3. Хажиахметова, Е. Ш. Криптовалюта – деньги XXI века / Е. Ш. Хажиахметова // Новая наука: от идеи к результату. – Агентство международных исследований, 2016. – № 11–2. – С. 177–179.

4. Яковлев, Д. К. Анализ потенциала применения цифровых валют в различных сферах экономической деятельности / Д. К. Яковлев // Московский экономический журнал. – 2020. – № 9. – С. 145–154.

УДК 330

К ВОПРОСУ О ПРЕДУПРЕЖДЕНИИ МОШЕННИЧЕСТВА С ОНЛАЙН-КРЕДИТАМИ

Захаров Д. С.
Могилевский институт МВД Республики Беларусь, г. Могилев, РБ
Научный руководитель: Шнейдерова Д. И.

Технологический прогресс и стремительное развитие социальной инженерии в условиях складывающейся общественной обстановки способствовали внедрению и распространению нового института кредитования населения в дистанционном формате посредством онлайн-заявок через сайты банков, либо Интернет- или мобильный банкинг. Отсутствие прямого контакта между сотрудником банка и клиентом, а также преимущества виртуальной сети и функциональных возможностей компьютерной техники оказали воздействие на появление усовершенствованных схем и методик мошеннических действий киберпреступников.

Под кредитом понимаются привлеченные и (или) собственные денежные средства, предоставленные банком другому лицу (кредитополучателю) в размере и на условиях, предусмотренных кредитным договором [1]. На сегодняшний день большинство крупных банков предлагают своим клиентам получение кредитов и оформление рассрочек посредством подачи онлайн-заявок с их дистанционным одобрением и перечислением суммы кредита на открытый расчетный счет. Пользуясь доверчивостью пользователей, их компьютерной безграмотностью, киберпреступниками были разработаны и апробированы порядка пяти мошеннических схем, направленных на завладение обманным путем денежными средствами, выдаваемыми банками своим клиентам в качестве кредитных.

Одним из самых распространенных методов кибермошенничества на территории Республики Беларусь является «вишинг», суть которого заключается в осуществлении преступниками телефонных разговоров от имени сотрудников того или иного банка, в процессе которых клиенту сообщается некоторая информация, требующая в ответ активных действий по предоставлению определенных конфиденциальных данных. Какие именно данные намеревается получить злоумышленник – зависит от преступной схемы. В одних случаях мошенник в разговоре с клиентом сообщает последнему, что с его счетом производятся подозрительные операции по переводу крупных сумм денежных средств и для их отмены необходимо сообщить сотруднику банка паспортные или анкетные данные, либо продиктовать номер кредитной карты и защитный трехзначный числовой код с ее обратной стороны, либо код из sms, пришедшего от банка для подтверждения операции, либо логин и пароль от Интернет- или мобильного банкинга. Получив какие-либо из указанных сведений, преступники без труда оформляют онлайн-заявки на максимально возможные суммы денежных средств, которые в последующем переводят с карт потерпевших на свои счета в зарубежных банках и обналичивают, либо оплачивают покупки в интернет-магазинах, приобретают криптовалюты на биржах и обменниках.

Иным образом складывается ситуация, когда потерпевшему сообщается информация, что на его имя в банке оформляется подозрительный кредит и для его отмены необходимо перейти в банкинг и оформить заявку на новый кредит на такую же сумму, пройти подтверждение путем двухфазной аутентификации и, если банком кредит будет одобрен, полученные средства перевести на указанный оператором счет для их сохранения от хищения [2].

При этом следует обратить внимание, что мошенники, совершая подобные действия, уже могут обладать определенными данными клиентов, в частности паспортными и сведениями о логинах и паролях от личных кабинетов банкинга, которые последние получают посредством скачивания или покупки клиентских баз в сети DarkNet. Такие звонки зачастую не вызывают подозрения у потерпевших, так как мошенники, в отличие от более известных схем, не требуют от пользователей предоставления им личных данных.

За последнее время набирает популярность вид «вишинга», при котором мошенники предлагают клиентам банка установить новое мобильное приложение, обладающее особыми преимуществами по осуществлению платежей и переводов, которое на самом деле представляет собой вредоносное программное обеспечение, позволяющее мошеннику получить доступ к реквизитам банковской карты, данным для авторизации в любом виде банкинга, а также дистанционно выполнять переадресацию входящих sms-сообщений от банка на номер преступника. Таким образом, имея всю совокупность информации, кибермошенники самостоятельно оформляют заявку на онлайн-кредит, подтверждают эту операцию защитным кодом-паролем и переводят денежные средства на свой счет.

Интересной представляется ситуация, когда мошенник под видом сотрудника службы безопасности банка сообщает клиенту, что на его имя оформляется кредит на большую сумму денежных средств и для предотвращения этой операции ему необходимо незамедлительно прибыть в ближайшее отделение банка. При этом преступник выясняет, за какой период времени клиент сможет доехать до отделения. По прошествии половины указанного потерпевшим времени мошенник повторяет звонок и сообщает, что преступные действия совершает сотрудник именно того отделения банка, куда направляется клиент, и для того, чтобы сохранить его денежные средства от хищения, необходимо немедленно перевести их на счет, указанный звонящим. Факт того, что счет зарегистрирован в другом банке, мошенник поясняет тем, что данный банк является страхующим, и как только ситуация будет прояснена, то денежные средства вернутся на счет клиента, чего, конечно же, не происходит. На тот случай, если клиенту позвонит другой оператор из банка для уточнения подозрительной операции по переводу крупной суммы, преступники также оставляют доверившемуся им потерпевшему необходимые инструкции и правильные ответы.

Вторым видом мошенничества с получением онлайн-кредитов является оказание помощи сторонним лицом в оформлении заявки на кредит для лиц, обладающих плохой кредитной историей, не работающих и пенсионеров. Распространение данный способ получил за счет эффективной рекламы в социальных сетях, на форумах и ресурсах для просмотра фильмов и киносериалов. Киберпреступники предлагают пользователям за небольшую плату в виде процента от оформленного кредита оказать сопровождение от момента подачи заявки до получения денежных средств на карту, для чего последним требуются личные и паспортные данные, а также полученная от банка информация. Доведя дело до момента получения денежных средств, мошенники, как и во всех остальных случаях, посредством доступа к Интернет-банкингу осуществляют их перевод на свои счета.

Схожим механизмом обладает третий вид мошенничества, при котором киберпреступники получают доступ к личным страницам пользователей различных социальных сетей или мессенджеров и вступают в переписку с близкими родственниками или знакомыми владельца страницы. В ходе общения мошенники просят у своих собеседников о помощи, указывая, что они получили крупную сумму денежных средств, но перевести их на свою карту не имеют возможности, так как истек срок ее действия, в связи с чем просят данные банковской карты собеседника, чтобы последний получил, обналичил и передал их в последующем законному владельцу. Кроме того, чтобы банк не сомневался, что денежные средства не попадут к преступникам, а будут переведены надежному получателю, требуется еще и копия страниц паспорта.

Двумя оставшимися не менее распространенными видами кибермошенничества являются создание и использование фишинговых и фарминговых сайтов банков. Фишинговые и фарминговые сайты представляют собой веб-страницы, по внешнему виду идентичные оригинальным ресурсам банка, на которых пользователю предлагают ввести логин и пароль для входа в личный кабинет. В отличие от фишинговых, фарминговые сайты копируют не

только дизайн веб-страницы, но и подменяют оригинальный IP-адрес на поддельный, ведущий к преступному сайту. Распространяются подобные ресурсы за счет спам-рассылок на электронную почту, всплывающей рекламы, смс-рассылок, а также при загрузке вредоносных программ, перенаправляющих пользователей на подставные сайты.

Таким образом, резюмируя вышеизложенное, необходимо отметить, что, несмотря на преимущества и перспективность цифровизации банковской сферы кредитования, негативным в этой связи является факт развития новых механизмов киберпреступности ввиду отсутствия должных мер защиты конфиденциальных данных пользователей. Представляется целесообразным осуществлять не только пассивные меры предупреждения мошеннических действий с онлайн-кредитованием, которые реализуются посредством информирования населения об известных практике механизмах преступлений и мерах по их недопущению, но и вводить в практику оказания услуг активные меры. В качестве таких активных мер следует привести внедрение опции блокировки удаленных каналов обслуживания, исключающую совершение любых операций вне отделения банка, а также обязательное уведомление о предстоящем списании денежных средств в большом объеме (лимит устанавливать по договоренности с клиентом банка).

Список литературы:

1. Словарь финансовых терминов – «кредит» [Электронный ресурс] / ОАО «АСБ Беларусбанк». – Режим доступа: https://belarusbank.by/ru/33139/press/finansovaya-gramotnost/-terminy/kredit. – Дата доступа: 01.12.2020.

2. Огурцова, Е. Эксперты рассказали о новой схеме мошенничества с онлайн-кредитами [Электронный ресурс] / Е. Огурцова // Финансовый портал «Banki.ru». – Режим доступа : https://www.banki.ru/. – Дата доступа : 01.12.2020.

УДК 330

ФАКТОРЫ РАЗВИТИЯ ЭЛЕКТРОННОГО БИЗНЕСА

Аникеенко А. В.
Гомельский государственный университет имени Ф. Скорины, г. Гомель, РБ
Научный руководитель: Дорошев Д. В., старший преподаватель

Доступность и непрерывный рост интернет-технологий (ИТ) создали большие возможности для пользователей во всем мире. Использование ИТ для ведения деятельности в режиме онлайн известно как электронный бизнес (E-Bussines).

В мире наблюдается бум новых технологий, особенно в сфере услуг (IT, телекоммуникации, интернет и др.). Благодаря технологическому прогрессу экономические операции стали намного проще и быстрее. Так, по данным Statista.com, в 2015 году розничные продажи электронной коммерции превысили $ 343 млрд. К концу 2019 году они составили $ 610 млрд [1].

Реальный двигатель новой экономики – электронный бизнес – является особенным источником конкурентных преимуществ предприятий и новым пространством для потребителей. Однако предприятия, осуществляя деятельность в области электронного бизнеса, могут сталкиваться с определенными проблемами, среди которых пока еще остаются ненадежное подключение к интернету, высокая стоимость доступа, а также невысокий уровень проникновения ИКТ.

Обратим внимание на основные факторы, с которыми сталкивается большинство организаций в настоящее время. Как государственные, так и промышленные предприятия широко признают, что с точки зрения потребителя вопросы информационной безопасности являются одним из основных препятствий на пути развития как электронной торговли, так и электронного бизнеса в целом. Было также признано, что восприятие риска в отношении