«Профилактика киберпреступности среди несовершеннолетних»

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Виды киберпреступлений

1. Финансово-ориентированные киберпреступления

Фишинг.

Кибермошенники любят собирать низко висящие фрукты, когда предоставляется возможность заразить компьютеры ничего не подозревающих жертв. В подобных схемах излюбленным средством злоумышленников является электронная почта. Суть метода заключается в принуждении получателя письма к переходу по ссылке от имени легитимной организации (банка, налоговой службы, популярного интернет магазина и т. д.). В подобных случаях целью, зачастую, является овладение банковскими данными.

Кибервымогательство.

Как правило, вначале у пользователя или компании, после загрузки вредоносного кода шифруются файлы, а затем поступает предложение о восстановлении в обмен на денежное вознаграждение (обычно в виде биткоинов или другой криптовалюты).

Финансовое мошенничество.

Большинство изощренных схем финансового мошенничества связано со взломом компьютерных систем операторов розничной торговли с целью получения банковских данных о покупателях (так называемые целевые атаки) или последующими манипуляциями полученной информацией.

2. Нарушение авторского права

Это одна из наиболее распространенных форм киберпреступлений. В первую очередь в эту категорию попадает выкладка в общий доступ музыки, фотографий, фильмов, книг и т. д. без согласия авторов.

3. Спам

Спам – чрезвычайно распространенный и многовариантный тип киберпреступлений. Сюда входит массовая рассылка по электронной почте, смс, мессенджерам и другим каналам коммуникации.

4. Социальные и политически мотивированные киберпреступления

Некоторые типы киберпреступлений направлены на изменения настроений в политической среде или нанесение намеренного вреда или снижения влияния отдельных личностей или группы людей.

5. Преступления на почве ненависти и домогательства

Терроризм

Группировки экстремистской направленности и воинственные народы все чаще используют киберпространство для запугивания, распространения пропаганды и иногда нанесения вреда IT-инфраструктурам.

Кибербуллинг

Это использование компьютеров и подключенных устройств для домогательств, унижения и запугивания личностей. Граница между кибербуллингом и некоторыми формами преступлений на почве ненависти зачастую размыта.

6. Противозаконная порнография

Груминг

Сетевой груминг связан с сексуальными домогательствами к несовершеннолетним. В процессе могут использоваться различные методы общения: смс, социальные сети, электронная почта, чаты и форумы.

Распространение наркотиков и оружия

Различные IT-решения, используемые для распространения легитимных товаров и служб, могут также использоваться злоумышленниками. Например, рынки даркнета, существующие во всемирной паутине, помогают контрабандистам продавать оружие и наркотики и в тоже время оставаться вне поля зрения правоохранительных органов.

Способы реализации киберприступлений

Существует четыре наиболее распространенных способа, которыми пользуются киберпреступники.

1. Использование вредоносных программ. Вероятно, вы понимаете, что существует множество методов эксплуатации систем, и насколько важно использоваться различными мерами безопасности: устанавливать длинные пароли и делать регулярные обновления.
2. DDOS атаки, когда злоумышленник пользуется коммуникационным сетевым протоколом для создания огромного количества запросов к

серверу или службе. В этом типе атак главная цель – вывести из строя объект воздействия.

3. Комбинация социальной инженерии и вредоносного кода. Наиболее известная форма подобного рода атак – фишинг, когда жертву принуждают к определенным действиям (нажатию на ссылку в электронном письме, посещению сайта и т. д.), что впоследствии приводит к заражению системы.
4. Незаконная деятельность: домогательства, распространение незаконного контента, груминг и т. д. В этом случае злоумышленники скрывают свои следы посредством анонимных профайлов, шифрованных сообщений и т.п.

Рекомендации по профилактике киберпреступлений среди несовершеннолетних

¨Установите с ребенком доверительные отношения и положительный эмоциональный контакт в вопросе использования сети Интернет. Оговорите с ребенком критический уровень опасности, когда решение в возникшей проблемной ситуации должно приниматься родителями (иным доверенным лицом, обладающим достаточным опытом и познаниями, например, старшим братом или сестрой) либо по согласованию с ними.

¨Установленные для ребенка правила работы в сети Интернет должны соответствовать его возрасту и развитию. Применение слишком мягких правил на начальном этапе освоения сети ребенком может повысить риск возникновения у ребенка различных угроз. А слишком жесткие правила либо запреты для ребенкамогут повлечь игнорирование им всяких правил.

¨Ребенку для работы в сети Интернет должен быть предоставлен в пользование компьютер со специфически настроенными параметрами. В обязательном порядке на компьютере должно быть установлено и настроено актуальное антивирусное программное обеспечение, установлен и настроен сетевой экран. Родителями должен контролироваться перечень установленного на компьютере программного обеспечения и его настройки.

Для детей от 7 до 10 лет:

- посещать только те сайты, которые Вы разрешили;
- советоваться с Вами, прежде чем совершить какие-либо новые действия, раскрыть личную информацию;
- сообщать Вам, если ребенка что-то встревожило либо было непонятно при посещении того либо иного сайта.
- запретите скачивать файлы из Интернета без Вашего разрешения;
- запретите общаться в Интернете с незнакомыми Вам людьми;
- запретите использовать средства мгновенного обмена сообщениями без Вашего контроля.

Для детей от 10 до 13 лет.

- создайте ребенку на компьютере собственную учетную запись с ограниченными правами;
- используйте средства фильтрации нежелательного контента;
- приучайте ребенка спрашивать разрешение при скачивании файлов из Интернета;
- поощряйте желание детей сообщать Вам о том, что их тревожит или смущает в Интернете;
- расскажите об ответственности за недостойное поведение в сети Интернет.

На данном этапе могут активно использоваться **программные средства родительского контроля**, к которым можно отнести следующие инструменты:

- услуга родительского контроля провайдера, оказывающего услугу доступа в сеть Интернет, позволяющая ограничить доступ кИнтернет сайтам, содержащим нежелательный контент;
- функции родительского контроля, встроенные в операционную систему (ограничение времени работы компьютера, ограничение запуска программ, в том числе игр);
- функции родительского контроля, встроенные в некоторые антивирусы (напримерKasperskyInternetSecurity, NortonInternetSecurity), позволяющие контролировать запуск различных программ, использование Интернета (ограничение по времени), посещение веб-сайтов в зависимости от их содержимого, пересылку персональных данных;
- специализированное программное обеспечение, предназначенное для выполнения функций родительского контроля, например, КиберМама, KidsControl, TimeBoss и другие.

Подростки в возрасте 14-17 лет.

- интересуйтесь, какими сайтами и программами пользуются Ваши дети;
- настаивайте на том, чтобы подросток не соглашался на встречу с друзьями из Интернета;
- напоминайте о необходимости обеспеченияконфиденциальности личной информации;
- предостерегайте детей от использования сети для хулиганства либо совершения иных противоправных деяний, разъясните суть и ответственность за совершение преступлений против информационной безопасности.

В случае установления фактов совершения противоправных деяний в сети Интернет в отношении детей рекомендуем родителям не умалчивать данные факты, а сообщать о них в зависимости от ситуации классному руководителю, педагогу социальному

учреждения образования, в правоохранительные органы по месту жительства.

Ответственность за совершение киберпреступлений

Напоминаем, что несовершеннолетние несут уголовную ответственность за совершение киберпреступлений с 14 лет! Условно, подобного рода противоправные деяния можно разбить на несколько групп:

- преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации как таковых (такие действия рассматриваются как посягательства на собственность и квалифицируются по статьям гл. 24 УК РБ);
- преступления, направленные на получение несанкционированного доступа к компьютерной информации, ее модификации, связанные с неправомерным завладением компьютерной информацией, разработкой, использованием либо распространением вредоносных программ и т.д. (такие действия рассматриваются как преступления против информационной безопасности и квалифицируются по статьям гл. 31 УК РБ);
- преступления, в которых компьютеры и другие средства компьютерной техники используются в качестве средства совершения корыстного преступления, и умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо путем введения в компьютерную систему ложной информации (такие действия рассматриваются как хищение путем использования компьютерной техники и квалифицируются по ст. 212 УК РБ).