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!