ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТНУПНОСТИ

Киберпреступления – преступления, связанные с использованием компьютерной техники (преступления против информационной безопасности, хищения путем использования средств компьютерной техники, шантаж, вымогательство, изготовление и распространение порнографических материалов и т.д.)

Понятия и их определения

Основные понятия, которые относятся к теме безопасного поведения в сети интернет и описывают виды киберпреступлений

Вишинг – это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии социальной инженерии, под разными предлогами, искусно играя определенную роль (как правило, сотрудника банка, технического специалиста и т.д.), вынуждают человека сообщить им свои конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой.

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Кибербуллинг – это травля с использованием цифровых технологий. Кибербуллинг может происходить в социальных сетях, мессенджерах, на игровых платформах и в мобильных телефонах. Это целенаправленная модель поведения, которая ставит своей задачей запугать, разозлить или опозорить того, кто стал объектом травли.

Кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти, либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка.

Мошенничество в виде лотереи – это электронное сообщение, информирующее вас о том, что вы выиграли огромную сумму денег, и для того, чтобы получить свой приз или выигрыш, вам нужно заплатить небольшую плату.

Нежелательный контент – это не только материалы (картинки, видео, аудио, тексты), содержащие насилие, пропаганду наркотических средств, азартных игр, но и различные вредоносные и шпионские программы, задача которых получить доступ к информации на компьютере владельца. Также к нежелательному контенту относятся сайты, запрещенные законодательством.

Скам – это мошенничество в сети Интернет:

Смишинг – вид мошенничества, целью которого является переход по ссылке из SMS и/или загрузки вредоносного программного обеспечения. Смишинг-сообщение обычно имеет схожий внешний вид сообщения от банка, государственного учреждения, оператора электросвязи, известного магазина, а также о внезапном выигрыше в лотерею или акции и т.д.

Фишинг – вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т.д.).

В Уголовном кодексе Республики Беларусь содержится ряд статей, предусматривающих уголовную ответственность за киберпреступления:

- ст.212 «Хищение путем использования компьютерной техники»;
- ст.349 «Несанкционированный доступ к компьютерной информации»;
- ст.350 «Модификация компьютерной информации»;
- ст.351 «Компьютерный саботаж»;
- ст.352 «Неправомерное завладение компьютерной информацией»;
- ст.353 «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»;
- ст.354 «Разработка, использование либо распространение вредоносных программ»;
- ст.355 «Нарушение правил эксплуатации компьютерной системы или сети»