МАТЕРИАЛ

для членов информационно-пропагандистских групп

(февраль 2025 г.)

**ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ СРЕДИ НЕСОВЕРШЕННОЛЕТНИХ**

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

На территории Браславского района наблюдаете рост (+86,7 %) числа зарегистрированных киберпреступлений в сравнении с аналогичным периодом 2023 года (с 17 до 29).

В структуре киберпреступлений, совершенных на территории Браславского района преобладают интернет-мошенничества (ст. 209 УК Республики Беларусь) (23 преступлений или 79,3 %), а также хищения путём использования компьютерной техники (ст. 212 УК Республики Беларусь ) (6 преступлений или 20,7 %).

Основными способами совершения преступления, предусмотренного ст. 209 УК Республики Беларусь является:

- продажа товара в сети Интернет в мессенджере «Инстаграм» (8 преступлений или 34,8%);

- убеждение злоумышленником оформления кредита и его дальнейшая передача злоумышленнику (9 преступления или 39,1%);

- продажа имущества на торговой площадке «Куфар» (3 преступления ли 13%);

- предложения заработка на бирже (3 преступления ли 13%).

Киберпреступления, совершаемые несовершеннолетними, в 2024 году на территории Браславского района не фиксировались.

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. Ответственность за такой «заработок» предусмотрена ст. 209 УК Республики Беларусь (Мошенничество).

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

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.).

С использованием украденной банковской карты производят покупки в Интернет-магазинах и различных онлайн-играх.

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! *(ст. 212 УК Республики Беларусь. Хищение имущества путем модификации компьютерной информации).*

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

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.

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.

Еще один вид киберпреступлений, совершаемых учащимися учебных заведений, это преступления, предусмотренные ст. 340 УК Республики Беларусь *(Заведомо ложное сообщение об опасности).*

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.

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.

Кроме этого в поле зрения правоохранителей попадают несовершеннолетние, совершающие несанкционированный доступ к компьютерной информации *(ст. 349 УК Республики Беларусь).* Как правило, несанкционированный доступ к компьютерной информации влечет за собой совершение ряда киберпреступлений, предусмотренных ст. 350 УК Республики Беларусь *(Уничтожение, блокирование или модификация компьютерной информации)* или ст. 208 УК Республики Беларусь *(Вымогательство).*

Уголовная ответственность за совершение таких киберпреступлений наступает с 16 лет!

**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. 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 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 или 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 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 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.

**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 хулиганств 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.

*Комиссия по делам несовершеннолетних Браславского районного исполнительного комитета*

*Отдел внутренних дел Браславского районного исполнительного комитета*