Прохорко Татьяна Николаевна
канд. юрид. наук, доцент
ФКОУ ВО «Пермский институт ФСИН России»
г. Пермь, Пермский край

МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация*: статья посвящена новому виду мошенничества, хищению компьютерной информации. В данном виде преступления хищением имущества являются не только денежные ресурсы, но и информация, которая появляется в процессе деятельности отдельного лица или группы людей и обладает признаками уникальности.*

Ключевые слова*: мошенничество, компьютерная безопасность, информация, электрические сигналы, компьютерное мошенничество.*

Наиболее противоречивым из преступных деяний, связанных с использованием лжи, манипуляций и эксплуатации чужой доверчивости, является мошенничество, совершаемое путем процедур ввода, видоизменения, стирания с жестких носителей или прекращения обращения к данным, имеющимся на компьютере. По мере того, как группы программ-вымогателей быстро совершенствуют свои бизнес-модели для координации своей деятельности и максимизации эффективности, также можно увидеть, что такие группы постоянно совершенствуют свои возможности по взлому сетей, компрометации критически важных систем и данных в целевой сети, поддержанию доступа к сети и успешному вымогательству у жертв.

Понятие компьютерной информации содержится в примечаниях к ст. 272 УК РФ, где под ней понимаются «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [1]. Из представленного определения можно сделать вывод, что данный вид информация – это такие сведения (сообщения, данные), которые хранятся, обрабатываются и передаются с помощью определенных

средств, которые называются машинными носителями, техническими устройствами и т. д.

В данном виде преступления хищением имущества являются не только денежные ресурсы, но и информация, которая появляется в процессе деятельности отдельного лица или группы людей и обладает признаками уникальности. Овладение подобными ресурсами может произойти в процессе:

– ввода данных, который, в свою очередь, доступно выполнить напрямую с клавиатуры или иного интерфейса для ввода, а также посредством записи со съемного хранилища данных;

– изменения имеющихся на компьютере данных, путем ручного исправления или посредством вредоносных программ, содержащих необходимый алгоритм;

– удаления имеющихся данных, алгоритмов или программного обеспечения, причем без возможности их восстановления, то есть путем безвозвратного уничтожения;

– вмешательства в работу компьютерной или периферийной техники.

Для того, чтобы противоправные действия можно было классифицировать, как компьютерное мошенничество, необходимо наличие ряда обстоятельств:

– достижение преступником совершеннолетия, так как, не являясь тяжким, подобное нарушение закона не допускает наказания лиц, не достигших 16 лет;

– наличие умысла, заключающегося в желании завладеть чужими данными, средствами или правами, отсутствие, которого не позволяет отнести деятельность к мошеннической;

– завершившийся безвозмездный переход к злоумышленнику средств, данных или прав на них, а также иной собственности в результате выполненных действий.

На современном этапе одним из распространенным видом мошенничества в сфере компьютерной информации является фишинг.

Фишинг (с англ. phishing) – это самый распространенный метод взлома паролей и кражи конфиденциальной информации в интернете. Платежные данные кредитной карты, банковское имя пользователя и пароль, данные с личных страниц пользователя, доступ к банковским счетам и т. д. представляют большой интерес для мошенников. Чтобы получить данную электронную информацию, они идут на разного рода уловки: выполняют массовую рассылку электронных писем (спам), именных сообщений от государственных и финансовых организаций, социальных сетей, создают фишинговые сайты, загрузочные страницы, всплывающие окна и т. д. [2].

Основным элементом фишинга является процесс создания дубликата или клона известного веб-сайта с целью кражи пароля пользователя или другой защищенной информации. Этот метод стал очень популярным, так как большинство пользователей чаще всего не соблюдают основные требования кибергигиены. Киберпреступники или мошенники постоянно совершенствуют названия и адреса своих фишинговых сайтов. В попытке придать веб-сайту легитимный и реалистичный вид для созданных фишинговых сайтов используют название известного бренда или организации в своих URL.

Злоумышленники всегда находятся в поиске любого способа, с помощью которого они могли бы обмануть людей и получить преимущество. Одним из таких способов является создание поддельных страниц входа, которые они отправляют жертвам в приложении к электронному письму. Здесь злоумышленники притворяются заслуживающим доверия человеком, таким как исполнительный директор организации.

Данный современный вид мошенничества можно определить, как форму атаки, включающую взаимодействие с людьми. Она используется для того, чтобы заставить пользователей или жертв совершать психологические ошибки, в результате чего они совершают ошибку в системе безопасности, выдавая важную информацию. Фишинг заключается в обмане пользователей с помощью поддельных веб-сайтов, которые выглядят так же, как официальные, или выда-

ют себя за кого-то заслуживающего доверия, и она включает в себя такие действия, как эксплуатация нормального человеческого поведения, такого как доброта и жадность. Человеческое поведение таково, что люди склонны легко поддаваться на все, что они считают бесплатным, или на все, что они считают заслуживающим доверия.

Тем самым фишинг является жизненно важной глобальной проблемой. Он используется для сбора конфиденциальной информации и является одной из наиболее широко используемых форм кибератак, нацеленных на организации и отдельных лиц, использующих вредоносные ссылки и электронные письма, которые кажутся законными. Временами становится трудно отличить вредоносные электронные письма от законных.

В то же время осведомленность пользователей о фишинговых атаках со временем возрастает. Банки, социальные сети и другие веб-сервисы предупреждают о различных мошеннических схемах, использующих методы социальной инженерии. Все это уменьшает количество откликов в фишинговой схеме – все меньше и меньше пользователей можно обманным путем заманить на поддельный сайт. Поэтому злоумышленники придумали механизм скрытого перенаправления пользователей на фишинговые сайты, получивший название «фарминг», который представляет собой процедуру скрытного перенаправления жертвы на ложный IP-адрес [2].

Злоумышленник распространяет специальные вредоносные программы на компьютеры пользователей, которые после запуска перенаправляют обращения на поддельные сайты. Это обеспечивает высокую скрытность атак, а участие пользователя сводится к минимуму – достаточно подождать, пока пользователь решит посетить интересующие злоумышленника сайты.

Для защиты от фарминг-атак необходимо применять такие меры как: использовать и регулярно обновлять лицензионное антивирусное программное обеспечение; использовать защиту электронного почтового ящика (отключение

предварительного просмотра); не открывать и не загружать вложения электронных писем от незнакомых и сомнительных адресатов.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ // Собр. законодательства Рос. Федерации. – 1996.

2. Фатахова Д.Р. Мошенничество в сети Интернет / Д.Р. Фатахова. М., 2020. С. 341–344.