

План-конспект по теме: «Профилактика киберпреступности среди несовершеннолетних»

В настоящее время в Республике отмечается бурный рост преступности в сфере высоких технологий. В 2020 году в сравнении с 2019 году киберпреступность возросла в 3 раза. В настоящее время процент киберпреступлений, совершенных несовершеннолетними лицами, составляет 1-2%. Таким образом, можно сделать вывод, что профилактика необходима и обязательна.

Своевременное доведение учащихся ответственности за совершение противоправных деяний в сфере информационной безопасности, а также разъяснение им сути криминализованных деяний, приведение понятных примеров может свести риск совершения преступлений данной категорией лиц до минимума.

Разберем статьи уголовного кодекса, по которым возможно привлечение к уголовной ответственности несовершеннолетних лиц.

Самой распространенной статьей уголовного кодекса Республики Беларусь является:

Статья 212. Хищение путем использования компьютерной техники. Необходимо отметить, что ответственность за деяния, предусмотренные ст. 212, наступает с 14-летнего возраста.

Самыми распространенными схемами преступлений ст. 212 УК Республики Беларусь, совершенных несовершеннолетними лицами являются:

В первую очередь детям необходимо объяснить, что банковская платежная карта является таким же предметом преступного посягательства как и велосипед или мобильный телефон.

1) 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 «Joom», «Aliexpress», 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 несовершеннолетнему лицу).

2) Хищение денег абонентов сотовой связи через мобильный банкинг. Схема базируется на услуге «A1-banking», предоставляющей доступ к электронному кошельку «A1-кошелек» УП «A1». Пользователям

этого сервиса оператор связи предлагает 100 рублей в качестве беспроцентного кредита.

Злоумышленники просят у человека телефон, чтобы позвонить, а на самом деле стремительно выполняют определенные манипуляции. За короткое время злоумышленники быстро подключаются к услуге А1-banking и переводят деньги, полученные при подключении, на подконтрольный счет. После этого, как ни в чем не бывало, возвращают телефон и удаляются.

Многие даже не сразу понимают, что пострадали от ловких действий преступников. Дело в том, что не все внимательно отслеживают свои расходы на связь, особенно когда привыкли держать на балансе крупную сумму. Однако спустя какое-то время человек замечает, что у него списали чересчур много денег. Обращается к мобильному оператору, чтобы прояснить ситуацию, и тут узнает, что стал жертвой преступников.

Статья 349. Несанкционированный доступ к компьютерной информации. Ответственность за деяния, предусмотренные ст.ст. 349-355, наступает с 16-летнего возраста.

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.

Статья 350. Модификация компьютерной информации

В качестве примера можно привести произведенные изменения компьютерной информации в системе либо сети, которые затрудняют либо исключают ее дальнейшее использование.

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.).

Так, в 2019 году несовершеннолетний Д. с использованием своей учетной записи, зарегистрированной в социальной сети «ВКонтакте», осуществлял переписку с различными пользователями, которые хотели продать или обменять свои игровые аккаунты игры «Битва Замков». После, договорившись о покупке, несовершеннолетний Д. получал от продавца логин и пароль игрового аккаунта. Затем, осуществив доступ к указанному игровому аккаунту, умышленно изменял пароль доступа к нему, тем самым блокировал доступ к указанному игровому аккаунту и связанной с ней компьютерной информацией правомерному

пользователю. Никаких денежных средств за игровой аккаунт несовершеннолетний Д. продавцу не перечислял.

О данной преступной деятельности несовершеннолетнего Д. стало известно, после обращения потерпевшего гражданина Российской Федерации в правоохранительные органы Республики Беларусь, так как злоумышленник не единожды обращал внимание в переписке, что он из Беларуси. По результатам проведенной проверки несовершеннолетний Д., привлечен к уголовной ответственности по ст. 351 УК Республики Беларусь и осужден к наказанию в виде 3-х лет ограничения свободы без направления в исправительное учреждение открытого типа.

Статья 352. Неправомерное завладение компьютерной информацией

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

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 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.

Кодексом об административных правонарушениях также предусмотрена ответственность за совершение несанкционированного доступа к компьютерной информации, не повлекшего существенного вреда.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

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 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.

Также необходимо учащимся ЗНАТЬ, как не стать ЖЕРТВОЙ киберпреступников, надо всего лишь соблюдать несколько простых правил безопасности в сети Интернет.

Правила безопасности детей в сети Интернет

На различных этапах становления личности и с приобретением опыта работы в сети используются различные подходы к обеспечению безопасности детей в Интернете, при этом необходимо учитывать следующие основные положения:

- Интернет – не отдельный виртуальный мир, а всего лишь составляющая часть реальности, соответственно в сети Интернет действуют те же моральные и правовые ограничения, что и в повседневной жизни. В сети недопустимы поступки, которые непозволительны в реальности.

- Анонимность в сети Интернет, во-первых, является мнимой, поскольку личность любого пользователя сети может быть установлена. Во-вторых, ребенку необходимо объяснять, что его собеседник также находится в состоянии такой анонимности, поэтому к указанным им сведениям о себе, выложенным фотографиям, текстам сообщений всегда необходимо относиться критично.

- Использование сети Интернет может нести некоторые опасности (вредоносные программы, небезопасные сайты, Интернет-мошенники и др.), поэтому каждое действие должно быть подкреплено соображениями безопасности. Недопустимо совершение действий, в безопасности которых ребенок не уверен.

- 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 возрасту и развитию Вашего ребенка. Применение слишком мягких правил на начальном этапе освоения сети ребенком может повысить риск возникновения у ребенка различных угроз. В то же время слишком жесткие правила либо запреты для ребенка, обладающего достаточным опытом и знаниями, могут повлечь игнорирование им всяких правил и использование выхода в сеть Интернет без какого-либо контроля родителей.

- Ребенку для работы в сети Интернет должен быть предоставлен в пользование компьютер со специфически настроенными параметрами. Он должен быть оснащен поддерживаемой производителем версией операционной системы с установленными актуальными обновлениями. 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. При необходимости на компьютере должно быть установлено специальное программное обеспечение, позволяющее контролировать и ограничивать деятельность ребенка в Интернете. Используйте лицензионное программное обеспечение.

- В настоящее время наблюдается бурный рост информационных технологий и сети Интернет, в частности. В связи с этим программные, организационные меры обеспечения безопасности постоянно развиваются. Родители должны быть нацелены на саморазвитие в данной сфере и корректировать поведение детей в соответствии со складывающимися условиями.

Рекомендации родителям

Интернет с детьми различных возрастных групп.

Для детей от 7 до 10 лет

Оптимальной формой ознакомления ребенка в таком возрасте с сетью Интернет будет совместная работа с ребенком за компьютером.

Приучите детей:

- 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;
- общаться в Интернете с незнакомыми Вам людьми;
- использовать средства мгновенного обмена сообщениями без Вашего контроля.

Постоянно беседуйте с детьми на тему использования ими сети Интернет: о действиях, посещенных сайтах, возможных новых знакомых.

Для детей от 10 до 13 лет

В данном возрасте ребенок уже обладает определенными навыками и познаниями о работе в сети, не готов к постоянному личному контролю со стороны взрослых, однако все еще требует контроля.

Рекомендации:

- создайте ребенку на компьютере собственную учетную запись с ограниченными правами;
- используйте средства фильтрации нежелательного контента;
- напоминайте о конфиденциальности личной информации;
- приучайте ребенка спрашивать разрешение при скачивании файлов из Интернета, при скачивании и установке программного обеспечения;
- поощряйте желание детей сообщать Вам о том, что их тревожит или смущает в Интернете;
- настаивайте на том, чтобы ребенок позволял Вам знакомиться с содержимым его электронной почты, учетных записей в социальных сетях, перепиской в средствах мгновенного обмена сообщениями;
- 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 к Интернет 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 (например KasperskyInternetSecurity, NortonInternetSecurity), позволяющие контролировать использование компьютера, запуск

различных программ (попытки запуска запрещенных программ блокируются), использование Интернета (ограничение по времени), посещение веб-сайтов в зависимости от их содержимого, загрузку файлов из Интернета, переписку с определенными контактами через Интернет мессенджеры и социальные сети, пересылку персональных данных, употребление определенных слов и словосочетаний в переписке через мессенджеры;

- специализированное программное обеспечение, предназначенное для выполнения функций родительского контроля, например, КиберМама, KidsControl, TimeBoss и другие.

Подростки в возрасте 14-17 лет

Рекомендации:

- интересуйтесь, какими сайтами и программами пользуются Ваши дети;

- настаивайте на том, чтобы подросток не соглашался на встречу с друзьями из Интернета без Вашего ведома;

- напоминайте детям о необходимости обеспечения

- конфиденциальности личной информации;

- предостерегайте детей от использования сети для хулиганства либо совершения иных противоправных деяний, разъясните суть и ответственность за совершение преступлений против информационной безопасности;

- обсудите с ребенком возможные риски при осуществлении покупок в сети.

В сети Интернет на сайтах провайдеров, производителей антивирусного программного обеспечения, а также на специализированных ресурсах можно найти рекомендации по обеспечению защиты детей от различных типов киберугроз. Также значимой для родителей может быть размещенная в сети информация о действиях, если ребенок уже столкнулся с какой-либо интернет-угрозой.

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.