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.

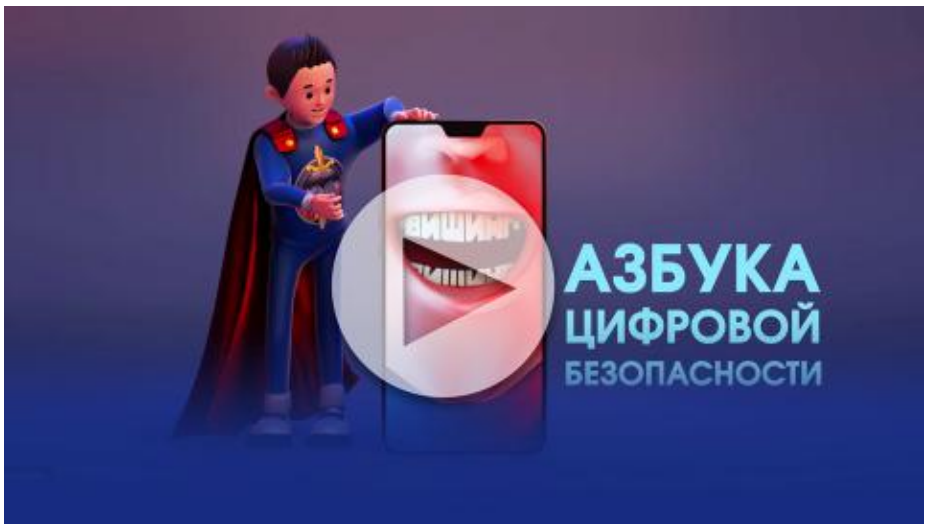
Слайд 4.

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.

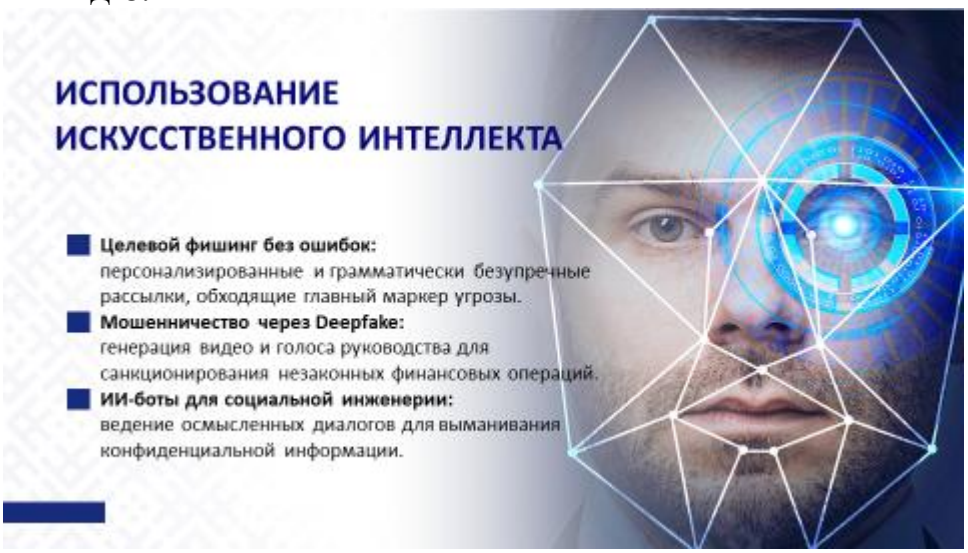
При видеозвонке следует обращать внимание на такие детали, как нечеткое или смазанное изображение лица говорящего, отсутствие или неестественная мимика лица.

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 безопасности, 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.

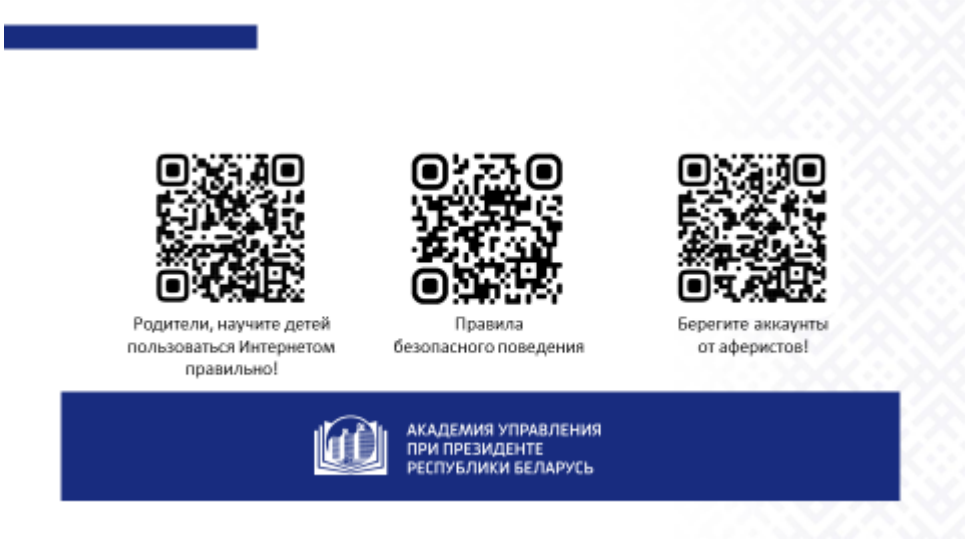
Важно научить детей цифровой грамотности и критическому мышлению. Им нужно понимать, что **Интернет – это отражение реального мира: в нем есть и хорошие, и плохие люди, и правила**

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.