Материалы

для членов

информационно-пропагандистских групп

(август, 2025 г.)

**Современные способы совершения киберпреступлений**

 *(дополнительная тема)*

В настоящее время киберпреступность представляет серьезную угрозу для развития экономики и общества. За последние годы количество киберпреступлений значительно увеличилось, что требует принятия срочных мер для защиты информации и обеспечения кибербезопасности. Одной из основных проблем является недостаточная осведомленность о кибербезопасности среди населения. Многие граждане не принимают достаточных мер предосторожности при использовании сети Интернет, что делает их уязвимыми перед преступниками.

В 2023 году в Витебской области совершено более 1,5 тысяч киберпреступлений, материальный ущерб составил свыше 2,5 миллионов рублей. Женщины в 2 раза чаще становятся потерпевшими, чем мужчины. Абсолютное большинство проживает в городах. Люди с высшим в равной степени, как и со средним образованием, подвержены обману. Среди жертв киберпреступников, в основном, экономически активные граждане, представляющие практически все сферы деятельности – бухгалтеры, экономисты, директоры, заместители директоров частных и государственных учреждений, начальники управлений и отделов госучреждений, педагоги, врачи и медсестры, студенты, юристы, программисты и представители других специальностей.

Мошенники регулярно меняют свои схемы обмана граждан, чтобы похитить их деньги.

Основными формами обмана являются телефонное мошенничество и фишинговые ресурсы.

**ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО – ВИШИНГ**

Мошенники под видом работников банка или государственных органов обращаются к гражданам, создают стрессовую ситуацию, сообщают о проблеме, а потом предлагают помощь в ее решении. При этом, чтобы войти в доверие, могут выслать фото служебных документов или даже выйти на видеосвязь в мессенджере.

Распространен способ, когда мошенники, используя различные вымышленные ситуации, убеждают потенциальных жертв установить **определенное мобильное приложение**. Оно дает возможность удаленно управлять устройством, на котором установлено. Также злоумышленники убеждают **оформить кредиты в банках**, а деньги перевести на «защищенный» счет.

Мошенники для совершения преступлений изучают свою жертву, собирают в сети Интернет данные о ней и ее интересах, окружении и прочем. Имея образец голоса или фото знакомых, могут создавать фейковые сообщения или видеосообщения.

Мошенники регулярно подбирают новые способы обмана, чтобы получить деньги. В сети Интернет размещают рекламу якобы **инвестиционных платформ**, которых на самом деле не существует, чтобы заманить вкладчиков и похитить их деньги. Первым шагом для связи с куратором является заполнение формы, где необходимо оставить свои имя и телефон. Далее с заинтересовавшимся связывается так называемый куратор, под руководством которого в надежде заработать легкие деньги потенциальная жертва сама переводит деньги на электронный кошелек. Чтобы получить хотя бы вложенные деньги обратно, мошенники требуют заплатить комиссии, взносы и т.д. Некоторое время мошенники рисуют жертве их прибыль, пока у обманутого человека не закончатся деньги, потом связь с ним прекращается. Деньги остаются на мошеннических счетах.

Чтобы не стать жертвой киберпреступника, как можно раньше закончите разговор с неизвестным лицом, кем бы он не представился.

**ФЕЙКОВЫЕ МАГАЗИНЫ в соцсетях.** Ежедневно в милицию обращаются и те, кто сами перевели **предоплату за товар**, который нашли в объявлениях в социальных сетях и на торговых площадках, и не получили его. Мошенники намеренно создают аккаунты от имени магазинов, в которых размещают объявления несуществующих товаров с заниженными ценами (обувь, одежда, мобильные телефоны, постельное белье, новогодние ели, садовые кресла-качалки-коконы и другие товары). Потенциальный покупатель связывается с администратором «магазина», ему обещают доставить товар после полной оплаты. Оплату предлагают произвести на банковскую карту или на счет через ЕРИП. Однако после получения денежных средств, товар не высылают, а покупателя блокируют.

**ФИШИНГ** С целью получения личных данных владельцев счетов мошенники создают страницы-клоны банков, сайтов театров, кальянных и инвестиционных (торговых) бирж.

Для предотвращения подобного необходимо:

* задуматься о причинах низкой цены на товар, отличающейся от цены за тот же товар на сайте или насторожиться почему у магазина нет сайта ;
* тщательно проверять информацию о магазине: связаться с продавцом по белорусскому номеру по мобильной связи, а не через Интернет;
* использовать отдельную карту для расчетов в сети Интернет;
* не переходить по ссылкам от неизвестных вам лиц;
* проверять адрес страницы, где вводите данные карты (для белорусских организаций в адресной строке должно быть так: «название сайта»/BY/«раздел сайта»);
* подключить в настройках карты бесплатную услугу от банка «3-D Secure».

**СВАТИНГ** В молодежной игровой киберсреде распространяется тренд под названием «сватинг». Его суть заключается в том, чтобы создать неблагоприятную обстановку госорганам, нарушить режим их работы, или отомстить своему обидчику, создав для него проблемы с правоохранительными органами.

**ПРЕДПРИЯТИЯ** В области регистрируются киберпреступления, направленные на завладение денежными средствами субъектов хозяйствования, в том числе, государственных предприятий Республики Беларусь.

Хакеры заранее планируют и получают несанкционированный доступ к данным организации, превращают их в беспорядочный набор символов и предлагают расшифровать их после перечисления денежных средств на указанный счет. Злоумышленники прежде всего рассчитывают на человеческие ошибки и слабости, а не на уязвимость программного обеспечения, которую гораздо сложнее преодолеть.

Необходимо понимать, что злоумышленник не сможет достичь своей цели и похитить денежные средства, если атака будет своевременно выявлена и остановлена, а это возможно на любом ее этапе при принятии соответствующих мер защиты, направленных на сохранение благосостояния, в том числе при соблюдении работниками следующих правил:

1. **обеспечивать должный уровень информационной безопасности** в соответствии с развитием и обновлением программного обеспечения, а также нормативно-правовыми актами Республики Беларусь
2. **регулярно осуществлять резервное копирование** важных данных;
3. **никогда не доверять отправителю электронного письма**, перепроверять указанную информацию, а также основные идентификационные данные и служебные заголовки электронных писем (можно узнать и проанализировать ip-адрес отправителя письма и иную необходимую информацию), прежде чем ответить на письмо, даже если вам пишет давний партнер с нового адреса;
4. **не переходить по ссылкам и не открывать вложения**, если отправитель письма не тот, кем он представился;
5. в случае изменения реквизитов расчетного счета партнера, **устанавливать данный факт по любым другим каналам связи** (лично, по телефону и т.д.);
6. **использовать ключ ЭЦП (электронной цифровой подписи) непосредственно при работе** с соответствующим программным обеспечением, извлекать его из USB-порта после окончания работы;
7. **тщательно проверять адрес сайта;**
8. **своевременно менять пароли к учетным записям**, в том числе при перемещении, увольнении или приеме нового работника;
9. **перепроверять происхождение сайта**, прежде чем ввести персональные данные (адрес, домен, дата создания, реквизиты доступа, финансовые сведения);
10. **немедленно сменить пароль и(или) заблокировать счета** в случае введения реквизитов доступа на подозрительном сайте;
11. **всегда быть бдительным** и проверять полученную информацию.

*Справочно:*

*Городокский район.*

*Оперативная обстановка по направлению деятельности противодействия киберпреступности в Городокском районе имеет негативную динамику увеличения числа регистрируемых киберперступлений за текущий период зарегистрировано 16, 2024 – 9 (рост числа зарегистрированных преступлений составил 43,75%). За прошедший период совершено 3 преступления относящееся к категории тяжких преступлений, за аналогичный период 2024 года, было совершено 1 преступление, относящееся к категории тяжких рост, составил (+300%).*

*По способам совершения киберпреступлений:*

*1) Основным и самым главным способом совершения мошенничеств (ст. 209 УК Республики Беларусь) на территории г. Городка и Городокского района (****всего совершено 10 преступлений, общий ущерб составил 53 000 рублей****), является звонок в мессенджерах «Вайбер», «Ватсап», «Телеграм», представителями МТС, водоканала и энергосбыта, под предлогом продления срока действия договора, завладевают паспортными данными лиц, которым звонят. Затем поступает звонок также посредством мессенджера от сотрудников правоохранительных органов (МВД, ДФР, КГБ, КГК и т.д.) в форменном обмундировании, зачастую в формате видео, на фоне расположена государственная атрибутика и портрет Президента Республики Беларусь, потерпевшему поясняют, что ему только что звонили мошенники, которых они сейчас разрабатывают, сейчас на их персональные данные мошенниками будет оформлен кредит, для предотвращения данной операции, необходимо оформить кредит и перечислить его на так называемый «безопасный счёт» для сохранности. Потерпевшие, убеждаясь, что действую по согласованию с правоохранительными органами, добровольно берут кредиты, передают данные банковских карт и при помощи различных приложений, мошенники дистанционно похищают денежные средства наших граждан;*

*2) Также на территории обслуживания ОВД Городокского райисполкома совершено 3 преступления предусмотренных ст. 208 УК Республики Беларусь (вымогательство), преступления совершены следующими способами:*

*– переписка с потерпевшим лицом на сайте знакомств в мессенджерах, после чего мошенник поясняет, что имеет проблемы с мобильным телефоном и просит потерпевшее лицо зайти с его аккаунта в своё мобильное устройство (к примеру icloud). Зайдя с аккаунта злоумышленника потерпевший теряет доступ к своему устройству, так как оно заблокировано и с целью разблокировки устройства, мошенник требует выплатить ему денежные средства;*

*– взлом сервера предприятия путем перехода по неизвестной ссылке, которая как правило поступает на электронную почту предприятия. После перехода по ссылке, все электронные документы предприятия блокируются без возможности восстановления. После чего злоумышленники требуют денежные средства за разблокировки электронных документов;*

*– переход по ссылке в мессенджере, после чего мошенники получают доступ к мобильному устройству потерпевшего лица, а также имеют возможность получения личных данных. После чего требуют денежные средства за нераспространение личных данных и даже в случае выплаты требуемых денежных средств, всё равно проводят распространение личных данных среди контактов потерпевшего (в том числе и фотографий интимного характера, находящихся в памяти мобильного устройства потерпевшего;*

*Общий ущерб от вышеуказанных преступлений составил 4 200 рублей.*

*3) заработки на бирже также являются распространенным способом совершения интернет мошенничеств, на территории Городокского района возбуждено 2 уголовных дела с общим ущербом 2700 рублей. Основным способом совершения данного преступления является переписка в мессенджерах с предложением заработка денежных средств, потерпевшее лицо в течении месяца обучают способам заработка (покупка акций и криптовалюты), после чего при внесении денежных средств потерпевшее лицо получает незначительную выгоду, а затем при внесении большей суммы денежных средств (в том числе путем оформления кредитов), и в последующем после внесения денежных средств мошенники перестают выходить на связь.*

*4) приобретение товаров в мессенджере «Инстаграм», потерпевший при просмотре ленты новостей в мессенджере, находит группу по продажи различных товаров. При переходе на главную страницу группы, видит большое количество положительных отзывов и при выборе товара начинает переписку с мошенниками. После чего при выборе конкретного товара договариваются о доставлении товара по почте и внесении предоплаты, после чего мошенники уведомляют, что товара нет в наличии и что необходимо вернуть денежные средства потерпевшему, для этого необходимо перейти по ссылке и ввести реквизиты БПК, при выполнении данных действий происходит списание денежных средств находящихся на счету потерпевшего и более ответов на сообщения не поступает.*

*Вымогательств в 2025 году возбуждено 2 уголовное дело по ч. 1 ст. 208 УК Республики Беларусь, а именно:*

*Значительная часть потерпевших лиц проживает* ***в городе – 13 (83,25%)****,* ***в сельской местности – 3 (18,75%)****.*

*Установлено, что потерпевшими признаны* ***8 мужчин (50%) и 8 женщин (50%)****. Имеют* ***высшее образование*** *– 3 (18,75%),* ***среднее-специальное*** *– 2 (12,5%),* ***среднее*** *– 8 (50%),* ***профессионально-техническое*** *– 3 (18,75%).*

*По социальному положению наибольшее количество относится к категории* ***рабочий*** *– 10 (62,5%),* ***учащиеся*** *– 3 (18,75%),* ***временно безработные*** *– 3 (18,75%).*

*По возрасту потерпевшие лица распределились следующим образом:*

*до 18 лет – 2 (12,5%);*

*от 18 до 30 лет – 2 (12,5%);*

*от 31 до 40 лет – 2 (12,5 %);*

*от 41 до 50 лет ­– 3 (18,75%);*

*от 51 до 60 лет – 3 (18,75%);*

*от 61 до 70 лет – 4 (25%);*

*от 71 до 80 лет – 0*

*от 81 года – 0*

*Самыми популярными способами совершения преступлений по-прежнему являются разговоры в мессенджерах ­– 12 (75%), взломы устройств – 3 (18,75%), покупки в социальных сетях ­– 1 (6,25%).*

*Общий ущерб составил 65 000 белорусских рублей.*

***Чтобы не стать жертвой мошенников, необходимо руководствоваться следующими правилами:***

*– МОШЕННИКИ УБЕЖДАЮТ, представляясь сотрудниками правоохранительных органов, банковских организаций или руководителями вашей организации убеждают в мессенджерах и социальных сетях:*

*–получить кредит, чтобы отменить якобы оформленный неизвестными на ваше имя другой кредит и перевести деньги на специальный счёт;*

*– установить программное обеспечение, якобы для предотвращения мошеннической атаки на ваш счёт;*

*– перевести накопления на якобы безопасный счёт, чтобы не изъяли при обыске;*

*– передать личные данные и код из смс, такие сведения предоставляют мошенникам доступ к счету и сервису.*

*В социальных сетях и на торговых площадках убеждают:*

*– перевести предоплату за несуществующий товар в лжемагазине или по измененным реквизитам банка;*

*– перейти по поддельной ссылке банковской системы и ввести личные данные (логин и пароль, номер и трехзначный код с оборотной стороны банковской карты, код из СМС, кодовое слово);*

*– перечислить деньги на карту или оплатить родственнику, другу, любящему человеку;*

*­­­– на поддельной бирже вложить деньги в проект, якобы для получения пассивного дохода.*