

МІНІСТЭРСТВА ЎНУТРАНЫХ СПРАЎ
РЭСПУБЛІКІ БЕЛАРУСЬ

УПРАЎЛЕННЕ ЎНУТРАНЫХ СПРАЎ
ГОМЕЛЬСКАГА АБЛАСНОГА
ВЫКАНАЎЧАГА КАМІТЭТА

вул. Камунараў, 3, 246050, г. Гомель

тэл/факс (0232) 50 88 07, 50 88 09
e-mail: uvd_gomel@mvd.gov.by

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

УПРАВЛЕНИЕ ВНУТРЕННИХ ДЕЛ
ГОМЕЛЬСКОГО ОБЛАСТНОГО
ИСПОЛНИТЕЛЬНОГО КОМИТЕТА

ул. Коммунаров, 3, 246050, г. Гомель

тел/факс (0232) 50 88 07, 50 88 09
e-mail: uvd_gomel@mvd.gov.by

01.10.2026 № 53/5/46432
На № _____ ад _____

Начальнику Главного
управления образования
Гомельского областного
исполнительного комитета
Смирнову Р.И.

О направлении материалов

Уважаемый Руслан Иванович!

Во исполнение подпункта 2.2 пункта 2 решения Гомельского областного исполнительного комитета от 27 августа 2026 года № 778 «Об эффективности принимаемых мер, направленных на профилактику и противодействие киберпреступности, выявление причин и условий, способствующих совершению киберпреступлений» направляю в Ваш адрес информационные материалы, содержащие актуальную профилактическую информацию по противодействию киберпреступности для учащихся 5-11 классов учреждений общего среднего образования и учащихся учреждений среднего специального образования, для использования при проведении в учреждениях образования мероприятий, в том числе информационных, классных (кураторских) часов, с несовершеннолетними обучающимися по освещению вопросов цифровой безопасности и ответственности за правонарушения в сети Интернет.

Приложение: на 11 л. в 1 экз.

С уважением,

Заместитель начальника
криминальной милиции управления



А.Г.Баранец

УВД ГОМЕЛЬСКОГО ОБЛИСПОЛКОМА
КРИМИНАЛЬНАЯ МИЛИЦИЯ
УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОФИЛАКТИЧЕСКОЙ РАБОТЫ
СРЕДИ НЕСОВЕРШЕННОЛЕТНИХ

Тема:

**«Актуальные способы совершения киберпреступлений.
Ответственность несовершеннолетних за совершение
киберпреступлений»**

Гомель, 2026 год

В настоящее время Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека. С одной стороны, это открывает перед белорусскими гражданами ряд перспектив, с другой – влечет появление новых рисков и угроз. Так, бурное развитие технологий, стремительный рост числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий, привело к увеличению количества киберпреступлений. Вопрос цифровой безопасности сегодня является одним из наиболее злободневных.

Не смотря на тот факт, что в основной своей массе потерпевшие – это молодые, трудоспособные граждане в возрасте от 18 до 40 лет, следует отметить и тот факт, что и несовершеннолетние граждане зачастую становятся жертвами киберпреступности. А в ряде случаев отсутствие надлежащего контроля за досугом несовершеннолетних со стороны родителей приводит к вовлечению указанной категории лиц в преступную деятельность.

Благодаря целенаправленной профилактической работе удается сдерживать число потерпевших в среде лиц, не достигших возраста 18 лет.

Вместе с тем, анализируя характер преступлений, совершенных в отношении несовершеннолетних, можно отметить, что наибольшее количество подростков – 32 % – подверглись вымогательству.

В 42 % случаев детей пострадали в результате блокировка «Iphone».

Среди мошенничеств наибольшее распространение получили преступления, совершенные под предлогом покупки товаров. Причем, в подавляющем большинстве случаев, несовершеннолетние пытались совершить покупку мобильных устройств Apple.

Обратимся к основным схемам киберпреступлений, совершаемых в отношении несовершеннолетних.

Блокирование мобильных устройств Apple.

Механизм блокирования мобильных устройств Apple реализуется не путем взлома операционной системы, а посредством методов социальной инженерии с использованием доверчивости детей.

Так, злоумышленник под различным предлогом вынуждает ребенка выйти из своего аккаунта Apple (iCloud) и войти на iPhone в «мошеннический» аккаунт, для чего мошенником предоставляется логин (адрес электронного почтового ящика) и пароль. С этого момента мобильный телефон жертвы «в руках» вымогателя. Он изменяет пароль от учетной записи, знание которого требуется для выхода из нее, после чего удаленно через облачный сервис iCloud активирует функцию «Найти iPhone», переводя таким образом устройство в режим пропажи, и полностью блокирует его.

Далее потерпевшему приходит сообщение (либо выводится на заблокированный экран), что телефон заблокирован, а для его разблокировки необходимо заплатить деньги. Также зачастую предоставляется контакт в Telegram лица, способного решить этот вопрос (как правило, это и есть злоумышленник, заблокировавший телефон). Характерно, что даже при выполнении требования вымогателя разблокировка устройства в подавляющем большинстве случаев не осуществляется.

Существует несколько основных предлогов, вынуждающих детей войти на своих устройствах в мошеннический аккаунт Apple.

Предлог 1. Реклама бесплатных игр и приложений в социальных сетях и мессенджерах.

Злоумышленники осуществляют размещение рекламы (чаще всего видеоролик в TikTok либо в Telegram), в которой указывается бесплатный способ скачать на iPhone то или иное приложение (AyuGram, Telegram Premium, позволяющие читать удаленные сообщения, забирать «звезды», скрывать статус онлайн и т.д.), игру («MINECRAFT», «PUBG Mobile», «Standoff 2» и др.) либо мод, получить на свой баланс игровую валюту.

Для установки данных предложений злоумышленники предлагают жертве войти на телефоне в предоставленный ими аккаунт Apple (iCloud).

Предлог 2. Трудоустройство.

Злоумышленник осуществляет размещение рекламы в сети Интернет о поиске сотрудника на вакансию, как правило, связанную с тестированием мобильных приложений для устройств Apple. После удачного «прохождения собеседования» потенциальному работнику предоставляется логин и пароль для входа в якобы корпоративный аккаунт Apple, который должен использоваться для работы либо загрузки необходимых приложений.

После входа соискателя на своем iPhone в предоставленную учетную запись Apple он оказывается в ловушке. Затем происходят события, аналогичные описанным выше.

Следует отметить, что работники сервисных центров не оказывают услуги по восстановлению устройств Apple либо учетных записей iCloud, заблокированных мошенниками. Разблокировать такое устройство возможно только путем обращения в службу технической поддержки компании Apple, приложив документы, подтверждающие законность его приобретения, представленные на слайде.

Процесс восстановления занимает от нескольких дней до недели, при этом устройство может быть сброшено до заводских настроек (все данные удалятся).

К примеру, в г. Гомеле несовершеннолетняя А., 2008 г.р., во время просмотра видеороликов в социальной сети «ТикТок» увидела ролик о том,

что, перейдя по учетной записи, указанной в ролике, можно восстановить удаленный аккаунт в мессенджере «Телеграм», что последняя и сделала. В дальнейшем телефон А. был заблокирован и пришло сообщение о том, что для того, чтобы разблокировать телефон, необходимо с другого телефона выполнить те же условия. Помочь А. решилась ее подруга Е., 2008 г.р., мобильный телефон которой в дальнейшем также был заблокирован.

Запомните:

- никогда и не под каким предлогом не входите на своем мобильном устройстве в чужую учетную запись Apple, даже, если Вас об этом просит друг и тем более – незнакомый человек из интернета;
- никому не сообщайте ваши логин и пароль от аккаунта Apple;
- не переходите по неизвестным ссылкам, пересланным Вам незнакомым человеком; не вводите на посторонних сайтах свои логин и пароль от аккаунта Apple (iCloud).

Вишинг

Детей младшего школьного возраста злоумышленники обманывают следующим образом. Ребенку в мессенджере поступает звонок от имени работника РУП «Белпочта» или операторов сотовой связи, которые под различными предложениями **пытаются узнать персональные данные родителей**, либо просят сообщить код из отправленного ими SMS-сообщения.

После их получения осуществляется второй звонок, якобы от представителя правоохранительных органов. Несовершеннолетнему сообщается о том, что он предоставил персональные данные мошенникам. В результате этого на их имя оформлены банковские счета, через которые перечислены крупные суммы денег, добытые преступным путем. Затем ребенку угрожают привлечением родителей к уголовной ответственности из-за него. Чтобы этого избежать, предлагается «спасти родителей», для чего необходимо выполнить процедуру обязательного «декларирования» денежных средств, находящихся дома. Ребенку под угрозой ареста или заключения под стражу родителей предлагается передать имеющиеся в доме денежные средства или оставить их в указанном злоумышленником месте для проведения процедуры «декларирования» или зачисления на «безопасный счет». При этом детям категорически запрещают рассказывать об этом кому-либо. После передачи сбережений сведения о входящих звонках и переписке удаляются преступником.

Запомните:

- государственные органы и банки никогда не требуют передать наличные через курьера и не звонят в мессенджеры;

- термина «безопасный счет» не существует. Никто не имеет права требовать у Вас PIN, SMS-коды или данные банковской платежной карты по телефону;
- любые угрозы «арестом родителей» – 100 % манипуляция;
- нельзя передавать личную конфиденциальную информацию в ответ на сообщения с неизвестных номеров.

Покупки товаров и услуг

Продолжает использоваться **схема хищения денежных средств с использованием торговой площадки «Kufar»**. Так, мошенниками размещается информация о продаже товаров, пользующихся спросом у подростков (телефоны марки «Iphone», брендовые вещи, спортивная аммуниция и др.) по цене в разы ниже рыночной стоимости. Ребенок, видя выгодное предложение, направляет продавцу сообщение, в котором уточняет интересующие его вопросы относительно товара и способ его получения.

В случае договоренности, продавец предлагает покупателю оформить доставку товара через почтовое отправление (Белпочта, Европочта и др.), предварительно оплатив услуги доставки. Для этого ребенку в мессенджер высылается ссылка на мошеннический (фишинговый) сайт, который визуально схож с официальным сайтом сервисов доставки товаров и почтовых отправлений (Белпочта, Европочта и др.). Однако, в его названии, как правило, заменен один или два символа. В данной ссылке указывается незначительная сумма оплаты (как правило, 2 рубля) и необходимость обязательного введения номера банковской платежной карты и трехзначного CVV кода, размещенного на оборотной ее стороне.

Кроме этого, предлагается заполнить специальную графу «Баланс карты» или «Остаток денежных средств на банковской карте». Выполнив указанные требования, подростку-покупателю направляется код авторизации, который он сообщает мошеннику, тем самым предоставляет удаленный доступ к запрошенному им остатку на его банковской карте, который он указал. После совершения хищения, товар не высылается, а покупателя блокируют.

Фейковые магазины в соцсетях.

Наравне со взрослыми несовершеннолетние пытаются совершить покупки в Интернет-магазинах (в частности Instagram). В данном случае мошенники намеренно создают аккаунты от имени магазинов, в которых размещают объявления несуществующих товаров с заниженными ценами. Потенциальный покупатель связывается с администратором «магазина» и обещает доставить товар после частичной или полной оплаты. Перевод

денег предлагают произвести на банковскую карту или на счет через ЕРИП, что притупляет бдительность. После получения денежных средств, интернет-магазин товар не высылает, а покупателя блокирует.

На что обратить внимание при столкновении с тем или иным предложением:

- слишком низкие цены. Если цена значительно ниже, акционный товар;
- отсутствие отзывов либо наоборот значительное количество исключительно положительных, оставленных в узкие временные рамки;
- неполная информация: отсутствие контактных данных, юридического адреса, информации о возможности возврата товара;
- плохое качество контента: низкое качество фото товара, отсутствие описания товара и др.;
- слишком большое количество подписчиков без активности;
- общение может быть переведено в мессенджер (зачастую Telegram);
- способы оплаты: исключительно предоплата на карты, банковские счета, электронные кошельки.

Распространение личной информации

В последнее время среди злоумышленников набирает популярность **вымогательство, связанное с угрозой распространения личной информации.**

В подавляющем большинстве случаев объектом преступления являются фотографии и видеозаписи интимного характера, переписка на сексуальную тему либо иная компрометирующая ребенка информация.

Первоначальная коммуникация злоумышленника и подростка происходит в приложениях либо на сайтах для знакомств (Mamba, Masked.love, Twinby, Mail.ru и др.) либо Telegram-чатах («Леонардо Дайвинчик» и др.), где мошенник выступает в качестве лица, противоположного пола, желающего познакомиться. Затем общение довольно быстро приобретает сексуальный подтекст. «Новый знакомый» предлагает обменяться интимными фотографиями. При этом для большей убедительности присылает заранее заготовленные якобы свои фотографии либо видео в обнаженном виде, а на самом деле скаченные в сети Интернет.

В случае если жертва «повелась» на данное предложение и сбросила свои интимные фотографии или видео, злоумышленник их сохраняет. Затем он сообщает, что распространит имеющиеся у него интимные фотографии потерпевшего среди его друзей и знакомых либо выложит в открытый доступ, если ему не заплатит за их нераспространение.

Запомните:

- никогда не отправляйте свои интимные фотографии и видео незнакомцам из Интернета;
- не оставляйте в сети Интернет о себе личную информацию и не делитесь с ней с незнакомцами;
- скройте данные о себе в настройках конфиденциальности в социальных сетях и мессенджерах;
- не переходите по неизвестным ссылкам, пересланным Вам незнакомым человеком;
- не вводите на посторонних сайтах свои личные данные и коды из сообщений.

Среди основных причин, по которым жертвами киберпреступников становятся подростки являются:

- недостаток цифровой грамотности (знаний в области безопасного общения в социальных сетях и мессенджерах);
- неосторожность при общении онлайн с незнакомыми людьми;
- отсутствие родительского контроля и поддержки;
- эмоциональная уязвимость в силу психовозрастных особенностей.

В настоящее время в Республике Беларусь наиболее распространенными преступлениями, совершаемыми несовершеннолетними либо при их соучастии в сфере киберпреступности являются: мошенничество (статья 209 УК Республики Беларусь), хищение имущества путем модификации компьютерной информации (статья 212 УК Республики Беларусь), незаконный оборот платежных инструментов, средств платежа и их реквизитов (статья 222 УК Республики Беларусь), заведомо ложное сообщение об опасности (статья 340 УК Республики Беларусь), а также такие административные правонарушения как незаконная предпринимательская деятельность (статья 13.3 КоАП Республики Беларусь) и незаконное предоставление реквизитов платежных инструментов (статья 12.35 КоАП Республики Беларусь).

В большинстве случаев несовершеннолетние совершают указанные противоправные деяния с целью заработка денежных средств, самоутверждения, будучи под воздействием со стороны ровесников или взрослых, либо ради собственного веселья. Зачастую подростки ищут в Интернете способы заработка и сталкиваются с мошенниками, порой даже не осознавая, что совершают незаконные действия.

Учитывая изложенное важно рассмотреть основные способы совершения преступлений и правонарушений, а также действия, которые будут квалифицированы в соответствии с нормами уголовного и административного законодательства.

Статья 212 Уголовного кодекса Республики Беларусь. Хищение имущества путем модификации компьютерной информации.

По указанной статье могут быть квалифицированы следующие действия несовершеннолетних:

1. С использованием банковской платежной карты третьего лица, без его ведома и разрешения, осуществлять снятие денежных средств в банкомате либо оплату покупок в торговых объектах с использованием платежного терминала;

2. С использованием банковской платежной карты третьего лица, без его ведома и разрешения, производить покупки в интернет-магазинах, маркетплейсах и различных онлайн-играх;

3. Активировать на мобильном телефоне третьего лица услуги, предоставляемые мобильными операторами и осуществлять переводы на свой абонентский номер телефона или банковский счет денежные средства, которые предоставляет компания в качестве кредита;

4. Хищение денежных средств с банковских платежных карт посредством фишинговых сайтов, которые создаются с целью оплаты товара или услуг;

5. Обналичивание в банкоматах похищенных денежных средств.

Уголовная ответственность за совершение таких киберпреступлений наступает с 14 лет. 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.

Статья 209 Уголовного кодекса Республики Беларусь. Мошенничество.

По указанной статье могут быть квалифицированы следующие действия несовершеннолетних:

1. Реализация несуществующих товаров, выставленных на продажу на различных интернет-ресурсах, публикация фальшивых объявлений об оказании услуг, а после совершение хищений денежных средств, переведенных на предоставленные гражданам платежные реквизиты в качестве предоплаты или полной оплаты;

2. Хищение денежных средств с использованием аккаунтов в различных мессенджерах, представляясь специалистами в сферах криптовалюты, валютно-фондовых бирж, сотрудников администраций онлайн-казино и иных лиц;

3. Обналичивание в банкоматах похищенных денежных средств.

Уголовная ответственность за совершение таких киберпреступлений наступает с 16 лет. Наказывается общественными работами, или штрафом, или исправительными работами на срок до двух лет, или арестом,

или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

Статья 222 Уголовного кодекса Республики Беларусь. Незаконный оборот платежных инструментов, средств платежа и их реквизитов.

Статья 12.35 Кодекса Республики Беларусь об административных правонарушениях. Незаконное предоставление реквизитов платежных инструментов.

В первую очередь, совершение преступления, предусмотренного статьей 222 УК, сопровождается желанием лица легко заработать денежные средств. Мошенники ищут добровольцев, которые за денежное вознаграждение готовы передать третьим лицам реквизиты банковских платежных карт, банковских счетов либо аутентификационных данных.

В случае, если лицо за денежное вознаграждение передает реквизиты банковских платежных карт или аутентификационных данных, находящихся в его собственном владении, то такое деяние квалифицируется по ст. 12.35 КоАП Республики Беларусь. Напротив, если лицо за денежное вознаграждение передает реквизиты банковских платежных карт или аутентификационных данных, которые в свою очередь находятся в законном владении иных лиц, то его действия будут квалифицированы по ст. 222 УК Республики Беларусь.

Ответственность за вышеуказанные нарушения уголовного и административного законодательства наступает с 16-летнего возраста. Статья 12.35 КоАП Республики Беларусь — влечет наложение штрафа в размере от пяти до тридцати базовых величин.

Статья 222 УК Республики Беларусь — наказывается штрафом, или исправительными работами на срок до двух лет, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

Статья 340 Уголовного кодекса Республики Беларусь. Заведомо ложное сообщение об опасности.

К заведомо ложным сообщениям об опасности относятся сообщения о готовящихся взрыве, поджоге или иных действия, 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.

Практика показывает, что мотивами для совершения заведомо ложных сообщений об опасности чаще всего хулиганские побуждения, а причинами: не желание посещать учебные занятия, месть одноклассникам, самоутверждение среди сверстников.

Несовершеннолетним необходимо знать, что ложное сообщение, к примеру, о заложенном в торговом центре или образовательной

организации взрывном устройстве, является не безобидной шалостью, а уголовно наказуемым преступлением.

Уголовная ответственность за совершение таких киберпреступлений наступает с 14 лет. Наказывается штрафом, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на срок до пяти лет.

Статья 13.3 Кодекса Республики Беларусь об административных правонарушениях. Незаконная предпринимательская деятельность.

Часть 3 настоящей статьи: осуществление предпринимательской деятельности, когда в соответствии с законодательными актами такая деятельность является незаконной и (или) запрещается.

В настоящее время молодые люди все больше начинают интересоваться криптовалютой и способами заработка денежных средств с ее использованием. Согласно пункту 2.6. Декрета Президента Республики Беларусь от 21.12.2017 г. № 8 «О развитии цифровой экономики», запрещается оказание содействия иным лицам в совершении или исполнении сделок с криптовалютой. То есть, физические лица имеют право осуществлять операции с криптовалютой исключительно в собственных целях, а это значит, что любое посредничество со стороны физического лица в сфере криптовалюты является незаконным. Ввиду чего, приобретение, отчуждение или обмен криптовалюты необходимо осуществлять только через резидента Парка высоких технологий.

Административная ответственность за совершение таких правонарушений наступает с 16 лет. Влечет наложение штрафа в размере от двадцати до пятидесяти базовых величин с конфискацией до ста процентов суммы дохода, полученного в результате такой деятельности, орудий и средств совершения административного правонарушения или без конфискации.

Рекомендации для безопасного использования сети Интернет.

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;

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).

Для подростков в возрасте от 14 до 17 лет:

- интересуюсь, 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 от использования сети для совершения 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 не умалчивать данные факты, а незамедлительно сообщать о них в правоохранительные органы.

Запомните, в случае, если Вы или Ваши близкие пострадали от действий злоумышленников, необходимо незамедлительно:

сделать скриншоты переписки и не удалять телефонные номера злоумышленников;

сообщить в милицию: по телефону 102 или в чат-бот МВД «Мы всегда рядом!»;

заблокировать банковскую карту или счет.