Количество пользователей сети интернет в Республике Беларусь и их сетевая активность имеют устойчивую тенденцию роста. Пользователи сети Интернет активно пользуются различными социальными сетями и абсолютное большинство из них пользуются социальными сетями с мобильных устройств. Например, количество белорусских посетителей ВКонтакте оценивается в 3,5 млн., Одноклассники - около 2,7 млн., рекламная аудитория Instagram составляет 2,1 млн. пользователей, Facebook- 1 млн.

В Беларуси около 11,87 млн. мобильных абонентов (126% населения), широкополосный доступ имеют 62% абонентов.

Согласно исследованиям, 85% белорусов имеет счёт в банке, 54 % делают покупки или оплачивают счета через интернет. Количество выданных банковских платежных карточек на январь 2020 года по данным Национального банка Республики Беларусь превысило 15,5 млн., инфраструктура их обслуживания включает более 121 тыс. объектов торговли и сервиса, более 4200 банкоматов, 3100 инфокиосков.

Указанные темпы проникновения информационных технологий и безналичных платежей во все сферы жизнедеятельности человека наряду с имеющей место неквалифицированностью и неосмотрительностью определенной части пользователей являются предпосылкой возрастающего количества компьютерных инцидентов.

В законодательстве Республики Беларусь предусмотрена ответственность, в том числе уголовная за совершение противоправных деяний в сфере высоких технологий.

Уголовным кодексом предусмотрен ряд преступлений, отнесенных к компетенции подразделений по раскрытию преступлений в сфере высоких технологий. Рассмотрим их подробнее.

Статья 212. Хищение путем использования компьютерной техники

Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

То же деяние, совершенное повторно, либо группой лиц по предварительному сговору, либо сопряженное с несанкционированным доступом к компьютерной информации,-

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, -

наказываются лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Необходимо отметить, что ответственность за деяния, предусмотренные ст.212, наступает с 14-летнего возраста.

Примером такого преступления может быть хищение денежных средств с найденной либо похищенной банковской платежной карточки с использованием банкомата, платежного терминала. В последнее время наиболее актуальны факты хищений с использованием реквизитов карт при осуществлении интернет-платежей, произведении расчетов на торговых площадках.

Статья 349. Несанкционированный доступ к компьютерной информации

Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, -наказывается штрафом или арестом.

Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, -наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Например - несанкционированный доступ (открытие и просмотр файлов, писем, переписки) к электронной почте, учетным записям на различных сайтах, в том числе в социальных сетях, к информации, содержащейся на компьютере, в смартфоне и защищенной от доступа третьих лиц.

Статья 350. Модификация компьютерной информации

Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации) - наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

Модификация компьютерной информации, сопряженная с

несанкционированным доступом к компьютерной системе или сети либо повлекшая по неосторожности последствия, указанные в части 3 статьи 349 Кодекса,-наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

В качестве примера можно привести произведенные изменения компьютерной информации: переписка в электронной почте, в социальной сети, в мессенджере с правами другого пользователя; изменение текстовой, графической и иной информации; внесение изменений в защищенные базы данных и т.д.

Статья 351. Компьютерный саботаж

1. Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж) -

наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.

2. Компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия, - наказывается лишением свободы на срок от трех до десяти лет.

Здесь мы говорим об умышленном уничтожении (удалении, приведении в непригодное состояние, шифровании) компьютерной информации либо ее блокировании (например, путем смены пароля доступа, изменении графического ключа и т.д.).

Статья 352. Неправомерное завладение компьютерной информацией Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда, -

наказываются общественными работами, или штрафом, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

В данном случае учитываются действия, связанные с копированием какой-либо значимой информации, повлекшие причинение существенного вреда. К примеру - копирование писем из электронной почты, личной переписки из социальных сетей, закрытых для просмотра третьими лицами фотографий с компьютера.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети -

наказываются штрафом, или арестом, или ограничением свободы на срок до двух лет.

Статья достаточно специфична и применяется при разработке, изготовлении и сбыте специальных программ и устройств, предназначенных для осуществления несанкционированных доступов, например, поддельных смарт-карт для просмотра закодированных каналов спутникового телевидения.

Статья 354. Разработка, использование либо распространение вредоносных программ

Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами -

наказываются штрафом, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Те же действия, повлекшие тяжкие последствия, - наказываются лишением свободы на срок от трех до десяти лет.

К уголовной ответственности по данной статье могут быть привлечены лица за разработку вредоносного программного обеспечения, а также разработку и использование вирусов, например, блокирующих смартфоны либо шифрующих компьютерную информацию на серверах.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда, - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.

То же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности, -наказывается лишением права занимать определенные должности или заниматься определенной деятельностью, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, -

наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Указанная статья может быть применена к лицам, имеющим доступ к компьютерным сетям и системам, в которых хранится значимая информация, халатные действия которых привели к нарушению функционирования таких систем.

Ответственность за деяния, предусмотренные cm. cm. 349-355, наступает с 16-летнего возраста.

Также с использованием сети Интернет может совершаться ряд иных уголовно наказуемых противоправных деяний:

мошенничество (ст.209 УК);

причинение имущественного ущерба без признаков хищения (ст.216 УК);

изготовление и распространение порнографических материалов или предметов порнографического характера (ст.343 УК, ст.343-1 УК);

клевета (ст.188 УК);

оскорбление (ст.189 УК);

разжигание расовой, национальной или религиозной вражды или розни (ст.130 УК) и иные.

На территории Слонимского района за 11 месяцев 2020 года наблюдается значительный рост +60 (по сравнению с 2019 годом) преступлений, связанных с завладением реквизитами пластиковых банковских карт и хищением средств с карт-счетов граждан, а также в сфере высоких технологий. Следует отметить, что, если ранее превалировали преступления, связанные со «взломом» и несанкционированным использованием учетных записей пользователей в социальных сетях с целью выманивания реквизитов банковских платежных карточек, . то в настоящее время хищения с карт-счетов граждан совершаются путем обмана граждан на торговых площадках при размещении ими объявлений о продаже различных товаров, а также при осуществлении звонков под видом сотрудников банков. В обоих случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению безопасного использования сети Интернет и некоторым несовершенством банковских инструментов.

Так, в 2020 году Слонимским РОСК возбуждено 113 уголовных дел по ст. 212 УК Республики Беларусь, 13 уголовных дел по ст. 349 УК Республики Беларусь, 1 уголовное дело по ст. 354 УК Республики Беларусь. Республики Беларусь. По большинству возбужденных уголовных дел, лица, совершившие преступления, не установлены.

Необходимо отметить, что преступность в сфере высоких технологий характеризуется высокой степенью латентности, в результате чего реальное количество киберинцидентов существенно выше.

В последнее время распространены следующие типичные ситуации, связанные с хищением денежных средств с карт-счетов граждан:

- граждане размещают объявления на торговой площадке Kufar.by о продаже различных товаров. После размещения объявления злоумышленник в мессенджере «Viber» либо «WhatsApp» связывается с гражданином, который разместил объявление. Затем интересуется актуально ли объявление, задает вопросы, касательно качества, характеристик товара, может согласиться сразу приобрести товар и предлагает перевести деньги продавцу на карточку, а также указывает, что можно воспользоваться услугой доставки товара через «Европочту» или «Белпочту», т.е. указывает, что после оплаты товара к продавцу придет курьер, который доставит товар покупателю (преступнику), при этом преступник указывает свои вымышленные данные и любой адрес места жительства на территории Республики Беларусь, либо их не указывает, сбрасывает покупателю фишинговую (имитирующую настоящий) ссылку на указанные службы доставки (например настоящий сайт имеет название Belpost.by., а фишинговый сайт может иметь различные названия, схожие с настоящим, например, Belpost.be, Belpost.site, Belpost.kz и др.) Покупатель переходит по данной ссылке, где система просит его ввести данные карты, CVV-кода, расположенный на обратной стороне карты, затем продавцу товара на мобильный телефон приходит код, который он в ходе переписки сообщает преступнику, затем, с карт-счета продавца моментально списываются все его денежные средства, после этого преступник на связь не выходит.

- гражданам, зачастую пожилым лицам, лицам пенсионного возраста (далее потерпевшие) на мобильный телефон, стационарный телефон, в мессенджерах поступают звонки с различных телефонов (при этом номера могут определяться как номера белорусских операторов связи, зарубежных операторов связи, номера под названием банков и др). Звонившее лицо, (далее преступник) представляется сотрудником банка (специалистом, менеджером, сотрудником службы собственной безопасности, может называть свои вымышленные данные). Зачастую преступники знают данные лиц, которым они звонят (например, фамилию или имя и отчество, которые могут получить из различных открытых источников, иногда преступники знают номер карты потерпевшего и им нужен код с обратной стороны карты и код, который поступит через сообщение на мобильный телефон). Преступник заводит доверительную беседу с потерпевшим и указывает, что по банковской карте наблюдается активность или с карты пытаются похитить деньги и на нее необходимо установить дополнительную защиту, интересуются у потерпевшего сколько у него имеется карт, каких банков, если преступник изначально представился представителем не того банка, то он указывает потерпевшему, что имеется возможность проводить операции по картам других банков, либо переключает на оператора другого банка и с потерпевшим продолжает беседу другой человек. Преступник делает все возможное путем различных уговоров и комбинаций, чтобы получить от потерпевшего данные карты, CVV-код, расположенный на обратной стороне карты и пришедший через смс-сообщение на телефон потерпевшего код. Потерпевшие без всяких затруднений передают вышеуказанные данные, после чего с банковской карты потерпевшего мгновенно списываются денежные средства на счета преступников, которые как правило, находятся за пределами Республики Беларусь.

Необходимо отметить, что совершение транзакций по банковским платежным карточкам самим владельцем, либо нарушение правил пользования карточками, выразившееся в передаче платежных реквизитов третьим лицам, практически не оставляет шансов вернуть денежные средства с использованием действующего в Беларуси принципа нулевой ответственности пользователей банковских карточек.

Как показывает практика, большинство потерпевших, столкнувшихся с подобными ситуациями, указывают, что про подобные способы хищения денежных средств с карт-счетов им ничего известно не было.

Согласно ст. 5 Закона Республики Беларусь от 04.01.2014 № 122-3 «Об основах деятельности по профилактике правонарушений, следует, что одним из субъектов профилактики являются местные исполнительные и распорядительные органы, которые согласно ст. 10 указанного Закона осуществляют меры общей профилактики в виде правового просвещения граждан куда можно отнести семинары, лекции выступления по вопросам профилактики правонарушений, размещение в общественных местах, зданиях (помещениях) организаций, государственных средствах массовой информации, в том числе распространяемых с использованием глобальной компьютерной сети Интернет на официальных сайтах субъектов профилактики информации о формировании правопослушного поведения, навыков по обеспечению личной и имущественной безопасности граждан, иные формы в соответствии в соответствии с актами законодательства.

Учитывая изложенное, приведем некоторые рекомендации для пользователей сети интернет, которые могут снизить вероятность совершения в отношении них противоправных деяний:

* для выхода в сеть интернет используйте устройства, на которых установлено специальное программное обеспечение, предназначенное для борьбы с вредоносной активностью, своевременно обновляйте его;
* используйте операционную систему с установленными обновлениями безопасности, актуальные версии другого программного обеспечения, скачанные из официальных магазинов приложений;
* при использовании известных Вам сайтов, обращайте внимание на их внешний вид и адрес: возможно Вы зашли на поддельную его копию;
* вводите личную информацию только на веб-сайтах, работающих с использованием защищенных протоколов (обычно в браузере рядом с адресом такого сайта отображается значок замка на зеленом фоне);
* не используйте одинаковые логины и пароли на различных сайтах;
* не используйте слишком легкие пароли, либо те, о которых можно легко догадаться (даты рождения, номера телефонов и т.д.), периодически изменяйте свои пароли;
* по возможности используйте двухфакторную аутентификацию, когда кроме ввода логина и пароля необходимо вводить временный код, отправляемый обычно на мобильный телефон в виде SMS-сообщения либо push-уведомления;
* остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях;
* с осторожностью относитесь к письмам, в которых запрашиваются данные счетов (финансовые учреждения почти никогда не запрашивают финансовую информацию по электронной почте), никогда не отправляйте финансовую информацию по незащищенным интернет-каналам;
* при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно необходимо проверить данную информацию с использованием других каналов связи (личная встреча, телефонный звонок, мессенджер, поддерживающий голосовую связь), либо в крайнем случае идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам;
* не храните реквизиты карты в открытом доступе, в том числе в виде фотографий, не передавайте карту третьим лицам;
* если Вы не используете банковскую платежную карточку для осуществления интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;
* используйте для платежей в сети интернет специализированные карточные продукты с отдельным счетом, обязательно подключите SMS- информирование о совершении расходных транзакций;
* при осуществлении интернет-платежей по возможности используйте технологии обеспечения дополнительной безопасности платежей, такие как 3-D Secure для международных платежных систем Visa и MasterCard или Интернет Пароль для платежной системы БЕЛКАРТ;
* не передавайте посторонним лицам никакой информации о данных своих банковских карт, поступающие Вам коды (настоящий сотрудник банка Вам не будет звонить и спрашивать у Вас информацию о карте, так как он ее самостоятельно может получить в банке);
* не вводите реквизиты своих карт на подозрительных Вам сайтах;
* в случае получения информации о несанкционированном списании средств с карточки незамедлительно принимайте меры к ее блокировке путем обращения в службу поддержки банка по телефону либо через интернет-банкинг, а также обращайтесь в банк с целью инициирования процедуры опротестования мошеннических транзакций, а также рассмотрения возможности возврата денежных средств в соответствии с принципом нулевой ответственности.

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, но в общем можно предложить пользователям в любой ситуации не терять бдительность и критическое отношение к происходящему в сети интернет.