ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Дорожкин И.В., ст. гр. 173602; Шарафанович Я.О., ст. гр. 173602

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Пулко Т.А. – канд. техн. наук

Аннотация. Использование компьютерных и информационных технологий в различных сферах жизни общества становится обязательным атрибутом для достижения максимальной эффективности данной сферы. В связи с этим сфера информационных технологий становится всё более популярной для различного рода мошенников и преступников. Через информационные технологии проходит значительный поток финансов и различной личной информации. Мошенники пользуются этим, пытаясь различными способами выкрасть деньги или же личную информацию пользователя, чтобы в дальнейшем использовать её в своих целях. В данной статье рассмотрены различные источники угроз и виды преступлений в сфере информационных технологий. Основными выводами являются меры предосторожности, способные уберечь пользователя от потенциальных опасностей деятельности правонарушителей.

Существует множество способов и схем, с помощью которых мошенники получают доступ к персональным данным пользователя, такими как пароли, данные банковских карт и многое другое.

Фишинг — вид интернет-мошенничества, который заключается в “выуживании” конфиденциальных данных у пользователя. Спецификой данного метода является то, что жертва мошенничества предоставляет свои данные добровольно. Для этого преступники используют специальные фишинговые сайты, email-рассылку, нацеленную рекламу. Как правило, мошенники маскируются под известные компании, социальные сети или сервисы электронной почты.

Кардинг — сфера киберпреступности, которая напрямую взаимодействует с деньгами обычных законопослушных граждан. При данном виде мошенничества производится операция с использованием платёжной карты, не инициированная её держателем. Кража денежных средств — одна из самых страшных опасностей для любого человека, но есть факторы, из-за которых на сферу кардинга стоит обращать особое внимание.

“Нигерийские” письма — вид мошенничества, основанный на массовой рассылке электронных писем. Своё название письма получили из-за того, что данный вид мошенничества получил наибольшее распространение в Нигерии, причём ещё до распространения интернета, когда письма распространялись по обычной почте. Однако такого рода письма могут приходить и из других стран, но всё же в основном из стран Африки, например, Анголы, Того, Гамбии, Сомали и других.

Кибервымогательство — вымогательство с использованием интернета. Как правило, при таком способе вымогательства пользователь получает сообщение, в котором говорится, что злоумышленники получили личную информацию и угрожают выложить её в открытый доступ.

Взлом социальных сетей и дальнейшее вымогательство денег — один из самых распространенных и часто встречающихся способов мошенничества. Такая популярность данного метода вытекает из ненадёжности большинства социальных сетей — их очень легко взломать. При этом, необязательно быть специалистом в области информационных технологий. На просторах интернета есть куча информации, как взломать ту или иную социальную сеть, поэтому справиться с этой задачей может даже абсолютно неподготовленный человек, никак не связанный с хакерством.

Преступники используют различные методы хищения данных, наиболее популярные методы представлены ниже:

Отслеживание нажатия клавиш. За отслеживание отвечают специальные программы, которые определяют, какие комбинации клавиш пользователь использует чаще всего. Данный способ обычно используется для выявления паролей от банковских счетов и других сервисов.

Подбор паролей. Если преступникам известна некоторая личная информация о пользователе, например имя, фамилия, год рождения и тому подобное, то они могут попытаться подобрать пароль исходя из этих знаний, используя разные комбинации таких данных в качестве пароля. Данный способ является наиболее простым и лёгким, но при этом срабатывает крайне редко, так как очень малое количество людей используют личную информацию в качестве пароля от чего-либо. Тем не менее, такие люди встречаются, и мошенники могут использовать этот факт.

Backdoor программы — программы, позволяющие преступникам входить в систему компьютера пользователя или выходить из нее. Такие программы помогают злоумышленникам удаленно контролировать деятельность пользователя, а также просматривать личную информацию, в том числе пароли.

Обман сети. Злоумышленники могут создавать ложные сети, например Wi-Fi. Правонарушитель может ждать свою жертву в общественном месте, где создаст сеть с названием

этого места. Когда пользователь подключится к такой сети, то преступник сможет отслеживать его действия в интернете, а также просматривать файлы вашего устройства или даже установить на него вирус или другую зловредную программу.

Как уже стало понятно из описания методов правонарушений в области информационных технологий, данные действия могут нести серьёзную опасность для финансов, конфиденциальности пользователя. Тем очевиднее факт, что необходимо знать способы защиты от киберпреступлений и их предостережения.

Необходимо помнить, что ни в коем случае нельзя передавать такие конфиденциальные данные как пин-код банковской карты, пароль электронной почты или аккаунтов в социальных сетях. Ни банк, ни соцсеть никогда не станут запрашивать такого рода данные используя электронную почту. Это самый простой способ защиты от фишинга.

Для защиты от вирусов рекомендуется установить на компьютер надёжный антивирус — программы, препятствующей распространению вируса на компьютере пользователя.

Нельзя вводить данные о банковской карте в непроверенных магазинах и вообще постараться предостеречься от любых онлайн-покупок. Оставлять данные о финансовой карте лучше либо на максимально проверенных сервисах, либо вообще нигде.

Для защиты от «нигерийских писем» не стоит высылать персональные данные или копии каких-либо документов и номера банковских счетов по запросу организаций, в которые пользователь не обращался, или людям, которых до этого никогда не знал.

Одним из самых действенных решений для защиты от блокировки персональных данных является резервное копирование данных. Стоит регулярно сохранять важные файлы и документы в облачное хранилище типа диска Google или на внешний жёсткий диск. Стоит отметить, что при копировании информации на резервный жёсткий диск стоит только тогда, когда пользователь что-то копирует или считывает с него. Если он окажется соединен с компьютером во время нападения, то его также зашифруют. Также, при хранении данных на жёстком диске нужно защитить его надёжным паролем, желательно с двухэтапной аутентификацией, это существенно снизит вероятность взлома облачного хранилища пользователя.

Список использованных источников:

[1] Информатизация - [Электронный ресурс]. – Режим доступа: http://multilang.pravo.by.

[2] Правонарушения в сфере информационных технологий - [Электронный ресурс]. – Режим доступа: https://www.elibrary. ru/download/elibrary_ 37130233_76877572.pdf.

[3] Фишинг - [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3.

[4] Кардинг - [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%80%D0%B4%D0%B8%D0%BD%D0%B3.

[5] Нигерийские письма - [Электронный ресурс]. – Режим доступа: https://nigeria.mfa.gov.by/ru/letters/.

[6] Кибервымогательство — это вымогательство в интрнете - [Электронный ресурс]. – Режим доступа: https://news.ykt.ru/.

[7] Виды киберпреступлений - [Электронный ресурс]. – Режим доступа: https://internetpolicy.kg/literacymodule/course_2/module1/glava1_2.html.

[8] Десять самых громких атак XXI века - [Электронный ресурс]. – Режим доступа: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e.

[9] Уголовный кодекс Республики Беларусь - [Электронный ресурс]. – Режим доступа: https://kodeksy-by.com/ugolovnyj_kodeks_rb.

[10] Инструкция: как не нарушить авторские права - [Электронный ресурс]. – Режим доступа: https://www.asi.org.ru/2020/04/23/instruktsiya-avtorskie-prava/.

[11] Что такое кардинг, и как защитишься от взлома, покупая в интернете - [Электронный ресурс]. – Режим доступа: https://trends.rbc. ru/trends/industry/60ae051f9a7947c4dc22101b.

[12] Как защититься от шифровальщиков-вымогателей: 5 советов - [Электронный ресурс]. – Режим доступа: https://www.kaspersky. ru/blog/ransomware-five-tips/31352/.