Руденко Е. О., Пацкевич А. П.

СПОСОБЫ МОШЕННИЧЕСТВА В ИНТЕРНЕТЕ И ПРОФИЛАКТИКА ЭТИХ ПРЕСТУПЛЕНИЙ

Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, lawcrim@bsu.by

Исследуются способы мошенничества в сети Интернет, проблемные аспекты в области раскрытия данного рода преступлений и обозначаются профилактические меры по работе с население во избежание увеличения количества противоправных действий.

Ключевые слова: мошенничество; Интернет; профилактика; расследование преступлений; фишинг; Интернет-ресурс.

С активным развитием информационных технологий некоторые категории преступлений также переходят в Интернет-пространство. Данный феномен касается не только компьютерной информации, но и экономической составляющей, а именно денежных средств граждан.

Показательным примером является мошенничество в сети Интернет. Согласно статистики МВД Республики Беларусь, в 2024 году количество этих преступлений увеличилось в 4 раза по сравнению с прошлым годом [1]. Наиболее распространенными видами являются мошенничества с использованием информационно-компьютерных технологий, они составляют более половины преступлений этого вида. Вслед за ними по количеству выделяются хищения путем модификации компьютерной информации [2]. Исходя из данной статистики можно сделать вывод о том, что данная проблема только набирает обороты и борьба с киберпреступностью является актуальной задачей на текущий момент.

Мошенничество с использованием информационно-компьютерных технологий приравнивается к ст. 209 УК Республики Беларусь и предполагает, что потерпевший либо иное лицо, которому имущество вверено или под охраной которого оно находится, сами добровольно передают имущество или право на имущество виновному под влиянием обмана или злоупотребления доверием. При этом отдельного акцента на том, что были использованы информационно-компьютерные технологии кодекс не содержит.

Хищение имущества путем модификации компьютерной информации закреплено в ст. 212 УК Республики Беларусь и предлагает умышленное противоправное безвозмездное завладение чужим имуществом с корыстной целью посредством противоправного изменения компьютерной информации, либо внесения в компьютерную систему заведомо ложной компьютерной информации.

Мы согласны с мнением российского юриста Д.А. Зыкова, предлагающего ввести в Уголовный кодекс России специальную статью 159-1 УК РФ «Компьютерное мошенничество», под которой им понимается «завладение чужим имуществом путем обмана, злоупотребления доверием, присвоения, растраты либо причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенное с использованием ЭВМ, системы ЭВМ или их сети» [3, с. 37–39]. Однако введение такого рода статьи на данный момент не предвидится ни в УК Российской Федерации, ни в УК Республики Беларусь.

При этом в роли альтернативного варианта обозначения мошенничества в Интернете в законодательной базе может выступать соответствующие дополнение в дефиницию определенных признаков, поскольку хищения с помощью сети Интернет не всегда вписываются в рамки привычного состава мошенничества.

Если обращаться к способам совершения мошенничества в Интернете, то образуется достаточно большой список. В числе ключевых выделяются фишинг, вишинг, нигерийские письма, создание фальшивых аккаунтов с продажей товаров, схемы заработка, взломы аккаунтов в социальных сетях [4].

Фишинг это получение конфиденциальных данных, в том числе и номера банковской карты путем отправления ссылок от имени банков, отделений почты, брендов и прочих организаций [5, с. 11]. Суть состоит в том, что переходя по ссылке, гражданин вводит персональные данные, после чего эта информация оказывается в руках преступников. Подобные махинации также производятся и на площадках по продаже товаров по типу Куфара. В личные сообщения пользователю поступает письмо о том, что продавец просит внести предоплату только за доставку, после чего отправляется фишинговая ссылка. Предлог может быть абсолютно любой, но итог один – после перехода по ссылке и ввода данных средства на банковской карте безвозвратно исчезают.

Вишинг – это способ мошенничества, в получении конфиденциальных данных, представляясь компетентным лицом (сотрудником банка или милиции, например) [6, с. 25–31]. В этом случае придумывается определенная легенда, которая рассказывается потерпевшему, после которой он переводит или отдает деньги злоумышленникам.

Достаточно часто встречается ситуация, когда мошенники говорят потерпевшему, что на него оформлен кредит или произошло списание суммы с банковского счета. Тогда жертву просят назвать данные своей карты, после чего происходит хищение денежных средств. Также поскольку некоторые банковские приложения для входа используют биометрические данные, мошенники могут попросить включить камеру на звонке, после чего получают доступ ко входу в мобильный банкинг.

В случае, когда они представляются сотрудниками милиции, обычно применяется следующая преступная схема: при телефонном звонке описывается ситуация, что близкий человек потерпевшего совершил преступление и чтобы уголовное дело не было возбуждено, следует отдать определенную сумму. В такой ситуации уже в дело вступают курьеры телефонных мошенников, которым и передаются денежные средства. Данный способ образует целую преступную цепочку и квалифицируется как преступление, совершенное группой лиц.

Нигерийские письма подразумевают, что после финансовой операции, потерпевшему полагается солидное вознаграждение [7, с. 122-124]. Частым примером являются лотереи, когда мошенники внушают жертве, что она выиграла в конкурсе и для получения выигрыша необходимо оплатить лишь комиссию за перед.

Создание фальшивых аккаунтов с продажей товаров обычно происходит в различных социальных сетях. Сутью данного мошеннического действия является завлечение пользователей в своеобразный Интернет-магазин, где обычно цены значительно ниже привычных и склонение к покупке товаров. После оплаты указанной суммы товар не приходит к покупателю, а через определенное время магазин и вовсе исчезает.

Схемы заработка являются достаточно новым видом мошенничества и предполагают размещение в социальных сетях видео о том, как быстро заработать деньги с минимальными вложениями. Потерпевший отправляет денежные средства мошенникам, а взамен обретает схему по обману таких же заинтересованных в работе лиц, как он, или вовсе теряет свои финансы. В итоге образуется целый круговорот с размещением в сети Интернет рекламы быстрых заработков, которые под собой имеют лишь финансовые потери.

При ситуации, когда аккаунт оказывается в руках злоумышленников, преступники обычно действуют по двум сценариям: либо начинают от имени потерпевшего просить деньги у его контактов, либо просить заплатить для восстановления доступа к социальной сети.

Для криминалистической характеристики мошеннических действий в сети Интернет важно иметь представление о способах совершения данных преступлений, о месте, времени, условиях, способствовавших совершению преступления. Данные знания, несмотря на их вероятностный характер, способны существенно снизить информационную неопределенность, в особенности на начальном этапе расследования преступления [8, с. 614-626].

Важную роль в расследовании дел о мошенничестве играют криминалистические рекомендации, применение которых позволяет

собрать наибольшее количество информации и не допустить ее потерю из-за несвоевременного фиксирования.

В первую очередь важно получить сведения об Интернет-ресурсе, на котором и были совершены противоправные действия. В качестве ресурса может выступать торговая площадка, электронная почта, социальная сеть, сайт. Данные должны быть отмечены в протоколе допроса потерпевшего со всеми необходимыми реквизитами (ссылка, идентификатор и прочее). При условии, что данный ресурс все еще функционирует, необходимо связаться с лицом, администрирующим ресурс, и запросить сведения об IP адресах его посещающих. По данным адресам становятся известными сведения о провайдере, который располагает данными абонентов и имеет информацию о физическом адресе подключения.

Однако в случае шифрования IP адреса или нахождения его в иностранном государстве возникают проблемы с получением сведений о физическом адресе. В такой ситуации необходимо действовать в соответствии с нормами международных договоров. При этом запрос сведений у зарубежных стран обычно либо игнорируется, либо существенно затягивается ввиду недостаточно грамотно сформулированной правовой базы по содействию в раскрытии данных преступлений. А поскольку случаи мошенничества в Интернете являются достаточно частыми, такая ситуация значительно тормозит процесс раскрытия дел, ввиду того что преступники обычно находятся за пределами Республики Беларусь.

В случае шифрования IP адреса с помощью специальных программ проблемы возникают уже с техническим оснащением органов уголовного преследования, которое существенно отстаёт от технологий, задействованных в преступных схемах.

Если мошеннические действия были совершены при помощи аккаунта в социальной сети или электронной почты через администрацию ресурса есть возможность узнать и номер, на который они привязаны. Но в большинстве случаев используются незаконно приобретенные анонимные SIM-карты или виртуальные номера, существующие лишь для приема звонков либо СМС для регистрации. Даже если данная информация и будет получена, то существенно не повлияет на раскрытие преступления ввиду невозможности таким образом установить личность мошенника.

Также в ходе расследования дела от потерпевшего получается и платежная информация в виде реквизитов счета или карты. По данным сведениям можно установить их держателя, однако в основном карты приобретаются незаконным путем и установить лицо, которое действительно получили незаконно добытые денежные средства, не представляется возможным.

Указанные трудности в изобличении Интернет-мошенников говорят о том, что в настоящее время имеется существенная необходимость в

повышении уровня компетенции в рамках современных технологий, выработке и модернизации норм международного сотрудничества в области киберпреступности, борьбе с анонимностью в сети Интернет и банковской сфере.

Важным аспектом в противодействии киберпреступности является применение профилактических мер среди населения. Существует необходимость в просвещении граждан о новых видах мошенничеств, создание специализированных ознакомительных ресурсов с данной тематикой. Внимательность и бдительность на просторах сети Интернет также окажет существенное влияние на борьбу с мошенничеством. Для этого необходимо тщательно проверять ссылки, под различным предлогом отправленные по электронной почте и СМС и в случае сомнения в их достоверности не переходить по ним, в случаях звонков от имени компетентных лиц следует удостовериться в их подлинности, самостоятельно связавшись с организацией, от имени которой ведется диалог, необходимо доверять только проверенным сайтам с продажей товаров, продавцам, информации, а также устанавливать двухфакторвную аутентификацию на социальные сети.

Таким образом, проблема мошенничества остро стоит в нашем государстве и только набирает обороты. Для борьбы с данным видом преступности необходимо задействовать не только государство, но и граждан. Основными тенденциями в области профилактики киберпреступности должны стать модернизация законодательства, усиленный контроль за деятельностью пользователей с сети Интернет, информированность населения о новых видах мошенничества, усовершенствование систем безопасности банковских приложений и личных аккаунтов граждан. Данные меры профилактического характера помогут сузить сферы преступных посягательств и позволят выявить многие из них на начальных этапах.

Библиографический список

1. В Беларуси в 4 раза выросло количество тяжких киберпреступлений [Электронный ресурс]. – Режим доступа: https://neg.by/novosti/otkrytj/v-belarusi-v-4-raza-vyroslo-kolichestvo-tyazhkikh-kiberprestupleniy/. – Дата доступа: 15.09.2024.

2. За два месяца 2024 г. в Минске зарегистрировано 850 киберпреступлений. Какие методы обмана в топе [Электронный ресурс]. – Режим доступа: https://minsknews.by/za-dva-mesyacza-2024-g-v-minske-zaregistrirovano-850-kiberprestuplenij-kakie-metody-obmana-v-tope/#:~:text%B9. – Дата доступа: 15.09.2024.

3. Минин, А. Я. О специфике противодействия киберпреступности / А. Я. Минин // Российский следователь. – 2013. – № 8. – С. 37–39.

4. Старостенко, О. А. Природа и способы совершения мошенничества с использованием информационно-телекоммуникационных технологий / О. А. Старостенко // Вестник Удмуртского университета. – Экономика и право. – 2020. – Т. 3.

5. Ларичев В. Д. Как уберечься от мошенничества в сфере бизнеса / В. Д. Ларичев // М.: Юристъ. – 1996. – С. 11.

6. Гладких, В. И. Компьютерное мошенничество: а были ли основания его криминализации? / В. И. Гладких // Российский следователь. – 2014. – № 22. – С. 25–31.

7. Никитина, И. А. Финансовое мошенничество в сети Интернет / И. А. Никитина // Вестник Томского государственного университета. – 2010. – № 337. – С. 122-124.

8. Тимофеева, В. В. Криминалистическое обеспечение расследования мошенничеств в сети Интернет / В. В. Тимофеева // Вопросы российской юстиции. – 2022. – № 17. – С. 614-626.