ПАМЯТКА
по профилактике киберпреступлений

Киберпреступление – вид правонарушения, непосредственно связанного с использованием компьютерных технологий и сети Интернет, включающий в себя распространение вирусов, нелегальную загрузку файлов, кражу персональной информации, хищение имущества.

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 киберпреступлений:

Статья 212. Хищение имущества путем модификации компьютерной информации
(ответственность наступает *с 14 лет*) *Наказывается штрафом или арестом, или ограничением свободы, или лишением свободы от 2 до 12 лет.*

Самыми распространенными схемами преступлений ст. 212 УК Республики Беларусь являются:

- Хищение денежных средств со счета найденной либо похищенной банковской платежной карточки (далее – БПК) с использованием банкомата, платежного терминала. В последнее время наиболее актуальны факты хищений с использованием реквизитов карт при осуществлении интернет-платежей (покупки в интернет магазинах, оплата подписок на различных сайтах, оплата различных бонусов в онлайн-играх и т.д.), а также завладение денежными средствами, хранящимися на счетах различных электронных платежных систем и сервисов (когда логин и пароль от электронной платежной системы стал известен преступнику)
- Хищение денег абонентов сотовой связи через мобильный банкинг.

Статья 349. Несанкционированный доступ к компьютерной информации (ответственность *с 16 лет) Наказывается штрафом или ограничением свободы, или лишением свободы до 7 лет.*

Например – несанкционированный доступ (открытие и просмотр файлов, писем, переписки личных данных пользователя и т.п., в нарушение установленного законодательством порядка) 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.

С*татья 350. Уничтожение, блокирование или модификация компьютерной информации *(наказывается штрафом или ограничением свободы, или лишением свободы от 3 до 10 лет)* (ответственность *с 16 лет)

Например, произведенные изменения компьютерной информации в системе либо сети, которые затрудняют либо исключают ее дальнейшее использование.

Статья 351. Компьютерный саботаж *(наказывается штрафом или ограничением свободы, или лишением свободы до 10 лет)* (ответственность *с 16 лет)*

*Например, у*мышленное уничтожение (удаление, приведение в непригодное состояние, шифрование) компьютерной информации либо ее блокирование (например, путем смены пароля доступа, изменении графического ключа и т.д.).

Статья 352. Неправомерное завладение компьютерной информацией

(наказывается штрафом или арестом, или ограничением свободы, или лишением свободы от 2 до 7 лет) **(ответственность *с 16 лет)*** *В данном случае учитываются действия, связанные с копированием какой-либо значимой информации (в обязательном порядке не находящейся в открытом доступе, т.е. защищенной паролем, либо содержание логинов и пароле от учетных записей полученные путем их «взлома»), повлекшие причинение существенного вреда.*
К примеру – копирование писем из электронной почты, личной переписки из социальных сетей, закрытых для просмотра третьими лицами.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети *(наказывается общественными работами, штрафом или ограничением свободы, или лишением свободы до 2 лет)* **(ответственность *с 16 лет)***
Статья достаточно специфична и применяется при разработке, изготовлении и сбыте специальных программ и устройств, предназначенных для осуществления несанкционированных доступов. Примером может служить изготовление и сбыт средств (смарт-карт, чипов и т.п.) для неправомерного просмотра зашифрованных телевизионных каналов.

Статья 354. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных, или аппаратных средств *(наказывается штрафом или ограничением свободы, или лишением свободы от 3 до 10 лет)* **(ответственность *с 16 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 *(наказывается штрафом или ограничением свободы, или лишением свободы от 2 до 7 лет)* **(ответственность *с 16 лет)*** *Указанная статья может быть применена к лицам, имеющим доступ к компьютерным сетям (в том числе к абонентам интернет-провайдеров) и системам, в которых хранится значимая информация, халатные действия которых привели к нарушению функционирования таких систем либо нарушению правил их использования.*

!!! Кодексом об административных правонарушениях Республики Беларусь также предусмотрена ответственность за совершение несанкционированного доступа к компьютерной информации, не повлекшего существенного вреда: **Статья 22.6. Несанкционированный доступ к компьютерной информации**

Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты, — влечет наложение штрафа в размере от двадцати до пятидесяти базовых величин.

Всё тайное всегда когда-то становится явным !

Подготовил педагог социальный УО БГКЛП Вакула В.А