«Противодействие киберпреступности» (Профилактическая беседа с учащимися)

Цель мероприятия:

Способствовать воспитанию правовой культуры учащихся, выработке ценностных установок о необходимости уважения и соблюдения прав человека, показать правила безопасного использования социальных сетей, мессенджеров и электронной почты.

Задача мероприятия:

1. Развивать правовое мировоззрение и нравственные представления.
2. Воспитывать нормы правильного поведения и нравственные качества личности.
3. Воспитывать чувства ответственности за свои поступки и действия.
4. Способствовать воспитанию общественно-активной личности

Оборудование мероприятия:

1. Информационный материал.
2. Фотоаппарат.
3. Тематический стенд
4. Столы, стулья.

Профилактика киберпреступности

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

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 все чаще фиксируются факты хищений с использованием реквизитов карт при осуществлении Интернет-платежей, а также завладение денежными средствами, хранящимися на счетах различных электронных платежных систем и сервисов.

Статья 349. Несанкционированный доступ к компьютерной информации

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

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

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

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

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

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

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

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.

Наблюдается отчетливая тенденция роста количества фактов совершения противоправных деяний в сети Интернет, которые выражаются, с одной стороны, во «взломе» и несанкционированном использовании учетных записей пользователей в социальных сетях, а с другой стороны – в совершении хищений с карт-счетов граждан путем мошенничества либо использования компьютерной техники. И в обоих случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению безопасного использования сети Интернет.

Сначала преступник получает несанкционированный доступ к средству связи с потенциальным потерпевшим, обычно это учетные записи в социальных сетях, электронные почтовые ящики, аккаунты в различных программах, предназначенных для обмена сообщениями, например, Skype. Обычно это становится возможным ввиду небрежного отношение владельца сайта к обеспечению сохранности конфиденциальной информации (логинов, паролей) о пользователях либо беспечности самих пользователей. При этом такая беспечность со стороны пользователей может проявляться в

- попадании на удочку лиц, создавших «фишинговый» (имитирующий настоящий) сайт;
- вводе логинов и паролей от своих учетных записей в соцсети или электронных почтовых ящиков на иных, не имеющих отношения к функционированию указанных сервисов, сайтах;
- использовании идентичных реквизитов для авторизации на различных ресурсах;
- использовании слишком легких паролей;

- отсутствии на устройствах средств, позволяющих блокировать работу вредоносных программ и др.

Получив реквизиты, злоумышленник заходит в учетную запись жертвы и осуществляет рассылку контактам владельца взломанной учетной записи сообщения мошеннического характера.

Следует констатировать, что фантазия преступников безгранична, вариантов формулировок таких просьб множество, приведем некоторые примеры таких сообщений:

- «Вася (к примеру), я нахожусь в России, у меня украли кошелек и телефон. Срочно нужны деньги на билет домой. Отправь мне на карт-счет (здесь может быть мобильный номер телефона, кошелёк в электронных платежных системах Яндекс.Деньги, QIWI, WebMoney или других) 5000 (мошенник имел ввиду российских, знал бы он, что в Беларуси указанная сумма столь существенна, он бы уточнил) рублей. Все верну по приезду.»;

- «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 отдашь мне. В долгу не останусь!»;

- «Я помогаю в сборе средств для лечения моей дальней родственницы, у нее серьезная болезнь, нужно много денег. Перечисли, если есть возможность, хоть какую-то сумму на кошелек».

В случае, когда потерпевший отзывается на уловку преступника и, будучи обманутым, сам осуществляет перевод средств на предложенные реквизиты, в действиях злоумышленника усматривается состав преступления, предусмотренного статьей 209 Уголовного кодекса Республики Беларусь «Мошенничество» (в зависимости от суммы похищенного максимальная ответственность может составлять как три, так и десять лет лишения свободы).

Когда имеет место предоставление потерпевшим платежных реквизитов и осуществление транзакций злоумышленником путем их ввода на различных сайтах, поддерживающих возможность совершения платежных операций, имеет место статья 212 «Хищение путем использования компьютерной техники» (также в зависимости от суммы максимальное наказание варьируется от 3 до 15 лет лишения свободы, при этом Законом не предусмотрена минимальная сумма хищения). При этом надеяться на то, что преступник в данной ситуации оставит на Вашем карт-счете хоть какую-то сумму, к сожалению, не приходится.

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.

Преступления в сфере высоких технологий и защита от них

За сравнительно небольшой промежуток времени количество пользователей сети Интернет в Республике Беларусь превысило пять миллионов человек. Сегодня по плотности проникновения широкополосного доступа на 100

человек Беларусь вышла на среднеевропейские показатели, а по скорости – на третье место в мире.

Количество абонентов сотовой связи продолжает увеличиваться. Указанные темпы проникновения информационных технологий во все сферы жизнедеятельности человека наряду с имеющей место неквалифицированностью определенной части пользователей являются предпосылкой возрастающего количества компьютерных инцидентов.

Учитывая изложенные выше факты, 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;

- при использовании известных Вам сайтов, обращайте внимание на их внешний вид: 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.);

- 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;

- если Вы не используете банковскую платежную карточку для осуществления Интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты.