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

КИБЕРБЕЗОПАСНОСТЬ И ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ

Слайд 1.

Электронные сервисы, интернет-банкинг, удаленная работа и учеба, онлайн-регистрации, интернет-магазины и маркетплэйсы – все это настолько прочно вошло в нашу повседневность, что иногда трудно поверить, как жили без этого раньше. Чем больше погружаемся в мир информационно-коммуникационных технологий *(далее – ИКТ)*, тем больше становимся уязвимее.

Кибератаки на информационную структуру – это одна из самых значительных и постоянно растущих угроз для глобальной безопасности в XXI веке. На фоне всеобщей цифровизации эта проблема не просто нарастает, а эволюционирует, на что влияет широкое использование искусственного интеллекта *(далее – ИИ)*, так как злоумышленники начинают использовать его для создания более изощренных вредоносных программ, автоматизации атак и анализа уязвимостей.

Кибератаки превратились из проблемы технических специалистов в одну из главных стратегических угроз национальной, экономической и общественной безопасности любой страны.

По результатам исследования, проведенного в прошлом году, Беларусь находится на 3-м месте в рейтинге стран СНГ, которые чаще всего подвергаются кибератакам.

Каждая пятая атака в Беларуси приходится на госсектор *(22%)*. На втором месте – сфера промышленности *(14%)*, а на третьей строчке – финансовая отрасль *(11%)*. Много атак также нацелены на сектор телекоммуникаций, сферы науки и образования *(8%)*.

Каждая вторая кибератака *(57%)* приводит к утечке конфиденциальных данных. Реже они нарушают основную деятельность *(16%)* или несут прямые финансовые потери *(8%)*. Более половины украденных сведений составляют персональные данные и коммерческая тайна. Актуальной проблемой остается кража денег с банковских карточек и электронных кошельков.

Слайд 2.

Согласно данным за 2024 год, наша республика по уровню кибербезопасности заняла 70-е место из 166 стран в рейтинге NSCI *(National Cyber Security Index, Национальный индекс кибербезопасности)*, уступив по этому индексу среди стран СНГ лишь Молдове, Азербайджану и России.

Рост и усложнение методов киберугроз требуют опережающего и комплексного реагирования.

В Беларуси принят ряд системных мер, и борьба с киберугрозами ведется на нескольких уровнях. Так, **на государственном уровне** Указом Президента Республики Беларусь № 40 «О кибербезопасности» реализуется **комплексный многоуровневый механизм противодействия кибератакам** на государственные органы и организации, критическую информационную инфраструктуру. Создан

Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты *(далее – Национальный центр кибербезопасности)*. Налажено международное сотрудничество в этой сфере.

Созданы необходимые правовые условия для защиты персональных данных и безопасности личности и общества при их использовании. Закон Республики Беларусь **«О защите персональных данных»**, принятый в 2021 году, устанавливает границы, определяющие, какую информацию о человеке можно собирать и распространять. Вместе с тем, чтобы защита персональных данных была по-настоящему эффективной, нужны общие усилия – не только государства, но и граждан.

Противодействие осуществляется и **на корпоративном уровне**. Организации и предприятия инвестируют в кибербезопасность и обучение сотрудников.

Для борьбы с киберугрозами **на индивидуальном уровне** требуется повышение цифровой грамотности населения, соблюдение элементарных правил цифровой гигиены.

Современные аспекты кибербезопасности

Киберпреступления транснациональны, злоумышленники используют анонимайзеры *(сервисы, позволяющие скрыть личные данные пользователя и обеспечить анонимность в Интернете)* и находятся за рубежом, что крайне затрудняет их задержание.

По данным Следственного комитета Республики Беларусь, отмечается уход более 80% вымогательств и более 90% мошенничеств в «онлайн»-схему, чему способствует в том числе низкий процент осведомленности граждан о преступных схемах, а также развитие способов совершения таких хищений.

Картина распространенных видов киберпреступлений в Беларуси повторяет глобальные тренды, но с акцентом на местные платежные системы и привычки населения.

По данным главного управления по противодействию киберпреступности криминальной милиции Министерства внутренних дел Республики Беларусь, за 9 месяцев текущего года в Беларуси по сравнению с аналогичным периодом прошлого года количество киберпреступлений снизилось почти на 11% *(за 9 месяцев 2025 года зарегистрировано более 13 тыс. случаев (13 420), треть из которых (4 121) – в г.Минске)*.

По статистике **женщины** *(65%)* чаще всего становятся жертвами мошенников, которые выманивают деньги путем психологических манипуляций по телефону *(77,9%)*, купли-продажи товаров и оказания услуг *(65,6%)*, благотворительности *(100%)*. **Мужчины** *(84,8%)*, как

правило, становятся жертвами мошенничества, связанного с использованием сайтов знакомств.

Слайд 3.

Справочно:

Возрастные группы *потерпевших:*

люди старше 50 лет *чаще становятся жертвами телефонных мошенничеств, обмана, доверчивости, легенд о помощи родственникам;*

молодежь до 30 лет *уязвима от мошеннических дистанционных сделок с недвижимостью (56,3%), псевдо-инвестиций в «биржи» и «розыгрышей или акций» (65,4%);*

лица среднего возраста *(30–49 лет) – наиболее массовая группа среди потерпевших от ИКТ-мошенничества с заключением гражданско-правовых договоров (53,1%).*

Безработные и неучащиеся *чаще попадаются в инвестиционные ловушки (46,2%), что может быть связано с поиском ими источников дохода или увлечением азартными схемами.*

По **способам совершения** мошенничества чаще всего происходят **от имени должностных лиц** *(28,2%)*. Аферисты представляются сотрудниками правоохранительных органов *(МВД, СК, ДФР, КГБ)* и работниками банковских организаций. Мошенники стали звонить от имени работников служб газа, водоканала, энергонадзора, мобильных операторов связи под предлогом окончания срока договора и предлагают для его продления сообщить цифровой код из смс. После передачи кода жертве звонит сообщник мошенника и уже представляется правоохранителем, запугивает тем, что человек передал личные данные и на его имя будут оформлены кредиты. А чтобы их избежать предлагает оформить встречные кредиты и полученные деньги перевести на указанный счет или банковскую карту.

При схеме обмана **от имени руководителей** *(Fake boss)*

(учреждений образования, здравоохранения, культуры, предприятий) мошенники запугивают подозрением в финансировании экстремистской деятельности, проведением обыска и изъятием денег, также предлагают данный факт держать в тайне и пообщаться с определенным сотрудником правоохранительных органов, который якобы для сохранения денежных средств предлагает «временно» перевести деньги на защищенный счет.

В телефонном разговоре не доверяйте незнакомым лицам, кем бы они не представились, если вы не ждете такого звонка.

Треть мошенничеств *(27,6%)* совершается под видом **продажи товаров в сети Instagram или Telegram** *(чаще всего мошенники «продают» автозапчасти, садовые качели, новогодние ели, морепродукты и другие товары)*. Злоумышленники предлагают потенциальным покупателям перевести предоплату за товар и обещают его выслать по почте или курьером, после чего общение прекращается, и «клиент» остается ни с чем.

Справочно:

Также наиболее распространенные преступные схемы:

***звонки от имени банка, сотрудника МВД, КГБ и иных государственных органов**, когда мошенник, используя технологию подмены номера, звонит с номера, похожего на официальный номер банка и сообщает о «подозрительной операции» с картой, «блокировке счета» или «попытке взлома», а для «защиты» или «отмены операции» просит сообщить CVV-код, данные из SMS-сообщения с кодом подтверждения, пароль из интернет-банкинга или перевести деньги на «безопасный» (на самом деле подконтрольный мошеннику) счет;*

***фишинговые SMS-сообщения и письма**, когда приходит SMS-сообщение или электронное письмо с сообщением о «блокировке карты», «проблеме с налогом», «выигрыше в лотерее», которое содержит ссылку на фишинговый интернет-ресурс (сайт – клон), который выглядит как официальный интернет-ресурс банка, налоговой инспекции или другого государственного органа, где требуется ввести логин, пароль, данные платежных средств, после ввода которых совершается хищение;*

***мошенничества в социальных сетях и мессенджерах** («Viber», «WhatsApp», «Telegram»), когда злоумышленник взламывает аккаунт в соцсети или создает фейковый, похожий на него, пишет близким родственникам от имени владельца аккаунта, что срочно нужны деньги на «очень важное дело» (попал в сложную ситуацию, попал в ДТП и др.), прося никому не звонить; либо аналогичная предыдущей схема, когда мишенью становятся друзья, а мошенник от имени друга пишет, что застрял за границей, у него украли деньги/документы, и просит срочно перевести средства;*

***фейковые интернет-магазины**, когда создается красивый сайт-одностраничник или группа в социальной сети (зачастую в «Инстаграм»), с огромными скидками на актуальный у населения товар (техника «Apple», садовая мебель, надувные бассейны,*

брендовая одежда и др.), а после предоплаты товар не приходит, а сайт или группы исчезают, либо сообщения жертвы далее игнорируются;

***мошенничества под видом государственных органов**, когда жертве поступает звонок от имени «судьи», «сотрудника МВД», «налоговой» с требованием срочно оплатить некий фиктивный долг, штраф или пошлину, угрожая арестом счетов или другим наказанием, просят установить приложение для удаленного доступа (например, «AnyDesk» или «TeamViewer») для «проверки счета», что дает им полный контроль над устройством потерпевшего;*

***финансовые пирамиды и инвестиционные мошенничества**, такие как предложения «высокодоходных инвестиций» в криптовалюту, биржи или стартапы с гарантированным высоким доходом. При этом на первом этапе могут даже выплачивать небольшие проценты, чтобы потерпевший внес еще больше денежных средств и привел родственников, друзей и знакомых, после чего проект закрывается, а денежные средства похищаются;*

***вымогательство на интимной почве** («сексторшен»), когда мошенник через соцсети знакомится с жертвой, втирается в доверие, склоняет к общению в видеочате интимного характера или к отправке откровенных фото, записывает видео или делает скриншоты, а затем шантажирует.*

Опасения вызывают набирающие обороты **вымогательства** *(526 случаев)* с использованием информационно-коммуникационных технологий: потерпевших под различными предлогами вынуждают на личных устройствах IPhone войти не в свою учетную запись. После входа IPhone блокируется как похищенный и становится не пригодным. Для разблокировки злоумышленники требуют выкуп.

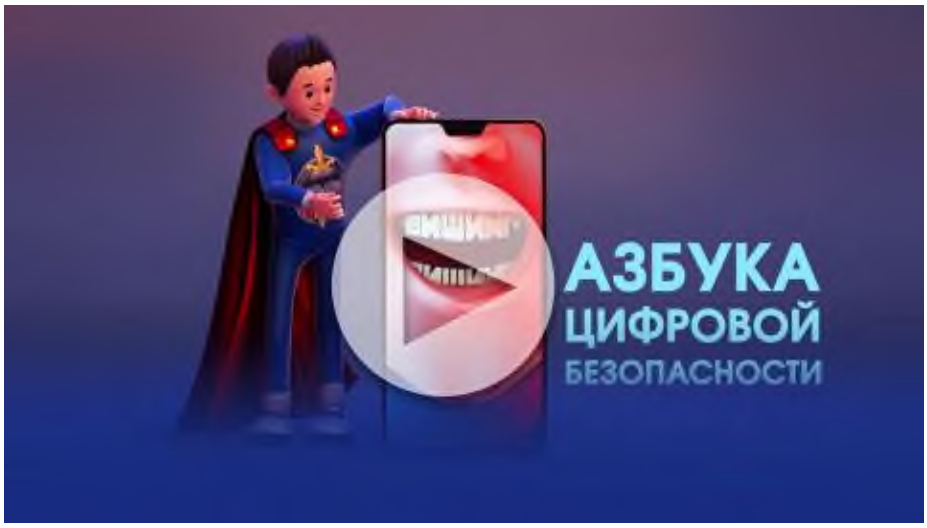
Поэтому ни в коем случае **нельзя входить на своем устройстве в чужую учетную запись**, владелец учетной записи может заблокировать устройство.

Слайд 4.

Следует отметить, что **фишинг** и **мошенничество с банковскими картами** являются самой массовой категорией кибермошенничества в Республике Беларусь.

При этом наряду с данными преступными схемами мошенники активно используют и такой метод фишинга, при котором конфиденциальные данные белорусских граждан добываются злоумышленниками посредством телефонных звонков. Этот вид мошенничества называется **«вишинг».**

Слайд 5. Видеоролик.



Справочно:

> ***Вишинг*** *– это устная разновидность фишинга, при которой злоумышленники посредством телефонной связи, используя приемы, методы и технологии психологического манипулирования, под разными предлогами, искусно играя определенную роль (как правило, сотрудника банка, технического специалиста и т.д.), вынуждают человека сообщить им свои конфиденциальные банковские или персональные данные либо стимулируют к совершению определенных действий со своим банковским счетом или банковской картой.*

По мере развития **информационно-коммуникационных технологий возрастают и возможности киберпреступников.** Некоторые мошеннические схемы получили новую жизнь благодаря искусственному интеллекту.

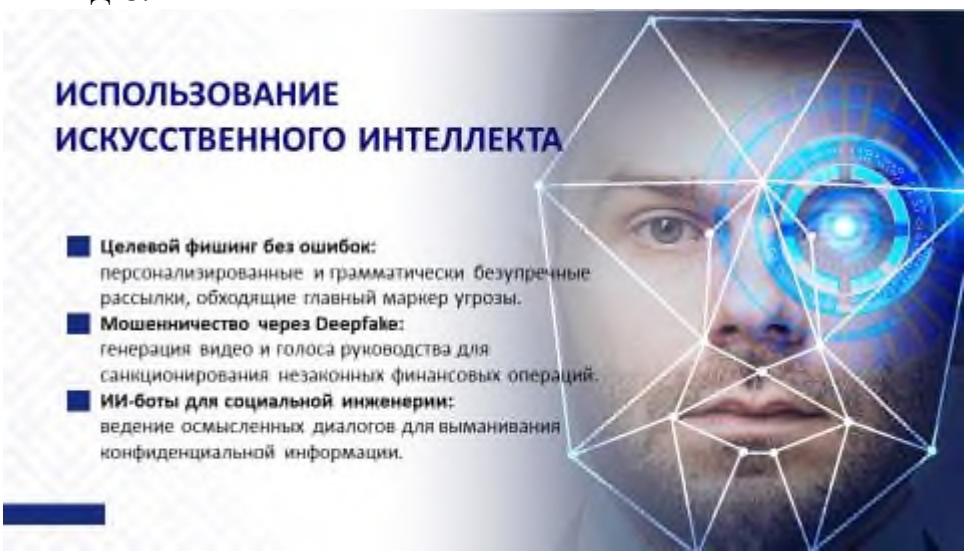
Растет количество случаев мошенничества с использованием **технологии Deepfakes** – это созданные искусственным интеллектом голосовые сообщения и видеозвонки от якобы коллег, друзей и родственников, как правило, с просьбой о срочном денежном переводе и др.

При видеозвонке следует обращать внимание на такие детали, как нечеткое или смазанное изображение лица говорящего, отсутствие или неестественная мимика лица.

Помните, что сотрудники банков и правоохранительных органов не звонят через мессенджеры с использованием видеосвязи. **При совершении денежного перевода под влиянием мошенников необходимо незамедлительно обратиться в органы внутренних дел** для сохранения денежных средств.

Даже когда искусственный интеллект используется во благо, нужно быть осторожным. Если работник организации думает, что загрузит документ в чат GPT и он все быстро сделает, то это прямой путь к утечке конфиденциальных данных. Документы отправятся на серверы в другом государстве, и законы нашей страны уже не могут гарантировать их безопасность.

Слайд 6.



Президент Беларуси А.Г.Лукашенко, выступая на III Минской международной конференции по евразийской безопансости, как одну из ключевых задач в целом обозначил необходимость принятия мер в области искусственного интеллекта: ***«Неуправляемая гонка в этой сфере превращает его из полезного ресурса в оружие. В перспективе – массового поражения»***.

Слайд 7.

Сотрудниками Министерства внутренних дел и Национального банка Республики Беларусь принимаются **меры, направленные на блокирование мошеннических операций**. В Беларуси с 1 марта 2024 г. действует **Указ Президента № 269**, который предоставляет банкам возможность приостанавливать подозрительные переводы и совместно с правоохранительными органами расследовать инциденты. Данный механизм позволяет достаточно эффективно взаимодействовать гражданам с органами внутренних дел, а им, в свою очередь, «в режиме 24 на 7» передавать указанную информацию банковскому сектору и получать от него эффективно и быстро информацию о лицах и инструментах, которые задействованы в противоправной деятельности. И самое главное – предпринимать меры, направленные на сохранение уже похищенных денежных средств у граждан и недопущения перевода их на зарубежные счета.

В связи с необходимостью защиты от мошенников банки устанавливают лимиты по снятию денег в банкоматах на территории Беларуси.

Борьба с этими преступлениями требует не только более совершенных технологий защиты, но и фундаментального повышения цифровой грамотности населения, поскольку именно человек остается наиболее уязвимым звеном в любой системе безопасности.

Цифровая грамотность населения

Кибербезопасность – это ответственность каждого из нас. Она начинается с таких простых вещей, как выбор надежного пароля для домашней электронной почты. Важно помнить, что один и тот же пароль нельзя использовать одновременно для рабочей почты, для регистрации на различных сайтах и в мессенджерах. К слову, личные данные чаще всего попадают к злоумышленникам из баз данных

магазинов *(мы оставляем фамилию, имя и отчество, адрес и телефон при регистрации для получения бонусных или скидочных карт)*.

Необходима элементарная **цифровая гигиена**, при которой **соблюдение простых правил поведения в сети** позволяет защитить персональные данные, финансы и устройства от кибермошенников.

Особую актуальность тема цифровой гигиены приобретает в отношении подрастающего поколения. Дети сегодня не только активно общаются в мессенджерах, но и погружаются в мир онлайн-игр, где их круг общения расширяется за счет незнакомцев. Среди них могут скрываться и киберпреступники, стремящиеся использовать ребенка для получения конфиденциальной информации. Неокрепшая психика, подверженность внушению и манипулированию делают их легкой «добычей» для злоумышленников.

Слайд 8.

Безопасность детей в сети – это не просто запреты, а создание защищенной среды и обучение правильному поведению. В семье необходимо выстраивать **доверительные отношения с ребенком**. Дети не должны искать понимания у незнакомцев в сети, а быть уверены, что могут рассказать родителям о любой странной или неприятной ситуации в сети без страха быть наказанным.

Важно договориться и установить четкие правила: какие сайты можно посещать, сколько времени проводить онлайн, какие приложения можно использовать.

Для младших детей рекомендуется создавать аккаунты вместе и знать их пароли. Использование **специализированного программного**

обеспечения родительского контроля позволит ограничивать время за экраном, фильтровать контент, блокировать нежелательные сайты.

Существует **множество преступных схем,** используемых кибермошенниками **в отношении несовершеннолетних детей**.

Слайд 9.

Справочно:

Способы киберпреступлений в отношении детей и подростков:

«бесплатные» подарки и розыгрыши*, когда ребенку для получения выигрыша предлагается перейти по ссылке и ввести платежные и иные данные его родителей. Основная цель – украсть данные банковских карт или учетных записей;*

«фейковые» запросы от друзей*, когда с использованием взломанного аккаунта друга ребенка просят помочь (перевести денежные средства), а ребенок, желая помочь, может не усомниться в личности просящего;*

«груминг»*, когда взрослый злоумышленник под видом сверстника втирается в доверие к ребенку в соцсетях или играх, постепенно выведывает личную информацию, манипулирует, вызывает чувство близости, а затем может выпрашивать интимные фото/видео или назначать личную встречу, что может привести к совершению в отношении ребенка действий сексуального характера, которые ребенок в силу возраста не может оценивать, как социально-значимые, считая происходящее игрой;*

«сексторшен»*, когда преступник, получив интимные фото или видео (добровольно отправленные ребенком или через взлом камеры), начинает шантажировать ребенка, вымогая как материальные блага, так и услугу, в том числе сексуального характера;*

кибербуллинг *(или травля), когда создаются группы и паблики для насмешек, унизительных комментариев, отправляются угрозы в личных сообщениях, чтобы причинить ребенку психологическую боль, что нередко может закончится депрессией или даже самоубийством;*

вовлечение в опасные сообщества*, пропагандирующие депрессивные течения, суицид, анорексию, насилие или экстремизм,*

которые преподносятся ребенку как что-то «модное», «крутое» и «запретное».

Слайд 10.

Важно научить детей цифровой грамотности и критическому мышлению. Им нужно понимать, что **Интернет – это отражение реального мира: в нем есть и хорошие, и плохие люди, и правила безопасности здесь так же важны, как и на улице**. Не экономьте на времени, чаще и больше разговаривайте со своими детьми!

Также в защите от преступных посягательств, в информировании и дополнительном внимании нуждаются и люди пожилого возраста.

****

За последнее время в республике произошли значительные позитивные сдвиги: удалось общими усилиями переломить тенденцию роста числа киберпреступлений, заметно вырос уровень цифровой защиты, демонстрирует оперативность и адаптивность к текущим вызовам белорусское законодательство в области кибербезопасности и др. Примечательно, что наш опыт борьбы с киберпреступниками активно применяют в других странах.

Как отметил **Президент Республики Беларусь А.Г.Лукашенко**, ***«абсолютную защиту от кибератак не гарантирует ни одна система защиты, но мы должны минимизировать риски»***. Этого возможно добиться, когда каждый участник информационных отношений, каждая организация будут ответственно подходить к выполнению требований по кибербезопасности, а каждый человек проявит бдительность и внимательность в случае ситуации с мошенниками.

Слайд 11.


Родители, научите детей пользоваться Интернетом правильно!
Правила безопасного поведения
Берегите аккаунты от аферистов!
АКАДЕМИЯ УПРАВЛЕНИЯ ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ

Тезисы общего материала
к единому дню информирования по теме:
КИБЕРБЕЗОПАСНОСТЬ И ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ

1. Кибератаки стали одной из главных стратегических угроз национальной, экономической и общественной безопасности любой страны.

2. Беларусь вошла в тройку стран СНГ, которые чаще всего подвергаются кибератакам (по уровню кибербезопасности наша страна заняла 70-е место из 166 стран).

3. Благодаря реализуемому комплексному многоуровневому механизму противодействия кибератакам в этом году **впервые** удалось **снизить** (почти на 11%) количество киберпреступлений. Однако в любой системе безопасности **наиболее уязвимым** звеном остается человек.

4. Социальный портрет жертв.

Женщины – путем психологических манипуляций по телефону, купли-продажи товаров и оказания услуг, благотворительности.

Мужчины – преступления, связанные с использованием сайтов знакомств.

Больше всех в защите от преступных посягательств **нуждаются** дети и люди пожилого возраста.

5. **Наиболее распространенные** схемы мошенничества: звонки от имени должностных лиц и руководителей (Fake boss), кража денег с банковских карт, вымогательство за разблокировку IPhone. Треть мошенничеств совершается под видом продажи товаров в сети Instagram или Telegram.

Некоторые мошеннические схемы получили новую жизнь благодаря искусственному интеллекту.

6. Президент Республики Беларусь А.Г.Лукашенко: «Абсолютную защиту от кибератак не гарантирует ни одна система защиты, но мы должны минимизировать риски». Всем нужно ответственно подходить к выполнению требований по кибербезопасности, проявлять бдительность и внимательность.

Сотрудниками МВД и Национального банка Республики Беларусь принимаются меры, направленные на блокирование мошеннических операций. Поэтому при совершении денежного перевода под влиянием мошенников необходимо **незамедлительно обратиться в органы внутренних дел.**

Необходима элементарная **цифровая гигиена**, при которой соблюдение простых правил поведения в сети позволяет защитить персональные данные, финансы и устройства от кибермошенников.

КИБЕРБЕЗОПАСНОСТЬ И ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ

Единый день информирования населения

ноябрь 2025 г.

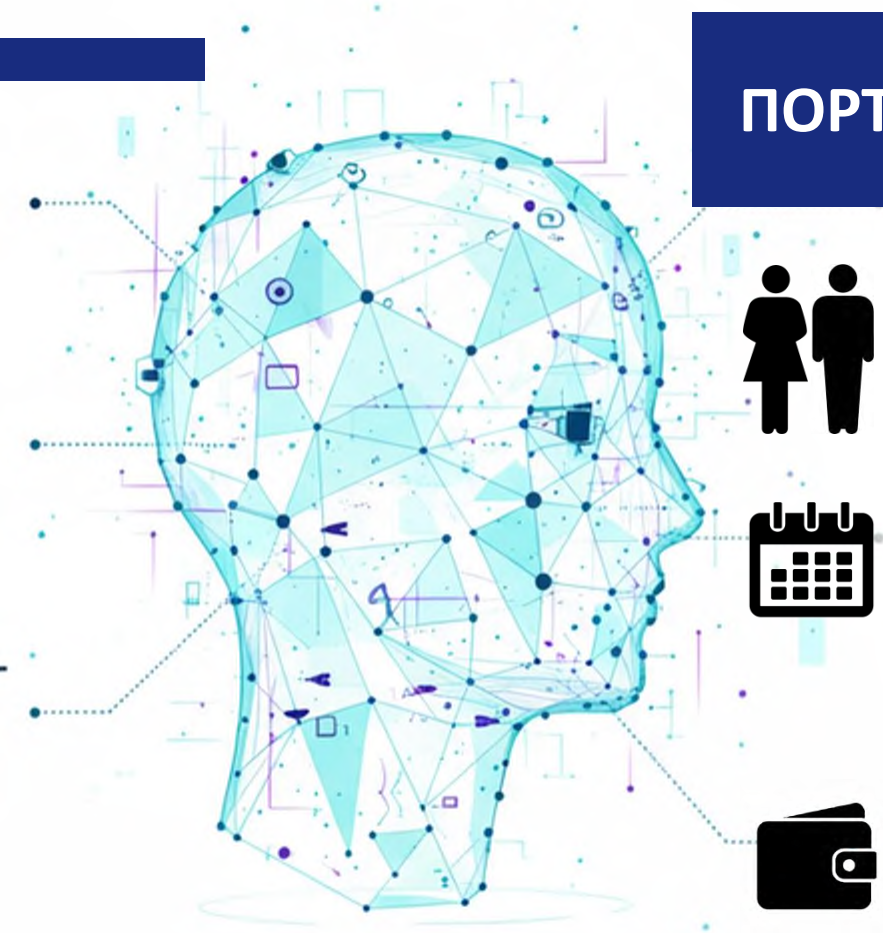
РОСТ КИБЕРАТАК В БЕЛАРУСИ

- **Позиция Беларуси:** 3-е место в СНГ по количеству кибератак

- **ОСНОВНЫЕ ЦЕЛИ АТАК:**
  Госсектор – 22%
  Промышленность – 14%
  Финансы – 11%

- **ПОСЛЕДСТВИЯ:**
  Утечка данных – 57% случаев
  Нарушение работы – 16%
  Финансовые потери – 8%

ПОРТРЕТ ЖЕРТВЫ МОШЕННИЧЕСТВА



Женщины

Телефонные мошенники — 77,9%

Обман в сфере услуг — 65,6%

Мужчины

Мошенничество на сайтах знакомств — 84,8%

Возраст

50+: телефонное мошенничество, «помощь родственникам»

До 30 лет: псевдо-инвестиции (65,4%), дистанционные сделки с недвижимостью (56,3%)

30-49 лет: ИКТ-мошенничество с договорами (53,1%)

Социальный статус:

безработные чаще попадают в инвестиционные ловушки (46,2%)

ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫЕ В СТРАНЕ

- звонки от имени банка, сотрудника МВД, КГБ и иных государственных органов
- фишинговые SMS-сообщения и письма
- мошенничества в социальных сетях и мессенджерах
- мошенничества при онлайн-покупках на площадках по продаже товаров
- фейковые интернет-магазины
- мошенничества под видом государственных органов
- финансовые пирамиды и инвестиционные мошенничества
- вымогательство на интимной почве

АЗБУКА ЦИФРОВОЙ БЕЗОПАСНОСТИ

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

- **Целевой фишинг без ошибок:** персонализированные и грамматически безупречные рассылки, обходящие главный маркер угрозы.
- **Мошенничество через Deepfake:** генерация видео и голоса руководства для санкционирования незаконных финансовых операций.
- **ИИ-боты для социальной инженерии:** ведение осмысленных диалогов для выманивания конфиденциальной информации.

Неуправляемая гонка в этой сфере превращает его *(прим. – искусственный интеллект)* ***из полезного ресурса в оружие. В перспективе – массового поражения.***

Президент Республики Беларусь А.Г. Лукашенко, III Минская международная конференция по евразийской безопасности, 28 октября 2025 г.

БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ — ЭТО НЕ ЗАПРЕТЫ, А ДОВЕРИЕ И ПРАВИЛА

Выстраивайте открытые отношения: ребенок должен знать, что может рассказать вам о любой проблеме без страха наказания.

Установите четкие границы: согласуйте время онлайн, разрешенные сайты и приложения.

Используйте технические средства: родительский контроль и общие аккаунты для младших детей.

РАСПРОСТРАНЕННЫЕ СХЕМЫ КИБЕРПРЕСТУПЛЕНИЙ ПРОТИВ ДЕТЕЙ

«Бесплатные» подарки

Цель: заманить на фишинговую страницу и украсть данные банковской карты.

Фейковые запросы от «друзей»

Цель: воспользоваться доверием и выманить деньги через взломанный аккаунт.

Груминг

Цель: выдавая себя за сверстника, войти в доверие, чтобы манипулировать и выпрашивать интимные фото/видео.

Сексторшен

Цель: шантажировать ребенка с помощью полученных интимных материалов.

Кибербуллинг

Цель: унизить и травмировать психологически через травлю в группах и личных сообщениях.

Деструктивный контент

Цель: вовлечь в опасные сообщества, пропагандирующие суицид, насилие и экстремизм.

4 КЛЮЧЕВЫХ ПРАВИЛА БЕЗОПАСНОСТИ В СЕТИ ДЕТЕЙ И ПОДРОСТКОВ

1 **Храни личное в тайне**
Не публикуй адрес, школу, геометки, данные документов и карт, планы семьи.

2 **Помни алгоритм «СТОП-СПРОСИ-РАССКАЖИ»**
СТОП, если что-то настораживает. СПРОСИ у родителей, если непонятно. РАССКАЖИ взрослым о любой угрозе или дискомфорте.

3 **Контролируй круг общения**
Добавляй в друзья только тех, кого знаешь лично. Настрой приватность профиля.

4 **Включай критическое мышление**
Не переходи по сомнительным ссылкам. Не верь слишком «выгодным» предложениям.

Родители, научите детей пользоваться Интернетом правильно!

Правила безопасного поведения

Берегите аккаунты от аферистов!

АКАДЕМИЯ УПРАВЛЕНИЯ
ПРИ ПРЕЗИДЕНТЕ
РЕСПУБЛИКИ БЕЛАРУСЬ

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

КИБЕРБЕЗОПАСНОСТЬ И ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ

(для представителей интеллигенции)

Давайте сегодня поговорим об Интернете, как о месте, в котором можно пропасть, и в котором реально пропадают многие люди. А бывает, и целые страны. «*Гибельное место Интернет*» – такая тема, согласитесь, звучит заманчивей, чем если просто сказать: «*Кибербезопасность и профилактика киберпреступности*». Хотя смысл разговора все равно будет именно такой.

Интернет как оружие против нас

Вспомним с вами, что Интернет создавался в американских военных лабораториях – и с тех пор все с ним связанное так или иначе и производится, и работает как оружие. Как оружие против нас.

Скажем, **спутниковый Интернет** обеспечивает связь на поле боя. **Социальные сети** позволяют собирать группы людей и анонимно управлять ими на расстоянии. **Криптовалюты** – неотслеживаемо оплачивать кураторов таких сетей и любых террористов в принципе.

Наверное, не многие обратили внимание, как зимой 2023 года через социальные сети попытались натравить членов интернет-сообщества «ЧВК Рёдан» на футбольных фанатов. Это был один из тренингов, одно из самых натуральных полевых учений. А получится ли зумеров-ботанов, не вылезающих из-за своих компов, вывести на улицы, да еще и стравить со спортивными «ультрас» *(организованные группы спортивных болельщиков)*?

Оказалось, что современные технологии позволяют уже и такое делать. Правда, правоохранители до реальных стычек им дойти не дали. Однако очевидно: Интернет из поля боя, где хозяева всего – англосаксы, дорос уже и до инструмента реального влияния на живых людей.

Любое нажатие на любой клавиатуре – это одновременно еще и письмо англосаксам, ибо ты можешь что хочешь делать и хоть как экранироваться, но клавиша есть клавиша. Плюс каждый современный гаджет докладывает «в центр» *(или в Лэнгли, или в «вашингтонский обком»)* обо всем, что происходит не только внутри него, но и вокруг. Таким образом западники – при желании – могут знать все о предпочтениях белорусского, например, пропагандиста.

Вплоть до того, где тот или та проводит выходные, куда сначала смотрит на легкомысленных картинках, о чем именно разговаривает в курилке и на что предпочитает тратить заработанные контрпропагандой гонорары.

Кибератаки на виртуальном поле боя

Сегодня ни один человек, ни одна страна не застрахована от того, чтобы стать объектом кибернападения. Массированные хакерские атаки являются одной из самых значительных и постоянно растущих угроз для глобальной безопасности в XXI веке. Взлом компьютерных систем способен парализовать целые отрасли промышленности, привести к масштабным экономическим преступлениям, остановить работу банков, закрыть аэропорты и т.д.

Вполне определенно по этому поводу высказался Президент Республики Беларусь А.Г.Лукашенко: ***«Во всем мире наблюдается рост кибератак. Причем атакуют прежде всего стратегические объекты, государственные органы, предприятия, банковскую систему. То есть целью их являются основные пункты жизнеобеспечения любого государства, в том числе и нашего. Это один из элементов гибридной войны, очень опасный элемент. Цель – нанести максимальный ущерб экономике и дестабилизировать в итоге общество. Следует обезопасить наше государство с учетом того, что у нас есть»***.

Надо понимать, что любое чужое программное обеспечение может быть изначально заражено закладкой с возможностью удаленного, скажем так, подрыва. А еще закладка может быть заложена аппаратно, на этапе конфигурирования чипов устройства. И если про *Виндовс*, например, мы обычно не думаем, как про мину замедленного действия, то любой современный смартфон теоретически может такой миной стать в любую минуту.

Мы ведь много раз с вами слышали или читали, как горят или взрываются батареи в мобильных телефонах, правда же? А если это они не сами? История *арабо-израильских пейджеров* показывает: очень даже может быть, что и не сами. Бояться этого каждый день, наверное, не нужно, но помнить об этом стоит.

Дополнительную опасность кибератакам и другим высокотехнологичным преступлениям придают **всеобщая цифровизация** и, следовательно, **зависимость вместе со стиранием границ**. Также – **доступность инструментов вместе с невысоким уровнем компьютерной грамотности** граждан. Кибератаки нынче стали **геополитическим инструментом** и используются для шпионажа,

дестабилизации обстановки, влияния на выборы и нанесения ущерба критической инфраструктуре без объявления открытой войны.

Справочно:

По результатам исследования компании Positive Technologies, число кибератак в странах СНГ выросло почти в 3 раза во II квартале 2024 г., если сравнивать с тем же периодом предыдущего года.

При этом Беларусь заняла 3-е место в рейтинге стран СНГ, которые чаще всего подвергаются кибератакам.

Каждая пятая атака в Беларуси приходится на госсектор (22%). На втором месте – сфера промышленности (14%), а на третьей строчке – финансовая отрасль (11%). Много атак также нацелены на сектор телекоммуникаций, сферы науки и образования (8%).

Каждая вторая кибератака (57%) приводит к утечке конфиденциальных данных. Реже они нарушают основную деятельность (16%) или несут прямые финансовые потери (8%). Более половины украденных сведений составляют персональные данные и коммерческая тайна. Для рядовых пользователей чувствительной остается кража денег на карточках и кошельках.

Как с этим бороться? В Беларуси одним из ключевых решений стало подписание Главой государства **Указа № 40 «О кибербезопасности»**, на базе которого в нашей стране сформирована **основа комплексного многоуровневого механизма противодействия кибератакам** на государственные органы и организации, критическую информационную инфраструктуру. Создан Национальный центр кибербезопасности, а многие крупные компании также сформировали собственные центры информационной безопасности.

С 1 марта 2024 г. в Беларуси функционирует **механизм противодействия несанкционированным платежным операциям**, когда у банков появилась возможность приостанавливать подозрительные переводы и совместно с правоохранительными органами расследовать инциденты.

Справочно:

Согласно опубликованным данным от Positive Technologies, в 2024 году наша республика заняла 70-е место из 166 стран в рейтинге NSCI (от англ. National Cyber Security Index, Национальный индекс кибербезопасности) по уровню кибербезопасности, уступив по этому индексу среди стран СНГ лишь Молдове, Азербайджану и России.

Интернет под контролем спецслужб

А еще Интернет, поскольку мы все к нему непрерывно обращаемся, вкладывает нам в головы свои смыслы. Свои – это те, которые прописаны в «Википедии», а оттуда попадают сначала в

школьные и студенческие головы, затем – и во все интеллектуальные конструкты модных мыслителей, чтобы потом стать якобы «общеизвестными». Сама же интернет-энциклопедия *(уже многократно было опубликовано)* как минимум с 2008 года редактируется Федеральным бюро расследований (далее – ФБР) и Центральным разведывательным управлением (далее – ЦРУ).

Неотвратимо грядет и время искусственного интеллекта (далее – ИИ). Уже сейчас Запад принимает ограничительные меры.

Справочно:

Университет Бонна разослал российским студентам уведомления о том, что они больше не могут посещать ряд курсов по ИИ, анализу данных и 3D-технологиям. Такое решение объясняется санкциями ЕС: обучение по этим направлениям является технической помощью Российской Федерации.

Когда немцам заявили, что это чистой воды дискриминация, сегрегация и нарушение прав человека, пресс-секретарь университета спокойно ответил, что они «открыты для всех иностранных студентов и против дискриминации, однако запрет на курсы дискриминацией не считается». Шансов на судебное решение, как понятно, нет.

Надо помнить, что большая часть социальных сетей не только создана англосаксами, но и курируется англосаксонскими спецслужбами напрямую. Недавно американский независимый портал MintPress News опубликовал итоги своих многочисленных расследований, из которых становится понятно, что люди из ЦРУ, ФБР, Госдепа, НАТО и других государственных институтов регулярно направляются на службу в социальные сети *(например, такие, как Facebook, Google, TikTok и Twitter)*.

Там они работают в специальных структурах *(скажем, отдел доверия и безопасности, управление безопасности и модерации контента и т.п.)*, фактически влияя на то, что видят и читают миллиарды людей по всему миру. Так же, как и на то, что обычные жители, граждане, избиратели не видят, не слышат и не читают.

В расследовании приведен большой список фамилий якобы бывших сотрудников ЦРУи ФБР, перешедших на работу в социальные сети и занимающих там важные с точки зрения формирования правил и контента должности.

Именно те «бывшие сотрудники» обычно решают, кого и что в соцсетях надо «минимизировать» *(подавлять)*, а кого или что «плюсовать» *(раскручивать)*.

Справочно:

Вот неполный список «бывших сотрудников», всего же таких агентов сотни:

***Дон Бертон**, которая в 2019 году оставила должность старшего советника по инновациям директора ФБР, чтобы стать старшим директором по стратегии и операциям в сфере права, государственной политики, доверия и безопасности в Twitter.*

***Джефф Карлтон –** командующий Корпусом морской пехоты и давний аналитик разведки ЦРУ и ФБР, в мае 2021 г. покинул Правительство, чтобы перейти в Twitter на должность старшего менеджера программы по доверию и безопасности.*

***Хейли Чанг –** бывший заместитель главного юрисконсульта Министерства внутренней безопасности и заместитель помощника директора ФБР, которая покинула бюро, чтобы стать заместителем главного юрисконсульта компании Meta и заниматься вопросами кибербезопасности и расследований.*

***Джои Чан**, который в 2021 году оставил пост командующего Армии США, чтобы стать менеджером программы доверия и безопасности в Meta.*

***Эллен Никсон –** бывшая агент ФБР, ставшая менеджером по расследованиям угроз Facebook.*

***Черрелл Й.** – бывший агент ФБР, работающий специалистом по вопросам политики в Twitter.*

***Аарон Берман** – агент ЦРУ до июля 2019 г., когда он покинул пост старшего менеджера по аналитике, чтобы стать старшим менеджером по продуктовой политике в области дезинформации в компании Meta, материнской компании Facebook, Instagram и WhatsApp. По словам А.Бермана, нынешняя должность делает его главой команды, которая пишет правила для Facebook, определяя, «что приемлемо, а что нет» для трех с лишним млрд пользователей платформы. Правила для почти половины населения Земли.*

Интернет как инструмент психологического манипулирования

Надо признать: нас приучили, а мы с вами, как и все остальные жители Земли, привыкли и к Интернету, и к смартфонам, и к социальным сетям, и к криптовалютам. И не собираемся ни от чего отказываться. И к продажам личных данных привыкли, и к постоянному контролю геолокации, и к прослушиванию окружающего пространства…

Поэтому давайте хотя бы инфогигиену соблюдать, хотя бы свою голову в чистоте держать. Это и будет наш минимальный вклад в кибербезопасность и в профилактику киберпреступности.

Справочно:

За 8 месяцев 2025 года Национальный центр защиты персональных данных получил 21 уведомление о нарушении систем защиты персональных данных, из которых два – об утечке. По требованию центра удалено более 3,3 млн записей, а также более 2,7 млн видео- и аудиозаписей, содержащих незаконно обрабатываемую конфиденциальную информацию.

В Беларуси созданы необходимые условия для защиты персональных данных и безопасности личности и общества при их использовании. Закон Республики Беларусь «О защите персональных данных», принятый в 2021 году, дает понять, какую информацию о человеке можно собирать и распространять, а какую не стоит.

Справочно:

Чтобы защитить свои личные данные в Интернете и избежать проблем, рекомендуется соблюдать несколько простых правил:

1. Всегда внимательно читайте, на что вы даете согласие. Изучайте политику обработки персональных данных, из текста которой можно понять, какие ваши данные будут собирать и как их использовать;

2. Используйте надежные пароли и включайте двухфакторную защиту, чтобы посторонний не смог взломать ваши аккаунты. Следует с максимальной осознанностью подходить к размещению личной информации в социальных сетях. Не следует опубликовывать паспортные данные, банковские реквизиты, фото билетов, служебные документы и т.п.;

3. Будьте осторожны с подозрительными письмами и звонками – это может быть попытка обманом получить персональные данные. Регулярно обновляйте программы и антивирусы, а для работы в Интернете выбирайте только проверенные сайты и приложения;

4. Бережно относитесь к своим и чужим данным: не сообщайте реквизиты карт, пароли и личную информацию незнакомым лицам, остерегайтесь мошенников и сомнительных сообщений, обращайтесь в правоохранительные органы. Всегда сохраняйте здоровый скептицизм и не торопитесь выполнять непроверенные инструкции.

Наиболее распространенными видами кибермошенничества в Республике Беларусь по-прежнему являются **фишинг,** то есть кража личных данных, и **мошенничество с банковскими картами**.

Справочно:

Примеры самых распространенных схем:

***звонки от имени банка, сотрудника МВД, КГБ и иных государственных органов**, когда мошенник, используя технологию подмены номера, звонит с номера, похожего на официальный номер банка и сообщает о «подозрительной операции» с картой, «блокировке счета» или «попытке взлома», а для «защиты» или «отмены операции» просит сообщить CVV-код, данные из SMS-сообщения с кодом подтверждения, пароль из интернет-банкинга или перевести деньги на «безопасный» (на самом деле подконтрольный мошеннику) счет;*

***фишинговые SMS-сообщения и письма**, когда приходит SMS-сообщение или электронное письмо с сообщением о «блокировке карты», «проблеме с налогом», «выигрыше в лотерее», которое содержит ссылку на фишинговый интернет-ресурс (сайт – клон), который выглядит как официальный интернет-ресурс банка, налоговой или другого государственного органа, где требуется ввести*

логин, пароль, данные платежных средств, после ввода которых совершается хищение;

мошенничества в социальных сетях и мессенджерах *(«Viber», «WhatsApp», «Telegram»), когда злоумышленник взламывает аккаунт в соцсети или создает фейковый, похожий на него, пишет близким родственникам от имени владельца аккаунта, что срочно нужны деньги на «очень важное дело» (сломался телефон, попал в сложную ситуацию, попал в ДТП и др.), прося никому не звонить; либо аналогичная предыдущей схема, когда мишенью становятся друзья, а мошенник от имени друга пишет, что застрял за границей, у него украли деньги/документы, и просит срочно перевести средства;*

мошенничества при онлайн-покупках на площадках по продаже товаров *(торговые площадки, маркетплейсы, соцсети), когда мошенник размещает привлекательное объявление о продаже товара (техника, детские вещи, животные) по заниженной цене, просит 100% предоплату на карту или через ЕРИП, после чего исчезает. Аналогичная, но обратная схема, когда жертва предлагает товар к продаже, а мошенник, используя его контакты в мессенджерах или социальных сетях, предлагает купить товар с доставкой, якобы оформленной онлайн, присылая фишинговую ссылку для оплаты, предназначенную для получения данных платежных средств и последующего хищения денежных средств;*

фейковые интернет-магазины*, когда создается красивый сайт-одностраничник или группа в социальной сети (зачастую в «Инстаграм»), с огромными скидками на актуальный у населения товар (техника «Apple», садовая мебель, надувные бассейны, брендовая одежда и др.), а после предоплаты товар не приходит, а сайт или группы исчезают, либо сообщения жертвы далее игнорируются;*

мошенничества под видом государственных органов*, когда жертве поступает звонок от имени «судьи», «сотрудника МВД», «налоговой» с требованием срочно оплатить некий фиктивный долг, штраф или пошлину, угрожая арестом счетов или другим наказанием, просят установить приложение для удаленного доступа (например, «AnyDesk» или «TeamViewer») для «проверки счета», что дает им полный контроль над устройством потерпевшего;*

финансовые пирамиды и инвестиционные мошенничества*, такие как предложения «высокодоходных инвестиций» в криптовалюту, биржи или стартапы с гарантированным высоким доходом, и по началу могут даже выплачивать небольшие проценты, чтобы потерпевший внес еще больше денежных средств и привел родственников, друзей и знакомых, после чего проект закрывается, а денежные средства похищаются;*

вымогательство на интимной почве *(«сексторшен»), когда мошенник через соцсети знакомится с жертвой, втирается в доверие, склоняет к общению в видеочате интимного характера или к отправке откровенных фото, записывает видео или делает скриншоты, а затем шантажирует, требуя деньги, угрожая разослать материалы всем друзьям и родственникам жертвы.*

Что тут можно и нужно делать, ведь борьба против такого вида преступлений – это совместная забота государства и самих граждан? Не надо бояться. Важно ежедневно соблюдать правила информационной гигиены – и делать это с тем же рвением, как мы все мыли руки после первых известий о COVID-19. Настаивать, чтобы так же вели себя и родственники, и знакомые, и коллеги. Учить информационной гигиене детей.

И помнить: в любой, даже самой продуманной системе безопасности – и особенно в самой продуманной – человек является самым слабым звеном. Поэтому в информационную эпоху повышать свою личную цифровую грамотность надо непрерывно.

Современные технологии играют все большую роль в различных отраслях, таких как космос, здравоохранение, промышленность, финансы, образование, транспорт... да во всех областях жизни! От чат-ботов до беспилотных автомобилей – искусственный интеллект меняет наш мир, делая его комфортнее и удобнее. Однако **масштаб воздействия ИИ** на человечество нам еще предстоит осознать.

«С одной стороны, современные технологии создают тысячи новых возможностей и перспектив. С другой стороны, они порождают множество рисков и угроз – фейки, дезинформация, атаки на критическую инфраструктуру. Имея способность к самообучению, этот инструмент (прим. – искусственный интеллект) ***может погубить человечество, если его выпустить из-под контроля… »,*** – вот на что обратил внимание Президент Республики Беларусь А.Г.Лукашенко 28 ноября 2024 г., выступая в Астане на саммите ОДКБ.

Коротко подытожим: какие бы эффективные меры защиты ни принимались на государственном уровне *(а они принимаются, просто об этом нельзя, по понятным причинам, говорить вслух)*, все-таки ключевую роль в обеспечении безопасности играет осведомленность и внимательность каждого из нас. Мы сами должны быть осторожными и одновременно готовыми адаптироваться к новым угрозам, чтобы быть в состоянии создавать как можно более безопасную среду для всех граждан.

Спасибо.

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

КИБЕРБЕЗОПАСНОСТЬ И ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ

(для работников предприятий реального сектора экономики)

Основным драйвером современности являются информационные технологии, радикальным образом влияющие на все сферы деятельности и наш образ жизни в целом. Как отметил на торжественной церемонии открытия в Минске Центра технического творчества детей и молодежи Президент Республики Беларусь Александр Лукашенко: ***«Если еще каких-то 20 лет назад компьютер и интернет были не в каждой белорусской семье, то в наши дни они, наряду с мобильными телефонами, стали обыденностью. В производство и быт постоянно приходят технологии, которые недавно казались абсолютной фантастикой. Умные города, роботы, беспилотники, искусственный интеллект – уже не просто споры ученых о близком будущем, но и наша реальность»***.

В наше время цифровизация проникла во все отрасли производства, без нее немыслимо функционирование сложных технических устройств, управление финансами, транспортными потоками, технологическими процессами, энергораспределением и прочее. Лавинообразно нарастающие потоки информации в структурах государственного и корпоративного управления уже невозможно обрабатывать без применения автоматических систем. На уровне повседневной жизни каждого из нас – подача воды, электроэнергии, тепла в наши дома, наполняемость полок в торговых сетях, работа светофоров и другое – регулируются цифровыми системами. Сложные бытовые приборы, значительно повысившие комфортность нашей жизни, работают с использованием искусственного интеллекта, пусть и в самом упрощенном его воплощении.

Вездесущий Интернет, сопровождающие нас повсюду мобильные телефоны и электронные платежные средства существенно изменили наши возможности по доступу к информации, способы межличностных контактов, формы социализации, перевернули представления о личном пространстве и размыли его границы.

Однако **использование цифровых технологий** во всех сферах и на всех уровнях **несет не только прогресс и удобства, но и создает предпосылки для различного рода противоправной деятельности**. Сегодня ни одна страна, ни один человек не застрахованы от того,

чтобы стать объектом кибератаки. Противоправная деятельность хакеров является одной из самых значительных и постоянно растущих угроз для глобальной безопасности в XXI веке. Взлом компьютерных систем способен парализовать целые отрасли промышленности, остановить работу банков, закрыть аэропорты, вывести из строя системы жизнеобеспечения и т.д.

По этому вопросу обозначил свою позицию Президент Республики Беларусь А.Г.Лукашенко: ***«Во всем мире наблюдается рост кибератак. Причем атакуют прежде всего стратегические объекты, государственные органы, предприятия, банковскую систему... Это один из элементов гибридной войны, очень опасный элемент. Цель – нанести максимальный ущерб экономике и дестабилизировать в итоге общество»***.

В Беларуси адекватной реакцией на нарастание киберугроз стало создание Национального центра обеспечения кибербезопасности. Многие крупные компании сформировали и аттестовали собственные центры информационной безопасности. На текущий момент в республике аттестовано 22 центра противодействия кибератакам.

Справочно:

Так, на базе Беларусбанка создан один из крупнейших в стране центров кибербезопасности, функционарующий круглосуточно. За 9 месяцев 2025 года им предотвращено порядка 100 млн атак на информационный контур банка.

С целью обеспечения технологического суверенитета совместно с Нацбанком создается национальное программное обеспечение для банков.

Для рядовых пользователей чувствительной проблемой является **нарастание масштабов вторжения в их жизнь различного рода мошенников**, сочетающих психологические приемы с использованием цифровых инструментов для вхождения в контакт с целью выманивания денег. Фактически жертва подвергается тому же воздействию, что и Буратино на «Поле Чудес» для добровольной передачи своих денег мошенникам, но уже без прямого физического контакта, а через посредство различных так любимых нами гаджетов, из которых как минимум один всегда находится с нами.

Кто воюет против нас по другую сторону интернет-фронта? Нет, не воюет – это слишком, правильнее поставить вопрос по-другому – кто играет против нас краплеными картами? Сравнение с карточной игрой будет наиболее верным, и там, и в интернет-мошенничестве психологические моменты – главное, блеф – основа всего.

Если нарисовать обобщенный портрет кибермошенника, то окажется, что это не жуткий урод с окровавленным кинжалом в руке и

бомбой в кармане. Напротив, хорошо нам известный, довольно милый «коллективный Остап Бендер», что не отменяет главного – он мошенник и авантюрист, «великий комбинатор», «идейный борец за денежные знаки», знающий, как и литературный персонаж, сотни сравнительно честных способов отъема *(увода)* денег *(наших денег)*. Это полная характеристика и здесь нет ни одного лишнего слова. Почему методы названы сравнительно честными? Потому, что мы отдаем деньги сами, своего рода добровольно.

Оставим специалистам из правоохранительных органов термины, которыми обозначают **различные виды кибермошенничества**, такие, например, как вишинг, уэйлинг, доксинг, смишинг, сексторшен, фишинг и другие. Достаточно будет сказать, что «фишинг» переводится как рыбалка, нас с вами пытаются «подсечь» с использованием различных видов фейковых наживок, на «блесну» разводки.

Еще раз повторим, что мошенники хорошие психологи и паразитируют на основных особенностях человеческой натуры.

Довольно часто мошенники, обращаясь к нам через интернет ресурсы, телефонный звонок, стараются «включить» самое святое – любовь к близким и приверженность дружеским чувствам. Вам предлагают отдать все за спасение друзей и близких, попавших в беду. В большинстве случаев срабатывает, так как именно это качество и делает нас людьми. *Но эксплуатация самых светлых чувств большего всего и оскорбляет нас нормальных людей – именно в этом случае хочется наказания для проходимцев по максимуму. Ведь, что они делают по большому счету, не просто отнимают наши деньги, они запускают инфляцию наиболее человечных проявлений, «учат» нас тому, что быть человеком не выгодно, сводя все именно к материальной, денежной выгоде.* Мы легче всего покупаемся на такие «разводки», но от них и легче всего себя обезопасить. **Важно не спешить с принятием решений и проверять доводимую до вас мошенниками информацию.** Поэтому именно в этих случаях злоумышленники при контакте с вами пытаются создавать ситуации искусственного цейтнота. Оставайтесь людьми, но будьте и благоразумны! Одно другому не мешает и не противоречит.

Другой прием паразитирует на нашем доверии к правоохранительным, судебным органам и банковским структурам. Конкретных схем отъема денег на этой основе десятки, от предложения отблагодарить за содействие в решении сложных проблем *(попросту говоря провокации на взятку)*, до консультации по спасению ваших сбережений на надежных счетах, рекомендаций «задекларировать» хранимые дома сбережения или настоятельной просьбе поучаствовать в

операции по разоблачению преступников, что часто сопровождается необходимостью оформления кредита *(кредит уходит на счета мошенников, а его погашение вешается на жертву)*. В этом случае ключевым моментом в действиях мошенников являются не столько жесткие временные рамки, сколько требование соблюдения секретности. Для нас с вами это звоночек. Все построение рассыпается, если встряхнуться от гипноза секретности и напрямую обратиться в правоохранительные органы. Ведь мы им доверяем, так давайте будем доверять до конца.

Мошенниками часто эксплуатируется такое естественное человеческое свойство как чувство доверия к кругу общения. Современный человек все чаще и все больше создает такой круг общения в соцсетях. Одно дело, когда такие контакты дублируют живое общение в кругу близких, друзей, знакомых, коллег по работе, по увлечениям. Другое дело, когда основу круга общения составляют виртуальные «друзья», которых мы никогда в глаза не видели в реальном мире. Сооруженную на этой почве доверительность мошенник может использовать в зависимости от обстоятельств, например, прося о помощи для себя или наших друзей и близких, либо шантажируя полученной от нас информацией не для посторонних, например, фото и видеоматериалами интимного характера. В описанных обстоятельствах хочется посоветовать стараться окружать себя реальными, а не виртуальными друзьями и знакомыми и не доверяться в соцсетях больше, чем в живом общении.

Мошенники часто спекулируют на нашем желании потратить свои деньги повыгодней. Жертва привлекается возможностью покупок на электронных площадках, в том числе фейковых, по значительным скидкам, выигрыша в лотерею, инвестиций в сверхприбыльные финансовые проекты и другое. Во всех этих случаях следует помнить, что бесплатный сыр бывает только в мышеловке. И всегда остается актуальным пожелание *«не гонялся бы ты, поп, за дешевизной»*.

Преступники следят за техническим прогрессом, постоянно изобретают новые способы мошенничества и выявляют другие направления для атак, используют комбинированные методы, многоходовки.

Справочно:

Вот лишь один из примеров многоходовой схемы с участием нескольких «игроков». Жертва просто отвечает на звонок и какое-то время общается с одним злоумышленником. Понимая, что это мошенник, кладет трубку. Следом звонит второй мошенник. Он представляется уже сотрудником правоохранительных органов и сообщает жертве, что якобы та совершила преступление, вступив в коммуникацию с преступником, возможно, даже участвовала в

финансировании какой-то экстремистской деятельности… Далее жертва переходит по ссылкам или сообщает свои данные, итог всегда один и тот же – деньги похищены.

Государство не остается равнодушным к проблеме и реагирует соответствующим образом. Так, с марта 2024 г. в Республике Беларусь функционирует в полном объеме **механизм противодействия несанкционированным платежным операциям**, который реализован посредством:

информационного взаимодействия между правоохранительными органами и поставщиками платежных услуг по обмену информацией об инцидентах с использованием автоматизированной системы обработки инцидентов Национального банка (далее – АСОИ);

внедрения в белорусских банках антифрод-систем, позволяющих в режиме реального времени выявлять несанкционированные платежные операции;

права банкам приостанавливать до 2-х рабочих дней переводы, в отношении которых имеются подозрения на несанкционированные платежные операции;

права правоохранительным органам приостанавливать на срок до 10 суток расходные операции по банковскому счету, счету по учету вкладов (депозитов), электронному кошельку клиента банка.

С марта 2024 г. по октябрь 2025 г. посредством АСОИ получено и проанализировано более 33 тыс. сообщений об инцидентах. Общая сумма ущерба по ним составила свыше 90 млн руб.

За указанный период банками приостановлено на 2 рабочих дня более 9 тыс. переводов *(в которых участвовало почти 8 тыс. счетов белорусских банков)* на общую сумму 9 млн руб., тем самым предотвратив хищение денежных средств у граждан Республики Беларусь.

Сейчас в Беларуси прорабатываются вопросы изменения и совершенствования порядка выдачи кредитов физлицам, чтобы исключить вероятность оформления кредитов третьими лицами. Обсуждается также принятие дополнительных мер для пресечения банками потенциально мошеннических операций, в частности при переводе денежных средств за рубеж.

Однако большая часть инцидентов связана с использованием методов воздействия социальной инженерии и психологического манипулирования. Здесь граждане обращаются в компетентные органы и службы зачастую с большим опозданием, и деньги вернуть уже проблематично.

Одной из мер профилактики на личном уровне является **серьезное отношение к своим персональным данным**, что касается и наших

платежных инструментов. Значительная часть мошеннических схем без персональных данных не работает. Не раздавайте их направо и налево по звонку, например, сотрудникам коммунальных служб, операторам связи, банковским служащим, при регистрации на сомнительных интернет-сервисах, торговых площадках, участии в различного рода социологических опросах и маркетинговых исследованиях.

Справочно:

Самыми «безобидными» последствиями при попадании ваших персональных данных и других данных не для общего пользования в руки мошенников может быть блокировка ваших телефонов или платежных карточек с требованием вознаграждения за разблокировку.

Нет никакой необходимости «выворачиваться наизнанку» о всех особенностях своей персоны в соцсетях. Из цифрового следа легко создаются профили. Такой «портрет» может работать не только во благо, но и на злоумышленников, становясь инструментом давления, манипуляций, шантажа или обмана, быть средством политической агитации и формирования общественного мнения. С развитием цифровых технологий и переноса все большего числа процессов в онлайн-среду ценность персональных данных, равно как и риски их неправомерного использования, стремительно возрастают.

Справочно:

За 8 месяцев 2025 года по требованию Национального центра защиты персональных данных удалено более 3,3 млн записей, а также более 2,7 млн видео- и аудиозаписей, содержащих незаконно обрабатываемую конфиденциальную информацию.

Гарантировать полную защищенность от мошенников киберэпохи сложно, но **при соблюдении ряда простых правил можно рассчитывать на достаточный уровень личной безопасности**:

- ни в коем случае не разглашайте персональные данные, не верьте на слово всем звонившим;
- никогда не устанавливайте приложения по просьбе незнакомцев – даже если ссылка ведет в официальный магазин;
- не прикладывайте карту к смартфону без крайней необходимости *(исключение – проверенные банковские приложения)*;
- тщательно проверяйте ресурсы и проекты, куда Вам предлагают вложить и «значительно приумножить» свой капитал;
- для инвестиций пользуйтесь услугами официально зарегистрированных на территории Республики Беларусь финансовых организаций;

- не переходите по сомнительным ссылкам на неизвестные ресурсы и не оставляйте там свои персональные и/или контактные данные;
- никогда не переводите деньги на неизвестные счета, а также не передавайте через посторонних лиц;
- обходите стороной предложения в социальных сетях о продаже товаров по «самым привлекательным ценам», не верьте броским заявлениям, что это якобы «секретная распродажа» или «эксклюзивные поставки прямиком от производителя», не вводите конфиденциальные данные на подозрительных сайтах;
- используйте отдельную банковскую карту для осуществления покупок в сети Интернет, на которой не хранятся большие суммы, и на которую не поступает регулярный доход в виде заработной платы.

Все рекомендации для взрослых актуальны **для детей и подростков**, но с существенными оговорками. Центральный момент – «жизнь» младших членов семьи в Интернете не может протекать без контроля со стороны взрослых. В любом случае ребенка желательно приучить **соблюдать правило «СТОП-СПРОСИ-РАССКАЖИ»**. «СТОП» – если что-то вызывает дискомфорт, поступило странное предложение или просьба сохранить что-то в секрете от родителей – необходимо немедленно прекратить такое общение. «СПРОСИ» – если что-то непонятно – спроси у родителей или другого взрослого, которому доверяешь. «РАССКАЖИ» – обязательно расскажи родителям, если кто-то в сети угрожает, шантажирует, выпрашивает фото или просит о встрече.

Следует помнить, что ребенок в результате воздействия кибермошенников может не только вынести из дому деньги, но быть втянут в преступные сообщества, суицидальные проекты, стать объектом травли с непредсказуемыми последствиями. В ряде стран ситуация явно вышла из-под контроля, и там пошли на прямые запреты доступа детей и подростков в соцсети.

Справочно:

Закон, запрещающий детям младше 16 лет пользоваться социальными сетями, правительство Австралии приняло еще в прошлом году. «Это обеспечит более надежную защиту для молодых австралийцев на критических этапах их развития», – сказано в сопутствующем заявлении премьер-министра страны. Ответственность за несоблюдение ограничений возложена на сами соцсети, от которых требуется «принять разумные меры», чтобы пользователи младше 16 лет не могли создавать аккаунты. За нарушение закона цифровые платформы обещали штрафовать на суммы до 49,5 млн австралийских долларов (32,3 млн долларов США). Кстати, такой

возрастной ценз практикуется в нескольких штатах Америки. К примеру, во Флориде пользователи до 14 лет не могут заходить на такие платформы, как Instagram и Facebook, а в штате Юта для их использования детям до 18 лет требуется разрешение родителей.

Европарламент предложил ограничить доступ к любым соцсетям в Евросоюзе детям в возрасте до 13 лет, с 13 до 16 лет евродепутаты предлагают разрешать подросткам пользоваться соцсетями только с разрешения родителей.

(Даже невозможно вообразить какие страшные обвинения в нарушении всех мыслимых и немыслимых прав и свобод посыпались бы в адрес, например, Беларуси или Российской Федерации при принятии ими подобных законов.)

Однако больше толку будет не от запретов или запугивания ребенка при разговоре с ним о безопасном поведении в сети Интернет, а в том случае, если научить его цифровой грамотности и критическому мышлению. Он должен понимать, что **Интернет – это отражение реального мира: в нем есть и хорошие, и плохие люди, а правила безопасности здесь так же важны, как и на улице**. Роль родителей и взрослых – быть проводником и надежной опорой подрастающего поколения в этом цифровом мире.

****

Мы живем в эпоху, когда современные цифровые технологии играют возрастающую роль во всех сферах жизнедеятельности, делая труд в разы производительней, коммуникации моментальными и безграничными, а быт беспрецедентно комфортным. Однако есть и обратная сторона, которую необходимо учитывать. ***«С одной стороны, современные технологии создают тысячи новых возможностей и перспектив. С другой стороны, они порождают множество рисков и угроз – фейки, дезинформация, атаки на критическую инфраструктуру»,*** – подчеркнул Президент Республики Беларусь А.Г.Лукашенко 28 ноября 2024 г., выступая в Астане на саммите ОДКБ.

Какие бы эффективные меры защиты не принимались на государственном уровне, все-таки ключевую роль в обеспечении безопасности играет осведомленность и внимательность каждого из нас. И если мы будем осторожны и готовы адаптироваться к новым угрозам, то сможем создать более безопасную среду для всех.

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

КИБЕРБЕЗОПАСНОСТЬ И ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ

(для молодежной аудитории)

Актуальность данной темы бесспорна. А молодежь может, наверно, возразит: *«Что нового вы нам расскажете, чего мы не знаем?»*. И по-своему будет права. Ведь в жизни современной молодежи все большую роль играют новые технологии. И это естественно. По сути, **информационно-коммуникационные технологии уже стали не просто частью жизни, но создали для вас новую действительность**. Вы практически живете в новой цифровой реальности, где можно моментально удовлетворить любую потребность: погуглить, сформировать свою ленту по интересам, улучшить внешность, собрать тусовку и стать популярным и т.д.

Безусловно, представители поколений Z *(зумеры – молодежь, родившаяся примерно с 1997 по 2012 год. При этом верхние и нижние границы дат могут немного варьироваться в разных классификациях)* и «альфа» *(родившиеся с начала 2010-х годов до середины 2020-х годов)* ассоциируются с людьми, идущими в ногу с технологическим прогрессом. И чувствуют себя «как рыба в воде», пользуясь современными информационно-коммуникационными технологиями.

Справочно:

По данным британского агентства Ofcom, каждый пятый «альфа»-ребенок в возрасте 3–4 лет имеет планшет, а в возрасте 5–7 лет – почти каждый второй, при этом ***минимальные навыки использования планшета дети приобретают уже к двум годам***.

Такая тенденция не может не настораживать. Особенно, учитывая тот факт, что «альфа»-дети обычно растут в семьях без братьев и сестер, и зачастую вместо общения они, как правило, посвящены сами себе. А если брать во внимание, что большинство современных родителей проводит с детьми мало времени в силу занятости, то для нового поколения, растущего с младенчества с планшетом в руках, цифровые технологии фактически стали способом коммуникации с миром и выражения себя.

Возможности для этого предоставляет и **развитие Интернета**.

По состоянию на 1 января 2025 г. в Беларуси количество абонентов и пользователей беспроводного широкополосного доступа к

сети Интернет на 100 жителей увеличилось с 92,6 до 106,93 *(при задании 95,5)*.

Общее количество абонентов стационарного широкополосного доступа в сеть Интернет на начало текущего года составляет порядка 3 млн 300 тыс. абонентов.

Более того, в Республике Беларусь принимаются меры, направленные на **сокращение «цифрового неравенства» между городским и сельским населением**. Так, завершается строительство волоконно-оптических линий связи к населенным пунктам с числом домохозяйств от 50 до 100. В частности, уже обеспечены 1 449 таких населенных пунктов, что составляет 88,8% от их общего количества.

Волоконно-оптические линии связи уже подведены ко всем населенным пунктам с числом домохозяйств 100 и более, присутствуют во всех многоквартирных жилых домах.

К слову, третий год подряд Республика Беларусь улучшает свои позиции по **Индексу развития информационно-коммуникационных технологий** (далее – Индекс ИКТ). Итоговый результат за 2025 составил 90,7 баллов против 88,5 баллов в минувшем году. При этом по итоговой оценке Индекса ИКТ Беларусь опередила такие страны как Бельгия, Канада, Германия, Италия, Казахстан, Турция, Узбекистан.

Таким образом, можно смело заявлять, что цифровые технологии уверенно встраиваются в повседневную жизнь белорусов. Активно развивается система электронного правительства, предоставляющая гражданам доступ к государственным услугам онлайн. Применяются роботизация и искусственный интеллект для диагностики и лечения пациентов. Внедряются электронные образовательные ресурсы, дистанционное обучение, онлайн-платформы в сфере образования. Уже привычными становятся цифровые и инженерные решения в городской и коммунальной инфраструктуре.

Вполне очевидно, что цифровизация сегодня – не тренд, а необходимость. Цифровые технологии *(большие данные, искусственный интеллект, блокчейн и пр.)* позволяют оптимизировать производственные процессы, повысить эффективность государственного управления, создать благоприятную среду для инновационного предпринимательства и др. Но есть и обратная сторона.

Так ли безопасно внедрение цифровых технологий во все сферы жизни? Какие опасности оно таит?

В первую очередь, **технологии могут ставить под угрозу неприкосновенность частной жизни**. Ведь практически любое взаимодействие с другими людьми или организациями связано с передачей личной информации: будь то оплата товаров картой,

использование интернет-сервисов для получения услуг, переписка по электронной почте, звонки по мобильной связи или подача заявок в коммунальные службы – это все примеры, где задействуются данные о человеке.

С развитием цифровых технологий и переноса все большего числа процессов в онлайн-среду **ценность персональных данных –** равно как и риски их неправомерного использования **– стремительно возрастают**.

Нарушения в сфере персональных данных мы наблюдаем каждый день: звонки с предложением поучаствовать в социологических опросах, маркетинговые исследования в обмен на скидку в магазине, спам на имейл и др. Персональные данные используются и более скрытно, чтобы влиять на нас через таргетированную рекламу *(от англ. target означает цель; реклама, которая направлена на определенный сегмент аудитории)* и управлять общественным мнением. Из цифрового следа легко создаются профили: поиски, лайки, посты… Даже открытый Instagram способен рассказать о человеке больше, чем он думает – от круга друзей до адреса. А ведь мало кто из молодежи об этом задумывается.

Такой «портрет» может работать не только во благо, но и на злоумышленников, становясь инструментом давления, манипуляций, шантажа или обмана, быть средством политической агитации и формирования общественного мнения.

При этом в личной жизни каждый из нас также использует персональные данные других граждан. Однако важно не нарушать их личное пространство. Ведь тема сохранения личных сведений – сверхчувствительная и важная. **Никто не имеет права распоряжаться чужими персональными данными без согласия человека.** Например, если человек ведет личную страницу в социальной сети и выкладывает фотографии иных граждан, для этого необходимо их согласие.

Не стоит считать, что представители молодежи не могут быть **жертвой киберпреступлений**. Это слишком самоуверенно.

Если рассматривать возрастные группы жертв кибермошенников, то **молодежь до 30 лет уязвима от мошеннических дистанционных сделок с недвижимостью** *(56,3%),* **псевдо-инвестиций в «биржи» и «розыгрышей или акций»** *(65,4%).*

Безработные и неучащиеся чаще попадаются в инвестиционные ловушки *(46,2%)*, что может указывать на поиск ими источников дохода или увлечение азартными схемами.

По статистике женщины *(65%)*чаще всего становятся жертвами мошенников. Обычно они страдают от телефонных мошенников,

которые выманивают деньги путем психологических манипуляций *(77,9%)*, а также от мошенничеств в сфере купли-продажи товаров и оказания услуг *(65,6%)*, в сфере благотворительности *(100%)*. Мужчины составили абсолютное большинство потерпевших от мошенничества с использованием сайтов знакомств *(84,8%)*.

Мошенники могут использовать различные схемы. Для молодежной среды характерны следующие.

Инвестиционные платформы

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

Справочно:

Молодой мужчина заинтересовался возможностью вложить свои деньги в инвестиционный проект. После того как он выполнил указания куратора и перевел деньги на цифровой кошелек, сумма его денег стала якобы увеличиваться, в своем аккаунте на платформе молодой человек видел прибыль, однако, как только он попытался вывести деньги, его сразу же заблокировали. Он дважды находил в интернете фирмы по оказанию помощи по выводу денег, однако ни одна «фирма» ему не оказала должных услуг, после чего мужчина обратился в милицию. Всего он потерял более 20 тыс. рублей.

Вовлечение в киберпреступность

Для получения за границей похищенных денег, а также для запутывания «цифровых следов» мошенникам необходимо перевести их через промежуточные счета, открытые в белорусских банках на подставных лиц *(«дропов»)*. Часто промежуточных счетов бывает более десятка. Имеются факты, когда полученные незаконным путем деньги проходили через 72 промежуточных банковских счета, доступ к которым мошенники покупали у их владельцев.

В нашей стране открыть банковский счет может дееспособный гражданин с 14 лет, то есть даже несовершеннолетние могут открыть банковские счета. Этим в своих целях пользуются преступники.

Находясь за границей, злоумышленники подбирают лиц, которые соглашаются открыть банковский счет на свое имя и продать за небольшую сумму реквизиты доступа к нему – это логины и пароли для входа в личный кабинет в интернет-банкинге, а также предоставить разовый смс-код или карту кодов.

Напрямую мошенники в интернете не могут размещать объявления о поиске таких лиц, поэтому свой интерес они прикрывают предложением различного другого заработка, не вызывающего подозрения. Например, в Telegram рассылают объявления о поиске курьеров в любом городе со стабильной оплатой труда, грузчиков, людей на вакансию «тайный покупатель», заманивают обещанием высокой и быстрой оплаты.

Чаще всего отзываются на такие вакансии лица с нестабильным или небольшим доходом, в большинстве – молодежь. Сначала инициатор объявления разочаровывает заинтересовавшегося подработкой, сообщает, что данная вакансия уже закрыта, и тут же предлагает иной вид заработка, например, оформить банковский счет и передать за вознаграждение данные для доступа к нему.

Кроме похищенных киберпреступниками денег по промежуточным счетам также могут проводиться деньги, полученные от незаконного оборота наркотиков. Важно понимать, что **ответственность за происхождение прошедших по банковским счетам денег несут владельцы таких счетов**.

В частности, статьей 222 Уголовного кодекса предусмотрена ответственность вплоть до 10 лет лишения свободы за изготовление в целях сбыта либо сбыт банковских платежных карт или иных платежных инструментов, таких как банковские счета или электронные кошельки, а также распространение данных доступа к ним.

Имеются факты, когда в преступную деятельность были вовлечены несовершеннолетние.

Справочно:

16 подростков из двух учреждений среднего специального образования небольшого города, связавшись с заказчиком из Интернета, оформляли на свое имя банковские карты и за вознаграждение от 15 до 50 рублей передавали их для использования неустановленным лицам. С использованием этих банковских карт киберпреступники переводили похищенные деньги. В отношении 8 подростков возбуждены уголовные дела, в отношении остальных – проводится проверка и решается вопрос о возбуждении уголовных дел.

<u>Операции с криптовалютой</u>

Имеются примеры **вовлечения подростков в преступную цепочку** другим способом.

Справочно:

14-летний ученик школы областного города попросил на некоторое время в пользование у своего 15-летнего одноклассника его банковскую платежную карту. Парень зарегистрировал аккаунт на криптовалютной бирже. Неизвестные лица связались с ним и предложили заработать. Молодой человек предоставил реквизиты банковской карты одноклассника, на которую он получил 10 000 рублей, а после чего для заказчиков купил криптовалюту на всю сумму. В ходе проверки установлено, что полученные деньги были похищены у пенсионера.

Таким образом, школьник оказал услуги по покупке-продаже криптовалюты третьим лицам, что влечет ответственность за незаконную предпринимательскую деятельность *(ч.3 ст. 13.3 КоАП Республики Беларусь)*. Совершение сделок на криптовалютной бирже подростками – не единичный случай. Через криптокошелек другого подростка прошло более 450 тыс. рублей.

За совершение сделок с криптовалютой в пользу третьих лиц грозит крупный штраф и обращение в доход государства до 100% суммы дохода, полученного в результате такой деятельности.

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).

Так, Указом 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.

Следует отметить, что Указ 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 – в частности, обменивать Bitcoin на Ethereum, торги криптовалютой)*, не связанных с непосредственным вводом или выводом денежных средств.

<u>Фейковые магазины в соцсетях</u>

Как было отмечено выше, Беларусь развивающаяся страна и граждане активнее пользуются цифровыми технологиями.

Ежедневно в милицию обращаются те, кто сами перевели **предоплату за товар**, который нашли в объявлениях в социальных сетях и на торговых площадках, и не получили его. Мошенники намеренно создают аккаунты от имени магазинов, в которых размещают объявления несуществующих товаров с заниженными ценами *(обувь, одежда, мобильные телефоны, постельное белье, автомобильные шины, новогодние ели, садовые кресла-качалки-коконы и другие товары)*. Потенциальный покупатель связывается с администратором «магазина» и обещает доставить товар после частичной или полной оплаты. Перевод денег предлагают произвести на банковскую карту или на счет через ЕРИП, что притупляет бдительность. После получения денежных средств, интернет-магазином товар не высылает, а покупателя блокирует.

Вымогательство на интимной почве *(«сексторшен»)*

Такие случаи не единичны в Беларуси. Мошенник через соцсети знакомится с жертвой, втирается в доверие, склоняет к общению в видеочате интимного характера или к отправке откровенных фото, записывает видео или делает скриншоты, а затем шантажирует, требуя деньги, угрожая разослать материалы всем друзьям и родственникам жертвы.

Фишинг

Это наиболее распространенная формами обмана с целью получения личных данных владельцев счетов. Вам приходит SMS-сообщение или электронное письмо с сообщением о «блокировке карты», «проблеме с налогом», «выигрыше в лотерее» и др., содержащее ссылку на фишинговый интернет-ресурс *(сайт – клон)*, который выглядит как официальный интернет-ресурс банка, налоговой или другого государственного органа, где требуется ввести логин, пароль, данные платежных средств, после ввода которых совершается хищение.

Справочно:

Молодая мама, находящаяся в декретном отпуске, перевела на предоставленный счет через ЕРИП 2 тыс. белорусских рублей за телефон, но не получила его. Тогда мошенники предложили ей получить свои деньги обратно на банковскую карту. Они направили в мессенджере ссылку, перейдя по которой, девушка ввела в ячейки номер карты и секретный код с оборотной стороны, предназначенный только для расходных операций. Завладев этими сведениями, мошенники обманули ее еще раз, списав с карты все деньги.

На самом деле, форм кибермошенничества существует много. Более того, чем лучше становятся инфраструктура, информационно-коммуникационные технологии, тем более

профессиональный и уровень киберпреступлений. Преступники следят за техническим прогрессом и постоянно изобретают новые способы мошенничества и выявляют другие направления для атак.

Например, **использование искусственного интеллекта** позволяет создать возможности для фишинга нового поколения, разрабатывая безупречные с грамматической и стилистической точки зрения фишинговые рассылки, адаптированные под конкретную жертву *(целевой фишинг),* когда пропадает главный маркер подделки – ошибки в тексте.

Борьба с этим требует не только более совершенных технологий защиты *(на базе того же искусственного интеллекта)*, но и фундаментального **повышения цифровой грамотности**.

Однако, несмотря на то, что молодежь зачастую считают «цифровыми аборигенами», многие из вас не обладают необходимыми для работы цифровыми навыками. Поэтому важно запомнить несколько простых правил:

никогда и никому не сообщайте ПИН-код, CW-код карты, пароли из SMS, коды доступа к интернет-банкингу;

не переходите по сомнительным ссылкам из SMS-сообщений и электронной почты;

не устанавливайте на свой смартфон или компьютер программы по просьбе незнакомцев;

проверяйте информацию, если вам звонят из «банка» или «милиции», положите трубку и перезвоните по официальному номеру организации;

не поддавайтесь панике и чувству спешки, мошенники всегда создают искусственный дефицит времени, чтобы вы не успели подумать;

включайте двухфакторную аутентификацию *(дополнительный уровень безопасности аккаунта)* везде, где это возможно.

****

Банковские платежные карты, мобильные телефоны, компьютеры, программы и сервисы – все это делает нашу жизнь более комфортной, но незащищенной от мошенников. День за днем появляются новые разновидности мошенничества в этой сфере, а значит каждый из вас должен владеть определенными навыками и знаниями, чтобы не дать себя обмануть.

Поэтому цифровая грамотность сегодня становится новой социальной нормой, а навыки безопасности в сети – такими же необходимыми, как и базовые образовательные умения.

Будьте бдительны!
Не дайте себя обмануть!