# Неделя финансовой грамотности

Стремительное развитие цифровых технологий, переход к безналичным расчетам, размещение в глобальной компьютерной сети Интернет персональных данных при достаточно низкой цифровой грамотности граждан, сопряженной с беспечным отношением к защите собственной информации, стали следствием увеличения количества регистрируемых киберпреступлений.

Злоумышленники активно используют в своей деятельности новейшие достижения науки и техники, применяют всевозможные компьютерные устройства и новые информационные технологии для совершения и сокрытия преступлений.

По итогам восьми месяцев 2025 года, в сравнении с аналогичным периодом прошлого года (далее – АППГ), количество зарегистрированных киберпреступлений на территории Минской области снизилось на **4,9 % (с 1580 до 1502),** что является **каждым пятым (22 %) уголовным делом на Минщине**. Вместе с тем число тяжких и особо тяжких киберпреступлений возросло **на 15,9 % (с 182 до 211)**.

Вместе с тем, на фоне снижения зарегистрированных киберпреступлений, уровень раскрываемости увеличился с **17,6 %** до **25,3 %**.

В структуре преступности преобладают мошенничества (ст. 209 УК), **712** преступлений, или **47,4 %,** хищения имущества путем модификации компьютерной информации (ст. 212 УК) **642** преступления, или **42,7 %** от общего количества зарегистрированных киберпреступлений.

Структурный анализ совершенных в текущем году мошенничеств свидетельствует о явном преобладании таких способов завладения деньгами потерпевших, как:

**1. Продажа несуществующего товара на различных Интернет-ресурсах 334 преступления, или 47 %.** Часто жертвами мошенников становятся пользователи сети Интернет, желающие приобрести различные товары в социальной сети **Instagram – 243 преступлений, или 34,1 %**. Продавцы, как правило, просят произвести предоплату за товар, однако такие действия заканчиваются одним – граждане перечисляют предоплату, а в дальнейшем связь с продавцом теряется, не получив долгожданный товар.

*Справочно: Для примера можно рассмотреть следующие мошеннические учетные записи:* ***original_brand.by, edelweis.resort, fox.store.by, EUROSHINA_BY, @airmac_by, flowerslovers.by, _belbet_off, happysale.by, techno-stok_by, elkihouse_by***.

**2. Обман граждан под предлогом вложения средств в криптовалюту либо сделок с ней на несуществующих биржах и иного заработка в сети Интернет, 97 преступление, или 13,6 %.**

*Справочно: Несуществующие инвестиционные проекты и мошеннические биржи – это обманные схемы, в которых инвесторам предлагается вложить средства в вымышленные или несуществующие бизнес-проекты, или финансовые инструменты с обещаниями высокой прибыли, которая на самом деле не может быть достигнута. К примеру, таких проектов можно привести «donald corporate», с помощью которого мошенники ввели в заблуждение жителя Минского района и завладели 72 560 белорусских рублей.*

**3. Звонки мошенников в мессенджерах (Viber, Telegram, WhatsApp) под видом сотрудников правоохранительных органов либо специалистов банковских и иных учреждений, вынуждающих потерпевших под различными предлогами получать кредиты и переводить денежные средства либо сбережения на подконтрольные злоумышленниками счета – 143, или 20,1 %.**

Основными способами совершения хищений имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса), являются:

**1. Также звонки мошенников в мессенджерах под видом сотрудников правоохранительных органов либо специалистов банковских и иных учреждений, в ходе которых злоумышленники получают доступ к банковским реквизитам граждан (56 %)**.

Такой способ называется «Вишинг» – это один из методов мошенничества с использованием социальной инженерии (социальная инженерия – это совокупность способов психологического воздействия на поведение человека с целью получения выгоды), который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль, под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию, или побуждают, убеждают вероятную жертву к совершению определенных действий
со своей банковской платежной картой

Он заключается в том, что злоумышленники, используя телефонную связь и, выдавая себя за сотрудников банка или правоохранительных органов, под различными предлогами вводят в заблуждение потерпевших, выясняя сведения о наличии банковских платежных карточках, их реквизитах, паспортных данных с целью последующего хищения денежных средств.

В большинстве случаев при совершении звонков мошенники используют интернет-телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи.

При этом всем известные мессенджеры Viber, Telegram и WhatsApp имеют возможность использования виртуальных номеров.

К примеру, злоумышленники звонят жертве от имени банковского работника и сообщают, что необходимо осуществить какие-либо действия с банковской платежной карточкой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо проводит подозрительную оплату.

Для большей достоверности в качестве имени пользователя они указывают официальный номер банка либо его название, а для «аватарки» используют логотип или эмблему банковского учреждения.

При этом зачастую они уже владеют минимальной информацией о лицах, которым звонят (имя, отчество, дата рождения, последние цифры банковской карты и др.), что способствует повышению доверия к звонящему и производит на него определенное впечатление.

В дальнейшем преступник просит сообщить информацию о банковской карте – номер, срок действия, трехзначный код на ее обороте, содержание СМС-сообщения, которое в ходе разговора поступает
на мобильный телефон, либо устанавливает мобильное приложение, позволяющее злоумышленнику получить удаленный доступ к мобильному телефону, в котором сегодня фактически у каждого имеется интернет-банкинг и, соответственно, доступ к банковскому счету.

**2. Использование фишинговых Интернет-ресурсов (23 %).**

Фишинг – вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям, данным лицевых счетов и банковских карт с использованием поддельных интернет-ресурсов, контролируемых злоумышленниками, внешне схожих с настоящими (например, поддельные страницы услуги «Интернет-банкинг» различных банков).

К примеру в прошлом году житель нашей области, при попытке совершить платёж за коммунальные услуги посредством системы Интернет-банкинга, воспользовался поисковой строкой сайта Google и перешёл, как оказалось, по ложной ссылке для оплаты. Злоумышленникам стали известны реквизиты банковской карты и в результате с его карт-счета было похищено почти 35 тысяч рублей.

Также в социальных сетях появилась реклама, обещающая «призы от Белагропромбанка». Переходя по ссылке, жертва попадает на поддельную банковскую страницу, на которой мошенники выманивают

номера телефонов и иные личные данные, что дает им полный доступ к счетам обманутых и даже возможность оформления онлайн-кредитов.

Распространены кибермошенничества от имени «Белпочты».

Схема довольно проста – злоумышленники присылают потенциальной жертве сообщение через интернет-мессенджер. В нем сообщают о необходимости уточнения адреса доставки почтового отправления и предлагают перейти по ссылке в Интернете. Невнимательный человек, не проверив адрес, по которому ему предлагают перейти, попадает на фейковый сайт, стилизованный под официальный сайт «Белпочты». Там клиента просят ввести свой адрес, якобы для доставки некоего почтового отправления, и оплатить тариф за услугу «Белпочты» прямо на этой странице, введя реквизиты банковской карты.

Появились случаи мошенничеств, связанных с созданием фейкового аккаунта в мессенджерах от имени руководителя учреждения, где работает потенциальная жертва.

Злоумышленники осуществляют рассылку сообщений с указанием того, что в скором времени гражданину позвонит или напишет сотрудник вышестоящей инстанции (Министерства образования, МВД, КГБ, КГК, СК, ОВД). Как правило, пугаясь, граждане говорят любую информацию, которую требует сотрудник. Далее просят установить удаленное программное обеспечение, позволяющее получить ему доступ к устройству, либо вести видеозапись с демонстрацией экрана мобильного телефона.

Наряду с этим в отчетном периоде зарегистрировано: **90** вымогательств (ст. 208), **15** фактов незаконного оборота средств платежа и (или) инструментов (ст. 222 УК), **16** заведомо опасных сообщения об опасности (ст. 340 УК) и **27** преступлений против компьютерной безопасности (глава 31 УК).

Преступления против компьютерной безопасности (глава 31 УК) в большинстве случаев возбуждаются по фактам неправомерного завладения учетными записями мессенджеров и социальных сетей, таких как **(Telegram (10), WhatsApp (1), Instagram (1)**, **блокировки учетной записи «Icloid» мобильных устройств «iphone» (6)**.

**Основные способы совершения вымогательств (ст. 208 Уголовного кодекса), можно разделить на три основные категории:**

1) связаны с **угрозой распространения личной информации потерпевших, которые последние желали сохранить в тайне** (14, или 15,5 %), как правило фотографий и видеозаписей интимного характера, которые, в большинстве случаев, потерпевшие самостоятельно

пересылали злоумышленникам, полагая, что общаются с потенциальным партнером противоположного пола для знакомства.

2) связаны с **блокированием компьютерной информации** физических лиц (75, или 83,4 %). При этом в подавляющем большинстве случаев отмечается блокирование учетных записей Apple ID посредством ввода авторизационных данных, предоставленных злоумышленниками под благовидными предлогами, что в последующем не позволяет потерпевшим полноценно использовать свои мобильные устройства.

3) связаны с **угрозой применения насилия** (1, или 1,1 %).

Стоит отметить, что **81 %** всех совершенных заведомо ложных сообщений об опасности по линии ПК, составляют **«сватерскую»** направленность, то есть отправку заведомо ложного сообщения об опасности от лица жертвы, посредством электронной почты.

Объектами заведомо ложных сообщений об опасности стали: учреждения образования – **7**; торговли (питания) – **6**; администрации (исполкомы) – **3**;

Основными факторами, способствующими совершению киберпреступлений, являются халатность, излишняя доверчивость граждан, мнимая возможность быстрого обогащения, получение крупных сумм денежных средств, а также недостаточное информирование населения о способах и методах применяемыми преступниками при совершении указанных преступлений.

Знание основных схем и способов обмана позволяет гражданам быть более внимательным и осторожным, что, в свою очередь, помогает предотвратить случаи совершения киберпреступлений.

В наше время информационные технологии проникают во все сферы жизни: работа, учеба, отдых, финансы и общение давно переместились в онлайн-пространство. Смартфоны, ноутбуки и планшеты стали неотъемлемыми спутниками каждого человека, предоставляя удобные инструменты для комфортной жизни. Однако эта легкость влечет за собой серьезный риск - киберпреступность.

Наши данные - имена, номера телефонов, истории покупок, пароли и банковские реквизиты - становятся лакомым кусочком для злоумышленников. Число преступлений в виртуальном пространстве неумолимо растет, превращая каждого пользователя в потенциальную жертву.

Осознавать эти угрозы и уметь грамотно реагировать на них жизненно важно. Давайте разберемся, какие бывают виды киберпреступлений, как распознать атаку и какие меры помогут защититься от них.

**Телефонное мошенничество** - один из самых распространённых видов преступлений. Мошенники используют манипуляции, запугивание и социальную инженерию, чтобы выманить у жертв деньги или личные данные.

Мошенники постоянно придумывают новые способы обмана, но цель у них всегда одна – запугать, вызвать панику и заставить вас быстро передать им деньги или персональные данные.

Если вам звонят и говорят одно из следующего - это 100% мошенники!

- Мы из Национального банка, ваши деньги в опасности! Переведите их на безопасный счет.
- Это КГБ/милиция/Следственный комитет. Вы должны помочь в расследовании!
- Назовите номер банковской карты, код из СМС, паспортные данные.
- Ваша карта заблокирована!
- Ваш родственник попал в беду (ДТП, сбил человека и т.д.).
- Вам нужно срочно установить приложение на телефон.

**Общие признаки телефонного мошенничества:**

- Вам звонят «важные лица» - банковские сотрудники, силовики, следователи.
- Вас пугают потерей денег, уголовным преследованием, проблемами у близких.
- Требуют передать деньги курьеру или перевести на «безопасный» счет.
- Спрашивают персональные данные (номер карты, код из СМС, паспорт).
- Давят на скорость - «нужно решить прямо сейчас, иначе будет поздно!»

**Что делать, если вам звонят мошенники?**

- Прекратите разговор! Просто положите трубку.
- Перепроверьте информацию! Перезвоните в банк, право-охранительные органы, родственникам и т.д.
- Никогда не сообщайте:
  - ✔ Паспортные данные.
  - ✔ Реквизиты карты (номер, CVC-код).
  - ✔ Логин и пароль от интернет-банка.

✔ Коды из СМС.

✔ Не устанавливайте приложения по указанию звонившего!

**Важно! Настоящие сотрудники банков и госорганов:**

- НЕ звонят в мессенджерах (Viber, Telegram, WhatsApp).
- НЕ звонят с зарубежных номеров.
- НЕ требуют перевода денег на "безопасные счета".

**❌ Если слышите подобное - это мошенники! ⛔ Будьте бдительны!**

**Мошенническая схема «Fake Boss»** - в настоящее время актуальная схема обмана работников организаций (предприятий, учреждений и т.д.)

Злоумышленники собирают сведения о работниках, при сборе которых уделяют особое внимание информации, касающейся принадлежности к соответствующей организации, а также имеющимся чатам и каналам, зарегистрированным в сети Интернет.

В дальнейшем злоумышленники, регистрируют учетные записи в различных мессенджерах, в особенности в мессенджере «Telegram». При регистрации аккаунта, указывают фамилию, имя и отчество руководителя интересующей организации, и добавляют его фотографию, полученную из открытых источников сети Интернет. Таким образом, злоумышленники создают поддельный аккаунт «руководителя организации», с целью введения в заблуждение подчиненного персонала.

В дальнейшем преступники в личных сообщениях от имени «руководителя организации» осуществляют общение с работниками.

Как правило, переписка ведётся на тему проверки деятельности организации компетентными органами, после чего «руководитель» указывает работнику на необходимость общения с неким представителем правоохранительных органов (следственного комитета, КГБ, Национального банка и т.д.), который в скором времени должен будет перезвонить. Через некоторое время сотруднику поступает звонок от «представителя правоохранительных органов», который, в ходе диалога, просит следовать его инструкциям:

- скачать и установить приложение (на самом деле выполняет функции удаленного доступа устройству);
- сообщить, сфотографировать реквизиты банковской платежной карточки и т.д.;

- требует перевести деньги на «защищенный банковский счет», задекларировать денежные средства и т.д.;
- предлагает поучаствовать в проведении спецоперации по поимке мошенников;
- оформить кредиты в банковских учреждениях, либо обратиться в банк для отмены заявок на кредит и т.д.

**✕ Если Вы слышите что-то подобное, немедленно положите трубку и лично перепроверьте информацию.**

**Фишинг** - это метод мошенничества, при котором злоумышленники выманивают личные данные (пароли, номера карт, коды из SMS) с помощью поддельных сайтов, писем или сообщений.

Основные виды фишинга:

**1.Фишинговые сайты**

- Вам приходит письмо или сообщение с просьбой войти в аккаунт (банк, социальные сети и т.д.).
- Ссылка ведёт на поддельный сайт, похожий на оригинальный, где просят ввести логин, пароль или данные карты.

**✕ Не вводите данные, если у вас есть сомнения в подлинности сайта!**

**2.Фальшивые письма и SMS**

- Приходит сообщение от «банка», «налоговой», «службы безопасности», «почты» или «интернет-магазина».
- Вас просят перейти по ссылке или скачать вложение, в котором может быть вирус.

**✕ Проверяйте отправителя, не открывайте подозрительные вложения!**

**3.Фишинг в социальных сетях и мессенджерах**

- Вам пишет «друг» или «коллега» и просит денег, ссылку на опрос или «интересное видео».
- После перехода по ссылке ваш аккаунт может быть взломан.

**✕ Свяжитесь с человеком напрямую, прежде чем выполнять его просьбу!**

Как защититься от фишинга?

- **Проверяйте адрес сайта перед вводом данных - он должен начинаться с "https://".**
- **Не вводите пароли и коды из SMS на подозрительных сайтах.**
- **Не переходите по ссылкам из писем и сообщений, если не уверены в их безопасности.**
- **Не скачивайте файлы из неизвестных источников - они могут содержать вирусы.**
- **Используйте двухфакторную аутентификацию (2FA) для защиты аккаунтов.**
- **Настройте антивирус и расширения для защиты от фишинга (например, Google Safe Browsing, Adblock, Adgurd и т.д.).**

**✕ Если вы стали жертвой фишинга - срочно смените пароли и свяжитесь с банком, если передали данные карты! Берегите свои данные!**

## Мошенничество на сайтах объявлений и в социальных сетях

**Как работают мошенники?**

- Выдают себя за известных продавцов (AliExpress, OZON, Lamoda и т.д.).
- Размещают объявления с продажей несуществующих товаров.
- Создают фейковые страницы в соцсетях, копируя бренды.
- Занижают цену на товар, создавая иллюзию выгодной сделки.
- Общаются только в мессенджерах, избегая звонков.
- Требуют предоплату или полную оплату на карту.

**Как не попасться?**

- Тщательно проверяйте информацию о продавце.
- Покупайте только у проверенных продавцов на официальных маркетплейсах.
- Избегайте слишком низких цен.
- Не переводите деньги на карту – пользуйтесь сервисами с защитой покупателя.
- Не соглашайтесь на "предоплату за доставку".

# Установка мошеннических приложений

**Как мошенники заставляют установить вирус?**

- Присылают ссылку в мессенджере «от имени оператора» или банка.
- Убеждают, что «нужно обновить приложение».
- Приложение получает доступ к SMS и банковским данным.

**Как распознать фальшивое приложение?**

- Оно установилось как «дополнительное» к уже имеющемуся.
- Просит доступ к SMS, контактам и экрану.
- Показывает логотип вашего оператора, но скачано не из официального магазина.

**Что делать?**

- Немедленно отключите интернет.
- Удалите приложение.
- Заблокируйте банковские карты, если заметили странные операции.
- Используйте только официальные магазины (Google Play, App Store).

**Вымогательство в социальных сетях** - это форма киберпреступления, при которой злоумышленники используют посты, фотографии, видеоролики или личную информацию пользователей, угрожая опубликовать компрометирующие материалы в обмен на выкуп.

Данная форма преступления нередко сопровождается созданием особого давления на жертву, вызывая у неё чувство стыда, страха и беспокойства.

Наиболее распространёнными целями для кибервымогателей являются молодые девушки и парни, предприниматели, знаменитости и политики. Причины выбора конкретных целей варьируются от личной мести до простой наживы.

**Примеры схем вымогательства:**

**Взлом личного профиля** (Мошенники получают доступ к аккаунтам пользователей через фишинговые сайты, подбор паролей или вредоносные программы. Захватив контроль над профилем, они начинают требовать выплату крупной суммы денег взамен на возвращение доступа владельцу).

**Распространение интимных материалов** (Самый известный пример вымогательства в социальных сетях - шантаж с публикацией

интимных изображений или видео. Злоумышленники могут проникнуть в закрытые группы или личные переписки, после чего угрожают разместить найденные материалы публично, если не получат требуемую сумму).

**Психологическое давление** (Некоторые мошенники применяют стратегию постепенного ухудшения состояния жертвы, доводя её до отчаяния, депрессии или чувства вины. Они будут угрожать раскрытия личных тайн друзьям, семье или работодателю, вынуждая жертву платить снова и снова).

**«Романтический» шантаж** (Многие мошенники прикрываются маской романтичного ухажёра, входя в доверие к девушке или молодому человеку, а затем неожиданно публикуют интимные подробности отношений или откровенные снимки, требуя компенсацию за молчание).

**Получение компрометирующих данных** (Случаи, когда пользователь сам выкладывает компрометирующую информацию (фотографии, видео, высказывания), которую позже используют злоумышленники для получения выгоды).

**Как защититься от вымогательства в социальных сетях?**

Несмотря на сложность проблемы, существуют действенные меры, способные значительно уменьшить риск подвергнуться такому виду киберпреступления:

**Повышение цифровой грамотности** (Пользователи должны чётко понимать риски публикации личной информации в интернете. Стоит избегать выставления интимных снимков, публикаций в закрытых группах и откровенных переписок).

**Создание сложных паролей** (Рекомендуется выбирать длинные пароли, содержащие буквы, цифры и символы, менять их каждые полгода и использовать менеджер паролей для хранения и синхронизации).

**Активация двухфакторной аутентификации** (Двухфакторная проверка снижает риск взлома аккаунта, поскольку злоумышленники не смогут воспользоваться только паролем).

**Контроль списка друзей и подписчиков** (Следует ограничить доступ к своим материалам, разрешив просмотр только узкому кругу проверенных людей. Частые чистки списков друзей снижают шансы на попадание злоумышленников в вашу жизнь).

**Минимизация личной информации** (Чем меньше личных данных открыто для публики, тем сложнее злоумышленникам использовать их в корыстных целях. Не указывайте точный адрес проживания, семейное положение, возраст и другие детали, которыми можно манипулировать).

**Не отвечать на угрозы** (Если вы стали объектом шантажа, важно не поддаваться требованиям вымогателей. Лучше сразу обратиться в правоохранительные органы и подать жалобу).

**Мошеннические инвестиционные биржи** - мошенники создают фальшивые инвестиционные платформы, заманивая людей обещаниями быстрой и легкой прибыли. Их цель - заставить вас перевести деньги и исчезнуть.

**Признаки мошеннической биржи:**

- Гарантируют высокую доходность при нулевых рисках. Если вам обещают огромные прибыли без риска - это обман. В реальном мире инвестиции ВСЕГДА сопряжены с риском.
- Неясные или запутанные условия. Такие платформы скрывают комиссии, требуют больших сумм для вывода или вовсе блокируют возможность забрать деньги.
- Фальшивые отзывы и поддельные рейтинги. Мошенники создают сайты и поддельные аккаунты, где якобы «успешные инвесторы» рассказывают, как они разбогатели.
- Агрессивное давление. «Вкладывай сейчас, пока не поздно!», «Только сегодня акция!» - если вас торопят, это явный признак мошенничества.
- Нет лицензии и прозрачной информации. Если у компании нет официальной регистрации, лицензий и четких данных о владельцах - бегите.

**Как защитить свои деньги?**

- Проверяйте компанию. Ищите лицензии, официальные документы, отзывы на независимых площадках.
- Не верьте обещаниям «золотых гор». Если доходность кажется слишком хорошей, чтобы быть правдой - это обман.

- Не принимайте поспешных решений. Мошенники давят на эмоции, но вы должны сохранять холодный разум.
- Советуйтесь с экспертами. Прежде чем инвестировать, проконсультируйтесь с независимым финансовым специалистом.
- Используйте только проверенные платформы. Доверяйте только известным и лицензированным инвестиционным компаниям.

**✕ Если вас просят внести деньги на неизвестную платформу - будьте осторожны! Не дайте себя обмануть!**

## Запомните фразы, которые используют преступники!

- назовите свои данные.
- задекларируйте ваши деньги.
- вам направлена ссылка.
- служба безопасности.
- это спецоперация.
- ваш аккаунт заблокирован.
- срок действия договора истекает.
- финансирование терроризма.
- безопасный счет.
- на вас оформили кредит.
- продиктуйте код из смс.
- уголовная ответственность.
- высокий доход.

➢ телефонные мошенники постоянно совершенствуют старые схемы и разрабатывают новые.

➢ аферисты активно используют современные технологии и психологические приёмы, чтобы создать иллюзию срочности и завоевать доверие жертв.

➢ люди получают звонки, на которые реагируют крайне импульсивно, не задумываясь о последствиях.

➢ не спешите с ответами, особенно если собеседник пытается вызвать панику.

✕ Осведомлённость – это ключевой инструмент в борьбе с мошенниками!!!

**Правовые основы проведения операций с криптовалютой -** Республики Беларусь развивающаяся страна и граждане активно 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 при помощи 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), 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 (например, обменивать Bitcoin на Ethereum).

**Запрещено:** покупать или продавать токены (криптовалюту) за денежные средства на иностранных криптобиржах и у физических лиц.

**Защищённость от киберпреступлений зависит от вашей готовности воспринимать информацию критично и сознательно подходить к выбору методов защиты. Только постоянный мониторинг окружающей обстановки и применение адекватных мер способны обеспечить сохранность ваших средств и личной информации.**

# Ответственность за совершение киберпреступлений

## Уголовный кодекс

**Статья 208. Вымогательство**

1. Требование передачи имущества или права на имущество либо совершения каких-либо действий имущественного характера под угрозой применения насилия к потерпевшему или его близким, уничтожения или повреждения их имущества, уничтожения, завладения, блокирования, модификации компьютерной информации, распространения клеветнических или оглашения иных сведений, которые они желают сохранить в тайне (вымогательство), -
(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок.
(в ред. Закона Республики Беларусь от 05.01.2015 N 241-З)

2. Вымогательство, совершенное повторно, либо группой лиц по предварительному сговору, либо с применением насилия, не опасного для жизни или здоровья потерпевшего, либо под угрозой убийства или причинения тяжкого телесного повреждения, либо соединенное с уничтожением или повреждением имущества, либо с целью получения имущественной выгоды в крупном размере -
(в ред. Закона Республики Беларусь от 15.07.2009 N 42-З)

наказывается лишением свободы на срок от трех до десяти лет со штрафом или без штрафа.
(в ред. Законов Республики Беларусь от 04.01.2003 N 173-З, от 15.07.2009 N 42-З, от 09.01.2019 N 171-З)

3. Вымогательство, совершенное организованной группой, либо с применением насилия, опасного для жизни или здоровья потерпевшего, либо повлекшее иные тяжкие последствия, либо с целью получения имущественной выгоды в особо крупном размере -
(в ред. Закона Республики Беларусь от 15.07.2009 N 42-З)

наказывается лишением свободы на срок от пяти до пятнадцати лет со штрафом.
(в ред. Законов Республики Беларусь от 04.01.2003 N 173-З, от 15.07.2009 N 42-З, от 09.01.2019 N 171-З)

Примечание. Под модификацией компьютерной информации в настоящей статье, статьях 212, 216, 350 и 354 настоящего Кодекса понимаются противоправное изменение компьютерной информации либо внесение в компьютерную систему заведомо ложной компьютерной информации.
(примечание введено Законом Республики Беларусь от 26.05.2021 N 112-З)

**Статья 209. Мошенничество**

1. Завладение имуществом либо приобретение права на имущество путем обмана или злоупотребления доверием (мошенничество) -

наказываются 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.
(в ред. Законов Республики Беларусь от 15.07.2009 N 42-З, от 05.01.2015 N 241-З)

2. Мошенничество, совершенное повторно либо группой лиц, -

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до четырех лет, или лишением свободы на тот же срок.
(в ред. Закона Республики Беларусь от 05.01.2015 N 241-З)

3. Мошенничество, совершенное в крупном размере, -

наказывается ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без штрафа.
(часть 3 статьи 209 в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

4. Мошенничество, совершенное организованной группой либо в особо крупном размере, -

наказывается лишением свободы на срок от трех до двенадцати лет со штрафом.
(в ред. Законов Республики Беларусь от 04.01.2003 N 173-З, от 22.07.2003 N 227-З, от 09.01.2019 N 171-З, от 17.02.2025 N 61-З)

**Статья 212. Хищение имущества путем модификации компьютерной информации**
(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Хищение имущества путем модификации компьютерной информации -

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.

2. То же деяние, совершенное повторно либо группой лиц по предварительному сговору, -

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до четырех лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.
(в ред. Закона Республики Беларусь от 17.02.2025 N 61-З)

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, -

наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух

до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

**Статья 222. Незаконный оборот платежных инструментов, средств платежа и их реквизитов**

(в ред. Закона Республики Беларусь от 17.02.2025 N 61-З)

1. Распространение из корыстных побуждений находящихся в незаконном владении лица реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам, электронным или виртуальным кошелькам, -

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.

2. Изготовление в целях сбыта или сбыт поддельных банковских платежных карточек, иных платежных инструментов и (или) средств платежа -

наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок.

3. Действия, предусмотренные частями 1 или 2 настоящей статьи, совершенные повторно, либо группой лиц, либо сопряженные с получением дохода в крупном размере, -

наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от трех до семи лет со штрафом или без штрафа.

4. Действия, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо сопряженные с получением дохода в особо крупном размере, -

наказываются ограничением свободы на срок от трех до пяти лет или лишением свободы на срок от трех до десяти лет со штрафом или без штрафа.

**Статья 349. Несанкционированный доступ к компьютерной информации**

(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), совершенный из корыстной заинтересованности либо повлекший по неосторожности причинение существенного вреда, -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Несанкционированный доступ к компьютерной информации либо самовольное пользование компьютерной системой или сетью, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, -

наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

**Статья 350. Уничтожение, блокирование или модификация компьютерной информации**

(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации, разрушение, блокирование либо нарушение работы компьютерной системы, сети или машинного носителя либо модификация компьютерной информации при отсутствии признаков преступления против собственности, повлекшие причинение существенного вреда, -

наказываются 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.

2. Те же деяния, совершенные повторно либо группой лиц по предварительному сговору, -

наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 настоящего Кодекса, -

наказываются лишением свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

**Статья 352. Неправомерное завладение компьютерной информацией**
(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Умышленные несанкционированное копирование, перехват компьютерной информации либо иное неправомерное завладение компьютерной информацией, повлекшие причинение существенного вреда, -

наказываются 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 срок до двух лет.

2. Те же деяния, совершенные повторно либо группой лиц по предварительному сговору, -

наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 настоящего Кодекса, -

наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

**Статья 354. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств**
(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Разработка, использование, распространение либо сбыт компьютерной программы или специального программного или аппаратного средства, заведомо предназначенных для нарушения системы защиты, несанкционированного доступа к компьютерной системе, сети или машинному носителю, несанкционированного уничтожения, блокирования, модификации компьютерной информации или неправомерного завладения компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя, -

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

2. Те же действия, совершенные группой лиц по предварительному сговору, -

наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Действия, предусмотренные частями 1 или 2 настоящей статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 настоящего Кодекса, -

наказываются лишением свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

**Статья 355. Нарушение правил эксплуатации компьютерной системы или сети**
(в ред. Закона Республики Беларусь от 26.05.2021 N 112-З)

1. Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этим системе или сети, повлекшее по неосторожности причинение существенного вреда, -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.

2. То же деяние, повлекшее по неосторожности последствия, указанные в части 2 статьи 349 настоящего Кодекса, -

наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

# Кодекс об административных правонарушениях

**Статья 11.1. Мелкое хищение**

Мелкое хищение имущества путем кражи, мошенничества, злоупотребления служебными полномочиями,

присвоения или растраты, хищения путем использования компьютерной техники, а равно попытка такого хищения -

влекут наложение штрафа в размере от двух до тридцати базовых величин, или общественные работы, или административный арест.

Примечание. Под мелким хищением в настоящей статье понимаются хищение имущества юридического лица в сумме, не превышающей десятикратного размера базовой величины, установленного на день совершения деяния, за исключением хищения ордена, медали Республики Беларусь, СССР или БССР, нагрудного знака к почетному званию Республики Беларусь, СССР или БССР, а также хищение имущества физического лица в сумме, не превышающей двукратного размера базовой величины, установленного на день совершения деяния, за исключением хищения ордена, медали Республики Беларусь, СССР или БССР, нагрудного знака к почетному званию Республики Беларусь, СССР или БССР либо хищения, совершенного группой лиц, либо путем кражи, совершенной из одежды или ручной клади, находившихся при нем, либо с проникновением в жилище.

**Статья 12.35. Незаконное предоставление реквизитов платежных инструментов**

(введена Законом Республики Беларусь от 17.02.2025 N 61-З)

1. Незаконное предоставление из корыстных побуждений находящихся в законном владении лица реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам, электронным или виртуальным кошелькам, -

влечет наложение штрафа в размере от пяти до тридцати базовых величин.

2. То же деяние, совершенное в течение одного года после наложения административного взыскания за такое же нарушение, -

влечет наложение штрафа в размере от двадцати до пятидесяти базовых величин, или общественные работы, или административный арест.

**Статья 13.3. Незаконная предпринимательская деятельность**

1. Предпринимательская деятельность, осуществляемая без лицензии, специального разрешения (лицензии), когда такие лицензия, специальное разрешение (лицензия) обязательны, либо с нарушением требований и условий осуществления видов деятельности, предусмотренных в специальных разрешениях (лицензиях), -

(в ред. Закона Республики Беларусь от 22.04.2024 N 365-З)

влечет наложение штрафа в размере от десяти до пятидесяти базовых величин, на индивидуального предпринимателя - от десяти до двухсот базовых величин с конфискацией до ста процентов суммы дохода, полученного в результате такой деятельности, или без конфискации, а на юридическое лицо - до пятисот базовых величин с конфискацией до ста процентов суммы дохода, полученного в результате такой деятельности, или без конфискации.

2. Предпринимательская деятельность, осуществляемая без государственной регистрации, когда такая регистрация обязательна, либо без указанной государственной регистрации и лицензии, специального разрешения (лицензии), когда такие лицензия, специальное разрешение (лицензия) обязательны, -

(в ред. Закона Республики Беларусь от 22.04.2024 N 365-З)

влечет наложение штрафа в размере до ста базовых величин с конфискацией предмета административного правонарушения, орудий и средств совершения административного правонарушения, а также до ста процентов от суммы дохода, полученного в результате такой деятельности, или без конфискации.

3. Осуществление предпринимательской деятельности, когда в соответствии с законодательными актами такая деятельность является незаконной и (или) запрещается, -

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, на индивидуального предпринимателя - от двадцати до двухсот базовых величин с конфискацией до ста процентов суммы дохода, полученного в результате такой деятельности, орудий и средств совершения административного правонарушения или без конфискации, а на юридическое лицо - до пятисот базовых величин с конфискацией до ста процентов суммы дохода, полученного в результате такой деятельности, орудий и средств совершения административного правонарушения или без конфискации.

4. Занятие предпринимательской деятельностью лицом, для которого законодательными актами установлен запрет на осуществление такой деятельности, -

влечет наложение штрафа в размере от десяти до тридцати базовых величин.

Примечание. 1. Под доходом от незаконной предпринимательской деятельности, осуществляемой без государственной регистрации, а равно полученным в результате осуществления предпринимательской деятельности, когда в соответствии с законодательными актами такая деятельность является незаконной и (или) запрещается, в настоящей статье следует понимать всю сумму выручки (дохода - для индивидуальных

предпринимателей, применяющих общий порядок налогообложения) в денежной или натуральной форме без учета затрат на ее (его) получение. Доход, полученный в натуральной форме, подлежит определению в денежном выражении.

2. Под доходом от незаконной предпринимательской деятельности, осуществляемой с государственной регистрацией без лицензии, специального разрешения (лицензии) либо с нарушением требований и условий осуществления видов деятельности, предусмотренных в специальных разрешениях (лицензиях), в настоящей статье следует понимать сумму выручки (дохода - для индивидуальных предпринимателей, применяющих общий порядок налогообложения) от реализации товаров (работ, услуг), имущественных прав, полученной (полученного) по этой деятельности, за вычетом косвенных налогов, а также понесенных при осуществлении указанной деятельности документально подтвержденных затрат по производству и реализации товаров (работ, услуг), имущественных прав, учитываемых при применении общего порядка налогообложения (в том числе таких затрат, понесенных в период применения особого режима налогообложения). Доход, полученный в натуральной форме, подлежит определению в денежном выражении.
(в ред. Закона Республики Беларусь от 22.04.2024 N 365-З)

**Статья 23.4. Несанкционированный доступ к компьютерной информации**

Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты, -

влечет наложение штрафа в размере от двадцати до тридцати базовых величин.