МАТЕРИАЛ
для членов информационно-пропагандистских групп
(март 2025 г.)

О ПРОФИЛАКТИКЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, В ТОМ ЧИСЛЕ ВЫМОГАТЕЛЬСТВ И МОШЕННИЧЕСТВ

Материал подготовлен
Управлением Следственного комитета Республики Беларусь
по Гродненской области

Состояние преступности в сфере противодействия киберпреступности.

Согласно статистике за 2024 год на территории Гродненской области по линии противодействия киберпреступности зарегистрировано **1848** преступлений (против 1529 в 2023 году), из которых **1715** (92,8%) – хищения денежных средств: **1056** (за 2023 год – 301) – совершенных **путем мошенничества**, 593 (1096) – путем модификации компьютерной информации и 66 (23) – путем **вымогательства**.

За январь – февраль 2025 года – **322** преступления (433 за аналогичный период 2024 г.), из которых **312** (96,8%) – хищения денежных средств: 181 (277) – путем мошенничества, 121 (105) – путем модификации компьютерной информации и 10 (18) – путем вымогательства.

Отмечается лавинообразный рост распространения злоумышленниками в социальных сетях, мессенджерах и иных интернет-ресурсах различного рода ссылок на фишинговые ресурсы, в том числе в ходе рекламы фейковых инвестпроектов и акций от имени крупных белорусских компаний, банковских учреждений и трейдинговых компаний по торговле активами, в том числе подкрепленной созданными посредством нейросетей и искусственного интеллекта дипфейками с поддельными изображениями и видеороликами известных медийных личностей и представителей власти.

В 2024 году отделом цифрового развития предварительного следствия УСК по Гродненской области (далее – ОЦРПС) по уголовным делам региона выявлен **121** фишинговый интернет-ресурс и инициирована их блокировка, в текущем году – **28**.

Кроме этого, ОЦРПС путем мониторинга сети Интернет дополнительно за последние 4 месяца выявлены до момента противоправного использования злоумышленниками в отношении

граждан республики **262** аналогичных фишинговых ресурса, по которым также приняты меры к блокировке. Их количество продолжает расти.

Хищение денежных средств **путем модификации компьютерной информации** злоумышленниками совершается в результате получения доступа к банковскому счету с использованием переданных владельцем счета реквизитов банковской карты, путем доступа к системе интернет-банкинг или к мобильному устройству потерпевшего через удаленные программы.

Хищение **путем мошенничества** совершается в результате использования преступником так называемых методов социальной инженерии, когда потерпевшего вынуждают под видом звонка от сотрудника банковского учреждения или правоохранительных органов (все чаще встречаются смешанные схемы от имени разных структур) добровольно осуществить перевод денежных средств для их «сохранения», «декларирования», под предлогом «избежать их изъятие в ходе обыска», с целью поимки мошенника или нечистого на руку работника банка, под предлогом инвестирования в трейдинговые биржи, активы и т.п., а также в качестве предоплаты за товар в фейковом интернет-магазине, за аренду жилья и т.д.

Зафиксированные факты **вымогательства** в Интернете в большей части связаны с высказыванием требований перевода денежных средств под угрозой блокировки «Айфона» после авторизации в чужой учетной записи iCloud, распространения в сети интимных материалов, «попавших» в руки злоумышленнику в ходе доверительной переписки на сайтах знакомств, в социальных сетях, мессенджерах. Доступ к таким материалам злоумышленник также может получить после взлома страниц в социальных сетях и в иных аккаунтах.

Наиболее распространенные схемы и способы, которые используют преступники для хищения денежных средств в сети Интернет.

1. Телефонные звонки **от имени работников банковских учреждений и сотрудников правоохранительных органов** (предлоги)**:**

банковский **счет в опасности** и необходимо перевести деньги на «безопасный счет»;

мошенники **оформили кредиты** на гражданина и для противодействия нужно оформить самому кредиты на максимальную кредитоспособность и перевести деньги на названные счета;

потерпевший участвует в некой **спецоперации** по поимке преступников либо якобы недобросовестных работников банка, поэтому необходимо выполнять нужные действия;

по счету гражданина зафиксированы **преступные финансовые операции**, поэтому будет проведен обыск, а чтобы этого избежать

необходимо «задекларировать» все имеющиеся средства путем перевода на специальный счет;

звонок от имени родственников, **якобы попавших в ДТП** и для смягчения ответственности надо перевести деньги либо передать их курьеру;

Гродненский МОСК	16.01.2025	ст.209 ч.3	Неустановленное лицо в январе 2025 посредством телефонных звонков в мессенджере «Viber», представившись сотрудниками правоохранительных органов, под предлогом сохранности денежных средств, завладело денежными средствами жительницы Гродно на общую сумму 12000 рублей, которые **последняя самостоятельно** перевела на указанный злоумышленником счет
Лидский РОСК	16.01.2025	ст.209 ч.3	Неустановленное лицо посредством переписки в мессенджере «Телеграмм», под предлогом **предотвращения последующих арестов банковских** счетов, завладело принадлежащими жителю г. Лида денежными средствами в сумме более 20 000 рублей, которые последний перевел на указанные злоумышленником счета

Все чаще схема со звонками приобретает гибридный характер. Причем, злоумышленники представляются не только работниками банков и сотрудниками правоохранительных органов, но и **операторов связи А1 и МТС,** указывают о необходимости скачать якобы официальное приложение либо перейти по ссылке и предоставить доступ к телефону, **а также работниками «**Энергосбыта», «Водоканала» и других служб под предлогом замены **счетчиков** – просят паспортные данные, затем поступает звонок от другого мошенника, который представляется сотрудником правоохранительных органов и указывает, что с использованием переданных личных данных на гражданина оформлены кредиты и нужно выполнять его инструкции – оформить новые кредиты, перевести все деньги на «безопасный счет», задекларировать и т.д.

ГМОСК	24.01.2025	ст.212 ч.3	Неустановленное лицо, 21.01.2025, посредством звонков в мессенджере «WhatsApp» под предлогом **продления договора по оказанию услуг оператора** сотовой связи, убедив установить **приложение удаленного доступа** «Мой МТС», совершило хищение принадлежащих жителю г. Гродно более 10 000 рублей, осуществив их перевод со счета потерпевшего на неустановленный счет злоумышленника
ГМОСК	20.01.2025	ст.212 ч.1	Неустановленное лицо 20.01.2025 посредством телефонных звонков в мессенджере «Viber», а также предоставления неустановленного фишингового сайта, представившись сотрудником «**Водоканала»**, завладело принадлежащими жительнице г. Гродно реквизитами БПК ОАО «Приорбанк», откуда перевело более 2 800 рублей на иные счета

СХЕМ при осуществлении звонков у злоумышленников МНОЖЕСТВО – но они используют 2 способа хищения (убеждают граждан перевести денежные средства **самостоятельно** либо пытаются **получить «ключи»** от счета – реквизиты банковских карт (БПК), коды из СМС, получить удаленный доступ к телефону путем предложения установить предложенную программу по предоставленной ссылке, перейти по ссылке и ввести в форму личные и финансовые данные).

НУЖНО ЗНАТЬ:

банковский счет **априори** в безопасности (если никакие личные данные гражданином не предоставлялись и не вводились на неизвестных ресурсах, особенно по предложению звонящих лиц, в том числе не устанавливались какие-либо программы);

работники банка, сотрудники правоохранительных органов **не будут просить личные данные**, **коды** из СМС, просить совершать какие-либо действия со счетом, **не звонят в мессенджерах**;

работники банка **САМОСТОЯТЕЛЬНО** при подозрениях **заблокируют** счет/аннулируют кредит и т.п.

При таких просьбах в ходе звонка – необходимо взять паузу (обдумать происходящее: со счетом же ничего не совершал, карту не терял), **не передавать никаких данных и не совершать никаких действий**; ПРИ ЛЮБЫХ ПРОСЬБАХ ПРЕДОСТАВИТЬ ЛИЧНЫЕ ЛИБО ФИНАНСОВЫЕ ДАННЫЕ - **завершить разговор** и перезвонить в свой банк либо в ОВД;

Кроме этого, потерпевшему звонящим также могут высылаться в мессенджере фотографии служебных удостоверений, злоумышленники инструктируют как себя вести при оформлении кредита в банке. Преступники действуют настолько убедительно, что зачастую потерпевшие осуществляют переводы в течение нескольких дней, имея реальное время подумать над происходящим. Очень часто происходят инсценировки с несколькими лицами (звонящими)

2. ТОРГОВЛЯ на ФЕЙКОВЫХ ТРЕЙДИНГОВЫХ БИРЖАХ и участие в фейковых инвестпроектах («БелТрансГАЗ, «Газпром Инвест» и т.п.) Схемы отмечаются **большим ущербом**.

В сети интернет размещены множество интернет-сайтов, имитирующих различные **фейковые интернет-биржи** для заработка денежных средств на торгах. Спам реклама о данных сайтах распространяется повсюду в сети Интернет. Нередко переходу на такой сайт предшествует знакомство в сети парня с «девушкой», рекламирующей определенный сайт как «прибыльный». Доверчивые граждане переходят по ссылке, не проверив историю и отзывы ресурса, вступают с так называемыми представителями биржи в переписку.

Граждан убеждают в высоких доходах, чему способствуют содержащиеся на ресурсе красивые фейковые отзывы об эффективности торгов. Убеждают перечислять деньги на предоставленные номера банковских счетов, нередко на криптокошельки. Для убедительности создают «жертвам» личные аккаунты на данных сайтах, где якобы отображаются суммы внесенных денежных средств. А когда человек решает вывести «имеющие на счету» и вложенные деньги, начинается «история» о необходимости внесения налога, страховки, компенсации и т.д., вынуждая потерпевшего вносить очередные суммы денег средств. При этом «жертве» вначале могут дать заработать около 100 рублей для создания видимости успешности проекта.

ГМОСК	30.01.2025	ст.209 ч.3	Неустановленное лицо, в период времени с 13.01.2025 по 23.01.2025, находясь в неустановленном месте, посредством переписки в мессенджере «Телеграм» с аккаунта @LubimovaTat1, под предлогом инвестирования **денежных средств на бирже**, завладело денежными средствами жителя г. Гродно на общую сумму 16 000 рублей, которые потерпевший в самостоятельно перевел на счета, указанные злоумышленником (platformdonald.com)
Волковысский РОСК	21.01.2025	ст.209 ч.3	Неустановленное лицо, в период с 26.12.2024 по 21.01.2025, находясь в неустановленном месте, по средствам мобильного приложения «Ватсапп», под предлогом заработка в сети Интернет при осуществлении торговли на валютной бирже, на неустановленном интернет-ресурсе, обманным путем убедило жительницу Волковысска перечислить 18 000 рублей на различные счета по представленным реквизитам

НУЖНО ЗНАТЬ

ряд фейковых сайтов в сети Интернет позиционируют себя биржами, коими не являются, нет полных гарантий в заработке и исключении потери денежных средств;

такие сайты могут быть созданы за считанное время из любой точки мира, найти их владельцев крайне затруднительно;

абсолютное большинство таких сайтов имеют в Интернете крайне отрицательные отзывы, которые легко найти путем поисковых запросов в сети;

фейковые биржи, как правило, созданы (зарегистрированы) не более года назад, а то и месяцы до начала функционирования, что легко проверить в сети Интернет;

для указанной деятельности нужные большие познания и опыт работы с официальными известными интернет-ресурсами, абсолютное большинство таких ресурсов и реклама на них в социальных сетях – **ФЕЙК!**

Кроме этого, в сети Интернет распространяется много фейковых ресурсов, рекламирующих услуги от имени юристов, юридических и других организаций, агентств и фондов в оказании помощи по возврату переведенных средств мошенникам и лжеброкерам, когда злоумышленники вновь попросят перевести денежные средства за сои услуги, предоставить реквизиты счета и так далее. Известны случаи, когда таким образом граждане дважды теряли своим деньги.

3. Третья схема – **фейковые интернет-магазины** по **продаже товаров** (обувь, одежда, мебель, цветы, морепродукты и т.д.) и **предоставлении услуг**, в частности в социальной сети **«Инстаграм».** Страницы с изображением красивых товаров, у которых стоимостью ниже рыночной, с большим числом подписчиков и рядом положительных отзывов – не вызывают у будущих жертв сомнений в подлинности. Желая приобрести тот или иной товар, граждане осуществляют перевод денег за них в качестве предоплаты или полной оплаты на подконтрольные злоумышленникам счета.

Щучин	22.01.2025	ст.209 ч.1	Неустановленное лицо, находясь в неустановленном месте, в социальной сети «Instagram» с сетевым именем «by.littlekids» (ID 44902229717), в период с 11.01.2025, под предлогом продажи детской коляски, совершило хищение денежных средств жительницы Щучина в сумме более 500 рублей, которые были перечислены последней на банковский счет злоумышленника
ГМОСК	27.01.2025	ст.209 ч.1	Неустановленное лицо, в период с 22.01.2025 по 16.29 часов 23.01.2025, посредством переписки в социальной сети «Instagram» с имени пользователя @hall_konfiscate и в мессенджере «Telegram» с имени пользователя @Artemhall, под предлогом продажи мобильного телефона «iPhone 14 Pro», завладело принадлежащими жителю Гродно денежными средствами в сумме 1000 рублей, которые последний перевел на указанный злоумышленником счет

<u>НУЖНО ЗНАТЬ:</u>

ранее неизвестные интернет-магазины, работающие только по предоплате и предлагающие товары стоимостью ниже рыночной, исключительно с положительными отзывами – высокий риск потери средств;

фотографии имеющихся товаров на множестве разных фонов (в разных помещениях) – один из признаков фейкового магазина, данные фото скачаны в сети Интернет;

подобные фейковые аккаунты легко создаются в считанные часы, отзывы и подписки искусственно накручиваются, их владельцы могут находиться в любой точке мира, что усложняет их установление;

более безопасно осуществлять покупки в интернет-магазинах на известных и проверенных интернет-площадках (известные маркетплейсы);

при онлайн-покупках рекомендуется не использовать основную банковскую карту, а оформить виртуальную и перед совершением покупки переводить на нее необходимую сумму.

4. Четвертая – ФИШИНГ - фишинговые сайты банков (интернет-банкинг, акции по выплате бонусов и вознаграждений за прохождение опросов), а также – фишинговые СЕРВИСЫ служб доставки или оплаты (от имени «CDEK», «Europochta» и др.)

В сети Интернет могут появляться ряд сайтов, имитирующих стартовые страницы интернет-банкинга. Желая зайти в приложение, граждане ищут страницу интернет-банкинга своего банка путем поискового запроса в браузере. Нередко в первых результатах поиска за названием аббревиатуры финансового учреждения кроется ссылка на фишинговый сайт, внешне ничем не отличающийся от оригинала, но имеющий иной адрес в браузерной строчке. Отличаться может одним символом от правильного адреса. Вводя на таком сайте логин и пароль владелец счета предоставляет доступ к интернет-банкингу, а это полный доступ к счету. Через считанные минуты денежные средства переводятся на иной счет.

Нередко пользователи сети могут наткнуться на различные рекламные акции белорусских банков, размещенные на неофициальных веб-сайтах. Как правило, для получения вознаграждения, там необходимо ввести реквизиты банковской карты, 3-хзначный номер и поступивший код из СМС, но вместо выигрыша происходит списание денежных средств со счета.

ГМОСК	06.08.2024	ст.212 ч.1	Неустановленное лицо 30.07.2024, находясь в неустановленном месте, с использованием фишинговой ссылки «https://oprosbyn.online», под предлогом прохождения опроса на качество услуг ЗАО «Альфа-Банк», завладело реквизитами БПК и кодами из СМС жительницы Гродно и похитило с ее карт-счета 8000 рублей

Стоит помнить, что фишинговые ссылки могут быть предоставлены и на сайтах покупки/продажи товаров, под видом покупки товаров с предоставлением форм для ввода реквизитов БПК для получения денежных средств. Нередки случаи, когда после получения злоумышленником денежного перевода, с целью дальнейшего хищения он под видом возврата средств (например, товар закончился) убеждает потерпевшего предоставить перейти по предоставленной ссылке и в фейковое поле на интернет-странице ввести реквизиты БПК якобы для

получения средств обратно, однако, завладев реквизитами, с их использованием злоумышленник похищает денежные средства с карт-счета

Лидский РОСК	06.01.2025	ст.212 ч.1	Неустановленное лицо, 05.01.2025, находясь в неустановленном месте, посредством переписки в мессенджере «Telegram» от имени пользователя «Роман», представившись продавцом магазина «seafood.by», под предлогом возврата денежных средств за непредоставленный товар, с использованием фишинговой ссылки https://transfer-bell.online/835a2f53-0475-4506-87b0-9ae74e8621ed, завладело денежными средствами жительницы г. Лида в сумме более 860 рублей

НУЖНО ЗНАТЬ

При осуществлении доступа к системе интернет-банкинг помните:

нельзя искать сайт интернет-банка **путем поискового запроса** в браузере. Адрес сайта банка (страницы интернет-банкинга) нужно знать и вводить «вручную» в адресной строке. А лучше добавить в список закладок браузера, или использовать мобильное приложение. **Акции от имени банков о выплате средств за прохождение анкетирования или опроса – ФЕЙК! Не вводите личные или финансовые реквизиты после перехода по неизвестным ссылкам.**

5. Пятая – интернет вымогательство. В ходе доверительного общения в сети Интернет (например, с парнем от имени девушки в мессенджере или социальной сети) **злоумышленник получает интимные материалы, после чего** за неразглашение их требует перевода денежных средств. Известны ряд фактов, когда при аналогичных переписках с «обратной стороны сети» пользователь просит на Айфоне авторизоваться потерпевшего в чужой учетной записи **iCloud**, после чего, зная пароль, удаленного блокирует телефон и требует деньги за разблокировку.

НУЖНО ЗНАТЬ

за «аватаркой» друга или случайного знакомого может скрываться преступник, не стоит распространять в сети личные материалы или финансовые данные;

никогда не входите по просьбе случайных знакомых в учетную запрись **iCloud** или иные

6. Шестая – набирает популярность у злоумышленников **схема «Фейк-босс»**

Следственным комитетом отмечается рост преступлений, сопровождаемых несанкционированным доступом к учетным записям

интернет-мессенджеров и социальных сетей в отношении работников организаций и предприятий.

Злоумышленники изучают средства обмена сообщениями (данные участников переписки, содержание сообщений в чатах, группах, каналах и личных переписках) в различных мессенджерах и социальных сетях, используемых работниками для коммуникации, определяют учетные записи руководителей, создают копии их учетных записей и вступают в личную переписку с иными участниками таких чатов.

В ходе переписки, выдавая себя за руководителя, злоумышленник сообщает вымышленные сведения о том, что работником интересовались сотрудники правоохранительных органов (называет данные этих «сотрудников») и настаивает на сохранении конфиденциальности факта общения. Указанный психологический прием в ряде случаев снижает уровень критической оценки гражданином последующих действий преступников, обеспечивая беспрекословное выполнение поступающих от них указаний.

Далее гражданину поступают звонки посредством мессенджеров или телефонной связи от якобы сотрудников правоохранительных органов, а также банковских учреждений, в некоторых случаях с демонстрацией посредством мессенджеров фотографии поддельных служебных удостоверений. В ходе беседы псевдосотрудники убеждают в необходимости совершения определенных действий, в том числе по перечислению денежных средств под различными мошенническими предлогами.

НУЖНО ЗНАТЬ:

при поступлении подобных сообщений в мессенджерах проверять принадлежность соответствующей учетной записи тому лицу, именем которого учетная запись названа и (или) фотоизображение которого присутствует в профиле (сверить абонентский номер, связаться с владельцем учетной записи по иным каналам связи);

никому не сообщать реквизиты банковских карт, аутентификационные данные для доступа к банковским счетам, содержание sms-сообщений, поступивших на личные абонентские номера;

в случае осуществления несанкционированного доступа к учетной записи интернет-мессенджера или социальной сети принимать незамедлительные меры по уведомлению о случившемся граждан, общение с которыми осуществлялось в указанном интернет-мессенджере или социальной сети, с целью предупреждения о возможных попытках осуществления в отношении них преступных действий;

незамедлительно информировать о выявленных попытках руководство организации (предприятия) для принятия мер по упреждению подобных действий и правоохранительные органы для реагирования.

Также (реже) в Гродненской области фиксируются иные схемы киберпреступлений:

оплата на сомнительных сайтах **услуг оформления виз** для выезда в другие страны;

перевод денег **«возлюбленному»**, представляющемуся женщинам в переписке в мессенджере «военным», «врачом», «умирающим миллионером», «актером», попавшему в сложную ситуацию, требующую оплаты расходов для приезда в Республику Беларусь, растаможивания «ценного подарка» и т.п. (например, известен факт общения от имени актера Киану Ривза);

завладение деньгами в виде предоплаты по объявлениям об **аренде жилья;**

завладение под видом фейковых объявлений о помощи больным людям **(благотворительность)**,

хищение путем просьб **об одолжении** денежных средств в социальной сети или в мессенджере обратившемуся **в переписке «другу»**.

ВАЖНО ЗНАТЬ:

ряд сайтов либо аккаунтов могут быть фейковыми, они создаются в любой точке мира, нельзя решать любые финансовые вопросы в сети Интернет, обстоятельства уточнять личным звонком или при встрече; нельзя сообщать личные и финансовые данные; переходить по неизвестным ссылкам и сайтам, когда потребуется ввод личных данных и реквизитов (паспортные данные, реквизиты БПК, коды из СМС, логины и пароли к ученым записям, скачивание программ, подтверждение запроса на подключение аккаунта на второе устройство и т.д

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, но всем гражданам в любой ситуации следует не терять бдительность, обдуманно относится ко всему происходящему в сети Интернет. Необходимо мыслить критически и не принимать поспешных решений. Посоветуйтесь с членами семьи или друзьями. Ведь в большинстве случаев излишняя доверчивость и неосмотрительность самих граждан способствует совершению вышеуказанных преступлений.