«Профилактика киберпреступности среди несовершеннолетних»

С каждым годом интернет-мошенники становятся все моложе. Современные подростки проводят в Интернете большую часть своего времени, но возможности Всемирной паутины каждый использует по-разному. Преступность среди несовершеннолетних всегда вызывает повышенное внимание. Проблема преступлений среди несовершеннолетних, является одной из самых существенных социально-правовых проблем общества.

Целью индивидуальной профилактики преступлений, совершаемых несовершеннолетними, является исправление и перевоспитание несовершеннолетнего.

Статья 212 УК Республики Беларусь. Хищение имущества путем модификации компьютерной информации.

Какие действия несовершеннолетних могут квалифицироваться по статье 212 УК Республики Беларусь?

1) С использованием похищенной банковской карты осуществляют снятие денег в банкомате либо оплачивают с использованием платежного терминала покупки в торговых точках (магазины, кафе и т.д.).

2) С использованием украденной банковской карты производят покупки в Интернет-магазинах и различных онлайн-играх (Aliexpress, Joom, WorldofTanks и т.д.).

3) Активируют на мобильном телефоне другого человека услугу, предоставляемую компанией А1, «V-банкинг» и переводят на свой абонентский номер телефона деньги, которые предоставляет компания в качестве кредита.

Уголовная ответственность **за совершение таких киберпреступлений** наступает с 14 лет!

Статья 222 УК Республики Беларусь. Незаконный оборот средств платежа и (или) инструментов.

Все чаще в социальных сетях и мессенджерах пользователям стали приходить сообщения с предложениями без особых усилий за день заработать до 100 долларов. Что для этого нужно? Всего ни чего, оформить на себя банковскую карту в банке, на который укажет мнимый работодатель, и передать сообщением полученные реквизиты карты потенциальному работодателю.

Как правило, все общение проходит в сети Интернет без личного контакта. Истории, для чего нужна работодателю банковская карта чужого человека, различны. В основном это необходимость перевода денег на счета в Беларуси, а сам он не может, так как находится в другой стране.

Человек, согласившийся на такие условия сделки, становиться так называемым «ДРОПОМ» – подставным лицом в серых схемах

кибермошенников. Дроп – этот тот человек, который соглашается, чтобы его банковская карта стала «транзитной» для украденных мошенниками денег. Дроп переводит незаконно полученные денежные средства между разными счетами. Такая цепочка переводов нужна для того, чтобы запутать следы киберпреступников и усложнить работу милиции.

Дропы бывают «разводные» и «неразводные». Отличие их только в том, что неразводные осознают всю тяжесть совершаемых им деяний и умышленно занимаются этим. В большинстве своем это студенты, школьники, малоимущие, которые нуждаются в финансах. Разводные «дропы» не знают о том, что идут на преступление. Они думают, что действительно работают, получают зарплату и т.д.

В каких схемах могут участвовать подростки?

Обналичивание денег в банкоматах: действия – принять деньги, снять деньги, взять себе процент, остальное переслать заказчику. Вот по такой нехитрой схеме и работают дропы.

Банковский перевод: предоставь мнимому работодателю свои реквизиты банковской карты, подождать когда на нее зачислят украденные деньги, переслать деньги на счет который укажет заказчик, оставить себе процент на банковской карте.

Пересылка товара: действия такие: дать свой адрес, принять посылку, переслать посылку на нужный адрес\отдать в руки (и такие есть), получить вознаграждение. Главное – наличие паспорта и прописки.

Дропы могут понадобится и для других дел. Например, покупка симкарт с помощью которых в дальнейшем совершаются преступления.

Какие последствия ждут «дропов» в дальнейшем?

Ответственность за такие действия наступает по ст. 222 УК Республики Беларусь (незаконный оборот средств платежа и (или) инструментов).

Ответственность наступает с 16 летнего возраста.

Статья 340 УК Республики Беларусь. Заведомо ложное сообщение об опасности.

Еще один вид киберпреступлений, совершаемых учащимися учебных заведений, это преступления, предусмотренные ст. 340 УК.

К заведомо ложным сообщениям об опасности относятся сообщения о готовящихся взрыве, поджоге или иных действиях, создающих опасность для жизни и здоровья людей либо причинения ущерба в крупном размере либо наступления иных тяжких последствий. При этом данные сведения являются заведомо ложными, то есть не соответствующими действительности, вымышленными, надуманными.

Материальный и имущественный ущерб, связанный с работой бригад скорой помощи, МЧС и иных спасательных служб, вынужденных проводить проверку ложного сообщения, а также убытки, понесенные иными организациями, взыскиваются с лица, совершившего такое преступление.

Практика свидетельствует, что мотивами заведомо ложных сообщений об опасности чаще всего являются озорство и хулиганские побуждения. Причинами: не желание посещать занятия, месть одногруппникам, самоутверждение среди сверстников.

Поэтому необходимо знать, что телефонный звонок с ложным сообщением, к примеру, о заложенном в торговом центре или образовательной организации взрывном устройстве, является не безобидной шалостью, а уголовно наказуемым преступлением.

За совершение данного преступления предусмотрено наказание до 5 лет лишения свободы, а в случае если преступления совершено повторно либо группой лиц по предварительному сговору, либо преступлением причинен крупный ущерб или наступили иные тяжкие последствия – до 7 лет лишения свободы.

Правоохранительные органы в настоящее время обладают достаточными техническими и оперативными возможностями, позволяющими устанавливать личности преступников независимо от способа заведомо ложного сообщения об опасности.

Интернет сохраняет ВСЕ!

Статья 209 УК Республики Беларусь. Мошенничество.

Несовершеннолетних могут «втягиваться» в преступные схемы так называемые телефонные мошенники, которые звонят гражданам и под предлогом не привлечения из близкого родственника, который оказался виновником ДТП, к уголовной ответственности договариваются о передаче денег через курьера. В роли курьера в основном выступают молодые люди, которые хотят подзаработать. В сети Интернет идет массовая рассылка сообщений с предложением сомнительного заработка.

Кроме этого в поле зрения правоохранителей попадают несовершеннолетние, совершающие несанкционированный доступ к компьютерной информации (ст. 349 УК Республики Беларусь).

Статья 349. Несанкционированный доступ к компьютерной информации

В частности, несовершеннолетние осуществляют несанкционированный доступ к электронной почте, учетным записям на различных сайтах, игровых платформах, в том числе в социальных сетях, а также к информации, содержащейся в компьютере, смартфоне, с использованием различных программ удаленного доступа, методов социальной инженерии, таких как «вишинг» и «фишинг» (когда

получаешь логины и пароли путем обмана и введение в заблуждение владельца информацией). Как правило, несанкционированный доступ к компьютерной информации влечет за собой совершение ряда киберпреступлений, предусмотренныхст. 350 (уничтожение, блокирование или модификация компьютерной информации) или ст. 208 УК (вымогательство).

Чаще всего несанкционированный доступ осуществляют к учетным записям социальных сетей «ВКонтакте» и «Instagram».

Уголовная ответственность**за совершение таких киберпреступлений**наступает с 16 лет!

Максимальный срок наказания по ст. 349 УК составляет 7 лет лишения свободы, по ст. 350 УК – 10 лет лишения свободы, по ст. 208 УК – 15 лет лишения свободы.

Причинами и условиями, способствующими совершению преступлений и правонарушений, являются:

- индивидуальные свойства, возрастные, психологические и иные особенности личности правонарушителя в условиях его неблагоприятного воспитания и формирования (возрастные изменения психики, психические расстройства, вредное влияние микросреды, бытовые взаимоотношения, пропаганда жестокости и насилия, низкая организация воспитательной работы, низкий культурный и образовательный уровень учащихся и т.п.);
- обстоятельства непосредственной ситуации, в которой было совершено правонарушение (не осознание несовершеннолетними последствий совершенного деяния, отсутствие контроля за поведением, неучастие в личной жизни несовершеннолетнего родителей, близких).

Общая профилактика правонарушений, совершаемых подростками, должна осуществляется в основных сферах:в семье,по месту жительства, в учебных заведениях.

Рекомендации по профилактике киберпреступлений среди несовершеннолетних.

Первое и самое главное правило «Установите с ребенком доверительные отношения и **положительный** эмоциональный контакт в вопросе использования сети Интернет».

Расскажите ребенку об ответственности, которая может наступить за совершение им киберпреступлений, а также о возрасте, с которого наступает уголовная ответственность за данные деяния.

Разъясните подростку, что есть и другие не менее негативные последствия совершения ими преступлений или правонарушений. Привлечение к административной или уголовной ответственности является основанием для постановки несовершеннолетнего на учетв Инспекцию по делам несовершеннолетних, занесения информации в общереспубликанскую единую государственную базу данных о

правонарушениях, которая содержится там на протяжении всей жизни, что впоследствии может послужить препятствием для получения визы, поступления в специализированный ВУЗ (Академия МВД, Военная академия), прохождения службы в правоохранительных органах, занятия высших должностей и т.п. Здесь можно и упомянуть и о гражданской ответственности. Она только кажется такой незначительной, по сравнению с уголовной и административной. На самом деле именно она очень часто идет рядом с ними и довольно больно может ударить по «карману». Несовершеннолетний в возрасте от 14 до 18 лет самостоятельно несет ответственность за причиненный вред. Если средств подростка будет недостаточно для возмещения вреда, то возмещать вред полностью или в недостающей части придется родителям.

Рекомендации для безопасного использования Интернета.

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, социальному педагогу учреждения образования, в правоохранительные органы по месту жительства.

Начальник ОВД Ельского райисполкома Г.Д.Яцухно