Об актуальных способах и методах совершения киберпреступлений, а также рекомендации по их недопущению

Глобальная сеть Интернет стала незаменимым средством повседневной связи и обмена информацией по всему миру, и преступники этим пользуются. Киберпреступность стремительно расширяет свой масштаб, она проникла во все сферы общественной жизни, включая бизнес-структуры, общественную и личную жизнь граждан.

Практически ежегодно в столице наблюдается рост регистрируемых преступлений, совершенных в сфере высоких технологий. Устойчивая тенденция увеличения количества совершаемых киберпреступлений обусловлена активным развитием информационных технологий. Широкое вовлечение процессов, связанных с жизнедеятельностью общества, в интернет-среду объективно изменило вектор противоправных деяний, все более направляя его в киберпространство.

В 2025 году киберпреступления в структуре общей преступности составили более трети (38,0%).

Справочно: 2015 год – 3,8%; 2016 год – 4,3%; 2017 год – 6,5%; 2018 год – 9,1%; 2019 год – 16,3%; 2020 год – 37,4%; 2021 год – 25,6%; 2022 год – 25,2%; 2023 год – 33,7%; 2024 год – 37,6%.

Принятые в 2025 году всеми заинтересованными предупредительные меры, в части проведения качественной профилактической работы с широким охватом населения, направленной на упреждение совершения киберпреступлений, в целом благоприятно повлияли на состояние криминогенной обстановки в сфере противодействия киберпреступности, что выразилось в снижении к концу 2025 года таких преступных деяний с сохранением указанной тенденции в предстоящем периоде.

Так, по итогам 2025 года количество зарегистрированных киберпреступлений в г. Минске снизилось на 11,5% в сравнении с 2024 годом (с 6 632 до 5 872).

В отчетном периоде отмечается снижение числа учтенных мошенничеств (-15,3%; с 3 499 до 2 964), совершенных с использованием информационно-коммуникационных технологий (далее – ИКТ), хищений путем модификации компьютерной информации (-3,6%; с 2 335 до 2 250), незаконных оборотов платежных инструментов, средств платежа и их реквизитов (-64,8%; со 145 до 51), заведомо ложных сообщений об опасности (-30,5%; со 187 до 130) и преступлений против компьютерной безопасности (-23,8%; с 227 до 173).

В структуре киберпреступности, как и прежде, превалируют ИКТ-мошенничества и хищения путем модификации компьютерной

информации (50,5% и 38,3% соответственно). В общей структуре преступности доля киберпреступлений незначительно возросла, составив 38,0% (2024 г. – 37,6%).

На фоне снижения количества зарегистрированных киберпреступлений увеличилось число особо тяжких и тяжких киберпреступлений (+18,3%; с 1 001 до 1 184), за счет роста тяжких мошенничеств (+21,4%; с 618 до 750) и хищений путем модификации компьютерной информации (+6,2%; с 354 до 376).

Из 1 184 тяжких киберпреступлений практически две трети составили мошенничества (63,3%; 750), треть – хищения путем модификации компьютерной информации (31,8%; 376), 3,9% (46) – незаконный оборот платежных инструментов, средств платежа и их реквизитов. Еще 1,0% (5 и 7 соответственно) составили вымогательства и заведомо ложные сообщения об опасности.

Подавляющее большинство зарегистрированных вымогательств сопряжено с блокировкой учетных записей Apple iCloud (157 из 302 или 52,0%) и угрозой распространения личной либо компрометирующей информации потерпевших (98 из 302 или 32,5%).

В отчетном периоде потерпевшими от вымогательств стали 299 человек, 155 из которых женщины (51,8%). При этом у 116 потерпевших женского пола злоумышленники вымогали денежные средства за разблокировку аккаунтов Apple (iCloud), из которых 74-м жертвам (на момент совершения преступления) исполнилось 8-17 лет.

Триггерами для предоставления несовершеннолетними потерпевшими доступа к своему «облаку» послужили: установка игр (Minecraft, Toca Boca World), «откат» операционной системы к предыдущей версии обновления, а также установка различных модификаций (upgrade) мессенджера Telegram (в основном возможность просмотра переписки конкретно интересующего пользователя).

Справочно: в 2025 году потерпевшим от блокировки учетных записей Apple iCloud стал 41 мужчина, из них 19 – возраста 11-17 лет.

Каждое четвертое зарегистрированное мошенничество относятся к категории тяжких (750 из 2 964).

В общем числе зарегистрированных мошенничеств преобладают:

- преступления, связанные с приобретением несуществующих товаров (услуг) на интернет-ресурсах (1 481 из 2 964 или 50,0%);
- звонки от имени представителей правоохранительных органов, банковских учреждений, сотовых компаний, работников коммунальных и телекоммуникационных предприятий, медицинских организаций (29,4%; 871 из 2 964);
- инвестирование (12,2%; 362 из 2 964).

От преступных посягательств кибермошенников в 2025 году пострадало 2 984 гражданина, из которых 1 741 женщина (2024 г. – 3 700, из которых 2 249 женщин).

1 503 человека пытались приобрести товары либо услуги посредством интернет-ресурсов (из них 782 – женщины). Путем вишинга мошеннические действия совершены в отношении 933 человек, из них более половины (489 или 52,4%) – в отношении граждан возраста 60 лет и старше (из них женщины – 394 или 80,6%).

Практически каждое второе хищение путем модификации компьютерной информации совершено путем фишинга (42,4%; 954 из 2 250). Еще треть таких преступных деяний осуществлена путем вишинга (765 или 34,0%), т.е. посредством звонков на стационарную и (или) мобильную связь, либо в мессенджеры (Telegram, Viber, WhatsApp) от псевдосотрудников правоохранительных органов, банковских учреждений и иных организаций. Каждое девятое хищение путем модификации компьютерной информации (255 из 2 250 или 11,3%) связано с физическим доступом к банковским платежным картам (далее – БПК) либо к системе дистанционного банковского обслуживания потерпевших (похищенные, утерянные, добровольно переданные БПК, использование мобильного телефона жертвы и т.п.).

Каждое шестое зарегистрированное хищение путем модификации компьютерной информации относится к категории тяжких (376 из 2 250).

Жертвами хищений путем модификации компьютерной информации стали 2 163 гражданина, из которых 1 375 (63,6%) женщин.

Справочно: от фишинга пострадало 972 гражданина, из них 636 женщин; от вишинга – 770 граждан, из которых 528 женщин.

Всего же в результате преступных посягательств по линии ПК по итогам 2025 года в столице пострадало 5 596 человек.

Актуальные способы совершения киберпреступлений

Мошенничества, связанные с приобретением несуществующих товаров (услуг) на интернет-ресурсах

Основная доля мошенничеств, совершаемых в столице, связана с приобретением различных товаров *(цветочная продукция, мобильные телефоны, предметы одежды, шины, мебель, сезонные товары, продукты питания и пр.)* и услуг *(аренда недвижимости, помощь в оформлении виз, туров и т.п.)* в сети Интернет.

Так, в социальной сети «Instagram» злоумышленники создают поддельные (фейковые) аккаунты (страницы) с высокими рейтингами

и отзывами покупателей, внушительным количеством подписчиков, где предлагают продажу товара по явно заниженной стоимости. Как правило, продажа интересующего товара предусматривает 100% предоплату (реже частичную), после внесения которой псевдопродавцы перестают выходить на связь с покупателем либо вовсе удаляют аккаунты.

Пример 1: в первых числах января текущего года Степан посредством социальной сети «Instagram» нашел интернет-магазин («Seafood.by»), специализирующийся на продаже морепродуктов. Для оформления заказа в шапке профиля была размещена ссылка на аккаунт в мессенджере «Telegram». Степан перешел по ссылке и оформил заказ на приобретение красной икры (500 гр.), произведя при этом полную предоплату за товар и его доставку на предоставленный продавцом номер БПК (150 бел.руб.). В связи с тем, что в оговоренный срок икра доставлена не была, Степан связался с продавцом и потребовал вернуть деньги. Продавец в свою очередь предоставил Степану ссылку (фишинговый сайт Альфа-Банка) для возврата денежных средств. Перейдя по указанной ссылке, Степан ввел полные реквизиты своей банковской платежной карты (16-значный номер, срок действия и CVV), после чего с нее были похищены все денежные средства.

Пример 2: 29.01.2025 Татьяна и Олег в мессенджере "Telegram" в группе "FlattyBy" нашли объявление о сдаче в аренду квартиры в г. Минске. Молодые люди списались с лицом, разместившим указанное объявление, и договорились об аренде квартиры. «Арендодатель» сообщил о необходимости внесения залога в размере 300 бел.рублей. Олег совершил перевод денежных средств в размере 300 бел.рублей на предоставленный ему номер БПК. В последующем неизвестное лицо заблокировало Олега в мессенджере "Telegram", а объявление было удалено.

Пример 3: в социальной сети «Instagram» 37-летний минчанин обнаружил аккаунт по продаже техники «hall_konfiscate». Перейдя по ссылке, указанной в шапке профиля, минчанин стал вести переписку в Telegram-канале с пользователем «Артем Кажуро» по поводу приобретения мобильного телефон марки «Iphone 14 pro» стоимостью 945 бел.рублей (с доставкой). В ходе переписки с неизвестным лицом, мужчина выбрал доставку указанного гаджета курьером, после чего внес 100% предоплату путем перевода на счет, реквизиты которого ему были предоставлены. После этого ему поступило сообщение, что заказ принят и доставка товара будет осуществлена через два дня. В назначенный день товар минчанину доставлен не был, после чего он потребовал у продавца вернуть денежные средства, либо же доставить телефон, сообщив также о своих намерениях обратиться в ОВД, однако переписка была удалена лжепродавцом.

Пример 4: в социальной сети «Instagram» 38-летний Виктор нашел аккаунт с туристическими услугами. Он связался с менеджером, который предложил «горящий тур» в Турцию по выгодной цене. Виктор согласился, после чего представитель турагентства сообщил, что вылет на отдых запланирован

через несколько дней, поэтому необходимо внести 100% предоплату. Мужчина перевел 6000 белорусских рублей на предоставленный счет, после чего с ним перестали выходить на связь и удалили переписку.

Что должно **насторожить** покупателя, если он приобретает товары онлайн?

- подозрительно низкие цены на товар;
- 100% предоплата;
- требование продавца ввести паспортные данные или полные реквизиты БПК;
- предложение перейти по ссылке.

! Рекомендации:

1. не совершайте покупки в магазинах из социальных сетей, если у вас требуют полную предоплату;
2. не переходите по подозрительным ссылкам и не вводите личные данные и реквизиты БПК;
3. заведите отдельную банковскую платежную карту для оплаты товаров и услуг в сети Интернет и переводите на нее сумму равную сумме покупки;
4. выбирайте надежных продавцов и проверяйте их репутацию через поисковую строку любого браузера.

Звонки от имени представителей правоохранительных органов, банковских учреждений, сотовых компаний, работников коммунальных и телекоммуникационных предприятий, медицинских организаций и т.п. (вишинг)

Злоумышленник звонит на стационарный телефон и в разговоре сообщает о необходимости дистанционного продления (перезаключения) договора на оказание услуг, замены устаревшего оборудования, оперативной сверки показателей счетчиков и пр. При этом для верификации и удобства требует предоставить персональные данные (идентификационный номер паспорта, номер мобильного телефона, иные личные данные). В это время параллельно на мобильный телефон жертвы (как правило посредством мессенджера «Viber»), поступает звонок якобы от сотрудника правоохранительных органов или банка, который сообщает, что в данный момент по стационарному телефону жертва общается с мошенниками и что разговор необходимо прервать. После этого «псевдоправоохранитель» действует по стандартной мошеннической схеме и сообщает, что:

- на имя потерпевшего оформили кредиты;

- с расчетных счетов потерпевшего осуществляется финансирование террористической деятельности либо военных действий в Украине;
- необходимо оказать помощь правоохранительным органам в поимке аферистов;
- в связи с тем, что в отношении потерпевшего возбуждено уголовное дело и у него в ближайшее время по месту жительства будет проведен обыск, необходимо срочно обезопасить накопленные денежные средства, для чего осуществить их декларирование либо перевод на специальный «безопасный» счет;
- оказать содействие другим жертвам мошенников, которые в силу возраста или физических особенностей не могут самостоятельно обратиться в банк для зачисления наличных денежных средств на безопасный счет.

После всего услышанного жертва испытывает эмоциональный шок. Ведь сложно поверить, что это все четко спланированная мошенническая схема. Потерпевшие, идя на поводу аферистов, следуют их инструкциям и добросовестно исполняют все, что те от них требуют, даже продают собственное жилье и вырученные деньги также переводят на предоставленные злоумышленниками счета.

Необходимо отметить, что мошенники до такой степени втираются в доверие жертв, что при попытках ИСТИННЫХ сотрудников милиции или работников банковских учреждений их образумить, чаще всего игнорируют все разумные доводы.

Пример: В начале мая 60-летнему Николаю Анатольевичу на домашний телефон позвонила женщина, которая представилась сотрудницей «Энергосбыта» и сообщила о необходимости замены счетчиков. Пожилого мужчину данный факт не смутил, так как около 1 месяца назад он оставлял заявку на замену счетчиков.

Сотрудница «Энергосбыта» попросила предоставить идентификационный номер паспорта для подтверждения заявки. После окончания разговора с указанной сотрудницей, Николаю Анатольевичу на мобильный телефон посредством мессенджера «Viber» с белорусского мобильного номера телефона позвонил ранее неизвестный мужчина, который представился капитаном юстиции Князевым Виталием Владимировичем из управления Следственного комитета Республики Беларусь и в ходе разговора пояснил, что у них сработала специальная система по предупреждению мошеннических звонков с неизвестных номеров. В ходе диалога Князев В.В. пояснил, что пожилой минчанин стал жертвой мошенников, которые по личному номеру паспорта через подставных лиц берут кредиты. Также Князев В.В. пояснил, что с потенциальным потерпевшим должен связаться специалист из Национального Банка Республики Беларусь. После окончания звонка от Князева В.В., посредством мессенджера «Viber» позвонил

неизвестный мужчина, который представился как Исаев Игорь Леонидович - специалист Национального Банка, и пояснил, что в настоящее время участились случаи мошенничества в Республике Беларусь, а именно после предоставления личных данных происходит взятие кредитов, снятие пенсий по предоставленным данным. В ходе беседы Исаев И.Л. разговаривал очень четко, ссылался на нормативно-правовые акты Республики Беларусь, в связи с чем каких-либо сомнений у Николая Анатольевича по данному поводу не возникло. В процессе разговора Исаев И.Л. пояснил, что все банковские карточки Николая Анатольевича решением Национального Банка будут заблокированы, и все денежные средства пропадут. Также Исаев И.Л. указал, что зафиксированы попытки получения кредитов в различных банках столицы. Для того, чтобы вычислить мошенников, нужно взять контрольные кредиты, и в последующем сделать перевод по их погашению. Николай Анатольевич снял последние денежные средства, которые у него имелись, после чего направился в банковские учреждения, где оформил договоры на кредиты. При оформлении указанных кредитов сотрудники банков интересовались, для каких целей ему нужны денежные средства и не находится ли он под влиянием третьих лиц, а также предупреждали о мошенниках, на что тот пояснил, что денежные средства нужны на личные нужды.

Получив кредитные средства, Николай Анатольевич перевел их на реквизиты банковской карты, которые указал ему Исаев И.Л.

Необходимо отметить, что при осуществлении потерпевшим переводов, представители банков уточняли, куда, кому и с какой целью Николай Анатольевич переводил деньги, разъясняя ему, что он действует нелогично и скорее всего находится под чьим-то влиянием, то есть мошенников.

Наряду с этим, потерпевшему по мобильной связи звонил участковый инспектор милиции и расспрашивал, кому тот делал переводы. Во время разговора с участковым Николай Анатольевич «плавал» и понимал, что все то, что ему описывает НАСТОЯЩИЙ сотрудник милиции в качестве преступной схемы, аналогичным способом происходит и с ним сейчас. В тот момент Николай Анатольевич начал осознавать, что свои кредитные деньги он перевел мошенникам, однако участковому также не сказал правду, обманув его, что распоряжается деньгами по своему усмотрению и попросил впредь его не беспокоить.

Не желая быть обманутым со стороны якобы спецслужб, 60-летний мужчина решил позвонить Исаеву И.Л. и сообщить о своих предположениях об участии в противоправных действиях, однако Исаев И.Л. уверил его, чтобы тот ни от кого не брал трубки, кроме него, Князева В.В., а также Сафронова Кирилла Алексеевича, который в последующем позвонил по видеосвязи и представился начальником Следственного отдела и руководителем Князева В.В. Сафронов К.А. разъяснял потерпевшему, что все деньги по кредиту ему вернут. При этом Сафронов К.А. был одет в форменное обмундирование, в связи с чем каких-либо сомнений у Николая Анатольевича снова не возникло.

Далее в ходе телефонной беседы Исаев И.Л. сообщил, что Николаю Анатольевичу нужно будет ехать в Москву, чтобы помочь в специальной операции по выявлению мошенников.

Так, по указанию Исаева И.Л., с использованием кодового слова, озвученного им же, мужчина забрал крупную сумму денежных средств у двух минчанок (75 и 45 лет), которые передали ему денежные средства в целлофановых пакетах. Далее по указанию Исаева И.Л., Николай Анатольевич приобрел билет на поезд до Москвы.

По приезду в г. Москва, Николай Анатольевич заселился в гостиницу «Канна» и проживал там на протяжении суток. На следующий день ему позвонил Исаев И.Л., который сообщил, что тот должен встретиться с его коллегой. Далее по прибытию в указанное Исаевым И.Л. место, к Николаю Анатольевичу подошел молодой человек 28-30 лет неопрятного внешнего вида. Николай Анатольевич передал ему денежные средства, после чего вернулся обратно в гостиницу. По возвращению в гостиницу Исаев И.Л., Князев В.В. и Сафронов К.А. перестали выходить «на связь».

По возвращению в г. Минск к Николаю Анатольевичу по месту жительства прибыли сотрудники столичной милиции, которые сопроводили его в ближайшее РУВД. И только в РУВД Николай Анатольевич окончательно убедился, что с ним до этого общались мошенники.

При беседе с сотрудниками милиции Николай Анатольевич пояснял, что неоднократно слышал в новостях и телепередачах о преступных схемах мошенников, более того помочь разобраться в ситуации ему пыталась и супруга, но Николай Анатольевич решил игнорировать все ее доводы, полагая, что он сам знает, как лучше поступить, и в итоге стал жертвой аферистов и соучастником преступления.

Нередки случаи, когда после установки программы удаленного доступа злоумышленник оформляет онлайн-кредит на имя потерпевшего без его ведома. Название приложения (программы удаленного доступа) преступник может завуалировать под приложение интернет-банкинга и иное.

Кроме того, распространена следующая схема обмана: гражданину поступает звонок от «специалиста компании оператора сотовой связи («A1», «МТС», «Life») с использованием различных мессенджеров (WhatsApp, Viber, Telegram). В ходе телефонного разговора злоумышленник под предлогом обновления официального приложения, продления договора обслуживания и т.п., отправляет ссылку для скачивания вредоносного файла (формата «.apk»).

После скачивания и запуска указанного файла, производится установка приложения удаленного доступа внешне схожего с официальным приложением оператора сотовой связи. Установленное приложение обладает функциональными возможностями, предоставляющими доступ злоумышленнику к функциям мобильного

телефона, в том числе камере, микрофону, файлам, хранящимся на устройстве, списку контактов, смс-сообщениям и др. Полученные сведения могут быть использованы для совершения хищения денежных средств с банковских счетов и иных противоправных действий в отношении владельца мобильного телефона (завладение информацией и иное).

В связи с изложенным, при проведении профилактической (разъяснительной) работы с гражданами необходимо акцентировать внимание последних именно на скептическом отношении, излишней доверчивости и развитии критического мышления к различного рода звонкам, поступающим им как посредством мобильной связи, так и посредством городских телефонных линий, под видом сотрудников правоохранительных органов, Национального банка Республики Беларусь и иных банковских учреждений, представителей операторов сотовых компаний, работников «Энергосбыта», «Водоканала», «Мингаза», «Белтелекома» и т.п.

! Рекомендации:

1. ни под какими предлогами не сообщайте посторонним паспортные данные, не предоставляйте информацию о реквизитах банковской карты (номере, сроке ее действия, ПИН-коде, CVV2/CVC2 коде) или одноразовые пароли, поступившие на мобильный телефон, даже если звонят лица, представляющиеся сотрудниками правоохранительных органов, медицинских и банковских учреждений, операторов сотовой связи, работниками коммунальных служб или телекоммуникационных компаний;
2. не оформляйте кредиты по указанию третьих лиц;
3. не проводите через банкоматы и иные устройства самообслуживания (включая систему дистанционного банковского обслуживания) никакие операции под психологическим давлением или по инструкциям, полученным по телефону или мессенджерам;
4. не устанавливайте на мобильный телефон приложения по просьбе третьих лиц, даже если они настоятельно этого требуют;
5. не становитесь курьером мошенников путем собирания денежных средств у других граждан, попавших в неприятную жизненную ситуацию;
6. при поступлении ЛЮБОГО сомнительного звонка, незамедлительно завершите разговор и обратитесь в милицию.

ПОМНИТЕ, сотрудники правоохранительных органов, медицинских и банковских учреждений, операторов сотовой связи, работники государственных организаций и предприятий, коммунальных служб

или телекоммуникационных компаний НИКОГДА не выясняют ваши персональный данные по телефону!

Для оформления заявок на оказание услуг по телефону, указание идентификационного номера паспорта либо реквизитов банковской пластиковой карты НЕ ТРЕБУЕТСЯ!

Инвестирование (трейдинг и другие способы легкого заработка в сети Интернет)

Особо актуальная на сегодняшний день схема обмана под предлогом дополнительного заработка, связанного с инвестициями или трейдингом («финансовые эксперты» обещают высокий доход).

Посты и рекламные баннеры в сети Интернет (соцсетях) часто обещают быстрый и очень высокий доход. Их цель – завлечь людей на мошеннические сайты, где якобы можно инвестировать деньги в ценные бумаги и получить прибыли больше, чем на других площадках.

Иногда такие сообщения (посты) появляются на страницах, которые мошенники специально создают под видом обычных пользователей. Также злоумышленники заводят фейковые аккаунты реально существующих банков или известных финансовых экспертов, и размещают публикации от их имени.

Часто для обмана злоумышленники создают сайты, которые сложно отличить от настоящих сайтов банков и брокерских компаний. А еще выкладывают посты в соцсетях от имени вымышленных людей или выступают под видом компетентных экономистов, рекламируя подозрительные инструменты с высоким доходом.

Как правило, мошенники предлагают повышенную доходность. Обычные вклады в рублях приносят 10-15% годовых. Мошенники же обещают, как минимум 20-30%, а иногда и больше – это может быть и 70%, и 250% в год.

Но важно помнить: высокая доходность связана с большими рисками и гарантировать ее невозможно. Для мошенников же достоверность цифр значения не имеет, главное – зацепить внимание человека и заставить его зарегистрироваться на сайте.

Затем они просят якобы «пополнить свой счет», а по факту – перевести деньги, чаще всего на карту физического лица или электронный кошелек.

После регистрации мошенники «прикрепляют» к обманутому пользователю так называемого «финансового эксперта», который якобы должен советовать активы к покупке и помогать инвестировать. На самом деле его задача – убедить человека вложить как можно больше денег. «Эксперт» будет говорить, что торговля идет хорошо и Вы получаете

прибыль, но растущие цифры на сайте ничего не значат: деньги не попадают на биржу, а мошенники могут имитировать любой доход.

Фейковый рост депозита внушает доверие, это побуждает отправить мошенникам еще больше денег. Иногда, чтобы им доверяли, мошенники переводят жертве небольшую сумму под видом прибыли с биржи. Так они пытаются показать, что их схема заработка работает и нужно вкладывать еще.

Вернуть свои деньги практически невозможно. Если отказаться от новых переводов или сказать, что денег нет, мошенники будут давить: говорить, что нужно брать кредит, продавать телефон, автомобиль, недвижимость, ведь сейчас есть уникальная возможность заработать и все вложения окупятся. А если человек решит настоять на выводе денег, его попросят оплатить комиссию.

Интернет-мошенники – хорошие психологи, которые знают, как вызвать интерес, расположить собеседника к себе и убедить человека расстаться с собственными сбережениями.

<u>Пример 1:</u> в январе 2025 года Екатерина в мессенджере «Telegram» обнаружила пользователя «@confidential_inf8», который рассказал о возможностях дополнительного заработка путем оформления ставок на спортивные события. Со слов злоумышленника, он обладал информацией о «покупных» матчах и играх, в виду чего гарантировал стабильный заработок через ставки. Будучи введенной в заблуждение, Екатерина в вышеуказанный период времени под предлогом оплаты налогов и страховых взносов для вывода выигрыша осуществила неоднократные пополнения предоставленных злоумышленником счетов на сумму не менее чем 20 568 бел.рублей. Однако вывести выигрыш не удалось.

<u>Пример 2:</u> 65-летний Александр в октябре 2024 года в сети Интернет нашел предложение о дополнительном заработке путем вложения в инвестиции. В последующем в период с ноября 2024 г. по январь 2025 г. Александр со своей БПК осуществлял переводы денежных средств на БПК, реквизиты которых были ему предоставлены, после чего совершал под руководством "менеджера" сделки. После каждого перевода денежных средств со своих БПК, Александр видел, что баланс его счета на бирже также пополняется, ввиду чего спокойно продолжал совершать сделки. После середины января пенсионер решил вывести с лицевого счета на бирже около 13 тысяч долларов США, однако ему поступило сообщение с просьбой внести дополнительный платеж в сумме 1 875 долларов США «для фиксации курса обмена», путем перевода на криптокошелек. Заявитель понял, что общение с ним вели мошенники. Здесь необходимо отметить, что для совершения вышеописанных сделок пенсионер взял в банке кредит на сумму 10 000 бел.рублей, а также некоторую сумму денежных средств брал в долг у знакомых. Таким образом, сумма ущерба составила порядка 73 000 бел.рублей.

Не единичны случаи, когда жертвы такого рода мошенничеств пытаются самостоятельно вернуть похищенные денежные средства посредством поиска «юридической помощи» в сети Интернет.

Пример: Владимир, вложивший в 2024 году в фейковую торговую биржу порядка 6 тысяч евро, в социальной сети «Instagram» нашел компанию, которая оказывает юридические услуги по возврату похищенных денежных средств (криптовалюты). Так, за «запуск процедуры возврата» и под иными «весомыми» предлогами Владимир перевел указанной компании 1 650 долларов США. Само собой деньги минчанину так и не вернули ни в первом, ни во втором случае.

! Рекомендации:

1. не верьте обещаниям легкого заработка в интернете. Прежде чем вкладывать деньги в какие-либо проекты, проверьте достоверность предложения поиском в браузере или по телефонам организаций, размещенным на их сайтах;
2. ведите переписку и совершайте сделки только на официальных биржах.

Взлом аккаунта (учетной записи)

Не теряют своей актуальности мошенничества, сопряженные с несанкционированным доступом (взломом) к учетным записям в различных социальных сетях и мессенджерах (Одноклассники, ВКонтакте, INSTAGRAM, Telegram, Viber и прочие) и последующей рассылкой сообщений с просьбой перевода денежных средств в долг либо оказания материальной помощи на лечение.

Пример: 31.01.2025 Максиму в мессенджере «Telegram» пришло сообщение с учетной записи его девушки Веры о необходимости перевода 150 бел.рублей для осуществления ею выкупа покупок с маркетплейса «Wildberries». Ничего не заподозрив, Максим осуществил перевод денежных средств на указанные в сообщении от Веры реквизиты БПК. Спустя 10 минут молодому человеку позвонила его девушка и сообщила, что ее учетную запись в мессенджере «Telegram» взломали и стали рассылать сообщения различного содержания всем ее контактам, после чего Максим понял, что отправил денежные средства мошенникам, и обратился в милицию.

! Рекомендации:

1. для обеспечения безопасности своих аккаунтов необходимо устанавливать сложные пароли и двухэтапную аутентификацию;
2. не переходить по ссылкам из различных сообщений, поступивших даже от родных и знакомых людей;

3. при поступлении подобного рода сообщений созвонитесь с человеком, который просит у вас финансовой помощи, для удостоверения правдивости происходящего.

Звонки от имени руководителей организаций

В 2024 году появилась новая схема мошенничества, которая остается актуальной и в настоящее время (схема «Fake boss»). Для реализации такой схемы злоумышленники предварительно изучают чаты трудовых коллективов в мессенджерах и социальных сетях, собирают информацию об организации и руководителях, создают учетные записи от их имени. В последующем с помощью поддельного (фейкового) аккаунта руководителя преступники вступают в переписку с подчиненными и, используя авторитет начальника и доверие к нему, дают определенные указания либо разъяснения.

Чаще всего лжеруководитель требует оказать содействие правоохранительным органам в проверке на предмет причастности к финансированию террористической деятельности либо под предлогом одалживания денежных средств (сообщения могут быть как текстовыми, так и голосовыми).

<u>Пример 1:</u> 29.01.2025 Василисе в мессенджере «Telegram» поступило сообщение от пользователя, аккаунт которого был внешне похож на аккаунт главврача поликлиники, где она работает. В сообщении говорилось о том, что с ней в скором времени в мессенджере «Telegram» свяжется куратор из КГБ. Через некоторое время Василисе поступило сообщение от пользователя, который представился как «Марцинкевич Алексей». Последний сообщил, что на имя Василисы был оформлен кредит, денежные средства из которого были отправлены в Украину и для того, чтобы избежать проблем, женщине необходимо перевести оставшиеся у нее денежные средства на безопасный счет. Ей были предоставлены реквизиты, на которые она в последующем осуществила денежный перевод в размере 2 250 бел.рублей. Далее при общении с коллегами Василиса узнала, что главврач имеет другой аккаунт в мессенджере «Telegram», после чего поняла, что все это время она общалась с мошенниками.

<u>Пример 2:</u> в конце декабря 2024 года с ведущим инженером одного из государственных научных учреждений посредством мессенджера «Telegram» связалось неизвестное лицо, которое представилось ее директором и предупредило, что ей будет звонить сотрудник КГБ. После этого женщине в указанном мессенджере от неизвестного лица, подписанного как «Стрельцов Анатолий Сергеевич», поступил звонок, в ходе которого неизвестный мужчина представился сотрудником КГБ и пояснил, что банковские счета последней используются для финансирования экстремистских организаций, в связи с чем, во избежание ареста правоохранительными органами, женщине необходимо

перевести денежные средства на «безопасный» счет. В последующем потерпевшая перевела на предоставленные аферистом реквизиты денежные средства в размере 1 550 бел.рублей.

! Рекомендации:

1. при поступлении подобного рода сообщений (звонков), необходимо убедиться в достоверности аккаунта и номера телефона, а также связаться с руководителем по стационарной связи либо иным возможным способом.

Знакомства в Интернете

Знакомства в мессенджерах или социальных сетях все чаще заменяют реальные встречи. Однако стоит внимательно относится к знакомствам в интернет-пространстве, так как за красивым снимком профиля может скрываться мошенник.

Пример 1: Валентина (60 лет) в начале ноября 2024 года в социальной сети «TikTok» познакомилась с мужчиной по имени «Михаэль». Общение продолжилось в мессенджере «Telegram». В канун нового года Михаэль сообщил женщине, что отправил ей посылку, в которой содержались различные вещи, драгоценности и денежные средства.

Через некоторое время на электронную почту пенсионерки поступило сообщение от ранее неизвестного пользователя, зарегистрированного под именем «Christopher Erica», который сообщил, что необходимо оплатить денежные средства за доставку посылки, и указал реквизиты банковского счета. Данную информацию также продублировал Михаэль в мессенджере «Telegram». В связи с чем, по инструкции данного пользователя, женщина направилась в банковское учреждение, где через кассу осуществила перевод денежных средств в размере 5 210,25 бел.рублей на предоставленный ей счет.

Через несколько дней от Михаэля пришло сообщение о необходимости оплаты «растаможки» посылки. В связи с чем пенсионерка через банковское учреждение осуществила еще 2 перевода денежных средств в размере 9 552,13 и 9 552,12 бел.рублей.

В последующем Михаэль сообщил, что денежные средства не поступили ему на счет. Женщина пыталась как-то решить данный вопрос в переписке, а также предложила встречу, однако Михаэль написал, что банк обманывает и денежные средства никуда не направил, и от личной встречи отказался. Пенсионерка осознала, что стала жертвой мошенника. Таким образом, виртуальный «возлюбленный» обманным путем завладел денежными средствами пенсионерки в общем размере 24 314,50 бел.рублей.

Пример 2: Людмила (69 лет) при просмотре ленты в социальной сети «TikTok» увидела ранее незнакомого пользователя (врач Dan Patrick, гражданин Британии), с которым стала вести личную переписку в мессенджере

«WhatsApp», ввиду возникшей между ними симпатии. В процессе общения Dan Patrick пояснил, что в настоящее время находится в Йемене, но желает прилететь в г. Минск и увидеться с Людмилой. Ввиду того, что у него в настоящее время якобы не активирована банковская карта, он попросил Людмилу купить ему билет путем перевода на карту лица, имеющего отношение к авиакомпании. Женщина согласилась и 22.01.2025 через банковское учреждение перевела 3 028 бел.рублей.

После Dan Patrick пояснил, что агент приобрел ему билет лишь до Турции и для того, чтобы долететь до г. Минска, необходимо купить еще один билет стоимостью 2 000 долларов США. Для подтверждения своих слов он прислал фотографии из Турции, в связи с чем Людмила уверилась, что общение ведет с реальным человеком. После долгих уговоров, пенсионерка перевела еще 3 069 бел.рублей. В процессе дальнейшего общения с Dan Patrick, он пояснил, что якобы вторая сумма денежных средств не дошла, и попросил внести еще такую же сумму.

Людмила поняла, что общалась с аферистом и обратилась в ОВД. Общая сумма ущерба потерпевшей составила 6 097 бел.рублей.

! Рекомендации:

1. тщательно изучайте аккаунт собеседника;
2. как можно лучше узнайте нового знакомого;
3. созванивайтесь по мобильному телефону и/или по видеосвязи;
4. не ведитесь на просьбы оказать материальную помощь, тем более не отправляйте деньги на «посылки», «госпошлины», «лечение» и прочее незнакомым вам людям;
5. ни под какими предлогами не переходите по подозрительным ссылкам, отправленным вам собеседником, и не вводите личные данные и тем более реквизиты банковской платежной карты.

Фишинг

Фишинг – вид интернет-мошенничества, это когда мошенники создают фейковые (поддельные) сайты или присылают письма и сообщения, чтобы украсть у пользователя пароли, деньги или другую личную информацию.

Как понять, что сайт – фейк (поддельный)?

- внимательно посмотрите на адрес в браузере – если есть странные буквы, цифры или что-то лишнее это плохой знак;
- убедитесь, что в адресе есть https: и значок замка – это значит, что интернет-соединение защищено;
- если сайт оформлен с ошибками в тексте или странными картинками, это должно насторожить;

- если сайт настойчиво требует срочно ввести пароли, данные карты или другую личную информацию – будьте осторожны.

Как отличить фишинговое письмо или сообщение?

- в письме могут грозить заблокировать аккаунт, если вы не выполните определенные требования;
- часто такие письма содержат много ошибок и небрежный стиль, а также ссылку на странный сайт, где просят ввести конфиденциальные данные;
- иногда мошенники просят подтвердить пароль или номер телефона.

Пример 1: в начале мая т.г. Денис в социальной сети «Instagram» обнаружил аккаунт по продаже цветов «estefliwers.by». Перейдя в данный профиль и изучив ассортимент, мужчина решил сделать заказ. В связи с тем, что указанный магазин затребовал 100% предоплату товара Денис со своей банковской карты перечислил 130 бел.рублей на предоставленные продавцом реквизиты. В ходе дальнейшего общения продавец сообщил о необходимости оплаты доставки, после чего поступила ссылка для оформления доставки. Перейдя по данной ссылке, Денис ввел реквизиты своей банковской карты и коды из СМС-сообщений. После чего с его БПК было списано 125 бел.рублей.

Пример 2: Петр решил на месяц снять квартиру. Так, на сайте «Domovita.by» он нашел объявление о сдаче в найм жилья в г. Борисове. В объявлении был указан контакт для связи в мессенджере «Viber». В ходе переписки девушка, которая представилась Дианой, попросила внести предоплату в размере 500 бел.рублей, для чего предоставила номер БПК, на которую Петр перевел указанную сумму. Однако позже она написала, что квартира уже сдана и предложила вернуть Петру деньги, для чего предоставила соответствующую ссылку (https://alfabank-by.dostavka10.info/receiving/176749185). Петр перешел по указанной ссылке, ввел реквизиты своей БПК, а также код из СМС-сообщения. После этого с его БПК было списано 885 бел.рублей.

Пример 3: Михаил зашел в свой персональный аккаунт в социальной сети «Instagram», после чего начал просматривать информационную ленту. В ходе просмотра отобразился информационный пост (реклама) от ЗАО «Альфа-Банк» о получении вознаграждения (100 бел.рублей) за участие в прохождении опроса. После клика по информационному окну открылся опрос от банка. Петр начал давать ответы по вышеуказанному опросу, введя свои ФИО, идентификационный номер паспорта, номер мобильного телефона и коды подтверждения (3-D Secure). После чего с его БПК произошло списание денежных средств в размере 9 990 бел.рублей.

! Рекомендации:

1. будьте осторожны с тем, что читаете и на что кликаете (нажимаете) в интернете;

2. учитесь распознавать признаки мошенничества;

3. включите в аккаунтах в социальных сетях, мессенджерах и электронных почтовых ящиках двухфакторную аутентификацию – дополнительный уровень защиты;

4. используйте сложные пароли и не повторяйте их на разных сайтах;

5. всегда ставьте антивирус и регулярно его обновляйте.

Вымогательство

В 2024 году и в настоящее время получила распространение новая форма вымогательства с использованием информационно-коммуникационных технологий.

Из такого рода преступлений можно условно выделить четыре основные категории:

1) связаны с блокированием учетных записей Apple iCloud, посредством ввода авторизационных данных, предоставленных злоумышленниками под благовидными предлогами, что в последующем не позволяет потерпевшему полноценно использовать свое мобильное устройство.

Пример: *Ольга решила установить взломанную версию мессенджера «Телеграмм» под названием «AyuGram», нашла видеоматериал в приложении «TikTok», в котором говорилось о таком приложении, после чего решила написать комментарий под вышеуказанным видеоматериалом с просьбой отправить подробную инструкцию по установке вышеуказанного приложения. Так, через некоторое время, девушке поступило от неизвестного со ссылкой на учетную запись в мессенджере «Telegram» с никнеймом «iOsHelp». После перехода в указанную учетную запись мессенджера «Telegram», Ольга решила написать сообщение данному пользователю, который в итоге ответил и предложил помощь по установке приложения «AyuGram». Так, неизвестное лицо, используя учетную запись «iOsHelp» сообщило, что для установки вышеуказанного приложения необходимо выйти из приложения «iCloud» и ввести данные, которые оно предоставит, что Ольга и сделала. В результате данных действий последняя потеряла доступ к своему мобильному телефону «IPhone 12 mini». Вышеуказанный мобильный телефон в настоящий момент находится в нерабочем состоянии в связи с блокировкой учетной записи. Позже Ольге посредством мессенджера «Telegram» поступило сообщение, что для разблокировки ее мобильного телефона необходимо перевести денежные средства в размере 150 долларов США.*

2) вымогательства, связанные с угрозой распространения личной информации потерпевших, которую последние желают сохранить в тайне (как правило фотографии и видеозаписи интимного характера, хранящиеся

в переписках, закладках, скрытых альбомах различных электронных ресурсов). В ряде случаев, потерпевшие сами делятся своим интимным контентом с малознакомыми людьми.

Пример: сотрудниками столичной милиции установлена причастность несовершеннолетнего жителя г. Мозыря, который, представляясь девушкой, вступал в переписку с мужчинами, в процессе которой склонял последних к обмену интимными фотографиями. После чего, посредством мессенджера «Telegram» потерпевшим поступали сообщения от пользователя мужского пола с угрозами распространения указанных интимных фотографий во всех социальных сетях. За нераспространение указанного компромата у потерпевших вымогали денежные средства.

3) вымогательства, связанные с оказанием услуг интимного характера.

Пример: молодой человек просматривал интернет-ресурс по оказанию интим-услуг, где его заинтересовало одно из объявлений. После этого он осуществил несколько звонков на указанные в объявлении абонентские номера, однако на звонки никаких ответов не последовало. Через несколько часов парню позвонил неизвестный и сообщил, что на его имя оставлена заявка на оказание интимных услуг, и для того, чтобы её снять, последнему необходимо оплатить 3 000 бел.рублей, иначе пострадают его родные. Неустановленное лицо предоставило реквизиты БПК, на которую молодой человек перевел 404,50 бел.рублей. После перевода указанной суммы неустановленное лицо сообщило, что необходимо перевести еще 600 бел.рублей, что парень и сделал.

4) вымогательства, связанные с блокировкой учетных записей (аккаунтов) в социальных сетях и мессенджерах.

Пример: минчанин в мессенджере «Telegram» нашел сообщество «Work on» в котором предлагают различную подработку. Далее, чтобы начать работать, молодой человек перешел по вредоносной ссылке. После перехода по указанной ссылке доступ к собственному gmail-аккаунту был утерян. Немногим позже молодому человеку в мессенджере «Telegram» поступило сообщение, что за разблокировку аккаунта последний должен перевести неизвестному лицу 390 бел.рублей.

! Рекомендации:

1. никогда не вводите на своем устройстве чужие данные Apple ID или iCloud;
2. не отключайте Face ID или Touch ID по просьбе посторонних лиц;
3. загружайте приложение только из официальных источников (App Store, Google Play и др.).

Сваттинг
(заведомо ложное сообщение об опасности)

Сваттинг – заведомо ложный вызов милиции, аварийно-спасательных служб, путем фальшивых сообщений о минировании, убийствах, захвате заложников и т.п. от имени другого лица.

Этот термин происходит от названия штурмовой группы «SWAT» (Special weapons and tactics) – специализированной полицейской единицы в США и многих других странах. Если есть угроза, при которой необходимо вмешательство этой единицы, последствиями иногда становится эвакуация учреждений образования, административных учреждений, крупных торговых объектов. В западных странах «сваттинг» расценивается как разновидность терроризма, поскольку его используют для запугивания и создания риска получения телесных повреждений или даже смерти.

Сваттинг в первую очередь свойственен среде, где люди (чаще всего молодые) объединяются по каким-то целям. Например, в онлайн-играх. У них есть термин «вызвать милицию на дом» - когда для того, чтобы, к примеру, досадить обидчику, ему на дом вызывают правоохранителей, либо сообщают о заминировании какого-либо объекта.

В последние годы сваттинг из забавы любителей онлайн-игр и хакеров превратился в массовое явление и большую проблему для правоохранительных органов различных стран. Жертвами хулиганов становятся как обычные люди, так и знаменитости.

В Республике Беларусь за последние пять лет возросло количество случаев поступления сообщений на электронную почту о ложном минировании объектов. Подобные «шалости» дорого обходятся государству, а для виновных чреваты весьма нешуточными последствиями.

За совершение указанных действий грозит наказания в виде лишения свободы сроком до пяти лет, а в случае повторного совершения, либо группой лиц по предварительному сговору, либо повлекшее причинение ущерба в крупном размере, либо повлекшее иные тяжкие последствия, до семи лет лишения свободы.

Незаконный оборот платежных инструментов, средств платежа и их реквизитов

В 2022-2023 году и по настоящее время, чаще в молодежной среде, отмечается рост количества преступлений, связанных с продажей реквизитов платежных инструментов (банковских платежных карт, логинов и паролей к системе дистанционного банковского обслуживания).

Организаторами преступных групп, совершающими киберпреступления, все активнее в противоправную деятельность вовлекается молодежь, для совершения действий, предусмотренных статьей 222 Уголовного кодекса Республики Беларусь (незаконный оборот платежных инструментов, средств платежа и их реквизитов).

Зачастую подростки находят объявления в Интернете (мессенджерах), где им предлагают оформить на свое имя банковскую карту и продать ее реквизиты, тем самым предоставив доступ к банковским счетам, «привязанным» к карте, либо электронным кошелькам (как правило «заработок» за такие действия составляет от 20-40 рублей за реквизиты одной БПК). В дальнейшем, реквизиты этих платежных инструментов используются при совершении преступных сделок.

Вступившим в силу Законом Республики Беларусь от 17 февраля 2025 г. №61-З «Об изменении кодексов по вопросам уголовной ответственности» дифференцируется ответственность за незаконный оборот платежных инструментов (ст. 222 УК РБ и ст. 12.35 КоАП). Так, за распространение чужих (находящихся в незаконном владении) реквизитов банковских платежных карточек сохраняется уголовная ответственность. Такие же действия в отношении собственных (находящихся в законном владении) реквизитов банковских платежных карточек будут влечь административную ответственность.

Операции с криптовалютой

Беларусь развивающаяся страна и граждане активнее пользуются цифровыми технологиями.

Порядок осуществления сделок с криптовалютой в настоящее время определен Указом Президента Республики Беларусь от 17 сентября 2024 г. №367 «Об обращении цифровых знаков (токенов)» (далее – Указ №367).

Указом №367 установлена обязанность для физических лиц совершать операции по покупке-продаже криптовалюты за денежные средства (белорусские рубли, иностранную валюту или электронные деньги) только у криптобирж (операторов обмена криптовалют), являющихся резидентами Парка высоких технологий, а также перечислять (переводить) денежные средства со своих банковских счетов, электронных кошельков исключительно указанным резидентам ПВТ. Совершение операций по купле (продаже) криптовалюты на иностранных криптобиржах и у физических лиц является незаконным и запрещается.

Указ №367 не вводит запрет в отношении операций по переводу криптовалюты на зарубежные торговые площадки и не ограничивает возможность использования физическими лицами таких площадок для

совершения операций обмена (например, обмен криптовалюты одного вида на криптовалюту другого вида, торги криптовалютой), не связанных с непосредственным вводом или выводом денежных средств.

Таким образом, в настоящее время в Беларуси действуют следующие нормы:

Разрешено покупать токены (криптовалюту) за денежные средства только на белорусских криптобиржах, являющихся резидентами Парка высоких технологий; обменивать токены на другие токены на любых криптоплатформах без ограничений, например, обменивать Bitcoin на Ethereum.

Запрещено покупать или продавать токены (криптовалюту) за денежные средства на иностранных криптобиржах.

УПК КМ ГУВД Мингорисполкома