Раздел третий

УКРЕПЛЕНИЕ ЗАКОННОСТИ И БОРЬБА С ПРЕСТУПНОСТЬЮ

БЕССОНОВА ИННА ВЛАДИМИРОВНА
кандидат юридических наук, доцент кафедры уголовного права и криминологии Оренбургского института (филиала) Университета имени О.Е. Кутафина (МГЮА), 460000, г. Оренбург, ул. Комсомольская, 50, orenburg@msal.ru

АВИНОВ МИХАИЛ СЕРГЕЕВИЧ
студент магистратуры по программе «Магистр уголовного права и уголовного судопроизводства» Оренбургского института (филиала) Университета имени О.Е. Кутафина (МГЮА), 460000, г. Оренбург, ул. Комсомольская, 50, orenburg@msal.ru

ВЛИЯНИЕ ПАНДЕМИИ COVID-19 НА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

BESSONOVA INNA VLADIMIROVNA
Candidate of Legal Sciences, Associate Professor of the Department of Criminal Law and Criminology, Orenburg Institute (Branch) of Moscow State Law University named after O.E. Kutafin, 460000, Orenburg, Komsomolskaya Street, 50, orenburg@msal.ru

AVINOV MIKHAIL SERGEEVICH
postgraduate student of the program «Criminal Law and Criminal Procedure», Orenburg Institute (Branch) of Moscow State Law University named after O.E. Kutafin, 460000, Orenburg, Komsomolskaya Street, 50, orenburg@msal.ru

IMPACT OF THE COVID-19 PANDEMIC ON COMPUTER INFORMATION CRIMES

Аннотация: *В статье исследуются вопросы уголовной ответственности за преступления в сфере компьютерной информации. Рассмотрено влияние пандемии на составы компьютерных преступлений. На основе обобщения теоретических позиций сформулирована авторская позиция по исследуемому вопросу.*

Ключевые слова: *пандемия, коронавирус, преступления в сфере компьютерной информации, киберпреступления.*

Review. *The article examines the issues of criminal liability for crimes in the field of computer information. The impact of the pandemic on the constituent elements of computer crimes is considered. Based on the generalization of theoretical positions, the authors' position on the issue under study is formulated.*

Keywords: *pandemic, coronavirus, computer information crimes, cybercrime.*

Пандемия, вызванная коронавирусом в марте 2020 года, является не самым очевидным фактором, повлиявшим на киберпреступность, ведь переход от традиционных видов преступности в информационную сферу начался еще задолго до нее. Однако COVID-19 значительно ускорил процесс трансформации преступности, что объясняется ситуативным положением, в котором оказалось мировое сообщество, – чем больше деятельности в киберпространстве, тем больше риски, в том числе и уголовно-правовые.

Итак, первой предпосылкой для возникновения активности преступников в сфере компьютерной информации стали нормативно правовые акты, вынудившие все население пользоваться электронными средствами общения и компьютерными технологиями. Так в целях недопущения распространения COVID-19 были приняты: Указ Президента РФ

№ 239 от 02.04.2020 «О мерах по обеспечению санитарно-эпидемиологического благополучия населения на территории Российской Федерации в связи с распространением новой коронавирусной инфекции (COVID- 19)»; Указ Президента РФ от 20.10.2021 № 595 «Об установлении на территории Российской Федерации нерабочих дней в октябре - ноябре 2021 г.». Законное ограничение передвижений граждан и установление «режима самоизоляции» способствовали переводу всех сфер коммуникаций в дистанционный формат.

Соответственно, второй предпосылкой развития киберпреступности стал массовый переход на удаленную работу, онлайн продажи, электронное обращение в государственные органы и т.д. Результатами вынужденного перевода большинства рабочего населения в дистанционный формат стали как увеличение неграмотных пользователей сети «Интернет», так и повышение нагрузки на провайдеров услуг связи, что в свою очередь приводит к уязвимости всей сети.

Еще одной, третьей предпосылкой установления благоприятной среды для действий преступника в сфере компьютерной информации можно назвать ухудшение общего психологического состояния граждан, так как страх перед неизвестностью, непривычный уклад жизни становятся раздражителями и снижают внимательность к возможным опасностям. Так, инфантильные, напуганные и загнанные в четыре стены люди думают, что звонок из банка о том, что их банковский счет подвергся атаке и требуется срочный перевод денежных средств, поможет им спасти последние сбережения, либо же размещенная вирусная реклама в сети интернет о том, как правильно необходимо лечиться от Covid-19, откроет им ящик Пандоры и они смогут помочь всем своим родственникам.

Значительное увеличение количества киберпреступлений подтверждают статистические данные, размещенными государственными структурами. В соответствии с официальным докладом Министерства внутренних дел Российской Федерации (далее – МВД РФ) об уровне преступности за 2020 год число преступлений, связанных с использованием информационно-коммуникационных технологий, выросло более чем на 94 % по сравнению с соответствующим периодом прошлого года[1].

Существует значительный разрыв между информационным развитием и информационной безопасностью, так как для наличия второго требуется грамотное и полное понимание первого. Ввиду отсутствия такой связи создается свобода воли для преступника, который готов находить новые способы организации своей деятельности доселе неизвестные пользователям цифровых носителей. Немаловажными причинами столь активной заинтересованности злоумышленниками цифровой площадкой являются:

- территориальная удаленность и наличие хакерских программ, позволяющих скрыть местоположение преступных серверов;

- низкая осведомленность пользователей о цифровых возможностях и оснащенности мошенников для осуществления киберпреступлений, и как следствие – неразработанный план действий граждан при попадании в опасную ситуацию в сети;

- уязвимость электронных баз данных перед атакой злоумышленников, немногочисленность или полное отсутствие сотрудников по кибербезопасности как в отделах компаний, так и в государственных структурах.

Все вышеназванные предпосылки и причины способствовали массовому распространению конфиденциальной информации граждан, нарушению персональных данных, активному мошенничеству и, соответственно, результатом стали уход от ответственности преступников и слабая раскрываемость подобного рода нарушений закона.

Рассмотрим более детально схемы развития преступлений в сфере компьютерной информации, появившиеся в 2020 году при «благоприятных» условиях для злоумышленников.

Так, необходимость быстрого создания дистанционного рабочего доступа практически во всех компаниях повлекло к игнорированию информационной безопасности. При организации удаленной работы персонала возникает ряд сложностей. Например, вход сотрудников из дома в корпоративные сети компании сопутствует появлению таких новых уязвимостей, как плохо защищенные домашние маршрутизаторы, слабые пароли на персональных компьютерах, зараженные вирусами домашние компьютеры. В офисе за защитой интернет-канала присматривают системные администраторы, что невозможно в условиях дистанционной работы из дома. Настройка роутера и подключение к сети неквалифицированными специалистами, то есть самостоятельно каждым сотрудником — это существенные риски безопасности[2]. Необходимо отметить, что некоторые злоумышленники специализируются на уязвимостях программного обеспечения корпоративных маршрутизаторов, на которые чаще всего нацелены вирусы, замаскированные под обычные файлы и рассылаемые по электронной почте. По данным экспертов в области кибербезопасности за последний год из-за уязвимостей в аппаратной составляющей были потенциально скомпрометированы данные в 63 % компаний[3].

Кроме этого, начали выявляться проблемы информационной защищенности даже таких цифровых гигантов, как Microsoft, Яндекс, Google. Например, в октябре 2020 года в корпоративном мессенджере

[1] См.: Фалалеев М. Айфон вместо отмычки // Российская газета. 2020. 20 авг. № 8239.

[2] Касторский Г.Л. Киберпреступность в период пандемии коронавируса COVID-19 / Г.Л. Касторский, А.Г. Форкош // Молодой ученый. 2020. № 52 (342). С. 196-198. URL: https://moluch.ru/archive/342/77143/ (дата обращения: 15.03.2022).

[3] Кропачев С.Ю. Актуальные вопросы противодействия мошенническим действиям в экономической и предпринимательской сфере в связи с распространением коронавирусной инфекции // Евразийское научное объединение. 2020. № 4-3 (62). С. 196-200.

MicrosoftTeams закрыли уязвимость, через которую взломщик мог получить доступ ко всем учетным записям в организации. Примерно в то же время разработчики Zoom для macOS исправили ошибки, которые позволяли захватить контроль над устройством[4]. Для совместной работы с документами и обмена файлами сотрудники нередко использовали личные аккаунты на бесплатных сервисах, например Яндекс.-Диск и GoogleDocs. Как правило, для них недоступно централизованное управление правами, которое позволило бы защитить конфиденциальные данные. В связи с этим известны случаи, когда содержимое документов из таких хранилищ попадало в поисковую выдачу.

В условиях резкого перехода на цифровое пространство наиболее незащищенными группами стали школьники и пожилые граждане, слабо проинформированные об угрозах в Сети. Они чаще всего становятся жертвами киберпреступников, которые используют их компьютеры для загрузки и рассылки вирусных ссылок через электронные спам-сообщения об инфекции COVID-19. Следует также отметить, что, когда проведение очного обучения или совещания оказались невозможными, и стали востребованными сервисы видеосвязи, появилась возможность сокрытия коммуникации преступников для осуществления противоправных целей. Так, с момента начала пандемии COVID-19было зарегистрировано 1,7 тысячи новых доменов, содержащих название сервиса популярной видеосвязи Zoom[5].

Активизации действий мошенников способствовало распространение различных «фейковых» новостей на фоне недостаточности официальной информации и недоверия граждан к сообщениям государственных органов. При этом, их активность была направлена как на крупные компании, так и на обычных граждан. На различных форумах «даркнета» активизировалась продажа компромата, в том числе и на госслужащих и знаменитостей. Это произошло по причине роста фишинговых[6] атак, рассылке документов с прикрепленным вредоносным кодом и т.п. Ключевым средством для успешного действия мошенников стала самая обсуждаемая и интересуемая граждан тема – коронавирус[7]. Аналитический центр InfoWatch в отчете приводит статистику, которая свидетельствует о том, что в настоящее время в России в четыре раза увеличилась рассылка фишинговых сайтов[8]. В результате таких атакв руки злоумышленников попадали логины и пароли пользователей, перешедших по ссылке или открывших вирусное вложение. В результате этого в свободном пользовании киберпреступников оказались большие объемы данных с личной информацией людей, используемой для вымогательства.

Как замечает заместитель председателя правления Сбербанка России Станислав Кузнецов, «коронавирус стал темой номер один не только для мировых СМИ, но и для мошенников, которые используют сложившуюся ситуацию в своих целях; вирус затронул многие страны и вызвал всплеск киберпреступности»[9]. Согласно данным службы безопасности Сбербанка России с начала пандемии мошенники зарегистрировали более 4 000 доменов со словами «коронавирус», «covid» и т. д. При этом количество фишинговых рассылок с каждым кварталом периода самоизоляции рос на 30 %[10].

Выше было упомянуто, что с ростом числа пользователей цифрового пространства, растет и уровень применяемых способов мошенничества, преступники при каждом выявленном методе придумывают новый, все менее очевидный и все более практичный[11]. Так, помимо фишинговых писем с отдельными сайтами, содержащих интересную для людей информацию, злоумышленники часто стали использовать способ «мимикрии» с заведомо не опасными вебстраницами. В 2021 году участились случаи маскировки вирусных сайтов под настоящие кредитные организации или даже государственные службы/органы с помощью полного копирования фирменного стиля организации и даже доменного имени, за исключением одной-двух букв. Соответственно, в ходе обмана и заблуждения жертвы вводят логины и пароли от своих реальных банковских или социальных аккаунтов. Например, в июле 2021 г. администрация сети RSNet (Russian State Network, сегмент интернета для российских органов власти) сообщила об использовании домена государственных органов gov.ru для рассылки фишинговых писем, а с 8 по 21 октября 2021 г. в Зоне.ru зарегистрировано было 48 доменных имен, имитирующих портал Госуслуг[12].

[4] Год красного локдауна — как COVID-19 повлиял на кибербезопасность URL: https://www.kaspersky.ru/blog/pandemic-year-in-infosec/30316/ (дата обращения: 15.03.2022).

[5] Станислав Кузнецов: коронавирус породил новые схемы мошенничества. URL: https://ria.ru/20200413/1569949717.html (дата обращения: 15.03.2022).

[6] Фишинг — это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальной информации пользователей — логинов и паролей. Получая письмо, пользователь нажимает на ссылку в сообщении и попадает на фишинговый сайт, где ему предлагают поделиться личной информацией.

[7] Кропачев С.Ю. Актуальные вопросы противодействия мошенническим действиям в экономической и предпринимательской сфере в связи с распространением коронавирусной инфекции // Евразийское научное объединение. 2020. № 4–3 (62). С. 196-200.

[8] COVID-19: утечки периода пандемии. URL: https://www.infowatch.ru/analytics/reports/28595 (дата обращения: 15.03.2022).

[9] Станислав Кузнецов: коронавирус породил новые схемы мошенничества. URL: https://ria.ru/20200413/1569949717.html (дата обращения: 15.03.2022).

[10] Станислав Кузнецов: коронавирус породил новые схемы мошенничества. URL: https://ria.ru/20200413/1569949717.html (дата обращения: 15.03.2022).

[11] КиберпреступностьCOVID-19: рискиответныемеры // United Nations Officeon Drugsand Crime, 2020. URL: https://мвд.рф/upload/site151/doc/UPN_OON._Doklad_Prestupnost_i_Covid.pdf (дата обращения: 15.03.2022).

[12] Киберпреступность и киберконфликты: Россия. URL: https://www.tadviser.ru/index.php/ (дата обращения: 14.11.2021).

Ввиду роста IT-преступности органы МВД расширяют свои технические возможности, увеличивают штат специализированных сотрудников, но существуют обстоятельства, препятствующие более быстрому расследованию подобных преступлений.

Одним из таких препятствий является отсутствие налаженного контакта и низкая скорость обработки и обмена информацией между правоохранительными органами и банковскими учреждениями, операторами сотовой связи, интернет-провайдерами. По словам заместителя министра внутренних дел РФ начальника Следственного департамента МВД РФ генерал-лейтенанта юстиции Сергея Лебедева, «максимальная скорость обмена информацией сегодня могла бы существенно повлиять на эффективность расследования таких преступлений и своевременное установление личности преступников»[13].

Помимо этого, ввиду того что члены одной организованной преступной группы могут находиться на разных континентах или использовать различные способы маскировки своего места нахождения, а также свободно перемещаться, так как они «не привязаны» к месту преступления, требуется максимальная и быстрая международная интеграция правоохранительных органов. Однако, несмотря на положительные шаги в этом направлении, инициированные Россией в рамках 74-й сессии ООН по разработке всеобъемлющей международной конвенции о противодействии использования ИКТ в преступных целях[14], в реалиях 2022 года необходимо полагаться на самостоятельные силы и делать большой акцент именно на превентивных мерах. Выявление трансграничного характера преступления в настоящий момент, к сожалению, исключает возможность восстановления нарушенных прав граждан.

Таким образом, начавшаяся в 2020 году пандемия послужила сильным толчком к развитию преступлений в сфере компьютерной информации, что требует быстрого и мобильного реагирования правоохранительных органов. С этой целью было принято решение руководства МВД России о создании по отраслевому принципу в пределах имеющейся штатной численности подразделений, которые будут специализироваться на киберпреступности[15]. Также, хоть для многих это уже банально звучит, но повышение осведомленности, как во время всемирной пандемии, так и в любое другое время, является одной из главной задач государства в процессе устранения угроз и расширения возможностей предотвращения киберпреступлений, преимущественно совершаемых в отношении самых легкоуязвимых групп населения – детей и пожилых людей. Знание основных правил пользования сетью «Интернет» и своевременное оповещение граждан из официальных источников – главные способы защиты личной информации и электронных денежных средств.

Библиографический список

1. Касторский Г.Л. Киберпреступность в период пандемии коронавируса COVID-19 / Г.Л. Касторский, А.Г. Форкош. // Молодой ученый. – 2020. – № 52 (342). – С. 196-198.

2. Кропачев С.Ю. Актуальные вопросы противодействия мошенническим действиям в экономической и предпринимательской сфере в связи с распространением коронавирусной инфекции // Евразийское научное объединение. – 2020. – № 4-3 (62). – С. 196-200.

Рецензент: Плотников А.И., заведующий кафедрой уголовного права и криминологии Оренбургского института (филиала) Университета имени О.Е. Кутафина (МГЮА), д.ю.н., доцент.

[13] Сергей Лебедев: в виртуальном мире не выстроены барьеры для преступников. URL: https://ria.ru/20210820/kibermoshennichestvo1746425415.html/ (дата обращения: 14.11.2021).

[14] Противодействие использованию информационно-коммуникационных технологий в преступных целях // United Nations Officeon Drugsand Crime, 2019. URL: https://www.unodc.org/documents/Cybercrime/SG_report/ V1908184_R.pdf (дата обращения: 15.03.2022).

[15] Петров И. В структуре МВД России создается киберполиция. URL: https://rg.ru/2020/12/18/v-strukture-mvd-sozdaetsia-kiberpoliciia.html (дата обращения: 15.03.2022).