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.