УДК 338.5:621.395.7

55. КИБЕРПРЕСТУПЛЕНИЯ И ПРАВО

Васенко К.А., Мамай К.О.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ермакова Е.В. – канд. экон. наук

Аннотация. Мы живем в эпоху информатизации, когда персональные компьютеры и иные различные средства инфокоммуникаций стали неотъемлемой частью обыденного и нормального существования человека. Нашу жизнь уже не получается представить без информационных технологий. Благодаря их развитию, наша жизнь стала в разы проще, ведь такие технологии используются почти во всех сферах нашей повседневной жизни. Например, в образовательных заведениях эти технологии используются для обучения, стало возможным организовывать дистанционное обучение. Однако наряду с развитием технологий появились и негативные стороны этого процесса. Возник новый вид мошенничества — киберпреступность, то есть

правонарушения в сфере информационных технологий. Это неудивительно, ведь через компьютеры и мобильные устройства пользователей протекает значительный поток финансов и личной информации простых пользователей, а обмануть человека, лично с ним не контактируя, намного проще.

Существует множество способов и схем, с помощью которых мошенники получают доступ к персональным данным пользователя, такими как пароли, данные банковских карт и многое другое. Наиболее часто встречающимися являются: фишинг; кардинг;“нигерийские” письма; кибервымогательство.

Рассмотрим каждый вид мошенничества подробнее.

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 [1].

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 [2]. Кардеры используют ряд методов для кражи платёжных средств:

– фишинг, как и описывалось ранее, создаётся поддельный сайт, на котором пользователь должен ввести свои платёжные данные;

– взлом баз данных мелких предприятий, на примере магазинов, сервера которых плохо защищены, а иногда и самовольная продажа банковских данных самой компанией или её сотрудниками;

После получения данных карты, злоумышленники либо просто снимают с неё все сбережения, либо же продают карту на специальных магазинах, называемых “кардер-шопами”.

Но опасность кардинга состоит еще и в том, что обычный пользователь может быть привлечён к уголовной ответственности. Так от кардеров вам может прийти сообщение, где будет предлагаться с помощью некоторого сервиса оплачивать такси или заказывать еду по очень выгодной цене, нужно лишь сбросить дельцу указанную сумму и пользоваться услугами такси или доставки через данный сервис. Выполнив такие действия, вы вполне можете получить повестку в суд по уголовной статье в роли соучастника, ведь деньги, которые вы выслали мошенникам были положены на украденную карту и именно с неё оплачивались все счета данного сервиса. Подобные схемы возможны и при оплате перелётов, туров и других дорогостоящих услуг.

“Нигерийские” письма — вид мошенничества, основанный на массовой рассылке электронных писем [3]. 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 письма могут приходить и из других стран. Схема подобного рода мошенничества заключается в следующем:

1. В сети рассылается тысячи электронных писем с разного рода предложениями и услугами.
2. В случае, если мошенники получают от адресата ответное письмо, выражающее некоторую заинтересованность, преступники вступают в диалог с адресатом, пытаясь получить от него необходимые данные: счета, пароли, непосредственно деньги и тому подобное.
3. Переписка продолжается до тех пор, пока жертва не будет сама готова перечислить деньги мошенникам.
4. После перечисления денег возможны два сценария развития событий: если мошенники понимают, что их “клиент” безусловно верит им, то под каким-либо предлогом сообщают ему, что перечисленных им средств недостаточно, и необходимо выслать ещё; либо же переписка мошенников с их жертвой резко обрывается, а счёт, на который были переведены нужные средства моментально закрывается.

Стоит отметить, что некоторые пользователи, понимая, что их хотят обмануть, отвечают мошенникам из любопытства, интересуясь, что им могут предложить и как будут пытаться обманывать. Однако, этого делать не стоит. Причиной этого является то, что когда адресат отвечает на такое сообщение, то автоматически заносит себя в базу данных мошенников. Это может обернуться, как минимум, засоренной почтой, а, как максимум, на компьютер жертвы может выслаться опасный вирус, после чего не составит труда получить доступ к личным данным пользователя.

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 [4].

Хаккеры могут проводить кибератаки на различные серверы и компании, при этом условием неразглашения украденной ими информации является перевод денежных средств на указанный счёт.

В случае с несогласием выдвинутых требований, злоумышленники угрожают распространением личных фотографий дискредитирующего характера и других данных, относящихся к частной жизни, что может привести к разрушению прав человека, нарушению деловой репутации, а также привести к эмоциональному стрессу и другим видам морального вреда.

Некоторые типы киберпреступлений направлены на изменения настроений в политической среде или нанесение намеренного вреда или снижения влияния отдельных личностей или группы людей. Преступления на почве ненависти по отношению к личности или группе людей обычно совершаются на основе гендерной, расовой, религиозной, национальной принадлежности сексуальной ориентации и других признаков [5].

Зачастую объектами таких киберпреступлений могут стать крупные корпорации или даже целые государства.

Примером атаки на крупную корпорацию может стать взлом одной из самой популярной социальной сети мира Facebook в 2020 году. В результате хакерской атаки, в сеть утекли данные более чем 260 миллионов пользователей. После таких утечек суд обязал компании выплатить штраф в размере 5 миллиардов долларов, что является крупнейшим штрафом за утечки данных в истории.

Если говорить о преступлениях в отношении целого государства, то примером является взлом и получение доступа к 269 Гб секретных данных правоохранительных органов и спецслужб Соединенных Штатов Америки группировкой хакеров Anonymous. Среди этих данных содержались видеоролики, электронные письма, документы по планированию и разведке за последние 5 лет [6].

Список использованных источников:

1. Что такое фишинг ? [Электронный ресурс] : интернет-энциклопедия «Касперского». – Режим доступа: https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/.

2. Особо опасное мошенничество : что такое кардинг? [Электронный ресурс] : интернет-статья. – Режим доступа : https://drweb.ru/pravda/issue/?number=1211.

3. «Нигерийские письма» [Электронный ресурс] : интернет-энциклопедия «Касперского». – Режим доступа: https://encyclopedia.kaspersky.ru/knowledge/nigerian-letters/.

4.Что такое кибервымогательство? [Электронный ресурс] : интернет-статья «Keeper». – Режим доступа: https://www.keepersecurity.com/blog/ru/2024/01/15/what-is-cyber-extortion/.

5. Князькова, В.С. Дистанционные образовательные технологии: трансформация рынка образовательных услуг / В. С. Князькова // Управление информационными ресурсами : материалы XVIII Междунар. науч.-практ. конф., Минск, 10 марта 2022 г. ; Акад. упр. при Президенте Респ. Беларусь. - Минск : Академия управления при Президенте Республики Беларусь, 2022. - 412 с. - С. 185-187.

6. Беляцкая,Т. Н. Страхование рисков информационной безопасности / Т. Н. Беляцкая, В. С. Князькова // Технические средства защиты информации: тезисы докладов XVIII Белорусско-российской научно - технической конференции, Минск, 9 июня 2020 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол.: Т. В. Борботько [и др.]. - Минск, 2020. - С. 15 - 16.