УВД ГОМЕЛЬСКОГО ОБЛИСПОЛКОМА
КРИМИНАЛЬНАЯ МИЛИЦИЯ
УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

ОПОРНЫЙ ПЛАН-КОНСПЕКТ

Тема:
«Профилактика киберпреступности среди несовершеннолетних»

Гомель

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.

За 2 месяца текущего года в Гомельской области совершено несовершеннолетними 7 киберпреступлений. Все деяния несовершеннолетних квалифицированы по ст. 212 УК Республики Беларусь (хищение имущества путем модификации компьютерной информации).

3 преступления совершены несовершеннолетними путем хищения денежных средств с виртуальных карт потерпевших, зарегистрированных на абонентские номера оператора сотовой связи УП «А1».

3 – с использованием похищенных банковских карт при оплате покупок через платежные терминалы различных торговых объектов.

1 – реквизитами банковской платежной карты потерпевшего производилась покупка в интернет-магазине «JOOM».

Справочно:

Статья 212 УК Республики Беларусь:

1. Хищение имущества путем модификации компьютерной информации –

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно либо группой лиц по предварительному сговору, –

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, –

наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, –

наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

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, World of Tanks 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!

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

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, предусмотренных ст. 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 хищений имущества путем модификации компьютерной информации (ст. 212 УК Республики Беларусь)

и несанкционированного доступа к компьютерной информации (ст. 349 УК Республики Беларусь), 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 учет в 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 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 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 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.

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.