собственник которой явным образом объявил об ограничении ее использования» [15]. В дальнейшем в соответствии с разъяснениями Генеральной прокуратуры РФ[10] к охраняемой законом информации стали относить лишь «сведения, в отношении которых установлен специальный режим правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т.д.)» [16]. Таким образом, деяния по неправомерному доступу к компьютерной информации квалифицировались совокупно с нормами, предусматривающими ответственность за нарушение режима уголовно-правовой охраны отдельно взятого вида информации, например за нарушение авторских прав.

Однако ряд авторов не согласны с такой квалификацией и предлагают ограничить предмет преступления, предусмотренного ст. 272 УК РФ, только той охраняемой законом компьютерной информацией, которая «позволяет функционировать компьютеру и не содержит сведений о частной жизни (ст. 137, 138, 155 УК РФ), не является объектом авторского права (ст. 146, 147 УК РФ), коммерческой, банковской, налоговой (ст. 183 УК РФ) или государственной тайной (ст. 275 УК), данными предварительного расследования (ст. 310 УК РФ), сведениями о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса (ст. 311 УК РФ)» [17; 18]. Полагаем, что такой подход неприменим ввиду того, что он значительно ограничивает эффективность уголовно-правовых норм в противодействии неправомерному доступу к охраняемой законом компьютерной информации.

Проведенный в начале апреля 2020 г. компанией ESET опрос о готовности российских предприятий к оперативному переводу персонала на режим удаленной работы показал, что к нему была готова только каждая пятая компания (18 %), 71 % отметили недостаток ресурсов для полноценного перехода на режим удаленного офиса без финансовых потерь и других негативных последствий. О принятии соответствующих мер и организации дистанционных рабочих мест для части сотрудников сообщили 82 % респондентов. Основу указанных мер (81 % опрошенных) составляют инструктажи сотрудников[11]. Компании, специализирующиеся на выпуске программного обеспечения, фиксируют многократный (+300 %) рост числа запросов, касающихся обеспечения информационной безопасности удаленного доступа и предотвращения утечки данных.

Несмотря на кажущуюся невозможность организации должного уровня защиты информации при работе на домашних компьютерах, эксперты в области обеспечения информационной безопасности все же отмечают возможность применения ряда «софтов» и «капсульных решений», которые «позволяют изолировать корпоративные приложения в специальной шифрованной области в памяти смартфона с возможностью тонкой настройки того, что пользователь может с ними делать (запрет скриншотов, копирования, передачи файлов и прочее)». Единогласно отмечается эффективность установки либо обновления до наиболее актуализированной версии классических антивирусных программ.

Гораздо лучше дело обстоит при использовании сотрудниками, работающими дистанционно, корпоративных устройств и гаджетов, на которых предустановлена актуальная версия антивирусной программы и к которым у работодателя существует удаленный доступ, позволяющий обеспечивать контроль за деятельностью сотрудника по обращению со служебной информацией вплоть до возможности блокирования устройства и его «отката» до заводских настроек при злонамеренных действиях либо краже устройства или его потере. Отдельно специалистами рекомендуется устанавливать на корпоративные устройства дополнительный пакет антивирусных программ, значительно расширяющих функционал [19].

2. *Рост количества фишинговых атак и распространение вредоносных программ в связи с расширением цифровой аудитории*.

[10] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // Генеральная прокуратура РФ : офиц. сайт. URL: https://epp.genproc.gov.ru/ru/web/gprf/documents?item=4900252.

[11] ESET: только каждая пятая российская компания опасается утечек данных в связи с переходом на удаленную работу // ESET. URL: https://www.esetnod32.ru/company/press/center/eset-tolko-kazhdaya-pyataya-rossiyskaya-kompaniya-opasaetsya-utechek-dannykh-v-svyazi-s-perekhodom-na-udalennuyu-rabotu.

По данным отчета о состоянии цифровой сферы Digital-2020, число интернет-пользователей в мире выросло до 4,54 млрд, что на 7 % больше прошлогоднего значения. В России количество интернет-пользователей достигло 118 млн, что составляет примерно 81 % населения страны[12].

Массовая изоляция и приобщение к цифровым устройствам широкого круга пользователей, в том числе не обладающих достаточной цифровой грамотностью и не отличающихся безопасным поведением в Сети [20; 21], «возродили» уже слегка забытые преступниками фишинговые атаки [22; 23] и активизировали довольно «популярное» среди злоумышленников использование рекламного контента с вредоносным программным обеспечением.

Различные IT-компании, занимающиеся анализом угроз в области информационной безопасности, составляют свои «рейтинги» ключевых угроз в условиях пандемии.

Так, по данным аналитиков из Dimensional Research, 71 % специалистов по кибербезопасности сообщили об увеличении количества угроз или атак с начала вспышки коронавируса, при этом как основную угрозу большинство респондентов (55 %) отметили фишинг, затем следует функционирование вредоносных вебсайтов, которые якобы содержат информацию и советы о коронавирусе (32 %), распространение вредоносных программ (28 %) и вымогательство (19 %)[13].

Группа Mimecast Threat Intelligence проанализировала тенденции активности в цифровой сфере в течение первых 100 дней пандемии. В период с января по конец марта 2020 г. ежемесячный объем всех видов угроз в данной сфере увеличился на 33 % (например, количество спам-атак возросло на 26,3 %). Увеличилось обнаружение угроз (на 30,3 %) и вредоносных программ (на 35,16 %), блокировка кликов по URL (на 55,8 %)[14].

Исходя из данных Национального центра кибербезопасности Соединенного Королевства (NCSC) и Агентства по кибербезопасности и безопасности инфраструктуры Министерства внутренних дел США (CISS) можно выделить следующие виды рисков в связи с расширением цифровой аудитории в период пандемии:

– фишинг, применение тега/заголовка «коронавирус» или «COVID-19» в качестве приманки;

– распространение вредоносных программ с использованием для привлечения внимания жертв тематических приманок — коронавирус, COVID-19;

– регистрация новых доменных имен, содержащих формулировки, связанные с коронавирусом или COVID-19[15].

Хакерские сообщества [24] используют пандемию COVID-19 для наращивания объема операций, направленных против организаций, участвующих в реагировании на чрезвычайную ситуацию как на национальном, так и на международном уровне [25].

По информации Центра расследования киберинцидентов «Ростелеком-Солар», с начала марта 2020 г. наблюдается всплеск фишинговых атак [26]. Киберпреступники подделывают информацию об отправителях электронных писем с целью создать впечатление, что они получены из надежных источников, например от Всемирной организации здравоохранения или от человека с приставкой «доктор», предлагают пользователям перейти на сайты для бесплатной диагностики коронавирусной инфекции COVID-19 либо с интерактивной картой очагов заражения[16]. Компания Google ежедневно осуществляет блокировку около 18 млн фишинговых отправлений[17]. Такие электронные письма предназначены для того, чтобы обмануть получателей и заставить их предпринять какие-либо действия, например щелкнуть вредоносную ссылку или открыть вредоносное вложение.

Новые данные, собранные Google и проанализированные Atlas VPN, поставщиком услуг виртуальной частной сети (VPN), проливают больше света на эту область. Согласно отчету, в январе 2020 г. Google зарегистрировал 149 тыс.

[12] Digital 2020 Report // Wearesocial. URL: https://wearesocial.com/digital-2020.

[13] Web Surveys // Dimensional Research. URL: https://dimensionalresearch.com/services/web-surveys.

[14] Report: Cyber Criminal Activity Increasing During Pandemic // The Maritime Executive. URL: https://www.maritime-executive.com/article/report-cyber-criminal-activity-increasing-during-pandemic.

[15] Advisory: COVID-19 exploited by malicious cyber actors // National Cyber Security Centre. URL: https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory.

[16] Ibid.

[17] Google blocking 18m coronavirus scam emails every day // BBC. URL: https://www.bbc.com/news/technology-52319093?intlink_from_url=https://www.bbc.com/news/topics/cz4pr2gd85qt/cyber-security&link_location=live-reporting-story.

активных фишинговых сайтов, в феврале их число достигло 293 тыс., а в марте увеличилось до 522 тыс., что на 350 % больше, чем в январе [27].

По данным компании Avast, около 72 % всех вредоносных программ для устройств на базе операционной системы Android — это рекламные приложения, маскирующиеся под топовые развлекательные приложения и игры.

Использование преступниками вредоносного рекламного программного обеспечения, которое было признано одной из ключевых угроз для мобильных устройств, с начала 2020 г. возросло на 38 % [27]. Group-IB также отмечается более чем двукратное повышение в DarkNet спроса на фишинговых китов[18]. В списке TrendMicro первое место занимают спам-атаки (65,7 %), на втором месте находятся атаки с применением вредоносного программного обеспечения, включая трояны и программы-вымогатели (с 26,8 %), на третьем месте по частоте выявления — вредоносные URL и сайты (7,5 %)[19].

На мобильные телефоны теперь приходится больше половины времени, которое мы проводим в Интернете, — 50,1 %, а на мобильные приложения приходится 10 из каждых 11 минут пользования мобильным устройством[20].

Все, кто оказался на самоизоляции, кто пытался обезопасить себя, держась как можно дальше от других людей, старались получить любую информацию, связанную с COVID-19, в том числе с помощью мобильных приложений. Где есть спрос, всегда имеется и предложение. Киберпреступники активно воспользовались сложившейся ситуацией. Они размещали вредоносные приложения в магазинах приложений. Одним из таких, которое было доступно в Google Play, было приложение Corona Live 1.1, которое заявлялось как живой трекер случаев заражения COVID-19. Люди, использовавшие данное вредоносное приложение, считали, что отслеживают ситуацию с пандемией, но оно фактически вторгалось в их личную жизнь, получая доступ к местоположению и камере устройства, к хранящимся на нем фотографиям, видеофайлам. Собранная информация использовалась несколькими способами, в основном для взлома банковских счетов или даже для шантажа владельцев фотографий и видео. Google Play неоднократно удалялись подобные приложения и устанавливались правила для приложений подобного типа.

Отметим, что вопрос уголовно-правовой квалификации указанных деяний давно решен. Так, постановление Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г. № 48 резюмирует, что «мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ»[21].

Несмотря на наличие мер уголовно-правового характера, количество фишинговых атак продолжает возрастать в геометрической прогрессии. Это обусловлено значительными трудностями в расследовании указанной категории дел. Понимая, что возможности правоохранительных органов ограниченны и не всегда виновные выявляются и предаются правосудию, злоумышленники активно используют фишинг для хищений.

3. *Адаптация классических схем мошенничества при помощи методов социальной инженерии*.

Мошеннические посягательства, основанные на введении в заблуждение и обмане граждан, в условиях кризиса всегда приобретают новую жизнь.

По данным Центрального банка Российской Федерации, в 2019 г. объем мошеннических операций с банковскими счетами достиг 6,4 млрд р., большинство таких операций (69 %) проводилось с помощью социальной инженерии. В 2017 г. социальная инженерия использовалась в 75 % случаев кибермошенничества, в 2018 г. — в 79 % случаев, в 2019 г. — в 89 %, а в 2020 г. — уже в 90 % случаев. В обозримом будущем этот тренд только усилится, мошенники продолжат пользоваться низкой киберграмотностью населения [28].

[18] Конструктор для киберпреступления: Group-IB фиксирует бум на рынке фишинг-китов // Group-IB. URL: https://www.group-ib.ru/media/how-much-is-the-phish.

[19] Developing Story: COVID-19 Used in Malicious Campaigns // Trendmicro. URL: https://www.trendmicro.com/vinfo/ru/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

[20] State of Mobile 2020 Report. URL: https://s3.amazonaws.com/files.appannie.com/reports/2001_State_of_Mobile_2020_Main_EN.pdf.

[21] О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верхов. Суда РФ от 30 нояб. 2017 г. № 48 // Бюллетень Верховного Суда РФ. 2018. № 2.

По словам А. Арсентьева, руководителя направления аналитики и спецпроектов InfoWatch, выявлено уже больше 4 тыс. новых сайтов по теме COVID-19, из которых около 8 % относятся к мошенническим или как минимум к подозрительным. Можно выделить несколько разновидностей мошеннических посягательств.

Мошенничества, связанные с высоким спросом на определенные товары, защитные средства и лекарственные препараты для лечения осложнений новой коронавирусной инфекции. Отдельной «нишей» для мошенников стал резко возросший спрос на медицинские маски и антисептические средства. В наиболее популярных социальных сетях мошенники размещают фейковые объявления о продаже медицинских масок и антисептиков для рук, узнают данные платежных карт тех, кто пожелал воспользоваться предложением, и затем с помощью полученной информации совершают хищение денежных средств со счетов своих жертв. В феврале в Великобритании, по данным СМИ, злоумышленникам удалось таким образом похитить около 1 млн долл. США[22]. В компании «Крибрум», разработавшей систему мониторинга социальных медиа, зафиксировали 441 сообщение о продаже тестов, «вакцин», лекарств против нового вируса и 1 380 — о покупке. Нетрудно предположить, с какой динамикой они будут прирастать в количестве[23].

Полицейской службой Европейского союза было расследовано преступление о мошенничестве по факту обещания о перечислении компанией 6,6 млн евро фирме из Сингапура для приобретения спиртовых гелей и масок FFP3/2 и зафиксированы случаи продажи гражданам «чудодейственных» препаратов для профилактики коронавируса[24].

В Интернете и в социальных сетях появилось огромное количество предложений о продаже лекарственных препаратов [29], якобы помогающих при лечении осложнений новой коронавирусной инфекции.

Европейское медицинское агентство предупредило граждан, чтобы они не покупали лекарства в незарегистрированных онлайн-аптеках и у других поставщиков лекарственных средств, стремящихся использовать страхи и опасения людей во время продолжающейся пандемии COVID-19. Продавцы таких лекарственных препаратов могут утверждать, что их медикаменты лечат коронавирусную инфекцию[25]. Однако данные лекарства, скорее всего, являются поддельными. Они могут нанести серьезный вред здоровью граждан.

Пандемия сопровождается «инфодемией». С момента вспышки новой коронавирусной инфекции началось бурное распространение фальшивых новостей и вводящей в заблуждение фейковой информации [30]. Например, распространялись ложные сведения о профилактических мерах против коронавируса, таких как полоскание рта соленой водой, поедание душицы или даже питье отбеливателя [31]. Практика показывает, что в социальных сетях ложью делятся гораздо чаще, чем информацией, основанной на фактах.

Мошенничества, связанные с ужесточением введенных ограничений и требований в период пандемии. Активно используемые федеральными органами власти и органами власти субъектов мобильные СМС-рассылки, информирующие о введенных ограничениях и требованиях в связи с пандемией, также были взяты злоумышленниками на вооружение. В данном аспекте особую значимость приобретает разъяснительная работа с гражданами о возможности выдачи специального разрешения исключительно государственными органами без привлечения третьих лиц[26].

Так, в одной из социальных сетей был размещен пост с предложением приобрести за 1 500 р. пропуск с QR-кодом для передвижения по Москве и области. ГУ МВД России по Московской области официально заявило, что все подобные сервисы нелегальны и их использование грозит потерей не только денег, но и персональных данных[27]. Следует отметить, что все

[22] URL: https://news.sky.com.

[23] Данные представлены по состоянию на март 2020 г.

[24] Catching the virus cybercrime, disinformation and the COVID-19 pandemic. Report // Europol. 14 p. URL: https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf.

[25] COVID-19: Beware of falsified medicines from unregistered websites // EMA. URL: https://www.ema.europa.eu/en/documents/press-release/covid-19-beware-falsified-medicines-unregistered-websites_en.pdf.

[26] ВТБ заявляет о мошеннических действиях по оформлению QR-кодов // Comnews. URL: https://www.comnews.ru/content/205673/2020-04-17/2020-w16/vtb-zayavlyaet-o-moshennicheskikh-deystviyakh-oformleniyu-qr-kodov.

[27] Министерство внутренних дел РФ : офиц. сайт. URL: https://мвд.рф/news/item/20025145.

цифровые пропуска, появившиеся с введением ограничений или требований органов государственной власти в период пандемии, оформляются совершенно бесплатно.

В Москве, где в апреле 2020 г. был введен режим цифровых пропусков с использованием QR-кодов для перемещения по городу в период пандемии, зафиксированы случаи массового обращения к клиентам банков, в особенности пожилого возраста, с предложением помощи в оформлении необходимого разрешения. Полученные злоумышленниками в ходе телефонного общения персональные данные в дальнейшем использовались в преступных целях.

Мошенничества, связанные с распространением лжеинформации (фейков) о выдаче государственных субсидий и социальных выплат. В связи с кризисом, вызванным пандемией, преступники реанимировали способ выманивания средств со счетов под видом перевода социальных выплат. Они обещают жертве сумму в 30 тыс. р., якобы положенную всем россиянам в виде поддержки в нестабильный период. Но вместо выплат люди, как правило, лишаются своих средств.

Популярным стало и размещение в Сети фейковых объявлений о сборе несуществующей благотворительной организацией средств на изобретение вакцины от коронавируса. По данным компании ESET, злоумышленники распространяли новости от имени Всемирной организации здравоохранения, призывая пользователей перейти по вредоносным ссылкам с конфиденциальной информацией о COVID-19 либо с призывом сделать пожертвование для разработки вакцины[28].

В Центральном банке Российской Федерации, где аккумулируется информация обо всех подозрительных операциях, видят лишь один способ предупреждения таких действий мошенников: напоминание гражданам о том, что все обращения с незнакомых сайтов с просьбой сообщить данные карт — это признак мошенничества.

Специалисты по информационной безопасности отмечают, что попасться на удочку злоумышленников могут даже подготовленные граждане, поскольку преступники совершенствуют способы обмана, хорошо ориентируются в новостной повестке, пользуются современными технологиями и консультациями психологов.

Как это ни парадоксально, более широкое использование цифровых технологий после пандемии может привести к увеличению локализации многих аспектов кибербезопасности [32].

Пандемия COVID-19 спровоцировала широкое распространение фальшивых новостей по всему миру, и это стало реальной угрозой. Дезинформация, распространяемая с помощью цифровых технологий, применяется для дестабилизации внутригосударственной обстановки, создания панических настроений в обществе, разжигания межнациональной и религиозной розни, вовлечения масс в антигосударственные движения, совершения преступлений. Несомненно, верны слова Г. Бергера о том, что «высокие страхи, неуверенность и неизвестность есть плодородная почва для процветания и роста фальсификаций. Когда дезинформация повторяется и усиливается, в том числе влиятельными людьми, серьезная опасность заключается в том, что информация, основанная на истине, в конечном итоге окажет лишь незначительное влияние»[29].

Одним из действенных инструментов против распространения фейков, использования их в преступных целях следует признать введение 1 апреля 2020 г. уголовной ответственности за публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан (ст. 207.1 УК РФ), и публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия (ст. 207.2 УК РФ). Данные нормы, бесспорно, стали новеллами для уголовного законодательства и породили ряд трудностей. В частности, требовало разъяснения понятие заведомой ложности, признаки фейковой (ложной) информации. Довольно быстро Верховный Суд РФ разъяснил, что важным для привлечения к уголовной ответственности является мотив лица — желание посеять панику, парализовать работу госорганов и т.д.[30] Отдельно стоит отметить и «обстоятельства, представ-

[28] ESET: мошенники продолжают наживаться на пандемии // ESET. URL: https://www.esetnod32.ru/company/press/center/eset-moshenniki-prodolzhayut-nazhivatsya-na-pandemii.

[29] Во время этой пандемии коронавируса «поддельные новости» ставят под угрозу жизни людей // ЮНЕСКО. URL: https://news.un.org/en/story/2020/04/1061592.

[30] Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 1 : утв. Президиумом Верхов. Суда РФ 21 апр. 2020 г. // СПС «КонсультантПлюс».

ляющие угрозу жизни и безопасности граждан», пандемия также включена в их перечень. Относительно использования фейков для совершения мошеннических действий разъяснений не дается, однако полагаем, что понятие обмана, применяемое для классического мошенничества, в данном случае вполне уместно.

4. *Атаки на цифровые платформы для коммуникации, их взлом («Zoombombing»)*.

Пандемия коронавируса вынудила миллионы людей по всему миру оставаться в своих домах, и платформа Zoom стала не только залом для виртуальных встреч и деловых переговоров, аудиторией для занятий, но и местом встреч по интересам (для костюмированных вечеринок, церковных служб, заседаний книжных клубов и романтических свиданий). Подобно Instagram, Facebook и Twitter, Zoom стал ключевой частью интернет-культуры.

По мере того как приложение для видеоконференций Zoom набирает популярность (за два месяца 2020 г. аудитория увеличилась на 118,58 %, ежедневный прирост составил 1,58 %), формируется новая потенциальная проблема, связанная с конфиденциальностью и безопасностью в цифровой среде, под названием «Zoombombing» [33].

Пользователи приложения по всему миру заявляют об атаках неизвестных лиц на их персональные соединения в программе. Так, хакеры и тролли взламывают занятия в онлайн-классах и выкрикивают ненормативную лексику, видеоконференц-связь может быть прервана, например, порнографическими изображениями и/или оскорбительными изображениями и т.п. [33; 34].

Для обеспечения конфиденциальности видеоконференций пользователям рекомендуется:

– делать свои встречи приватными (в Zoom есть опции, требующие пароль, а также функция комнаты ожидания, позволяющая контролировать, кому разрешено звонить);

– не делиться ссылкой на собрание на общедоступных онлайн-форумах;

– ограничить совместное использование экрана только администратором мероприятия[31].

Аналогичные рекомендации распространяют и другие компании, предоставляющие услуги удаленной видео-конференц-связи с использованием облачных вычислений.

5. *Рост числа криминальных проявлений в онлайн-играх*.

В период пандемии популярность онлайн-игр взлетела до предела по всему миру. Генеральный директор Verizon Х. Вестберг сообщил, что игровой интернет-трафик вырос на 75 % за неделю с 15 марта 2020 г., когда США начали объявлять о карантинных ограничениях [35]. В тот же период средняя активность на самой популярной платформе для потоковой передачи видеоигр Twitch удвоилась [36]. Steam, ведущая платформа по распространению видеоигр, достигла пика в 23 млн одновременно присутствующих во всех играх онлайн-пользователей [37]. Процветание онлайн-гейминга не осталось без внимания киберпреступников. Им не потребовалось много времени, чтобы открыть для себя привлекательность виртуальных миров.

Традиционно проблемы с преступными проявлениями в онлайн-играх связаны с их использованием в качестве платформы для общения или самовыражения. Зачастую диалоги в онлайн-играх используются для распространения материалов экстремистского или сексуального характера [38].

Однако все чаще и чаще онлайн-игры эксплуатируются в криминальных целях для совершения финансовых преступлений [39], кражи личных данных [40], проведения азартных игр[32] и совершения коррупционных деяний в виде организации договорных игр в киберспорте [41].

Все это свидетельствует не о том, что онлайн-игры превратились в виртуальные логова, кишащие хакерами и иными преступниками, а просто о том, что, как и во многих других отраслях, криминальные риски в данной сфере в связи с пандемией возросли.

По мере процветания внутриигровой экономики разработчики игр должны взять на себя ответственность за защиту виртуальных миров, которые они создают, от реальных преступлений, а также находиться в тесном взаимодействии с правоохранительными органами для минимизации рисков.

6. *Увеличение спроса на порнографические материалы и, как результат, их широкое распространение через социальные сети, зашифрованные приложения и в DarkNet*.

ФБР выпустило предупреждение о том, что во время закрытия школ в период локдауна

[31] Security at Zoom // Zoom. URL: https://zoom.us/security.

[32] Australian police charge five men over match-fixing in online gaming // Irishtimes. URL: https://www.irishtimes.com/sport/australian-police-charge-five-men-over-match-fixing-in-online-gaming-1.4244441.

дети, которые играют в онлайн-игры и пользуются социальными сетями, могут стать жертвами сексуальных агрессоров, поскольку они проводят длительное время в сети Интернет. Кроме того, бóльшая часть контента, касающегося сексуальной эксплуатации детей, передается частным группам пользователей на форумах[33].

В период пандемии возросла также онлайн-активность педофилов, ищущих материалы о сексуальном насилии над детьми, что усугубляется нехваткой модераторов, которые выявляют и удаляют оскорбительные материалы из сетей. Интерпол также в настоящее время отслеживает и получает информацию от стран-членов в отношении изменений в других сферах преступности, таких как контрабанда и торговля людьми[34].

Фишинговые и вымогательские кампании запускаются для использования нынешнего кризиса в преступных целях [42] и, как ожидается, будут продолжать расширяться по своему масштабу. Судя по целому ряду показателей, активность вокруг распространения материалов о сексуальной эксплуатации детей в Интернете, как представляется, также будет расти. DarkNet продолжает функционировать, а вместе с ним процветают криминальные рынки и магазины поставщиков для распространения незаконных товаров и услуг[35]. Да и в целом во всем мире вокруг COVID-19 продолжает распространяться все больше дезинформации, что может иметь потенциально вредные последствия для общественных интересов[36].

Выводы

Подводя итоги исследования, необходимо отметить, что с позиции российского уголовного законодательства ответственность за совершение рассмотренных цифровых преступлений предусмотрена в гл. 28 «Преступления в сфере компьютерной информации» УК РФ, а также в ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ.

Поскольку треть населения мира продолжает находиться в той или иной форме изоляции, связанные с этим фактом изменения в структуре преступности уже наблюдаются. Воздействие пандемии COVID-19 на киберпреступность было наиболее заметным по сравнению с ее воздействием на другие виды преступной деятельности. Всплеск киберпреступности стал глобальной проблемой. Преступники смогли быстро адаптироваться и извлечь выгоду из тревог и страхов своих жертв. Пандемия создала и усилила колоссальный риск совершения кибератак. Преступная деятельность хакеров в основном нацелена на процессы увеличения зависимости людей от цифровых технологий.

Несомненно, что в условиях непрекращающегося локдауна стандарты безопасности ухудшились, поскольку многие организации не были готовы к удаленной работе. В ближайшее время число жертв киберпреступности будет только расти. Международные организации и правоохранительные органы многих стран выпускают большое количество рекомендаций по предупреждению совершения в отношении компаний и граждан преступных посягательств в цифровой сфере.

Правильное поведение человека в цифровом пространстве (равно как и в реальном) способствует предотвращению распространения различных угроз в виртуальном мире (как и в физической среде). Постоянное повышение культуры соблюдения информационной безопасности, развитие киберграмотности, поддержание цифровой гигиены на должном уровне минимизируют указанные риски.

Предложено применять следующую обобщенную группу профилактических мер технологического характера в период пандемии и после ее завершения:

1. *В отношении программного обеспечения и приложений*:

– скачивать программное обеспечение и приложения с проверенных источников (сайтов разработчиков и вендоров);

[33] FBI warns parents, teachers about increased risks of online child exploitation // KIRO7. URL: https://www.kiro7.com/news/local/fbi-warns-parents-teachers-about-increased-risks-online-child-exploitation/UFIRZBBOF5ACRNJ4XOUFTSDRHU.

[34] COVID-19 cyberthreats // Interpol. URL: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats.

[35] Viral marketing counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic : report. Europol, 2020. Apr. 17. 17 p. URL: https://www.europol.europa.eu/sites/default/files/documents/report_covid_19_-_viral_marketing_counterfeits.pdf ; Pandemic profiteering how criminals exploit the COVID-19 crisis : report. Europol. 14 p. URL: https://www.europol.europa.eu/sites/default/files/documents/pandemic_profiteering-how_criminals_exploit_the_covid-19_crisis.pdf.

[36] Catching the virus cybercrime, disinformation and the COVID-19 pandemic : report. Europol. 14 p. URL: https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf.

– систематически обновлять программное обеспечение и приложения в целях устранения возможных уязвимостей;

– использовать безопасные способы установки и обновления программного обеспечения и приложений.

2. *В отношении электронной почты*:

– не переходить по вредоносным ссылкам во входящих сообщениях в электронной почте;

– не открывать вредоносные вложения во входящих сообщениях в электронной почте.

3. *В отношении страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет*:

– использовать виртуальные частные сети для безопасного доступа в сеть Интернет;

– использовать протокол HTTPS с поддержкой шифрования для безопасного интернет-соединения;

– использовать менеджеры паролей, при этом исключить повторное использование паролей в сети Интернет;

– проверять источник каждого URL-адреса при переходе на страницы сайтов в сети Интернет (избегать посещения поддельных сайтов).

4. *В отношении цифровых устройств и гаджетов*:

– использовать сложный пароль от домашних Wi-Fi-устройств, маршрутизаторов и гаджетов;

– применять весь спектр системных возможностей брандмауэра, встроенного в цифровые устройства и гаджеты.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Naidoo R. A Multi-Level Influence Model of COVID-19 Themed Cybercrime / R. Naidoo. — DOI 10.1080/0960085X.2020.1771222 // European Journal of Information Systems. — 2020. — Vol. 29, no. 3. — P. 306–321.

2. Horberry M. UK Coronavirus Scams: Online and on your Doorstep / M. Horberry // Al Jazeera. — URL: https://www.aljazeera.com/news/2020/04/uk-coronavirus-scams-online-doorstep-200414220652029.html.

3. Mouton F. COVID-19: Impact on the Cyber Security Threat Landscape / F. Mouton, A. Coning. — DOI 10.13140/RG.2.2.27433.52325 // ResearchGate. — URL: https://www.researchgate.net/publication/340066124.

4. Герасимова Е.В. Криминологическая характеристика преступности, ее тенденции и динамика / Е.В. Герасимова, А.В. Миронов, А.Н. Рубищев. — DOI 10.47576/2712-7516_2022_1_1_68 // Журнал прикладных исследований. — 2022. — Т. 1, № 1. — С. 68–72.

5. Воронин Ю.А. Преступления в сфере обращения цифровой информации и их детерминанты / Ю.А. Воронин // Виктимология. — 2020. — № 1 (23). — С. 74–83.

6. Crick J.M. Coopetition and COVID-19: Collaborative Business-to-Business Marketing Strategies in a Pandemic Crisis / J.M. Crick, D. Crick. — DOI 10.1016/j.indmarman.2020.05.016 // Industrial Marketing Management. — 2020. — Vol. 88. — P. 206–213.

7. Begishev I.R. Information Infrastructure of Safe Computer Attack / I.R. Begishev, Z.I. Khisamova, G.I. Mazitova. — DOI 10.29042/2019-5639-5642 // Helix. — 2019. — Vol. 9, no. 5. — P. 5639–5642.

8. Infringements on Digital Information: Modern State of the Problem / E.Yu. Latypova, E.V. Nechaeva, E.M. Gilmanov, N.V. Aleksandrova. — DOI 10.1051/shsconf/20196210004 // Problems of Enterprise Development: Theory and Practice : Proceedings of the 17th International Scientific Conference. SHS Web of Conferences. — Samara, 2019. — Vol. 62. — Art. 10004.

9. Bokovnya A.Y. Study of Russia and the UK Legislations in Combating Digital Crimes / A.Y. Bokovnya, Z.I. Khisamova, I.R. Begishev. — DOI 10.29042/2019-5458-5461 // Helix. — 2019. — Vol. 9, no. 5. — P. 5458–5461.

10. Begishev I.R. Criminal Legal Ensuring of Security of Critical Information Infrastructure of the Russian Federation / I.R. Begishev, Z.I. Khisamova, G.I. Mazitova // Revista Gênero & Direito. — 2019. — Vol. 8, no. 6. — P. 283–292.

11. Satter R. Exclusive: Elite hackers target WHO as Coronavirus Cyberattacks Spike / R. Satter, J. Stubbs, C. Bing // Reuters. — 2020. — March 24. — URL: https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN.

12. Гаврилюк А. Враг изнутри: с переходом на удаленку число утечек вырастет вдвое / А. Гаврилюк // ComNews.ru. — 2020. — March 23. — URL: https://www.comnews.ru/content/205165/2020-03-23/2020-w13/vrag-iznutri-perekhodom-udalenku-chislo-utechek-vyrastet-vdvoe.

13. Cimpanu C. FBI Says Cybercrime Reports Quadrupled during COVID-19 Pandemic / C. Cimpanu // ZDNet.com. — 2020. — Apr. 18. — URL: https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic.

14. Доронин А.М. Уголовная ответственность за неправомерный доступ к компьютерной информации : автореф. дис. ... канд. юрид. наук : 12.00.08 / А.М. Доронин. — Москва, 2003. — 23 с.

15. Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации : дис. ... канд. юрид. наук : 12.00.08 / Д.Г. Малышенко. — Москва, 2002. — 166 с.

16. Русскевич Е.А. Неправомерный доступ к компьютерной информации: теория и судебная практика / Е.А. Русскевич // Судья. — 2018. — № 10 (94). — С. 46–50.

17. Винокуров В.Н. Предмет неправомерного доступа к компьютерной информации (ст. 272 УК) / В.Н. Винокуров, Е.А. Федорова // Законность. — 2021. — № 5 (1039). — С. 50–52.

18. Научно-практический комментарий к Уголовному кодексу Российской Федерации от 13 июня 1996 г. № 63-ФЗ / Н.А. Агешкина, М.А. Беляев, Ю.В. Белянинова [и др.]. — Саратов : Ай Пи Эр Медиа, 2013. — 848 с.

19. Ковалев Д. Как пандемия меняет ИБ-рынок / Д. Ковалев // ComNews.ru. — 2020. — 20 апр. — URL: https://www.comnews.ru/content/205669/2020-04-20/2020-w17/kak-pandemiya-menyaet-ib-rynok.

20. Beaunoyer E. COVID-19 and Digital Inequalities: Reciprocal Impacts and Mitigation Strategies / E. Beaunoyer, S. Dupéré, M.J. Guitton. — DOI 10.1016/j.chb.2020.106424 // Computers in Human Behavior. — 2020. — Vol. 111. — Art. 106424.

21. Digital Crime and its Impact in Present Society / Y.S. Rao, D. Pradhan, T.C. Panda, R. Rath // International Journal of Engineering Research & Technology. — 2020. — Vol. 8, iss. 1. — P. 1–6.

22. Frauenstein E.D. Susceptibility to Phishing on Social Network Sites: A Personality Information Processing Model / E.D. Frauenstein, S. Flowerday. — DOI 10.1016/j.cose.2020.101862 // Computers & Security. — 2020. — Vol. 94. — Art. 101862.

23. Tran C. Recommendations for Ordinary Users from Mitigating Phishing and Cybercrime Risks During COVID-19 Pandemic / C. Tran // ResearchGate. — 2020. — May. — URL: https://www.researchgate.net/publication/341526654.

24. Бегишев И.Р. Организация хакерского сообщества: криминологический и уголовно-правовой аспекты / И.Р. Бегишев, З.И. Хисамова, С.Г. Никитин. — DOI 10.17150/2500-4255.2020.14(1).96-105 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 1. — С. 96–105.

25. Mansfield-Devine S. Cybercrime in a Time of Coronavirus / S. Mansfield-Devine. — DOI 10.1016/S1361-3723(20)30045-2 // Computer Fraud & Security. — 2020. — Vol. 2020, iss. 5. — P. 1–3.

26. Самсонова А. Кибермошенники прикрываются коронавирусом / А. Самсонова // ComNews.ru. — 2020. — 18 March. — URL: https://www.comnews.ru/content/205071/2020-03-18/2020-w12/kibermoshenniki-prikryvayutsya-koronavirusom.

27. John C. Thousands of Malicious Coronavirus-Related Websites Are Created Daily / C. John // Atlas VPN. — 2020. — 26 March. — URL: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine.

28. Скобелев В. Сбербанк предложил меры против использующих социальную инженерию хакеров / В. Скобелев // ComNews.ru. — 2020. — 17 апр. — URL: https://www.comnews.ru/content/205668/2020-04-17/2020-w16/sberbank-predlozhil-mery-protiv-ispolzuyuschikh-socialnuyu-inzheneriyu-khakerov.

29. Big Data, Natural Language Processing, and Deep Learning to Detect and Characterize Illicit COVID-19 Product Sales: An Infoveillance Study on Twitter and Instagram / T. Mackey, J. Li, V. Purushothaman [et al.]. — DOI 10.2196/preprints.20794 // JMIR Public Health and Surveillance. — 2020. — Vol. 6, no. 3. — URL: https://publichealth.jmir.org/2020/3/e20794.

30. Rovetta A. COVID-19-Related Web Search Behaviors and Infodemic Attitudes in Italy: Infodemiological Study / A. Rovetta, A.S. Bhagavathula. — DOI 10.2196/19374 // JMIR Public Health Surveillance. — 2020. — Vol. 6, no. 2. — Art. e19374. — URL: https://pubmed.ncbi.nlm.nih.gov/32338613.

31. COVID-19 Infodemic: More Retweets for Science-Based Information on Coronavirus than for False Information / C.M. Pulido, B. Villarejo-Carballido, G. Redondo-Sama, A. Gómez. — DOI 10.1177/0268580920914755 // International Sociology. — 2020. — Vol. 35, no. 4. — P. 377–392.

32. The Implications of the COVID-19 Pandemic for Cybercrime Policing in Scotland: A Rapid Review of the Evidence and Future Considerations / B. Collier, S. Horgan, R. Jones, L. Shepherd // ResearchGate. — URL: https://www.researchgate.net/publication/341742472.

33. Andone D. FBI Warns Video Calls are Getting Hijacked. It's Called «Zoombombing» / D. Andone // Cable News Network (CNN). — 2020. — Apr. 2. — URL: https://edition.cnn.com/2020/04/02/us/fbi-warning-zoombombing-trnd/index.html.

34. Setera K. FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic / K. Setera // Federal Bureau of Investigation. — 2020. — March 30. — URL: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

35. Clifford T. Web Traffic Spiked 20% in one Week amid Coronavirus Shutdown, Verizon CEO Says / T. Clifford // CNBC Newsletters. — 2020. — URL: https://www.cnbc.com/2020/03/19/verizon-ceo-web-traffic-up-20percent-in-one-week-amid-coronavirus-shutdown.html.

36. Smith N. The Giants of the Video Game Industry Have Thrived in the Pandemic. Can the Success Continue? / N. Smith // The Washington Post. — 2020. — May 12. — URL: https://www.washingtonpost.com/video-games/2020/05/12/video-game-industry-coronavirus.

37. Batchelor J. Record Number of Steam Users Online During Coronavirus Outbreak / J. Batchelor // GamesIndustry.biz. — 2020. — March 16. — URL: https://www.gamesindustry.biz/articles/2020-03-16-record-number-of-steam-users-online-during-coronavirus-outbreak.

38. Parkin S. Microsoft Defends Ban of Call of Duty: Black Ops Players Using Swastika as Logo / S. Parkin // Gamasutra.com. — 2010. — Nov. 22. — URL: https://www.gamasutra.com/view/news/122273/Microsoft_Defends_Ban_Of_Call_Of_Duty_Black_Ops_Players_Using_Swastika_As_Logo.php.

39. Moiseienko A. Gaming the System: Money Laundering Through Online Games / A. Moiseienko, K. Izenman // Royal United Services Institute. — 2019. — Vol. 39, iss. 9. — URL: https://rusi.org/publication/rusi-newsbrief/gaming-system-money-laundering-through-online-games.

40. Cox J. Hacker Bribed «Roblox» Insider to Access User Data / J. Cox // Vice Media. — 2020. — May 5. — URL: https://www.vice.com/en_us/article/qj4ddw/hacker-bribed-roblox-insider-accessed-user-data-reset-passwords.

41. Yin-Poole W. Real-life US Politician Banned from Eve Online for Alleged Corruption / W. Yin-Poole // Gamer Network Limited. — 2019. — Apr. 9. — URL: https://www.eurogamer.net/articles/2019-04-09-real-life-us-politician-banned-from-eve-online-for-alleged-corruption.

42. Impact of Social Distancing During COVID-19 Pandemic on Crime in Los Angeles and Indianapolis / G. Mohler, A.L. Bertozzi, J. Carter [et al.]. — DOI 10.1016/j.jcrimjus.2020.101692 // Journal of Criminal Justice. — 2020. — Vol. 68. — Art. 101692.

REFERENCES

1. Naidoo R. A Multi-Level Influence Model of COVID-19 Themed Cybercrime. *European Journal of Information Systems*, 2020, vol. 29, no. 3, pp. 306–321. DOI: 10.1080/0960085X.2020.1771222.

2. Horberry M. UK Coronavirus Scams: Online and on your Doorstep. *Al Jazeera*. Available at: https://www.aljazeera.com/news/2020/04/uk-coronavirus-scams-online-doorstep-200414220652029.html.

3. Mouton F., Coning A. COVID-19: Impact on the Cyber Security Threat Landscape. *ResearchGate*. Available at: https://www.researchgate.net/publication/340066124. DOI: 10.13140/RG.2.2.27433.52325.

4. Gerasimova E.V., Mironov A.V., Rubishchev A.N. Criminological Characteristics of Crime, its Trends and Dynamics. *Zhurnal prikladnykh issledovanii = Journal of Applied Research*, 2022, vol. 1, no. 1, pp. 68–72. (In Russian). DOI: 10.47576/2712-7516_2022_1_1_68.

5. Voronin Yu.A. Crimes in the Sphere of Circulation of Digital Information and their Determinants. *Viktimologiya = Victimology*, 2020, no. 1, pp. 74–83. (In Russian).

6. Crick J.M., Crick D. Coopetition and COVID-19: Collaborative Business-to-Business Marketing Strategies in a Pandemic Crisis. *Industrial Marketing Management*, 2020, vol. 88, pp. 206–213. DOI: 10.1016/j.indmarman.2020.05.016.

7. Begishev I.R., Khisamova Z.I., Mazitova G.I. Information Infrastructure of Safe Computer Attack. *Helix*, 2019, vol. 9, no. 5, pp. 5639–5642. DOI: 10.29042/2019-5639-5642.

8. Latypova E.Yu., Nechaeva E.V., Gilmanov E.M., Aleksandrova N.V. Infringements on Digital Information: Modern State of the Problem. *Problems of Enterprise Development: Theory and Practice. Proceedings of the 17th International Scientific Conference. SHS Web of Conferences*. Samara, 2019. Vol. 62. Art. 10004. DOI: 10.1051/shsconf/20196210004.

9. Bokovnya A.Y., Khisamova Z.I., Begishev I.R. Study of Russia and the UK Legislations in Combating Digital Crimes. *Helix*, 2019, vol. 9, no. 5, pp. 5458–5461. DOI: 10.29042/2019-5458-5461.

10. Begishev I.R., Khisamova Z.I., Mazitova G.I. Criminal Legal Ensuring of Security of Critical Information Infrastructure of the Russian Federation. *Revista Gênero & Direito*, 2019, vol. 8, no. 6, pp. 283–292.

11. Satter R., Stubbs J., Bing C. Exclusive: Elite hackers target WHO as Coronavirus Cyberattacks Spike. *Reuters*, 2020, March 24. Available at: https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN.

12. Gavrilyuk A. The enemy within: a switch to remote work will double the number of leaks. *ComNews.ru*, 2020, March 23. Available at: https://www.comnews.ru/content/205165/2020-03-23/2020-w13/vrag-iznutri-perekhodom-udalenku-chislo-utechek-vyrastet-vdvoe. (In Russian).

13. Cimpanu C. FBI Says Cybercrime Reports Quadrupled during COVID-19 Pandemic. *ZDNet.com*, 2020, April 18. Available at: https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic.

14. Doronin A.M. *Criminal Responsibility for Wrongful Access to Computer Information. Cand. Diss. Thesis.* Moscow, 2003. 23 p.

15. Malyshenko D.G. *Criminal Responsibility for Wrongful Access to Computer Information. Cand. Diss.* Moscow, 2002. 166 p.

16. Russkevich E.A. Wrongful Access to Computer Information: Theory and Judicial Practice. *Sud'ya = Judge*, 2018, no. 10, pp. 46–50. (In Russian).

17. Vinokurov V.N., Fyodorova E.A. Unlawful Access to the Computer Related Data (art. 272 of the Criminal Code of the Russian Federation). *Zakonnost' = Legality*, 2021, no. 5, pp. 50–52. (In Russian).

18. Ageshkina N.A., Belyaev M.A., Belyaninova Yu.V. [et al.]. *Scientific and Practical Commentary to the Criminal Code of the Russian Federation dated June 13, 1996 No. 63-FZ*. Saratov, Ai Pi Er Media Publ., 2013. 848 p.

19. Kovalev D. How the pandemic is changing the information security market. *ComNews.ru*, 2020, April 20. Available at: https://www.comnews.ru/content/205669/2020-04-20/2020-w17/kak-pandemiya-menyaet-ib-rynok. (In Russian).

20. Beaunoyer E., Dupéré S., Guitton M.J. COVID-19 and Digital Inequalities: Reciprocal Impacts and Mitigation Strategies. *Computers in Human Behavior*, 2020, vol. 111. Art. 106424. DOI: 10.1016/j.chb.2020.106424.

21. Rao Y.S., Pradhan D., Panda T.C., Rath R. Digital Crime and its Impact in Present Society. *International Journal of Engineering Research & Technology*, 2020, vol. 8, iss. 1, pp. 1–6.

22. Frauenstein E.D., Flowerday S. Susceptibility to Phishing on Social Network Sites: A Personality Information Processing Model. *Computers & Security*, 2020, vol. 94. Art. 101862. DOI: 10.1016/j.cose.2020.101862.

23. Tran C. Recommendations for Ordinary Users from Mitigating Phishing and Cybercrime Risks During COVID-19 Pandemic. *ResearchGate*, 2020, May. Available at: https://www.researchgate.net/publication/341526654.

24. Begishev I.R., Khisamova Z.I., Nikitin S.G. The Organization of Hacking Community: Criminological and Criminal Law Aspects. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 1, pp. 96–105. (In Russian). DOI: 10.17150/2500-4255.2020.14(1).96-105.

25. Mansfield-Devine S. Cybercrime in a Time of Coronavirus. *Computer Fraud & Security,* 2020, vol. 2020, iss. 5, pp. 1–3. DOI: 10.1016/S1361-3723(20)30045-2.

26. Samsonova A. Cyber fraudsters are using the coronavirus as a cover. *ComNews.ru*, 2020, March 18. Available at: https://www.comnews.ru/content/205071/2020-03-18/2020-w12/kibermoshenniki-prikryvayutsya-koronavirusom. (In Russian).

27. John C. Thousands of Malicious Coronavirus-Related Websites are Created Daily. *Atlas VPN*, 2020, March 26. Available at: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine.

28. Skobelev V. Sberbank suggested measures to counteract hackers who use social engineering. *ComNews.ru*, 2020, April 17. Available at: https://www.comnews.ru/content/205668/2020-04-17/2020-w16/sberbank-predlozhil-mery-protiv-ispolzuyuschikh-socialnuyu-inzheneriyu-khakerov. (In Russian).

29. Mackey T., Li J., Purushothaman V., Nali M., Shah N. Big Data, Natural Language Processing, and Deep Learning to Detect and Characterize Illicit COVID-19 Product Sales: An Infoveillance Study on Twitter and Instagram. *JMIR Public Health and Surveillance*, 2020, vol. 6, no. 3. DOI: 10.2196/preprints.20794.

30. Rovetta A. COVID-19-Related Web Search Behaviors and Infodemic Attitudes in Italy: Infodemiological Study. *JMIR Public Health Surveillance*, 2020, vol. 6, no. 2. Art. e19374. DOI: 10.2196/19374.

31. Pulido C.M., Villarejo-Carballido B., Redondo-Sama G., Gómez A. COVID-19 Infodemic: More Retweets for Science-Based Information on Coronavirus than for False Information. *International Sociology*, 2020, vol. 35, no. 4, pp. 377–392. DOI: 10.1177/0268580920914755.

32. Collier B., Horgan S., Jones R., Shepherd L. The Implications of the COVID-19 Pandemic for Cybercrime Policing in Scotland: A Rapid Review of the Evidence and Future Considerations. *ResearchGate*, 2020, May 28. Available at: https://www.researchgate.net/publication/341742472.

33. Andone D. FBI Warns Video Calls Are Getting Hijacked. It's Called «Zoombombing». *Cable News Network (CNN)*, 2020, April 2. Available at: https://edition.cnn.com/2020/04/02/us/fbi-warning-zoombombing-trnd/index.html.

34. Setera K. FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic. *Federal Bureau of Investigation*, 2020, March 30. Available at: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

35. Clifford T. Web Traffic Spiked 20% in one Week amid Coronavirus Shutdown, Verizon CEO Says. *CNBC Newsletters*, 2020. Available at: https://www.cnbc.com/2020/03/19/verizon-ceo-web-traffic-up-20percent-in-one-week-amid-coronavirus-shutdown.html.

36. Smith N. The Giants of the Video Game Industry Have Thrived in the Pandemic. Can the Success Continue? *The Washington Post*, 2020, May 12. Available at: https://www.washingtonpost.com/video-games/2020/05/12/video-game-industry-coronavirus.

37. Batchelor J. Record Number of Steam Users Online During Coronavirus Outbreak. *GamesIndustry.biz*, 2020, March 16. Available at: https://www.gamesindustry.biz/articles/2020-03-16-record-number-of-steam-users-online-during-coronavirus-outbreak.

38. Parkin S. Microsoft Defends Ban of Call of Duty: Black Ops Players Using Swastika as Logo. *Gamasutra.com*, 2010, November 22. Available at: https://www.gamasutra.com/view/news/122273/Microsoft_Defends_Ban_Of_Call_Of_Duty_Black_Ops_Players_Using_Swastika_As_Logo.php.

39. Moiseienko A., Izenman K. Gaming the System: Money Laundering Through Online Games. *Royal United Services Institute*, 2019, vol. 39, iss. 9. Available at: https://rusi.org/publication/rusi-newsbrief/gaming-system-money-laundering-through-online-games.

40. Cox J. Hacker Bribed «Roblox» Insider to Access User Data. *Vice Media*, 2020, May 5. Available at: https://www.vice.com/en_us/article/qj4ddw/hacker-bribed-roblox-insider-accessed-user-data-reset-passwords.

41. Yin-Poole W. Real-life US Politician Banned from Eve Online for Alleged Corruption. *Gamer Network Limited*, 2019, April 9. Available at: https://www.eurogamer.net/articles/2019-04-09-real-life-us-politician-banned-from-eve-online-for-alleged-corruption.

42. Mohler G., Bertozzi A.L., Carter J., Short M.B., Sledge D. Impact of Social Distancing During COVID-19 Pandemic on Crime in Los Angeles and Indianapolis. *Journal of Criminal Justice*, 2020, vol. 68. Art. 101692. DOI: 10.1016/j.jcrimjus.2020.101692.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Хисамова Зарина Илдузовна — начальник отделения планирования и координации научной деятельности научно-исследовательского отдела Краснодарского университета Министерства внутренних дел Российской Федерации, кандидат юридических наук, г. Краснодар, Российская Федерация; e-mail: alise89@inbox.ru.

Бегишев Ильдар Рустамович — старший научный сотрудник Казанского инновационного университета имени В.Г. Тимирясова (ИЭУП), кандидат юридических наук, заслуженный юрист Республики Татарстан, г. Казань, Российская Федерация; e-mail: begishev@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Хисамова З.И. Цифровая преступность в условиях пандемии: основные тренды / З.И. Хисамова, И.Р. Бегишев. — DOI 10.17150/2500-4255.2022.16(2).185-198 // Всероссийский криминологический журнал. — 2022. — Т. 16, № 2. — С. 185–198.

INFORMATION ABOUT THE AUTHORS

Khisamova, Zarina I. — Head, Department of Planning and Coordination of Research Activities, Research Department, Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Ph.D. in Law, Krasnodar, the Russian Federation; e-mail: alise89@inbox.ru.

Begishev, Ildar R. — Senior Researcher, Kazan Innovative University named after V.G. Timiryasov (IEML), Ph.D. in Law, Honored Lawyer of the Republic of Tatarstan, Kazan, the Russian Federation; e-mail: begishev@mail.ru.

FOR CITATION

Khisamova Z.I., Begishev I.R. Digital crime in the context of a pandemic: main trends. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2022, vol. 16, no. 2, pp. 185–198. (In Russian). DOI: 10.17150/2500-4255.2022.16(2).185-198.