Основные аспекты профилактики киберпреступности в Республике Беларусь

В настоящее время интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека. С одной стороны, это открывает перед белорусскими гражданами и обществом ряд перспектив, с другой – влечет появление новых рисков и угроз. Так, бурное развитие телекоммуникационных технологий, стремительный рост числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий, привело к увеличению количества киберпреступлений. В материале подробно расскажем о том, что такое киберпреступность, от каких угроз и как нужно защищаться, чтобы обеспечить свою безопасности в интернете.

Что такое киберпреступность? Что относится к компьютерным преступлениям?

В настоящее время при характеристике компьютерных преступлений используется ряд понятий: информационное преступление, киберпреступление, преступление в сфере компьютерной информации, преступление в сфере высоких технологий, виртуальное преступление.

Согласно действующему законодательству Республики Беларусь в содержание понятия «компьютерная преступность» включают:

- преступления против информационной безопасности (модификация компьютерной информации, несанкционированный доступ к компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети и др.);
- хищения путем использования средств компьютерной техники;
- изготовление и распространение порнографических материалов или предметов порнографического характера, в том числе с изображением несовершеннолетнего;
- иные преступления так или иначе связанные с использованием компьютерной техники: доведение до самоубийства путем систематического унижения личного достоинства через распространение каких-либо сведений в сети Интернет, разглашение врачебной тайны, незаконное

собирание либо распространение информации о частной жизни, клевета, оскорбление, распространение ложной информации о товарах и услугах, заведомо ложное сообщение об опасности, шпионаж, умышленное либо по неосторожности разглашение государственной тайны, умышленное разглашение служебной тайны и др.

Таким образом, к компьютерным преступлениям относятся правонарушения, при совершении которых средства компьютерной техники выступают как орудия совершения преступления либо как предмет преступного посягательства.

Для справки: *в 2020 году в Республике Беларусь всего было зарегистрировано 95 тыс. преступлений, из них более 25 тыс. – компьютерные преступления (92 % от которых составляли хищения). В то же время еще в 2014 году их численность составляла всего 2,3 тыс., т. е. наблюдается рост подобных преступлений более чем в 10 раз.*

Какова цель киберпреступников?

Как правило, киберпреступники выдают себя за людей из действующих на законных основаниях организаций и учреждений, чтобы обманом вынудить граждан раскрыть личную информацию и предоставить преступникам деньги, товары и/или услуги.

Мишенью киберпреступников становятся информационные ресурсы, принадлежащие банковскому сектору, государственным органам и коммерческим организациям, а также конфиденциальная информация, персональные данные, имущество и денежные средства граждан.

Какие виды киберпреступлений выделяют в отношении граждан?

Наиболее распространенным видом проявления киберпреступности является хищение денежных средств с карт-счетов граждан. Причем в большинстве случаев эти преступления становятся возможны в результате беспечных действий потерпевших, предоставивших реквизиты доступа к своим банковским счетам.

Для справки: *за первые месяцы 2021 года зафиксирован рост количества хищений с банковских карточек белорусов более чем на 270 % по сравнению с этим же периодом 2020 года.*

Преступники завладевают реквизитами, необходимыми для осуществления преступных транзакций, посредством следующих способов.

1. **Фишинг** (от англ. fishing – 'рыбная ловля'). В качестве своеобразной удочки преступники используют специально созданный интернет-сайт с формой ввода на нем реквизитов доступа к банковскому счету, а в качестве наживки – некий сообщенный потерпевшему предлог для перехода на этот сайт и заполнения платежных реквизитов.

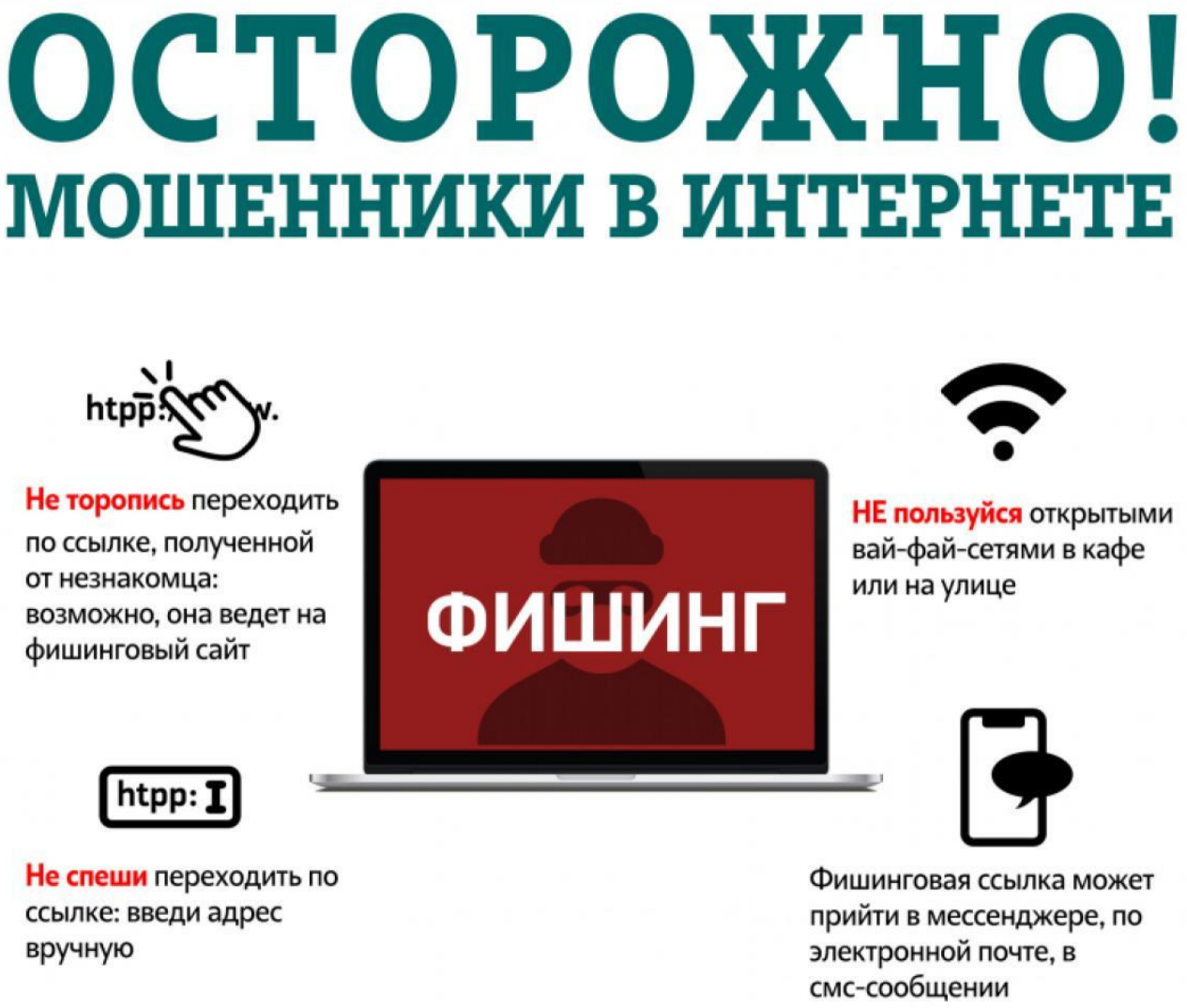
К примеру, преступник отслеживает на сайте kufar.by свежие объявления о продаже чего-либо. Просмотрев абонентский номер автора объявления, находит его в одном из мессенджеров (Viber, Telegram, WhatsApp) и вступает в переписку, якобы желая купить выставленный на продажу предмет. Затем пересылает в мессенджере ссылку на поддельную страницу предоплаты, где продавцу нужно ввести реквизиты своей карты для того, чтобы получить деньги от покупателя. При переходе по гиперссылке невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением сайтов известных сервисов (Куфар, ЕРИП, CDEK, Белпочта, сайты различных банков и др.). Адрес поддельной веб-страницы также может напоминать реальный (kufar-dostavka.by, erip-online.com, belarusbank24.xyz, cdek-zakaz.info и др.). Если жертва попадется на удочку и заполнит форму, соответствующие реквизиты доступа к банковскому счету оказываются у преступника. Через считанные минуты злоумышленник осуществляет доступ к банковскому счету и переводит денежные средства на контролируемые им банковские счета или электронные кошельки, зарегистрированные на подставных лиц.

Для справки: *наиболее часто для совершения такого вида киберпреступлений в Беларуси в 2020 году использовалась интернет-площадка «Kufar». Так, в 2018 году посредством нее было совершено 51 преступление, в 2019 году – 126, в первом полугодии 2020 года – 102, во втором полугодии 2020 года – 3 778.*

Гиперссылки на фишинговые сайты могут пересылаться не только в ходе переписки в мессенджерах, но и при общении в социальных сетях, а также размещаться на других сайтах, якобы что-то продающих или покупающих.

В последнее время участились случаи создания фишинговых сайтов, ориентированных под запросы пользователей в поисковых системах. Граждане попадают на них прямо из Google и Яндекса после запросов типа «Беларусбанк личный кабинет», «Белагропромбанк интернет-банкинг» и т. д. Увидев знакомый заголовок и логотип сайта в выдаче результатов поиска, но не удостоверившись в соответствии адреса сайта действительному доменному имени банковского учреждения, потерпевший заполняет открывшуюся форму авторизации, данные которой отправляются не банку, а преступнику.

Для справки: *часто при подмене оригинальных сайтов фишинговыми в именах данных ресурсов указаны наименования, созвучные с названиями банковских учреждений и сервисов: belarusbank-erip.online, ibank-belapb24.com, epey.by, e-rip.cc, erip.cc и иные. Пройдя по такому фальш-адресу и введя конфиденциальные сведения, человек отправит их мошеннику.*



2. Помощь другу.

Данный способ преступлений был наиболее распространен в 2017–2019 годах, но не потерял своей актуальности он и сегодня. Сначала преступники путем подбора пароля или фишинга осуществляют несанкционированный доступ (взлом) к страницам социальных сетей (в основном ВКонтакте). После этого иным пользователям, добавленным в раздел «Друзья» взломанной страницы, рассылаются сообщения с просьбой предоставить фотографию или данные банковской платежной карты под различными предлогами, например, чтобы срочно сделать какой-то безналичный платеж, так как карточка обратившегося якобы заблокирована. Также злоумышленник, скрывающийся под именем друга, может просить перевести ему на карту определенную сумму денег в связи с внезапным попаданием в сложную жизненную ситуацию. Доверчивый пользователь, полагая, что общается с настоящим владельцем страницы, переводит деньги либо сообщает преступнику реквизиты своей банковской карты (а часто и код безопасности, высылаемый в SMS-сообщении банковским учреждением), после чего с его карт-счета похищаются денежные средства.

Для справки: *еще одним видом мошенничества в социальных сетях, связанным с помощью другим людям, является деятельность фальшивых благотворительных фондов, которые осуществляют сбор денег на лечение. В таких случаях мошенники создают группу и распространяют информацию о том, что якобы нужны средства для лечения тяжелобольного человека (особенно часто ребенка). Чтобы не попасться на удочку мошенников, необходимо всегда запрашивать документы и дополнительные сведения.*

3. **Вишинг** (от англ. voice fishing – 'голосовой фишинг' или 'голосовая рыбная ловля'). Данный способ выражается в осуществлении звонка на абонентский номер потерпевшего или в его аккаунт в мессенджере (в основном это Viber или Telegram). В ходе голосового общения преступник представляется работником банка или правоохранительного органа (МВД, КГБ, Следственного комитета) и под вымышленным предлогом (пресечение подозрительной транзакции, повышение уровня безопасности пользования картой, перепроверка паспортных данных владельца банковского счета и т. д.) выясняет у потерпевшего сведения о наличии банковских платежных карточек, сроках их действия, CVV-кодах (трехзначный код на обратной стороне карты), паспортных данных, SMS-кодах с целью хищения денежных средств. В ряде случаев

злоумышленникам известны некоторые реквизиты банковских платежных карточек, а также анкетные данные лиц, на имя которых они выпущены. В большинстве случаев при совершении звонков преступники используют IP-телефонию.

Для справки: *упрощенно IP-телефония – система телефонной связи посредством сети Интернет, предоставляющая возможность осуществления звонков и голосового общения из специальных приложений с абонентами мобильных и стационарных телефонных сетей. При таком входящем звонке жертва видит на экране мобильного телефона либо подменный номер, либо короткий номер банка: современные протоколы мобильной телефонии и различные компьютерные программы позволяют осуществлять подобные телефонные звонки. Свои услуги в этом предлагают различные платные сервисы и сайты.*

Для того чтобы достоверно установить, является ли номер, с которого поступил звонок, абонентским номером телефонной сети или идентификатором IP-телефонии, необходимо направить запрос (запросы) в соответствующие телекоммуникационные организации Республики Беларусь.

Последствия использования злоумышленниками подобного способа мошенничества бывают весьма печальными. Так, например, в конце марта 2021 года злоумышленник позвонил через Viber 66-летней жительнице Борисова и представился сотрудником службы безопасности банка. Он сообщил, что в целях пресечения хищения с банковской платежной карточки женщине необходимо установить определенное приложение удаленного доступа, сообщить коды карты и прислать скриншоты из мобильного банкинга, что она и сделала. Позже, заподозрив неладное, пенсионерка пошла в банк и обнаружила, что с ее карт-счета пропало почти 40 тысяч рублей.

4. **Свободный доступ к банковской карте.** Не всегда для хищения с банковских счетов используются хитрые схемы. В ряде случаев причинами этого становятся утеря банковских карт, оставление их в легкодоступном месте, передача иным лицам для осуществления разовых платежей. При этом увеличивает риск остаться без заработанных денежных средств хранение PIN-кода рядом с картой (например, записанным на бумажке в кошельке или непосредственно на банковской карте). Разновидностью подобного легкомыслия является хранение фотоизображений банковских карт или платежных реквизитов в памяти мобильного телефона, в почтовом аккаунте или дистанционном облачном хранилище. При несанкционированном доступе к такому хранилищу преступник получает и беспрепятственный доступ к банковскому счету его владельца.

5. **Покупка с предоплатой.** Наиболее примитивной, но от этого не менее работающей формой интернет-мошенничества является размещение преступниками на виртуальных досках объявлений, тематических сайтах, в социальных сетях, группах интернет-мессенджеров объявлений о продаже каких-либо товаров по «бросовым» ценам. Однако для получения товара (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту или электронный кошелек. Правда, после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

6. **Шантаж.** В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства. К примеру, получив несанкционированный доступ к интернет-ресурсам (страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам) и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в сети Интернет.

7. **Иные мошенничества.** Также можно выделить еще несколько типов мошенничества, которые в недавнем прошлом часто успешно использовались на территории Республики Беларусь:

- просьбы пополнить счет определенного номера мобильного телефона или платежной карты в виде «Мама, пополни счет на 20 рублей. Мне не перезванивай – позже перезвоню. Нужно срочно!»;
- звонок с номера друга или родственника, в котором собеседник утверждает, что он сотрудник правоохранительных органов, просит вознаграждение, обещая предотвратить возбуждение уголовного дела в отношении близкого человека;
- когда мошенник звонит и сразу отменяет вызов, перезвонив на отобразившийся номер, абонент слышит автоответчик или гудки, в это время со счета его мобильного телефона списываются деньги, так как вызов совершается с применением переадресации на платный номер;
- когда приходит SMS-сообщение о некоем выигрыше, после чего абоненту предлагают отправить платное сообщение в ответ или отправить небольшую сумму на банковскую карту для получения «выигрыша»;
- когда приходит SMS-сообщение с гиперссылкой, пройдя по которой пользователь запускает процесс скачивания вируса;
- когда поступает звонок от «представителя сотового оператора», во время которого злоумышленники предлагают перерегистрировать SIM-карту, при этом пользователь вводит специальный код или отправляет SMS-сообщение, после чего с баланса его мобильного телефона списываются деньги;
- когда приходит SMS-сообщение или поступает звонок, в ходе которого сообщается, что абонент не оплатил штраф, после этого человеку предлагается произвести его оплату, перечислив деньги на «специальный» расчетный счет или пополнив банковский счет;
- когда приходит SMS-сообщение с информацией о том, что платежная карта заблокирована, и указывается номер, по которому можно получить справку или помощь; после звонка у абонента запрашивают PIN-код, CVV-код (трехзначный код на обратной стороне карты), номер карты и другие данные, необходимые для снятия денег с банковского счета.

Какие способы мошенничества бывают в отношении юридических лиц и индивидуальных предпринимателей?

Киберпреступления причиняют ущерб не только гражданам. Часто действия злоумышленников направлены на завладение денежными средствами юридических лиц (предприятий, учреждений и организаций) и индивидуальных предпринимателей. Однако и здесь главным условием, дающим возможность совершения подобных злодеяний, является человеческий фактор, т. е. грубые ошибки, допускаемые работниками: от руководителей до секретарей, бухгалтеров и менеджеров. Все чаще

потерпевшими становятся юридические лица и индивидуальные предприниматели, которые осуществляют деятельность при помощи зарубежных контрагентов.

Среди наиболее типичных форм посягательств хакеров на денежные средства и охраняемую информацию юридических лиц являются **BEC-атаки** (от англ. business email compromise – 'компрометация бизнес-переписки'). Реализация подобной схемы хищения возможна посредством получения несанкционированного доступа к электронной почте одной из сторон сделки. В этой ситуации злоумышленники обладают информацией о предмете, условиях договора и могут вести переписку, не вызывая подозрений (в случае необходимости ими направляются дополнительное соглашение, счет-проформа (инвойс) с измененными реквизитами банковского счета и контактными данными представителей фирмы путем их «наложения» на подготовленные ранее и сохраненные в сообщениях документы).

Кроме того, имеются случаи, когда от имени белорусских субъектов хозяйствования после взлома их корпоративной почты в адрес зарубежных партнеров также направлялись письма, счета-проформы с измененными банковскими реквизитами. В результате денежные средства, причитающиеся белорусским предприятиям за произведенную (поставленную) продукцию, переводились на счета мошенников.

Также возможна ситуация, когда после согласования существенных условий контракта с зарубежным партнером, а в отдельных случаях и его подписания, на электронную почту организации (предприятия) преступниками направляется сообщение якобы от имени сотрудника иностранного контрагента об изменении реквизитов обслуживающего банка и необходимости перечисления денежных средств на новый счет. При этом адрес электронной почты мошенников имеет существенное сходство с реальным, что часто остается незамеченным. Последующая переписка уже осуществляется с киберпреступниками. Далее под предлогом оплаты товаров иностранных компаний и вследствие предоставления по электронной почте ложных банковских реквизитов на счета мошенников перечисляются денежные средства со стороны субъектов хозяйствования как государственного, так и частного сектора экономики.

Как не стать жертвой киберпреступления?

1. Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и банковских карт, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов при отсутствии возможности достоверно убедиться, что эти люди те, за кого себя выдают.

В случае поступления звонка от «сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк. Необходимо принимать во внимание, что реальному сотруднику банка известна следующая информация: фамилия

держателя карты, паспортные данные, какие карты оформлены, остаток на счете.

Не следует сообщать в телефонных разговорах (даже сотруднику банка), а также посредством общения в социальных сетях полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

В случае если «сотрудник банка» в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, необходимо отвечать, что вы придете в банк лично, ведь все подобные вопросы нужно решать в отделении банка, а не по телефону.

Внимание! Помните, что сотрудники банковских учреждений никогда не используют для связи с клиентом мессенджеры (Viber, Telegram, WhatsApp).

2. Для осуществления онлайн-платежей необходимо использовать только надежные платежные сервисы, обязательно проверяя доменное имя ресурса в адресной строке браузера.

3. Не следует хранить банковские карты, их фотографии и реквизиты в местах, которые могут быть доступны посторонним лицам; это же относится к фотографиям и иным видам информации конфиденциального характера.

4. Следует воздерживаться от осуществления онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги, благотворительной и спонсорской помощи в пользу организаций и физических лиц при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают.

5. Не стоит перечислять денежные средства на счета электронных кошельков, карт-счета банковских платежных карточек, счета SIM-карт по просьбе пользователей сети Интернет.

6. Для доступа к системам дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг), электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам необходимо использовать сложные пароли, исключающие возможность их подбора. Стоит воздержаться от следующих паролей: дат рождения, имен, фамилий, т. е. тех, которые легко вычислить из общедоступных источников информации (например, социальных сетей).

7. При составлении платежных документов важно проверять платежные реквизиты получателя денежных средств.

8. При поступлении в социальных сетях сообщений от лиц, состоящих в категории «Друзья», с просьбами о предоставлении реквизитов банковских платежных карточек не следует отвечать на подобные сообщения, необходимо связаться с данными пользователями напрямую посредством иных средств связи.

9. При обнаружении факта взлома аккаунтов социальных сетей необходимо незамедлительно восстанавливать к ним доступ с помощью службы поддержки либо блокировать, а также предупреждать об этом факте лиц, с которыми общались посредством данных социальных сетей.

10. Нельзя открывать файлы, поступающие с незнакомых адресов электронной почты и аккаунтов мессенджеров, переходить по ссылкам в сообщениях о призах и выигрышах.

11. Необходимо использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему, установить антивирусную программу не только на персональный компьютер, но и смартфон, планшет, и регулярно обновлять ее.

12. Следует ознакомить с перечисленными правилами безопасности своих родственников и знакомых, которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.

Какие советы можно дать юридическим лицам, чтобы обезопасить себя от мошенничества?

1. Выработать четкий план реагирования и ознакомить работников с перечнем сведений, относящихся к коммерческой, служебной и иной тайне.

2. Исключить в своей деятельности использование бесплатных почтовых сервисов, а также принимать дополнительные меры защиты корпоративной электронной почты (подключение двухфакторной аутентификации, соблюдение требований к сложности пароля и периодичности его смены, использование антивирусного программного обеспечения).

3. Неукоснительно соблюдать правила пользования системой дистанционного банковского обслуживания.

4. Создавать резервные копии данных и хранить их на съемных носителях.

5. Проверять правильность адреса электронной почты контрагента при получении и отправке сообщений, а также поддерживать контакт с его представителем и согласовывать ключевые вопросы дополнительно посредством иных средств связи (телефонных переговоров, использования факсимильной связи, мессенджеров и проч.).

6. Не использовать рабочие устройства в личных целях, а служебные ящики электронной почты – для регистрации на торговых и развлекательных онлайн-площадках.

7. Наладить строгий действенный контроль за соблюдением утвержденных мер информационной безопасности (соответствие программного обеспечения, проверка отсутствия несанкционированного доступа к внешним информационным ресурсам и т.д.