УДК 343.9
DOI: https://doi.org/10.17308/law/1995-5502/2025/2/197-202

НАМЕТИВШИЕСЯ ТЕНДЕНЦИИ В РАЗВИТИИ КИБЕРПРЕСТУПНОСТИ

В. А. Шестак
Московская академия Следственного комитета Российской Федерации

А. С. Чеботарь
Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации

EMERGING TRENDS IN CYBERCRIME DEVELOPMENT

V. A. Shestak
Moscow Academy of the Investigative Committee of theф Russian Federation

A. S. Chebotar
Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation

Аннотация: выявлены основные факторы, оказавшие непосредственное влияние на неконтролируемый рост совершаемых преступлений в современном киберпространстве; установлена причинно-следственная связь между общемировыми событиями и неконтролируемым ростом киберпреступности в период с 2020 г. по настоящее время; проведен скрупулезный анализ статистических данных, представленных компетентными органами иностранных государств и международных организаций, относительно роста совершаемых киберпреступлений в течение последних трех лет; изучена структура исследуемого явления; раскрыты основные характеристики, присущие такому негативному явлению современности, как киберпреступность.
Ключевые слова: киберпреступления, пандемия COVID-19, несовершеннолетние, deepfake, вредоносное программное обеспечение, DDoS-атаки.

Abstract: the main factors that have had a direct impact on the uncontrolled growth of crimes committed in modern cyberspace have been identified; a causal relationship has been established between global events and the uncontrolled growth of cybercrime from 2020 to the present; a meticulous analysis of statistical data provided by competent authorities of foreign states and international organizations was conducted regarding the growth of cybercrimes committed over the past three years; the structure of the phenomenon under study was studied; the main characteristics inherent in such a negative modern phenomenon as cybercrime are revealed.
Key words: cybercrime, COVID-19 pandemic, minor, deepfake, disruptive malware, DDoS-attacks.

Ускоренная цифровизация, вызванная распространением новой коронавирусной инфекции «COVID-19» и введением жестких ограничительных мер большинством стран, в значительной степени повлияла на возникновение новых киберугроз и создание еще более изощренных методов совершения уже существующих. Так, значительный рост числа так называемых онлайн-покупок привлек большое количество кибермошенников, а страх населения перед новым, практически не изученным заболеванием, поиск несуществующих лекарств и тест-систем в сети Интернет позволил злоумышленникам заполучить неправомерный доступ к банковским счетам своих жертв.

В период с 2020 по 2021 г. в Российской Федерации число интернет-пользователей увеличилось на 6 млн (т. е. на 5,1 %) и в январе 2021 г. достигло 124 млн. По данным проекта WEB-Index, проникновение Интернета в России среди населения в возрасте до 44 лет в 2020 г. составило 90 %, а среди молодежи в возрасте от 12 до 24 лет – 100 %. По данным «Лаборатории Касперского», российские дети проводят в виртуальном пространстве гораздо больше времени, чем эта же группа населения во многих странах Европы и в США.

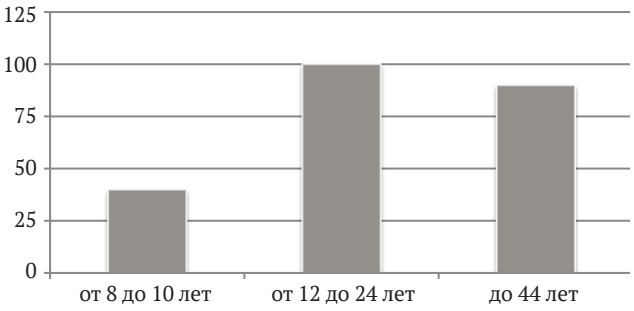

Рис. 1. Проникновение Интернета в России среди возрастных групп населения

В исследовании «Лаборатории Касперского» «Растим детей в эпоху Интернета» приняли участие 3,78 тыс. семей с детьми в возрасте от 8 до 16 лет, 540 из которых – семьи из Российской Федерации[1]. Согласно опросу, 58 % российских несовершеннолетних скрывают от родителей свои действия и опасную активность в сети Интернет. Причем каждый третий несовершеннолетний принимает определенные меры: 18 % респондентов выходят в сеть в отсутствие родителей дома, 16 % – устанавливают код-пароль на устройстве, 10 % – удаляют историю поиска и посещения сайтов в браузере; 14 % несовершеннолетних в возрасте от 14 до 16 лет используют специальные программы, скрывающие используемые ими приложения[2].

Рис. 2. Способы сокрытия активности в сети Интернет, предпринимаемые несовершеннолетними

Подобное бесконтрольное использование сети Интернет несовершеннолетними стало причиной взрывного роста распространения порнографических фото- и видеоматериалов с участием несовершеннолетних в виртуальном пространстве. Согласно отчету, предоставленному Национальным бюро регистрации преступлений (National Crimes Record Bureau), в 2020 г. было зафиксировано более чем 400%-ное увеличение количества киберпреступлений против несовершеннолетних по сравнению с показателями 2019 г.[3].

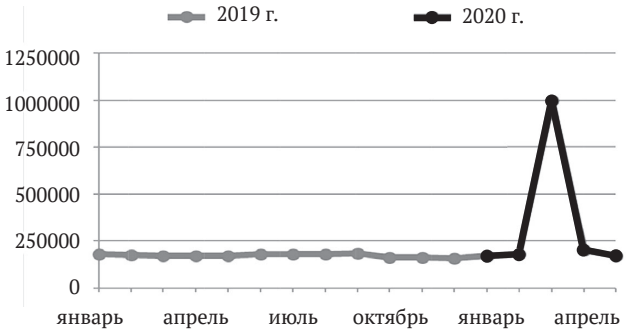

Рис. 3. Общее количество обращений, поданных в Европол Национальным центром по делам пропавших без вести и эксплуатируемых детей за 2019–2020 гг.

По данным Европол (Europol) и Национального центра по делам пропавших без вести и эксплуатируемых детей (National Center for Missing and Exploited Children), показатель объ-

[1] АО «Лаборатория Касперского» : сайт. URL: https://www.kaspersky.ru/about/press-releases/2016_news-12-05-16 (дата обращения: 13.01.2024).

[2] МИА «Россия сегодня» : сайт. URL: https://ria.ru/20160421/1416663245.html (дата обращения: 08.01.2024).

[3] The Economic Times : сайт. New Delhi. URL: https://economictimes.indiatimes.com/news/india/over-400-rise-in-cyber-crime-cases-committed-against-children-in-2020-ncrb-data/articleshow/87696995.cms (дата обращения: 09.01.2024).

ема распространения материалов сексуального насилия над детьми в киберпространстве начал стремительно расти с начала марта 2020 г. Примерно в это же время первые государства – члены Европейского союза ввели соответствующие ограничительные меры, направленные на борьбу с новой коронавирусной инфекцией[4].

Противодействие распространению запрещенного контента с участием несовершеннолетних осложняется тем, что большинство материалов, содержащих сцены сексуальной эксплуатации и надругательства над детьми, продаются на специально созданных форумах, сайтах и иных интернет-площадках, доступ к которым ограничен и предоставляется модераторами только после совершения злоумышленниками определенных противоправных деяний. Так, преступники, желающие заполучить доступ к запрещенному контенту, размещенному на такой запрещенной интернет-площадке, как «Dreamboard», должны самостоятельно загрузить «оригинальные» фото- и видеоматериалы, содержащие надругательство над детьми в возрасте до 12 лет[5].

Распространение в сети Интернет материалов, содержащих сексуальное насилие над несовершеннолетними, является далеко не единственным киберпреступлением, получившим наибольшую популярность с начала пандемии. Киберзлоумышленниками были созданы различные схемы торговли и сексуальной эксплуатации несовершеннолетних «online» (как активной, так и пассивной), посредством использования таких общедоступных приложений, оснащенных функциями видеочата, как, например, Skype. Важно отметить, что, по данным Европол (Europol), способ оплаты за доступ и просмотр запрещенного контента в прямом эфире является вполне легальным: злоумышленники осуществляют онлайн-переводы денежных средств через онлайн-банки.

По данным Верховного Суда Российской Федерации, в 2020 г. было осуждено около 200 человек за незаконное изготовление и оборот порнографических материалов среди несовершеннолетних (ч. 2 и 3 ст. 242 УК РФ), в том числе через различные сайты и онлайн-платформы; в отношении 12 злоумышленников были вынесены обвинительные приговоры за использование подростков в целях изготовления порнографии при помощи сети Интернет[6].

За 2021 г. Роскомнадзором было закрыто около 500 тыс. групп, содержащих запрещенный контент, 23 тыс. из которых были связаны с распространением детской порнографии. В 2022 г. было зарегистрировано 16 887 преступлений против половой неприкосновенности несовершеннолетних, для сравнения, в 2015 г. данный показатель составлял 12 175[7]. Кроме того, за последние пять лет отмечается увеличение числа преступлений, связанных с оборотом детской порнографии на 2,7 %.

Несовершеннолетние продолжают оставаться наиболее уязвимой группой населения для киберзлоумышленников с 2020 г., но далеко не единственной. В связи с введенными ограничительными мерами организации и предприятия были вынуждены внедрять различные системы и специальное программное обеспечение для дальнейшего осуществления своей деятельности, поскольку большинство руководителей и сотрудников было переведено на удаленный режим работы.

На основании всестороннего анализа данных и сведений, полученных от стран – членов Интерпол (Interpol), следующие киберпреступления были названы в качестве основных угроз.

Во-первых, пандемия COVID-19 предоставила злоумышленникам реальную возможность для пересмотра и обновления устаревших схем онлайн-мошенничества и фишинга, утративших былую эффективность. Так, киберзлоумышленники осуществляли рассылку фишинговых электронных писем на тему новой коронавирусной инфекции, часто выдавая себя за государственные органы и органы здравоохранения. Данный способ оказался действенным, поскольку жертвы киберзлоумышленников добровольно загружа-

[4] Europol. EXPLOITING ISOLATION : Offenders and victims of online child sexual abuse during the COVID-19 pandemic. URL: file:///C:/Users/user/Downloads/europol_covid_report-cse_jun2020v.3_0.pdf (дата обращения: 11.01.2024).

[5] См *Sanjeev K.* Crime against children in cyber world // Journal on contemporary issues of law. 2021. Vol. 5, Issue 9. P. 29.

[6] Судебный департамент при Верховном Суде Российской Федерации : официальный сайт. URL: http://www.cdep.ru/index.php?id=79 (дата обращения: 12.01.2024).

[7] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций : официальный сайт. URL: https://rkn.gov.ru/news/rsoc/news74048.htm?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 12.01.2024).

ли вредоносный контент и предоставляли свои персональные данные.

Во-вторых, киберзлоумышленники всё чаще прибегали к использованию различных вредоносных программ с целью извлечения финансовой выгоды, посредством воспрепятствования деятельности критически важных объектов инфраструктуры и медицинских учреждений и последующего вымогательства. Использование таких программ-вымогателей и DDoS-атак приводило к регулярным сбоям, а в некоторых случаях и к полному приостановлению деятельности учреждений и органов, которые стали объектом противоправной деятельности киберзлоумышленников, некоторым из них до сих пор не удается восстановить доступ к сведениям, представляющим особую важность.

В-третьих, в целях практической реализации преступных намерений, киберпреступниками активно использовались такие троянские вирусы, как: Remote Access Trojan, или RAT[8], info stealers, spyware, banking Trojans[9]. Посредством использования информации, связанной с COVID-19, киберпреступникам удавалось проникать в различные информационные системы с целью последующей кражи данных, денежных средств, а также компрометации и дискредитации сети.

С начала пандемии был зарегистрирован существенный рост доменов с ключевыми словами «COVID» и «Corona»: по состоянию на конец марта 2020 г. было зафиксировано более 116 тыс. доменов, 2022 из которых были признаны вредоносными, а 40 261 – «представляющими высокий риск». Недавно зарегистрированные домены содержали вредоносное программное обеспечение для сбора личной информации пользователя. С февраля по март 2020 г. Palo Alto Networks обнаружил 569%-ный рост регистрации вредоносных доменов, персонального обеспечения и фишинга[10]. Беспрецедентный рост регистраций доменов последовал за особым интересом пользователей к темам, связанным с новой коронавирусной инфекцией, по данным «Google Trends». Кроме того, в данный период времени были созданы вредоносные веб-сайты, имитирующие оригинальные порталы государственных служб, банков, национальных налоговых и таможенных органов и т. д.

Еще одной областью злоупотребления являлось создание мошеннических веб-сайтов компаний, осуществляющих продажу средств индивидуальной защиты, тестовых систем и аппаратов искусственной вентиляции легких. На поддельных веб-сайтах киберзлоумышленниками осуществлялась продажа контрафактных товаров или же получение оплаты за совершение онлайн-покупок без последующей доставки. В большинстве таких случаев денежные средства направлялись на зарубежные банковские счета, что не только осложняло установление виновного лица, но и последующее возмещение финансовых потерь.

В последнее время в значительной степени возросла роль социальных сетей в распространении так называемых «фейков». Данные платформы являются наиболее простыми и доступными каналами для распространения ложных сведений; приоритет отдается не достоверности сведений, а процессу взаимного обмена информацией. Поток дезинформации[11] в сети Интернет формируется не только обычными пользователями, а специально созданными для этих целей «ботами». В 2020 г. был зафиксирован взрывной рост распространения так называемых фейков и дезинформации, касающейся профилактики и лечения COVID-19, использования неэффективных и потенциально вредоносных мер профилактики. Подобное распространение заведомо ложных сведений в виртуальном пространстве представляет огромную угрозу для общественного здравоохранения.

В целях оказания должного противодействия распространению фейков Всемирная организация здравоохранения и государственные учреждения заинтересованных стран отслеживают и разъясняют недостоверные утверждения о способах лечения и профилактики новой коронавирусной инфекции. Кроме того, дезинформация,

[8] Remote Access Trojan представляет собой вирус, используемый разработчиками вредоносных программ для получения удаленного доступа к системе пользователя, включая возможность управления его «мышью» и клавиатурой, доступ к файлам и сетевым ресурсам.

[9] Interpol. COVID-19 Cybercrime Analysis Report – August 2020. URL: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (дата обращения: 18.01.2024).

[10] Palo Alto Networks, Inc. : сайт. – California. URL: https://catching-transparent-phish.github.io/catching_transparent_phish.pdf (дата обращения: 22.01.2024).

[11] Под дезинформацией следует понимать объективно неверную или ложную информацию, которая не подкреплена соответствующими доказательствами или экспертным мнением.

распространяемая в сети Интернет, оказала негативное влияние на темпы вакцинации в мире, что привело к появлению новых более патогенных штаммов COVID-19 и взрывному росту заболеваемости и смертности, а также неподъемной нагрузке на систему здравоохранения.

Факт распространения ложной информации, связанной с COVID-19, подтвердили 27 % стран, участвовавших в Глобальном исследовании киберпреступности (Global Cybercrime Survey); 21 % стран-респондентов выразили растущую озабоченность в связи с данной негативной тенденцией[12]. В основном вредоносная информация распространялась через такие социальные сети и мессенджеры, как WhatsApp*, Facebook*, Twitter* и иные. Некоторые страны – члены Интерпола (Interpol) выразили обеспокоенность по поводу нарастающей паники в обществе и социальных беспорядков, вызванных распространением ложных сведений о новой коронавирусной инфекции.

В настоящее время киберпреступники продолжают злонамеренно использовать последствия пандемии новой коронавирусной инфекции, но и не прекращают поиск новых уязвимостей для реализации своего преступного умысла, в том числе и на политической арене. Термин «deepfake», объединяющий в себе два понятия, а именно глубокое обучение «deep learning», т. е. обучение нейросетей, и подделку «fake», появилось в обиходе современных пользователей несколько лет назад. Прежде технология создания deepfake была известна и доступна лишь экспертам в области искусственного интеллекта, однако новейшие программы и приложения в значительной степени упростили процесс создания фальшивых видео- и аудиоматериалов для обывателей.

В настоящее время deepfake[13] признается одним из самых опасных способов применения искусственного интеллекта, поскольку конечный результат поддельного видео- или аудиоматериала может нанести непоправимый ущерб репутации отдельного человека или подтолкнуть пользователя, осуществляющего просмотр данного контента, к совершению противоправных деяний. Анализируемая авторами технология способна оказывать влияние на политику, а в будущем и вовсе может превратиться в одну из главных угроз национальной безопасности. Deepfake, первоначально созданная в развлекательных целях программа, была превращена киберзлоумышленниками в идеальный инструмент практической реализации преступного умысла.

В 2019 г. жительница Калифорнии лишилась 300 000 долл., став жертвой злонамеренного использования технологии deepfake. Через сайт онлайн-знакомств она познакомилась с мужчиной, который выдавал себя за вице-адмирала Военно-морской академии США Шона Бака. Женщина несколько раз общалась с мошенником в видеочате, не подозревая, что лишь просматривает отредактированные фрагменты общедоступных видеозаписей, принадлежащих реальному вице-адмиралу. Преступник убедил свою жертву перевести ему денежные средства для того, чтобы освободить его из «плена».

Количество поддельного контента в сети Интернет продолжает неуклонно возрастать. Так, согласно отчету Deeptrace, в начале 2019 г. насчитывалось более 7964 фальшивых видеороликов, тогда как девять месяцев спустя данный показатель достиг 14 678. По оценкам экспертов, ущерб от использования deepfake в мошеннических целях в 2020 г. превысил 250 млн долл.[14]

По данным экспертного центра кибербезопасности Positive Technologies, в 2024 г. ожидается рост числа киберинцидентов на 20 %. Данная негативная тенденция обусловлена низкой раскрываемостью преступлений, совершаемых в виртуальном пространстве, слабыми техническими возможностями обработки поступающей информации, установления личности и обнаружения киберзлоумышленников. Кроме того, киберзлоумышленники всё чаще прибегают к использованию нейросетевых технологий, облегчающих противоправное воздействие даже на защищенные объекты.

По результатам анализа статистики компетентных органов, авторы полагают возможным выделить основные внешние факторы, оказав-

[12] *Varga G.* Global Cybercrime Report : Which Countries Are Most At Risk? URL: https://seon.io/resources/global-cybercrime-report/ (дата обращения: 19.01.2024).

[13] «Deepfake» – это фотография, видео- или аудиозапись, которые, на первый взгляд, кажутся реальными, но были созданы или обработаны при помощи искусственного интеллекта. Лежащая в основе deepfake-технология может заменять лица, манипулировать их выражением и даже синтезировать речь.

[14] Inc. Russia : сайт. – Москва. URL: https://incrussia.ru/understand/deepfake-brandmonitor/ (дата обращения: 16.01.2024).

шие влияние на темпы и особенности развития современной киберпреступности. Так, в период с 2020 г. по настоящее время таким фактором стали ограничительные меры, введенные в связи с распространением новой коронавирусной инфекции, а наиболее уязвимой группой населения для посягательств со стороны киберзлоумышленников стали несовершеннолетние. Так, дети стали проводить гораздо больше времени в виртуальном пространстве, пренебрегая правилами безопасного поведения в сети Интернет и оставшись без соответствующего контроля родителей.

Кроме того, частота использования программ-вымогателей продолжает расти в геометрической прогрессии, преимущественно из-за значительно возросшей в период пандемии онлайн-активности пользователей и стремительного расширения цифровой среды. До сих пор большинство фальшивых фотоизображений и видеозаписей создавались и использовались в развлекательных целях, однако ничто не мешает киберзлоумышленникам использовать данную технологию для получения доступа к биометрической системе контроля и управления доступом за счет фальсификации основных черт лица и голоса жертвы. Помимо мошенничества и кражи денежных средств киберпреступники способны создавать фальшивые видеоролики, сюжет которых может нанести существенный вред репутации невиновных лиц, невольно ставших их участниками. Ожидается, что уже к 2025 г. ущерб от киберпреступности составит более 12 трлн долларов.

Библиографический список

Sanjeev K. Crime against children in cyber world // Journal on contemporary issues of law. 2021. Vol. 5, Issue 9. P. 28–36.

Varga G. Global Cybercrime Report : Which Countries Are Most At Risk? URL: https://seon.io/resources/global-cybercrime-report/

References

Sanjeev K. Crime against children in cyber world // Journal on contemporary issues of law. 2021. Vol. 5, Issue 9. P. 28–36.

Varga G. Global Cybercrime Report : Which Countries Are Most At Risk? URL: https://seon.io/resources/global-cybercrime-report/

Московская академия Следственного комитета Российской Федерации

Шестак В. А., доктор юридических наук, доцент, профессор кафедры криминалистики

E-mail: viktor_shestak@mail.ru

Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации

Чеботарь А. С., магистр права, аспирант кафедры уголовного права, уголовного процесса и криминалистики

E-mail: chebotar.a.s@mail.ru

Поступила в редакцию: 03.02.2024

Для цитирования:

Шестак В. А., Чеботарь А. С. Наметившиеся тенденции в развитии киберпреступности // Вестник Воронежского государственного университета. Серия: Право. 2025. № 2 (61). С. 197–202. DOI: https://doi.org/10.17308/law/1995-5502/2025/2/197-202

Moscow Academy of the Investigative Committee of the Russian Federation

Shestak V. A., Doctor of Legal Sciences, Associate Professor, Professor of the Department of Criminalistics

E-mail: viktor_shestak@mail.ru

Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation

Chebotar A. S., Master of Law, Post-graduate Student of the Department of Criminal Law, Criminal Procedure and Criminalistics

E-mail: chebotar.a.s@mail.ru

Received: 03.02.2024

For citation:

Shestak V. A., Chebotar A. S. Emerging trends in cybercrime development // Proceedings of Voronezh State University. Series: Law. 2025. No 2 (61). P. 197–202. DOI: https://doi.org/10.17308/law/1995-5502/2025/2/197-202