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.