Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

Мошенничество в сети интернет – актуальные проблемы и методы борьбы

Научный руководитель – Хабибулин Алик Галимзянович

Дидидзе Милана Аркадьевна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия
E-mail: ma.dididze@gmail.com

Интернет - неотъемлемая часть жизни человека в 21 веке. Многие процессы общественной жизни осуществляются в среде информационно-коммуникационной сети Интернет, что ведет к образованию мощной среды, содержащей огромное количество информации.

Необходимо отметить, что высокая динамика проникновения интернета в общественное развитие приносит не только явное преимущество обществу (напр., мгновенная оплата товаров, услуг, быстрый и удобный доступ к информации, беспрепятственная коммуникация в режиме онлайн), но и несет глобальные угрозы для экономической безопасности государства и общества. Одной из таких ключевых угроз является Интернет-мошенничество.

Согласно ч. 1 ст. 159 Уголовного кодекса Российской Федерации, мошенничество - это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием [1]. Предметом мошенничества является имущество или право на имущество. Также, мошенничество может быть совершено с использованием электронных средств платежа, где предметом преступления будут являться безналичные денежные средства, включая электронные денежные средства [2].

Количество преступлений, совершенных в сети Интернет растет, появляются новые способы совершения мошенничества с использованием электронных средств платежа, а соответственно увеличивается и сумма причиненного ущерба.

По официальным данным Министерства внутренних дел Российской Федерации за период с января по декабрь 2021, больше половины зарегистрированных преступлений - 55,3 % составляют хищения чужого имущества, среди которых мошенничество - 339, 606 тыс. с темпом прироста 1,2% [3]. В том числе, мошенничество с использованием электронных средств платежа (ст. 159.3 Уголовного кодекса Российской Федерации) - 10 258, мошенничество в сфере компьютерной информации (ст. 159.6 Уголовного кодекса Российской Федерации) - 431 [4].

Согласно официальной статистике Министерства внутренних дел Российской Федерации за период с января по декабрь 2017 года. по ст. ст. 159-159.6 Уголовного кодекса Российской Федерации было зарегистрировано 222 772 тыс. с приростом 6,6 % [5].

Анализируя статистику преступлений в сфере мошенничества за 4 года, можно сделать вывод, что количество зарегистрированных преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, неуклонно растет. Одним из ключевых факторов, влияющих на данный показатель, является компьютеризация всех сфер общественной жизни.

Еще в июле 2020 года Генеральный прокурор Российской Федерации Игорь Краснов в ходе совещания, посвященному мерам по борьбе с киберпреступностью указал, что с 2015 года количество таких преступлений возросло в 25 раз [6]. Это свидетельствует о том,

что информатизация общества становится практически неконтролируемой и порождает негативные явления в виде компьютерных преступлений.

Интернет - это виртуальное пространство, но за совершение деяний в этой среде предусмотрена юридическая ответственность. Это связано с тем, что Интернет-мошенничество приводит к финансовым потерям и социально-психологическим последствиям.

Анализ информационной базы позволяет сделать вывод о том, что нет единой классификации типов Интернет-мошенничества. Классификация мошенничества в сети Интернет зависит от методов исполнения, сферы взаимодействия, каналов коммуникации, коммуникативных средств и т.д. [7].

На сегодняшний момент в сети Интернет существует множество различных видов мошенничества: фишинг, лотереи, социальная инженерия, благотворительность, фальшивые интернет-магазины и т.д. Разберем более подробно наиболее распространенные виды мошенничества в сети Интернет.

1. Фишинг - незаконное получение контрольной информации и персональных данных [8]. Схема мошенничества при фишинге направлена на получение персональных данных держателя карты. Предметом мошеннических действий выступают логины и пароли пользователей банковских приложений, номера и ПИН-коды карт оплаты и др.

Фишинг в последние годы стал больше распространяться, так как владельцы банковских карт все больше стали пользоваться «дистанционной оплатой» услуг через Интернет без непосредственного использования самой карты, то есть для оплаты карта физически не нужна.

Финансовые потери при фишинге связаны с тем, что владельцы карт сами передают мошенникам персональную информацию и переводят деньги. С помощью обманных действий, которые выражены в рассылке почтовых сообщений от лица банка или платежных систем, в точности копирующих адрес, визуальное оформление страницы сайта и т.д., мошенники получают всю необходимую информацию и выводят денежные средства.

Основная проблема при фишинге - это не кибератаки, распространение компьютерных вирусов и взломы, а «социальная инженерия». Следовательно, способом реализации мошеннической атаки является сам человек, над которым совершались психологические манипуляции, а причиной - незнание пользователем методов безопасности в сети Интернет.

2. Телефонные мошенники. Одна из схем, когда мошенники звонят с зеркальных номеров, которые отображаются в системе распознавания как номера банков и просят войти по ссылке в личный кабинет под предлогом смены пароля, блокировки карты и т.д. Тем самым, мошенники пытаются подтвердить свой вход в «Личный кабинет» банка на другом устройстве и вывести деньги с телефона жертвы.

Основная проблема незаконного вывода средств мошенниками с банковских счетов заключается в том, что новые разработанные способы авторизации «Личного кабинета» пользователя несут и повышенные риски.

Другая схема мошенничества - мошенники звонят из бюро кредитных историй и сообщают о том, что от имени потенциального клиента поступили заявки на оформление кредита. Абонент сообщает, то не подавал заявки и для отмены действий они просят информацию о персональных данных. Через некоторое время звонят из банка и предоставляются сотрудниками банка, подтверждают получение заявки на кредит и сообщают о необходимости совершения «зеркальных действий», то есть просят взять кредит и перевести деньги на определенный банковский счет. Тем самым, абонент переводит деньги на счет мошенников и остается с непогашенным кредитом.

Таким образом, мошенники используют уловки социальной инженерии, чтобы потенциальная жертва следовала всем инструкциям. А в результате данных действий, банки не возвращают деньги, которые были добровольно перечислены на другой счет.

Подводя итог сказанному, следует сказать о том, что поле деятельности мошенников с развитием ресурсов сети Интернет только увеличивается, появляются новые способы мошенничества, а соответственно появляются и новые проблемы.

Для решения проблем в сфере Интернет-мошенничества необходимо разработать меры, которые будут направлены на блокировку программ, направленных на использование «зеркальных» номеров и скрытие IP-адресов местонахождения технического устройства.

Список литературы

1) Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.03.2022) // «Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954.
2) Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. О 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате». Пункт 5 // «Российская газета», № 280, 11.12.2017.
3) Министерство внутренних дел Российской Федерации. Состояние преступности в России за январь-декабрь 2021 года // ФКУ «Главный информационно-аналитический центр». Москва. 2021. С. 6.
4) Министерство внутренних дел Российской Федерации. Состояние преступности в России за январь-декабрь 2021 года // ФКУ «Главный информационно-аналитический центр». Москва. 2021. С. 30.
5) Министерство внутренних дел Российской Федерации. Состояние преступности в России за январь-декабрь 2017 года // ФКУ «Главный информационно-аналитический центр». Москва. 2017. С. 3.
6) ПРАВО.Ru: https://pravo.ru/news/223988/
7) Печалина М. К., Шилова В. А. Интернет-мошенничество как значимая характеристика «экранного мира» сети // Наука телевидения № 11. 2014. С. 325.
8) Цифровая революция в сфере финансов: правила безопасного поведения потребителя. Редакция «Российской газеты». М. 2019. Вып. 24. С. 160.