Материалы к теме: «Профилактика киберпреступлений, ответственность граждан за их совершение»

Вслед за развитием информационных технологий, их проникновением во все сферы жизнедеятельности человека закономерно растет количество регистрируемых 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

1. 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.

2. 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.

3. 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 с конфискацией имущества или без конфискации и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

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

наказываются лишением свободы на срок от шести до пятнадцати лет с конфискацией имущества 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, а также с использованием реквизитов карт при осуществлении интернет-платежей.

Статья 349. Несанкционированный доступ к компьютерной информации

1. 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.

2. 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.

3. 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

1. 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.

2. 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

1. 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.

2. 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

1. 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.

2. 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.

3. 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 *ст.ст.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.

В 2019 году на территории области наблюдался более чем трехкратный рост количества зарегистрированных киберпреступлений. За 12 месяцев учтено 930 таких преступлений (+630 к прошлому году или +210,0%), 66% из которых – хищения путем использования компьютерной техники. Общая сумма ущерба по преступлениям (с учетом покушений) в области превысила 446 тысяч рублей, в республике – 6,4 миллиона рублей.

Удельный вес преступлений в сфере высоких технологий, по которым установлен подозреваемый и производство по которым окончено, в Гродненской области составил 29,2%.

За 2019 год за совершение преступлений в сфере высоких технологий к ответственности привлечено 196 лиц, что на 87 больше аналогичного периода прошлого года, из них 7 (+5) несовершеннолетних, 42 (+15) женщины, 63 (+32) – ранее судимые.

В том числе только в ноябре в области учтено 96 фактов хищений с карт-счетов граждан, 77 из которых были совершены в сети Интернет, в результате чего держатели карт потеряли около 70 тысяч рублей. Средняя сумма хищения в указанном месяце составила около 725 рублей, максимальная – 6 900 рублей. В декабре злоумышленниками причинен имущественный ущерб белорусским гражданам и организациям на сумму более 1 миллиона рублей.

Среди актуальных на сегодняшний день видов преступлений, совершаемых **в отношении физических лиц**, необходимо выделить:

– завладение денежными средствами с карт-счета с использованием социальных сетей;
– хищение с карт-счета с использованием вишинга по телефону;
– завладение денежными средствами с карт-счета с использованием фишинга;
– несанкционированный доступ к учетной записи в соцсети, электронной почте.

В отношении предприятий и организаций совершаются следующие противоправные деяния:

– блокирование компьютерной информации путем ее шифрования с целью предъявления требований о денежной компенсации за разблокировку;
– заражение ПЭВМ вредоносным программным обеспечением (банковскими троянами) с целью дальнейшего хищения денежных средств предприятия через систему дистанционного банковского обслуживания.

Рассмотрим указанные выше группы преступлений подробнее.

Зачастую имеет место ситуация, когда со взломанной либо подложной учетной записи **в соцсети** осуществляется рассылка сообщений с целью перевода денежных средств либо передачи реквизитов банковской платежной карточки либо учетной записи в системе Интернет-банк. Например:

– «Привет, у тебя есть действующая банковская карточка? Мою заблокировали, а как раз сегодня мне должны перечислить деньги. Можно я дам реквизиты твоей карты, на нее придут деньги, потом переведешь мне, когда мою карту разблокируют. В долгу не останусь!»;

– «Какого банка у тебя карточка? Мне нужна VISA или MasterCard для оплаты в интернете. Можешь дать реквизиты или сфотографировать? Там еще на обратной стороне три цифры есть. Тебе на телефон должен придти код, напиши сюда. Нет, не беспокойся, я деньги верну с комиссией.»;

– «Можешь дать логин и пароль от интернет-банкинга. В моем выдает какую-то ошибку, хочу проверить, есть ли в твоем такой баг. Платежей делать не буду, мы же друзья!»

Трендом последних месяцев 2019 года стал **вишинг** — форма мошенничества, основанная на социальной инженерии. Злоумышленники, используя телефон и играя определенную роль (чаще всего сотрудника банка), под разными предлогами выманивают персональные данные (например, реквизиты платежных карт), чтобы заполучить денежные средства клиентов банков.

Предлогом для передачи данных могут быть:

– осуществление по карте мошеннической операции и необходимость срочной ее отмены;
– оформление через интернет-банкинг онлайн-кредита и принятие срочных мер по его отклонению и т.д.

При этом в зависимости от ситуации злоумышленники пытаются завладеть следующей информацией:

– идентификационный номер и иные паспортные данные;
– номер карты, срок действия, имя владельца, CVV/CVC-код;
– коды подтверждения, приходящие на Ваш номер телефона;
– реквизиты доступа к системе Интернет-банк (логин, пароль, сеансовый ключ).

Еще одним способом завладения реквизитами является **фишинг** – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения рассылок электронных сообщений, в которых содержится ссылка на сайт, внешне неотличимый от настоящего.

После того как пользователь попадает на поддельную страницу, мошенники пытаются побудить пользователя ввести на ней свои логин и пароль доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Нередко жертвами киберпреступников становятся и белорусские предприятия и организации. В результате проведенного анализа обозначены возможные **причины заражения корпоративных ПЭВМ**:

- ошибки в настройке системы безопасности локальной сети;
- использование устаревшего либо контрафактного программного обеспечения, не поддерживаемого производителями;
- использование программного обеспечения, полученного из сомнительных источников;
- отсутствие обновляемого антивирусного программного обеспечения;
- посещение пользователями подозрительных Интернет-ресурсов;
- просмотр пользователями входящих электронных писем от незнакомых собеседников и открытие прилагаемых файлов. Зачастую злоумышленники рассылают письма с приложением документов, архивов, исполняемых файлов, под которые маскируется вредоносное программное обеспечение.

При этом все чаще именно неосмотрительные и непрофессиональные действия обычных пользователей становятся причиной ущерба для предприятий, измеряемого в некоторых случаях десятками тысяч рублей.

Во избежание различного рода киберинцидентов на уровне пользователя можно дать следующие **рекомендации**:

- использовать сложные пароли и периодически их менять;
- не сохранять пароли в браузерах, не хранить их в электронном виде или на бумажных носителях в доступных местах;
- использовать антивирусное программное обеспечение;
- устанавливать на мобильные устройства и персональные компьютеры приложения только из проверенных источников;
- не переходить по подозрительным ссылкам, не открывать подозрительные письма и вложения к ним;
- не использовать для переписки e-mail, к которому привязаны устройства, учетные записи, Интернет-банкинг;
- обмениваться сообщениями в мессенджерах только полностью удостоверившись в личности собеседника.

Держателям банковских карточек необходимо:

- внимательно ознакомиться с правилами пользования банковскими платежными карточками Вашего банка;

- не передавать карту и ее реквизиты третьим лицам, в том числе в ходе Интернет-переписки либо по телефону лицам, представляющимся сотрудниками банка;
- использовать отдельную карту для Интернет-покупок и не хранить на ней деньги;
- подключить услуги 3D-Secure, SMS-информирование, установить необходимые лимиты;
- осуществлять оплату в сети Интернет на проверенных ресурсах, работающих по безопасному протоколу https.

В любой ситуации необходимо проявлять бдительность и своими действиями не создавать условия для совершения в отношении Вас преступлений.

В случае совершения в отношении Вас противоправных деяний, рекомендуем Вам в кратчайшие сроки обратиться в органы внутренних дел по месту жительства либо обнаружения факта совершения преступления.