УДК 343

© Лидия Константиновна Еськова
старший преподаватель кафедры
уголовного права и криминологии
юридического факультета
ВЮИ ФСИН России
lidiy_1987@mail.ru

Yeskova Lidia K.
senior lecturer of Criminal Law
and Criminology Department
of VLI of the FPS of Russia

© Дарья Павловна Гусарова
курсант 45 группы 4 курса
юридического факультета
ВЮИ ФСИН России

Gusarova Darya Pavlovna
cadet of group 45, 4th year,
Faculty of Law
of VLI of the FPS of Russia

ВЗЛОМ АККАУНТА КАК ПРЕСТУПЛЕНИЕ ПРОТИВ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ПРОБЛЕМЫ СОВРЕМЕННОГО МИРА

Hacking an account as a crime against computer information: problems of the modern world

Аннотация. В данной статье рассматривается ряд проблем одной из самых распространенных форм преступлений в сфере компьютерной информации, а именно взлома аккаунтов в социальных сетях, в современном мире. В статье также рассматриваются вопросы разграничения данного состава преступления со смежными и новые способы взлома.

Abstract. This article examines a number of issues related to one of the most common forms of crime in the field of computer information, namely hacking accounts in social networks, in the modern world. The article also examines the issues of distinguishing this crime from related ones and new methods of hacking.

Ключевые слова: взлом, аккаунт, компьютерная информация, преступление, интернет.

Keywords: hacking, account, computer information, crime, internet.

В наше время, когда компьютеры и интернет стали неотъемлемой частью нашей повседневной жизни, взлом аккаунтов стал одной из самых распространенных форм преступлений в сфере компьютерной информации. Взломщики используют разнообразные методы и техники, чтобы получить доступ к чужим аккаунтам и украсть личную информацию или использовать ее в своих целях. Однако помимо непосредственного ущерба для отдельных пользователей взлом аккаунта является серьезным преступлением против компьютерной информации в целом. С каждым годом количество случаев взлома растет, а его последствия становятся все более опасными и разрушительными. Такие преступления создают огромные угрозы для

безопасности и конфиденциальности данных пользователей, а также подрывают доверие к системам хранения информации.

Данная тема является как никогда актуальной, так как в России участились случаи взлома популярных блогеров в Instagram (относится к компании Meta, которая признана экстремистской и запрещена на территории РФ). От имени знаменитостей мошенники обманывают доверчивых подписчиков, а служба безопасности соцсети требует деньги за возврат страниц. Об этом 24 октября 2023 года сообщили сразу несколько блогеров. Кибератаке подвергся аккаунт одной знаменитости в соцсетях. Девушка подозревает, что к этому причастны сотрудники соцсети. По ее словам, за возврат страницы после взлома у нее тоже требуют деньги.

Взлом аккаунта - это не только личная проблема каждого пользователя, но и глобальная угроза для компьютерной безопасности в целом, и поэтому требует серьезного внимания и действий со стороны всех заинтересованных сторон.

В современном мире, где цифровые технологии играют все более значимую роль в нашей повседневной жизни, безопасность компьютерной информации становится одной из основных проблем. Взлом аккаунта – это одно из самых распространенных и серьезных преступлений, связанных с компьютерной информацией, которое квалифицируется ст. 272 «Неправомерный доступ к компьютерной информации» Уголовного кодекса Российской Федерации от 8 янв. 1997 г. № 1-ФЗ (далее – УК РФ). Взлом аккаунта – это незаконное получение доступа к чужому электронному профилю или системе без разрешения владельца. Это может быть социальная сеть, электронная почта, онлайн-банкинг или другие сервисы, которые хранят личные данные пользователей.

Целью злоумышленников обычно являются получение конфиденциальной информации или украденные учетные данные для дальнейшего использования в мошеннических целях. Невозможно не согласиться с мнением Судьяровой М. С., которая отмечает повышенную виктимность самих субъектов персональных данных, благодаря их пренебрежительному поведению злоумышленник может получить доступ к различным персональным данным лица, например, если лицо использует для различных учетных записей одинаковые пароли, то это позволяет получить сведения о человеке из различных источников и в большем объеме [3, с. 109]. То есть проблемы существуют не только со стороны систем хранения данных аккаунтов, но и со стороны самих владельцев этих аккаунтов.

Проблема взлома аккаунтов стала особенно острой благодаря развитию интернета и возросшему числу пользователей онлайн-платформ. Злоумышленники используют различные методы и техники для взлома аккаунтов, такие как фишинг, вредоносное программное обеспечение или слабые пароли. Они могут получить доступ к аккаунту с целью украсть личные данные, распространять спам, шантажировать пользователя или даже использовать его аккаунт для незаконных действий.

Последствия взлома аккаунта могут быть катастрофическими для пострадавшего. Утечка персональной информации может привести к финансовым потерям, нарушению конфиденциальности и даже к преступлениям против собственности. Кроме того, повреждение репутации и потеря доверия пользователей также являются серьезными последствиями этого преступления.

Для борьбы со взломами аккаунтов необходимо использовать комплексный подход. Пользователи должны быть осведомлены о методах предотвращения атак и следовать базовым правилам безопасности – создавать надежные пароли, не использовать одинаковые пароли для разных сервисов и быть осторожными при открытии ссылок или приложений из ненадежных источников.

Организации, предоставляющие онлайн-сервисы, также должны принимать меры для защиты своих пользователей. Это включает в себя использование современных методов аутентификации, шифрования данных и систем мониторинга, чтобы обнаруживать подозрительную активность.

В целом, проблема взлома аккаунтов является серьезной угрозой для компьютерной информации и требует непрерывного развития и совершенствования методов защиты. Безопасность онлайн-платформ должна быть приоритетом как для пользователей, так и для организаций, чтобы поддерживать доверие и сохранять конфиденциальность личных данных.

Одним из основных вопросов, с которыми сталкиваются жертвы взлома аккаунтов, является популярные методы и инструменты, используемые злоумышленниками для осуществления такого преступления. Рассмотрим некоторые из них.

Первый наиболее распространенный метод – это перебор паролей. Злоумышленники используют специальные программы, которые автоматически генерируют и проверяют множество возможных паролей до тех пор, пока не будет найдено правильное сочетание символов. Для защиты от такого типа атаки рекомендуется использовать сложные пароли, состоящие из букв разного регистра, цифр и специальных символов.

Еще один распространенный метод взлома аккаунтов – это фишинг. Фишинг (*phishing*, от *fishing* – рыбная ловля, выуживание) представляет собой вид интернет-мошенничества. Целью данного мошенничества является получение логина и пароля к банковским картам и учетным записям [4, с. 156]. Злоумышленники создают поддельные веб-сайты или отправляют электронные письма, имитирующие официальные запросы от известных сервисов. Чтобы не стать жертвой фишинга, рекомендуется быть предельно осторожными при переходе по ссылкам из непроверенных источников.

Еще одним методом взлома аккаунтов является использование слабых механизмов аутентификации. Некоторые сервисы все еще допускают возможность аутентификации только по паролю, что делает аккаунты более уязвимыми для взлома. Для усиления безопасности рекомендуется использовать двухфакторную аутентификацию или другие дополнительные механизмы проверки подлинности.

Также необходимо обратить внимание на использование обновленного программного обеспечения и операционной системы, так как уязвимости в них могут использоваться злоумышленниками для получения доступа к аккаунтам. Регулярное обновление программных продуктов и установка последних патчей безопасности поможет минимизировать риски взлома. Патч – это набор изменений в компьютерной программе или вспомогательных данных, предназначенных для ее обновления, исправления или усовершенствования. Оно включает в себя исправление уязвимостей в системе безопасности и других ошибок, причем такие исправления обычно называются исправлениями или исправлениями ошибок.

Взлом аккаунта – серьезное преступление, которое наносит ущерб как физическому лицу, так и организациям. Понимание популярных методов и инструментов взлома аккаунтов поможет пользователям принять необходимые меры для защиты своих данных и предотвратить возможные атаки. Важно помнить, что безопасность информации – это задача каждого пользователя и организации.

В современном мире взлом аккаунтов является одним из наиболее распространенных и опасных видов преступлений, связанных с компьютерной информацией. Однако, несмотря на то, что данное деяние признается противозаконным практически во всех странах мира, законодательство и наказания за взлом аккаунтов остаются сложной и актуальной проблемой.

Законодательство различается от страны к стране, а также может иметь разные подходы к определению понятия «взлом аккаунта». В некоторых юрисдикциях это считается уголовным преступлением, в других – административным или гражданским правонарушением. Это создает сложности для правоприменения и обеспечения единого подхода к борьбе с данной проблемой.

Одна из основных сложностей заключается в том, что зачастую жертва взлома аккаунта испытывает трудности с доказательством факта преступления и выявления конкретного злоумышленника. Часто хакеры используют анонимные прокси-серверы и другие технические средства для скрытия своей личности, что делает идентификацию затруднительной.

Кроме того, наказание за взлом аккаунта не всегда соответствует уровню преступности. В некоторых случаях суд может принять решение о штрафе или условном осуждении, которые не являются достаточно строгими мерами в отношении серьезного преступления против компьютерной информации. Это может создавать неправильные стимулы для потенциальных злоумышленников и подорвать доверие к эффективности правосудия.

Для решения данных проблем необходимо разработать единый международный подход к законодательству и наказаниям за взлом аккаунтов. Это позволит обеспечить более эффективное пресечение данного вида преступлений и повысить уровень безопасности компьютерной информации.

В заключение хотелось бы сказать, что законодательство и наказания за взлом аккаунтов представляют сложную задачу для правоохранительных органов и судебных систем. Необходимы дальнейшие усилия по

совершенствованию уголовного законодательства и разработке эффективных механизмов пресечения данного вида преступлений. Только таким образом можно достичь снижения уровня взлома аккаунтов и защитить компьютерную информацию от злоумышленников. Необходимо решать данные проблемы в соответствии с вышеуказанными требованиями, а также внести в официальные нормативные правовые акты понятие «взлом аккаунта» для правильной квалификации данного вида преступления, а также для понимания населением такой противоправной деятельности.

Список литературы

1. Блогеры пожаловались на взлом аккаунтов и требование денег за восстановление. URL: https://sapa.media/2023/10/24/blogery-pozhalovalis-na-vzlom-akkauntov-i-trebovanie-deneg-za-vosstanovlenie/ (дата обращения: 28.11.2023).
2. Уголовно-исполнительный кодекс Российской Федерации от 8 января 1997 г. № 1-ФЗ: принят Гос. Думой 18 дек. 1996 г. // Собр. законодательства Рос. Федерации. – 1997. – № 2, ст. 198.
3. Судьярова М. С. Персональные данные как предмет преступлений против компьютерной информации / М. С. Судьярова // Актуальные вопросы российского права: сборник статей Всероссийской научно-практической конференции, Пенза, 5 июля 2022 года. – Пенза : Наука и Просвещение (ИП Гуляев Г. Ю.), 2022. – С. 109-111.
4. Сазонова Е. С. Фишинг как вид интернет-мошенничества / Е. С. Сазонова, А. В. Головин // Наука молодых – будущее России: сборник научных статей 4-й Международной научной конференции перспективных разработок молодых ученых. В 8 томах, Курск, 10-11 декабря 2019 года / отв. ред. А. А. Горохов. – Курск : Юго-Западный государственный университет, 2019. – Т. 5. – С. 156-158.
5. Понятие патча (вычислительного). URL: https://en.wikipedia.org/wiki/Patch_(computing)#SECURITY (дата обращения: 02.12.2023).