DOI 10.58351/2949-2041.2024.17.12.017

Романюк Олег Анатольевич, студент,
Южный федеральный университет, г. Ростов-на-Дону
Romanyuk Oleg Anatolyevich, Southern Federal University

НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ОПАСНОСТЬ И ПРОТИВОДЕЙСТВИЕ
UNAUTHORIZED ACCESS TO COMPUTER INFORMATION: DANGER AND COUNTERACTION

Аннотация: Статья посвящена анализу опасности и противодействия неправомерному доступу к компьютерной информации как одного из видов преступлений, связанных с посягательством на сведения (данные), представленные в цифровой форме. Внимание уделено исследованию причинного комплекса и основных способов совершения преступлений в сфере обращения информации, представленной в цифровой форме. Автором сформулированы основные направления минимизации неправомерного доступа к компьютерной информации.

Abstract: The article is devoted to the analysis of the danger and counteraction to unlawful access to computer information as one of the types of crimes related to encroachment on information (data) presented in digital form. Attention is paid to the study of the causal complex and the main ways of committing crimes in the field of information circulation presented in digital form. The author has formulated the main directions of minimizing unauthorized access to computer information.

Ключевые слова: неправомерный доступ; компьютерная информация; способ преступления; противодействия; информационная безопасность.

Keywords: unauthorized access; computer information; method of crime; counteraction; information security.

В настоящее время в нашей стране, как и во всём мире, сформировался переход к информационному обществу, информация в котором обладает намного большей ценностью, значимостью и важностью в отличии от предшествующего индустриального периода. В результате технического прогресса в сфере информационных технологий, как никогда ранее, актуализировались проблемы защиты информации от неправомерных посягательств. Кроме того, развитие таких технологий стало требовать соблюдение строгой конфиденциальности обращаемой в сети информации, а отсутствие своевременного реагирующего надлежащего правового регулирования в этой сфере привело к возникновению большого количества проблем, оказывающих отрицательное влияние на становление в ней цивилизованных отношений.

Во многих странах ущерб от преступлений в сфере информационных технологий создает нелегальные доходы, исчисляющиеся суммами, сопоставимыми с бюджетами крупных городов. Одним из преступлений в рамках этой сферы является несанкционированный доступ к компьютерной информации в противозаконных целях. При этом может использоваться чужое имя, изменение физических адресов технических устройств, остаточная информация, модификация информации и программного обеспечения, подключение записывающих устройств к каналам связи, маскировка под законного пользователя путем раскрытия его пароля (если нет средств аутентификации). При наличии незащищенных файлов несанкционированный доступ возможен и вследствие поломок. Такие преступления хотя и не всегда причиняют серьёзного материального ущерба потерпевшей стороне, тем не менее требуют к себе особого внимания.

В подавляющем большинстве случаев осуществление неправомерного доступа к компьютерной информации представляет собой двухзвенную и трехзвенную структуру, поскольку требуется тщательная подготовка к совершению преступления, изучению объекта посягательства и уровня его безопасности, разрабатывается специальное программное обеспечение для неправомерного доступа и прилагается много усилий для сокрытия своей личности [1].

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 [2, с. 329], программ для мобильных устройств, позволяющих перехватывать сетевой трафик, расшифровывать имена и пароли пользователей, нахождение слабых мест в системах защиты информации и файлов законного пользователя, использование услуг провайдера, не фиксирующего данные о своих пользователях [3], распространение программных средств, анонимизации личности преступника, предоставление на безвозмездной основе профессиональных «хакерских» инструментов. 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 [4].

На основании вышесказанного, для того, чтобы обезопасить себя от такого вида противоправных посягательств любому грамотному пользователю просто необходимо не терять бдительность при работе в современной сфере информационных технологий. Каждый пользователь должен понимать, что соблюдение несложных правил информационной безопасности позволит избежать в последствии не простых для законопослушного гражданина проблем.

Каждый пользователь должен понимать, что нельзя поддаваться соблазну легко решить ту или иную порой срочную задачу, переслав пароли, логины, паспортные данные, ПИН-коды и прочую подобную информацию в соцсетях, мессенджерах, чатах или по электронной почте. При пользовании информационными системами, а равно где бы то не было, настоятельно рекомендуется использовать сложные логины и пароли, длина которых должна быть не менее 8 символов, в числе которых обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы. Воспользовались чужим компьютером? После этого недостаточно просто закрыть страницу, на которую вы заходили. Не забывайте предварительно выходить из всех аккаунтов, соцсетей и мессенджеров на устройстве. В противном случае человек, который сядет за этот компьютер после вас, получит возможность войти в вашу учетную запись и сделать с ней всё, что ему заблагорассудится. Очень важно контролировать наличие антивирусной программы, актуальность обновлений, а при подключении к рабочему компьютеру внешних носителей информации проверять их содержимое с помощью средств антивирусной защиты. Установка приложений из других источников, так называемых ломаных или пиратских версий, может закончиться тем, что не только придется тщательно чистить компьютер или телефон от вирусов, но и как следствие предоставить возможность злоумышленнику получить к ним доступ. Всегда следует обращать внимание на то, что написано в адресной строке браузера и если сайт начинается с HTTPS – все в порядке, это безопасное соединение и здесь можно вводить конфиденциальную информацию. Если же адрес начинается с HTTP – это значит, что соединение не защищено. Также слева от HTTPS должен быть значок в виде замка. Для большей уверенности в безопасности соединения можно кликнуть на него и просмотреть информацию во всплывающем окне.

Что касается противодействия со стороны государства, то помимо прогнозирования, разработки научно-обоснованных рекомендаций, реализации технических мер защиты информации, крайне важна интеграция практического опыта сотрудников органов внутренних дел. Речь идёт о сотрудниках 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 [5].

Стремительное развитие сферы информационных технологий, затронувшее всё мировое сообщество и породившее неизбежный рост в этой сфере преступлений, в том числе связанных с рассмотренным в рамках данной статьи преступлением, в наше время не может не требовать к себе особого внимания и изучения. К сказанному следует добавить острую необходимость в наши дни в разностороннем развитии правоохранительной практики, нуждающейся в квалифицированных и научно-обоснованных рекомендациях, требующихся для современного расследования преступлений, связанных с неправомерным доступом к охраняемой законом информации.

Список литературы:

1. 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-soversheniya-prestupleniya-kak-sostavoobrazuyuschiy-priznak-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 20.12.2024).

2. Савельева А. А. О способах совершения неправомерного доступа к компьютерной информации // Молодой ученый. 2020. № 48 (338). С. 328 – 329.

3. Кононуха И.Д. Способы совершения неправомерного доступа к компьютерной информации // 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.

4. 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.

5. Назмеева Л. Р. Неправомерный доступ к компьютерной информации: мониторинг и основные направления противодействия // Вестник Казанского юридического института МВД России. 2023. №. 4. С. 132-132. DOI: https://doi.org/10.37973/KUI.2023.83.81.017 (дата обращения: 20.12.2024).