Научная статья
УДК 343.9
DOI: 10.37973/KUI.2023.83.81.017

НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: МОНИТОРИНГ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ

Лейсан Рафиковна Назмеева,
Казанский юридический институт МВД России, Казань, Россия,
nazmeevalr@mail.ru

Аннотация

Введение: статья посвящена анализу динамики и тенденциям неправомерного доступа к компьютерной информации как одного из видов преступлений, обладающих повышенной степенью общественной опасности, связанных с посягательством на сведения (данные), представленные в цифровой форме.

Материалы и методы: методологическую основу исследования составили сравнительно-правовой, хронологический, статистический и другие методы. Материалами исследования послужили статистические данные Главного информационно-аналитического центра МВД России, Экспертно-аналитического центра InfoWatch, а также научные труды по проблематике исследования.

Результаты исследования: в статье проанализирована динамика роста неправомерного доступа к компьютерной информации. Особое внимание уделено исследованию причинного комплекса и основных способов совершения преступлений в сфере обращения информации, представленной в цифровой форме.

Обсуждение и заключение: автором сформулированы основные направления минимизации неправомерного доступа к компьютерной информации.

Ключевые слова: неправомерный доступ; компьютерная информация; способ преступления; статистика преступлений; хищение информации

Для цитирования: Назмеева Л.Р. Неправомерный доступ к компьютерной информации: мониторинг и основные направления противодействия // Вестник Казанского юридического института МВД России. 2023. Т. 14. № 4 (54). С. 132 – 137. DOI: 10.37973/KUI.2023.83.81.017

Scientific article
UDC 343.9
DOI: 10.37973/KUI.2023.83.81.017

ILLEGAL ACCESS TO COMPUTER INFORMATION: MONITORING AND MAIN DIRECTIONS OF COUNTERACTION

Leysan Rafikovna Nazmeeva,
the Kazan Law Institute of MIA of Russia, Kazan', Russia,
nazmeevalr@mail.ru

Abstract

Introduction: the article presents the analysis of dynamics and trends of illegal access to computer information as one of the types of socially dangerous crimes related to infringement of information (data) provided in digital form.

Materials and Methods: the methodological basis of the study was comparative-legal, chronological, statistical and other methods. The research materials were statistical data of the Main Information and Analytical Centre of the Ministry of Internal Affairs of Russia, InfoWatch Expert Analytical Centre, as well as scientific works on the research issues.

Results: the article analyses the dynamics of the growth of illegal access to computer information. Special attention is paid to the study of the causal complex and the main ways of committing crimes in the sphere of circulation of information presented in digital form.

Discussion and Conclusions: the author has formulated the main directions for minimising illegal access to computer information.

Keywords: illegal access, computer information, method of crime, crime statistics, information theft

For citation: Nazmeeva L.R. Illegal Access to Computer Information: Monitoring and Main Directions of Counteraction. Bulletin of the Kazan Law Institute of MIA of Russia. 2023;14(4):132 – 137. (In Russ.). DOI: 10.37973/KUI.2023.83.81.017

Введение

В последние десятилетия XX века активное развитие информационно-коммуникационных технологий оказывает воздействие на общественные, экономические институты, формируя новые подходы к регулированию отношений, связанных с оборотом информации. Интеграция информации в единое мировое информационное пространство способствует увеличению ее значимости, возможности оперирования в компьютерных сетях, персональных компьютерах, смартфонах и периферийных устройствах и наступлению эпохи передачи компьютерной информации (*сведений, (сообщений, данных), находящихся в электронно-цифровой форме, зафиксированные на материальном носителе либо передающиеся по каналам связи посредством электромагнитных сигналов[1]*) на различные расстояния.

В условиях действенных процессов всеобщей информатизации прослеживается тенденция формирования криминальных угроз, проявляющаяся в увеличении количества преступлений, затрагивающих сферу обращения компьютерной информации.

Обзор литературы

Стремительное использование информационных технологий и различных технологических процессов во всех отраслях деятельности сопровождается, с одной стороны, возрастанием роли информационных активов и технологий, с другой – неизбежностью криминализации современных способов получения и использования информации. Актуальные аспекты противодействия неправомерному доступу к компьютерной информации рассматривались в научных трудах А.А. Харламовой, И.В. Бессоновой, Е.В. Затуливетрова, М.В. Савельевой, А.В. Бачиевой и др.

Результаты исследования

Сформировавшееся единое мировое информационное пространство обусловливает становление информации наиболее значимым стратегическим ресурсом, создающим безграничные возможности для научно-технического прогресса, детерминируя развитие более совершенных способов информационной коммуникации. На фоне всеобщей тенденции развития и повсеместного внедрения информационных технологий прослеживается динамика роста неправомерного доступа к компьютерной информации *(статьей 272 Уголовного кодекса Российской Федерации предусматривается уголовная ответственность за неправомерный доступ к компьютерной информации [2, с. 163]).*

Согласно статистическим данным Главного информационно-аналитического центра Министерства внутренних дел Российской Федерации, в 2022 году количество фактов неправомерного доступа к компьютерной информации составило 9308 ед., что на 45,6% больше аналогичного периода 2021 года (в 2021 г. – 6392 ед. (+55,7%), 2020 г. – 4105 ед. (+69,63%)[1].

Высокий уровень криминализации рассматриваемого вида деяний проявляется в электронной коммерции и сфере оказания услуг[2], обусловленный переходом на дистанционный режим осуществления деятельности с применением высокотехнологичных способов совершения безналичных расчетов и платежей. В результате вынужденного перехода на дистанционный формат увеличилось количество пользователей сети Интернет, не имеющих соответствующих знаний в области информационной безопасности, повысилась загруженность использования услуг провай-

[1] Состояние преступности в России // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/folder/101762/ (дата обращения: 14.04.2023).

[2] Объем утечек информации в РФ увеличился более чем в 2 раза. URL: https://www.itsec.ru/news/obiom-utechek-informazii-v-rf-uvelechilsia-bolee-chem-v-2-raza (дата обращения: 25.05.2023).

деров связи, что способствовало росту уязвимости всей сети [3, с. 63] и прогрессивной динамике развития угроз в информационной сфере.

Значительный разрыв между информационным развитием и информационной безопасностью, низкая осведомленность пользователей информационных ресурсов и программно-аппаратных средств о цифровых возможностях совершения преступлений создают предпосылки для массового распространения информации ограниченного доступа и нарушения защиты цифровых данных пользователей. По данным российского экспертно-аналитического центра InfoWatch, в 2022 году в мире зарегистрировано 6856 ед. хищений информации ограниченного доступа, что почти в три с половиной раза больше, чем за аналогичный период прошлого года (в 2021 – 1920 ед.), из них в России – 710 ед., что на 47% больше за аналогичный период предыдущего года[1]. Например, в первой половине 2022 года опубликованы сведения об утечках информации из российских компаний: авиакомпании «Победа», интернированного провайдера цифровых услуг «Ростелеком», мирового поставщика связи (телекоммуникационной компании) «ВымпелКом», информационно-развлекательного портала Ykt.ru, медиаплатформы «Мир тесен», социально-развлекательной сети Fotostrana.ru, сервисов «Яндекс.Еда», Delivery Club, информационно-развлекательного ресурса Pikabu, Московской школы управления «Сколково»[2].

На фоне повышения ценности информации, находящейся в ограниченном доступе, в условиях повсеместной цифровизации и снижения уровня ее защищённости количество хищений персональных данных в 2022 году составило 36% (в организациях) и 28% (у частных лиц), учетных данных у частных лиц – 41%, коммерческой информации – 17% (в организациях), государственной тайны – 1,4%, платежной информации – 4% (в организациях)[3]. Впервые среди лиц, осуществляющих хищение вышеуказанной информации, превалируют внешние нарушители (хакеры и неизвестные лица) по сравнению с аналогичными периодом прошлого года, где основными нарушителями выступали сотрудники организаций[4]. Согласно исследованиям уровня обеспечения информационной защищенности организаций, входящих в государственную, промышленную и финансовую отрасли[5], в большинстве случаев (в 74% протестированных организаций) скомпрометированы доменные учтенные данные сотрудников от действий внешнего нарушителя и получен несанкционированный доступ к конфиденциальной информации (в 90% протестированных организаций). Одним из основных факторов, способствующих данному процессу, выступает освоение и применение программно-аппаратных комплексов, обладающих современными высокотехнологическими свойствами и структурой используемых информационных технологий и технических средств, которые позволяют выбирать специфический алгоритм противоправных действий для осуществления хищения информации.

Анализ статистических данных[6] за период с 2020 по 2022 годы о количестве зарегистрированных преступлений за неправомерный доступ к компьютерной информации и лицах, привлеченных к уголовной ответственности за вышеуказанные общественно опасные деяния[7], свидетельствует о латентности рассматриваемых преступлений и тенденции роста количества неправомерного доступа к компьютерной информации, приобретающих профессионально-усложненный характер и предполагающих обладание теоретическими знаниями и практическими умениями в сфере информационных технологий, а также навыками при осуществлении технических манипуляций с помощью информационных устройств. Особенность данной категории преступлений проявлятся в механизме их совершения, обстановке и временном диапазоне реализации противоправных действий [4, с. 74].

В подавляющем большинстве случаев осуществление неправомерного доступа к компьютерной информации представляет собой двухзвенную и трехзвенную структуру, поскольку требуется тщательная подготовка к совершению

[1] Утечки информации ограниченного доступа в мире 2022 г. URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-mire-2022-g (дата обращения (30.05.2023).

[2] Исследование утечек информации ограниченного доступа в первой половине 2022. URL: https://www.infowatch.ru/sites/default/files/publication_file/issledovanie-utechek-informatsii-ogranichennogo-dostupa-v-i-polugodii-2022.pdf (30.07.2023).

[3] Актуальные киберугрозы: итоги 2022 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ cybersecurity- threatscape-2022/ (дата обращения: 29.07.2023).

[4] Там же.

[5] Итоги пентестов – 2022. URL: https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2021-2022/ (дата обращения: 29.07.2023).

[6] Состояние преступности в России // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/folder/101762/ (дата обращения: 14.04.2023).

[7] Данные судебной статистики. Судебный департамент при Верховном Суде Российской Федерации за 2020 – 2022 гг. URL: http://www.cdep.ru/index.php?id=79 (дата обращения:24.09.2023).

преступления, изучению объекта посягательства и уровня его безопасности, разрабатывается специальное программное обеспечение для неправомерного доступа и прилагается много усилий для сокрытия своей личности [5].

Стремительно развивающаяся архитектура виртуального пространства обусловливает трансформацию способов совершения рассматриваемых общественно опасных деяний, т.к. их содержание могут составлять самые разнообразные действия в зависимости от использования в своем арсенале технических решений и модифицированного программного обеспечения, преступных навыков и умений, интеллектуальности, направленные на возможность неправомерного доступа к информации [6].

По мнению специалистов, наиболее распространенными способами совершения неправомерного доступа к компьютерной информации являются: использование вредоносных программ, а также программ удаленного управления устройством, системной поломки и подборки пароля, посредством замаскированных интернет-страниц, внедрение определенных команд в программы набора [7, с. 329], программ для мобильных устройств, позволяющих перехватывать сетевой трафик, расшифровывать имена и пароли пользователей[1], нахождение слабых мест в системах защиты информации и файлов законного пользователя, использование услуг провайдера, не фиксирующего данные о своих пользователях [8], распространение программных средств анонимизации личности преступника, предоставление на безвозмездной основе профессиональных «хакерских» инструментов[2]. В 26% случаев неправомерного доступа к компьютерной информации, совершенных с применением интернет-технологий, применялись дистанционные методы, основанные на использовании средств доступа к компьютерам либо охраняемой законами информации [9].

В связи с этим актуализируется необходимость оперативного и качественного реагирования государства и общества на возрастающее негативное влияние неправомерного доступа к компьютерной информации на состояние информационной сферы путем обеспечения раскрываемости рассматриваемого общественно опасного деяния и принятия комплекса мер по минимизации их криминализации.

Обсуждение и заключение

Таким образом, на основании проведенного исследования представляется целесообразным рассмотреть основные аспекты нивелирования неправомерного доступа к компьютерной информации:

прогнозирование направлений развития преступной активности криминальных элементов в информационной сфере на основе статистических данных и материалов уголовных дел. Реализация данного направления прослеживается в аналитической деятельности, заключающейся в сборе, накоплении, обобщении и комплексном анализе поступающей информации о происходящих социально-экономических, политических, межгосударственных и иных процессах, влияющих на криминогенную обстановку.

постепенная интеграция практического опыта сотрудников органов внутренних дел, осуществляющих противодействие противоправному использованию информационно-коммуникационных технологий, и знаний специалистов ведущих IT-компаний в образовательный процесс с целью действенной подготовки квалифицированных специалистов, обладающих достаточными навыками и знаниями при организации раскрытия преступлений и способных осуществлять и участвовать в процессуальных действиях при расследовании неправомерного доступа к компьютерной информации;

разработка научно-обоснованных рекомендаций по организации и тактике проведения следственных действий, проведения качественного осмотра компьютерных и иных электронных устройств и безопасного извлечения необходимой информации, формирования доказательственной базы с последующим внедрением методики выявления и раскрытия неправомерного доступа к компьютерной информации, с учетом особенностей совершения рассматриваемого общественно опасного деяния;

активизация через средства массовой информации виктимологической профилактики институтов гражданского общества путем правового просвещения и проведения дополнительного обучения граждан и раскрытия методов неправомерного доступа к компьютерной информации.

реализация технических мер защиты информации путем модификации программного обеспечения на современных информационных системах и устройствах, выступающей ключевой задачей минимизации уязвимых мест в компьютерных системах и устройствах, которые направлены на воспрепятствование неправомерного доступа к компьютерной информации.

[1] Утечки информации ограниченного доступа в мире 2022 г.// https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-mire-2022-g (дата обращения 28.06.2023).

[2] Там же.

СПИСОК ИСТОЧНИКОВ

1. Кузьмин М.Д. Проблемы расследований преступлений, совершенных с использованием облачных хранилищ в сети Интернет // Полицейская деятельность. 2020. № 1. URL: https://nbpublish.com/library_read_article.php?id=32413 (дата обращения: 11.05.2023).
2. Харламова А.А. Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации // Вестник Уральского юридического института МВД России. 2020. № 2. С. 162 – 167.
3. Бессонова И.В., Авинов М.С. Влияние пандемии COVID-19 на преступления в сфере компьютерной информации // Труды Оренбургского института (филиала) Московской государственной юридической академии. 2022. № 2 (52). С. 62 – 65.
4. Затуливетров Е.В. Неправомерный доступ к компьютерной информации // За нами будущее: взгляд молодых ученых на инновационное развитие общества: сборник научных статей 3-й Всероссийской молодежной научной конференци, Курск, 3 июня 2022 года. Том 4. Курск: Юго-Западный государственный университет, 2022. С. 72 – 75.
5. Канубриков В.А., Османов М.М. Способ совершения преступления как составообразующий признак преступлений в сфере компьютерной информации // Образование и право. 2021. № 5. URL: https://cyberleninka.ru/article/n/sposob-sovershheniya-prestupleniya-kak-sostavoobrazuyuschiy-priznak-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 30.07.2023).
6. Савельева М.В. Неправомерный доступ к компьютерной информации: проблемы квалификации // Евразийское Научное Объединение. 2019. № 10-1 (56). С. 62 – 65.
7. Савельева А. А. О способах совершения неправомерного доступа к компьютерной информации // Молодой ученый. 2020. № 48 (338). С. 328 – 329.
8. Кононуха И.Д. Способы совершения неправомерного доступа к компьютерной информаци // Международная научно-практическая конференция «Преступность в СНГ: проблемы предупреждения и раскрытия преступлений»: сборник материалов, Воронеж, 23 мая 2019 года. Том Часть 1. Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2019. С. 204 – 206.
9. Бачиева А.В., Светличный Е.Г. Способы совершения неправомерного доступа к компьютерной информации // Актуальные проблемы юридической науки и практики: Гатчинские чтения-2018: сборник научных трудов по материалам Международной научно-практической конференции, Гатчина, 25 мая 2018 года. Том 1. Гатчина: Государственный институт экономики, финансов, права и технологий, 2018. С. 268 – 271.

REFERENCES

1. Kuz'min M.D. Problemy rassledovanij prestuplenij, sovershennyh s ispol'zovaniem oblachnyh hranilishch v seti Internet // Policejskaya deyatel'nost'. 2020. № 1. URL: https://nbpublish.com/library_read_article.php?id=32413 (data obrashcheniya: 11.05.2023).
2. Harlamova A.A. Nepravomernyj dostup k komp'yuternoj informacii: tolkovanie priznakov i nekotorye problemy kvalifikacii // Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii. 2020. № 2. S. 162 – 167.
3. Bessonova I.V., Avinov M.S. Vliyanie pandemii COVID-19 na prestupleniya v sfere komp'yuternoj informacii // Trudy Orenburgskogo instituta (filiala) Moskovskoj gosudarstvennoj yuridicheskoj akademii. 2022. № 2 (52). S. 62 – 65.
4. Zatulivetrov E.V. Nepravomernyj dostup k komp'yuternoj informacii // Za nami budushchee: vzglyad molodyh uchenyh na innovacionnoe razvitie obshchestva: sbornik nauchnyh statej 3-j Vserossijskoj molodezhnoj nauchnoj konferenci, Kursk, 3 iyunya 2022 goda. Tom 4. Kursk: YUgo-Zapadnyj gosudarstvennyj universitet, 2022. S. 72 – 75.
5. Kanubrikov V.A., Osmanov M.M. Sposob sovershheniya prestupleniya kak sostavoobrazuyushchij priznak prestuplenij v sfere komp'yuternoj informacii // Obrazovanie i pravo. 2021. № 5. URL: https://cyberleninka.ru/article/n/sposob-sovershheniya-prestupleniya-kak-sostavoobrazuyuschiy-priznak-prestupleniy-v-sfere-kompyuternoy-informatsii (data obrashcheniya: 30.07.2023).
6. Savel'eva M.V. Nepravomernyj dostup k komp'yuternoj informacii: problemy kvalifikacii // Evrazijskoe Nauchnoe Ob"edinenie. 2019. № 10-1 (56). S. 62 – 65.
7. Savel'eva A. A. O sposobah sovershheniya nepravomernogo dostupa k komp'yuternoj informacii // Molodoj uchenyj. 2020. № 48 (338). S. 328 – 329.

8. Kononuha I.D. Sposoby sovershenіya nepravomernogo dostupa k komp'yuternoj informaci // Mezhdunarodnaya nauchno-prakticheskaya konferenciya «Prestupnost' v SNG: problemy preduprezhdeniya i raskrytiya prestuplenij»: sbornik materialov, Voronezh, 23 maya 2019 goda. Tom CHast' 1. Voronezh: Voronezhskij institut Ministerstva vnutrennih del Rossijskoj Federacii, 2019. S. 204 – 206.
9. Bachieva A.V., Svetlichnyj E.G. Sposoby sovershenіya nepravomernogo dostupa k komp'yuternoj informacii // Aktual'nye problemy yuridicheskoj nauki i praktiki: Gatchinskie chteniya-2018: sbornik nauchnyh trudov po materialam Mezhdunarodnoj nauchno-prakticheskoj konferencii, Gatchina, 25 maya 2018 goda. Tom 1. Gatchina: Gosudarstvennyj institut ekonomiki, finansov, prava i tekhnologij, 2018. S. 268 – 271.

Информация об авторе:
Назмеева Лейсан Рафиковна, кандидат экономических наук, старший преподаватель кафедры экономики, финансового права и информационных технологий в деятельности органов внутренних дел Казанского юридического института МВД России, nazmeevalr@mail.ru
Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Nazmeeva Leysan R., senior lecturer of the department of economics, financial law and information technologies in the activities of internal affairs bodies of the Kazan Law Institute of MIA of Russia, candidate of economic sciences, nazmeevalr@mail.ru
The author has read and approved the final version of the manuscript.

Статья получена: 08.08.2023.
Статья принята к публикации: 20.12.2023.
Статья опубликована онлайн: 28.12.2023.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.