Кибербезопасность цифровой трансформации

Автор: Алексей Лукацкий

Table of Contents

Влияние кибербезопасности на цифровую трансформацию

Цифровая трансформация в отличие от обычной автоматизации отличается значительно бОльшим «оцифровыванием» существующих процессов и, что, пожалуй, самое главное, изменением культуры организации, которая решила достичь новых показателей деятельности за счет внедрения новых цифровых технологий. Но именно изменение культуры предприятия, решившего начать свою цифровую трансформацию, в контексте обеспечения кибербезопасности (в данном случае мы не будем делать разницу между терминами «кибербезопасность» и «информационная безопасность», рискую погрузиться в терминологические дебри, которые в контексте данного раздела не так уж и важны)мало чем отличается от того, о чем уже не первый год говорят все лучшие практики в области формирования культуры информационной безопасности (ИБ). Мы привыкли рассматривать деятельность служб ИБ как запретительную, которая зачастую только мешает работать и достигать поставленных целей. Однако формирование культуры ИБ направлено на получение сотрудниками определенных навыков и умений, которые формируют такое поведение в области работы с информацией и информационными системами, которое не вызывает отторжения у персонала и даже не требует от них особых усилий.

Ровно этим же приходится заниматься и в рамках цифровой трансформации – изменением поведения людей, которые на уровне своих навыков, а не слов и заявлений, безопасным образом работают с различными прорывными технологиями. Именно прорывные технологии несут с собой новые не только возможности, но и риски, осознавать которые должна любая организация и любой специалист по цифровой трансформации, который решил за счет них вырваться в конкурентной борьбе или сделать жизнь граждан (если мы говорим о государственных предприятиях) лучше. Именно об этих рисках и способах управления ими мы и поговорим в этой главе. Но так как прорывных технологий, на которых строится цифровая трансформация, достаточно много, то мы сфокусируемся на четырех самых основных из них:

- Блокчейн и смарт-контракты
- Квантовые вычисления
- Машинное обучение
- Биометрия.

Именно для них мы попробуем поставить себя на место хакера и посмотреть, как можно нарушить работу этих прорывных технологиях, и как можно противостоять этим нарушениям.

Таблица 1. Разница между инноваторами и хакерами

	Инноватор	**Хакер / специалист по кибербезопасности**
Основной фокус	Что произойдет в случае нормальных входных данных?	Что произойдет в случае аномальных входных данных?
Отказ в редких условиях и сочетаниях	Что-то, что я смогу игнорировать или чем я могу **пренебречь**	Что-то, что я смогу использовать для **нарушения**

Блокчейн

Ваша компания решила внедрить у себя блокчейн. Для контроля цепочки поставок, для ведения базы данных мошеннических операций, для борьбы с контрафактом, для контроля активов, для ведения юридически значимых реестров/кадастров/баз данных, для проведения платежей, для системы идентификации… Насколько ваша текущая стратегия ИБ учитывает эту новую, широко разрекламированную технологию, сулящую множество преимуществ?

Рисунок 1. Пример проекта по управлению цепочками поставок на блокчейне

Вы, безусловно, слышали, что блокчейн – это распределенная структура, в которой узлы взаимодействуют друг с другом по принципам пиринговой сети (P2P); что каждый узел имеет копию всего распределенного реестра (всех транзакций); и что чем больше узлов, тем блокчейн устойчивее и надежнее. При этом с точки зрения безопасности считается, что блокчейн изначально защищен на алгоритмическом уровне и почти не подвержен атакам.

Однако на самом деле все обстоит немного иначе. Бизнес почти никогда не применяет открытый публичный блокчейн, знакомый нам по множеству криптовалют. В бизнес-проектах применяется закрытый блокчейн – публичный (или консорциум) или частный. В последних двух случаях, многие свойства блокчейна становятся не такими очевидными. Во-первых, у вас ограниченное число участников. А во-вторых, у вас может появиться центральный орган контроля (в частном закрытом блокчейне). Например, проведенное в Москве и в Нижнем Новгороде дистанционное электронное голосование по поправкам к Конституции, было построено как раз на базе частного закрытого блокчейна, все бразды управления которым были сосредоточены в руках всего одного ведомства. С одной стороны, у нас снижается вероятность реализации некоторых угроз, например, создание альтернативной, измененной, более длинной цепочки, или появление в реестре

неавторизованных участников. С другой – у нас остаются риски, недооценка которых может свести на нет все преимущества блокчейна.

Риски ИБ для блокчейна

В условиях применения закрытого блокчейна ваша стратегия цифровой трансформации должна быть готова к следующим рискам и вытекающим из них вопросам, требующим ответа:

1. Как мы защищаем конечные узлы, участвующие в блокчейне? Программа-вымогатель, зашифровавшая все узлы распределенного реестра, приведет к тому, что блокчейн перестанет быть доступен, хотя информация в нем будет по-прежнему защищена. В этой технологии безопасность сдвигается в сторону персональных компьютеров и серверов, участвующих в формировании блоков, и поэтому защита операционных систем, сетевой инфраструктуры, приложений, управления ключами становятся как никогда важными. Одним антивирусом тут точно не обойтись и нужно внедрять более эффективные технологии внутренней кибербезопасности.
2. Мы готовы к атакам, которые приведут к «отказу в обслуживании»? Работа закрытого блокчейна, особенно частного, может быть нарушена направленной DDoS-атакой, направленной как на центральный орган контроля или на ограниченное число пользователей распределенного реестра. И вновь риски в этом случае возникают не в криптографической плоскости.
3. Как мы боремся с «мусором» на входе? В блокчейне действует принцип «мусор на входе – мусор на выходе» и злоумышленники могут внести в блокчейн неожиданную или вредоносную информацию. Каким образом обеспечивается аутентификация участников распределенного реестра, контроль доступа к нему, и контроль вносимой информации?
4. Мы готовы к квантовым компьютерам? Насколько долгосрочное хранение мы должны обеспечить в блокчейне? Если это ипотечные договора, кадастровые записи, закладные и другие долговременные блоки информации, срок жизни которых может измеряться десятилетиями, то квантовые компьютеры, о которых мы еще поговорим дальше, могут представлять реальную угрозу, так как они могут практически на лету найти криптографические ключи, используемые для защиты записей распределенного реестра. Во всем мире, для борьбы с этой проблемой применяют так называемую гибкость в выборе и переходе на новые криптографические алгоритмы (так называемая cryptoagility), но в России это, пока невозможно, так как у нас разработаны и приняты в качестве стандартов только по одному алгоритму для основных задача – шифрования, хеширования, электронной подписи.
5. Мы готовы к приходу ФСБ? Надо понимать, что блокчейн неразрывно связан с криптографией, которая в России находится под достаточно жестким наблюдением и контролем со стороны криптографического регулятора, который очень не любит применения несертифицированных и вообще несогласованных с ним решений. На момент написания статьи автор не располагает информацией о наличии в России как минимум одного блокчейн-проекта, который бы был построен на сертифицированной криптографии, хотя такие работы ведутся в отношении Мастерчейна, проекта Ассоциации «Финтех» и пр.

Смарт-контракты

Возможно, вы планируете использовать не сам блокчейн, а его производную – смарт-контракты, то есть код, который запрограммирован на автоматическое исполнение в децентрализованной сети, когда выполняются определенные условия или правила. В смарт-контрактах гарантируется исполнение договоров именно так, как определено, и невозможно внесение каких-либо изменений никаким из объектов в распределенной сети. Смарт-контракт беспристрастен, прозрачен, некоррумпирован и построен на устойчивом к атакам блокчейне. Идеальная ситуация для бизнеса, не правда ли? С помощью смарт-контрактов можно автоматизировать простые операции – авторизация платежей, выдача сертификатов, начисления и т.п.

Но не стоит забывать, что смарт-контракт – это обычный код, который пишут люди, которым свойственно ошибаться (случайно или осознанно). Сегодня известно немало атак на смарт-контракты (BatchOverflow, MAIAN, Reentrancy, Bad Randomness и др.), в результате которых участники договорных отношений теряли деньги. Поэтому дополнительно к вопросам, которые должны быть учтены в стратегии цифровой трансформации для безопасности блокчейна, я бы добавил еще ряд вопросов, уже для смарт-контрактов:

- Как мы обеспечиваем качество кода смарт-контракта? Внедрен ли у нас на предприятии SDLC (Security Development Lifecycle) или мы считаем, как и раньше, что отсутствие собственных разработчиков не требует соблюдения нами правил безопасного программирования?
- Кто проверяет условия смарт-контракта на наличие уязвимостей, ошибок, неполных условий контракта и явно мошеннических действий? В обычных договорах это делают юристы, служба экономической безопасности, отделы продаж. Обладают ли они компетенциями делать тоже самое и для смарт-контрактов? А обладают ли такой квалификацией ваши специалисты по ИБ?
- Как мы обеспечиваем аудит и контроль смарт-контрактов? Это не только часть законодательных требований, но и здравый смысл. Службы аудита и внутреннего контроля готовы к работе со смарт-контрактами?

Рекомендации по ИБ

Заданные выше вопросы уже сами по себе дают ответы на то, какие меры защиты должны быть реализованы для обеспечения безопасности блокчейна. Но если их систематизировать, то можно выделить 3 уровня архитектуры обеспечения кибербезопасности проектов на базе блокчейна:

- Уровень бизнес-логики. На этом уровне, помимо оценки необходимости применения блокчейна, определятся его модель, роли и ответственность участников блокчейна, а также правила исполнения и частота смены бизнес-логики в приложениях.
- Уровень криптографии и контроля доступа. На этом уровне определяются правила авторизации участников распределенного реестра, необходимость шифрования содержимого блоков, управление криптографическими ключами, а также вопросы нормативного регулирования, влияющего на проект. Сейчас в Европе очень активно обсуждается вопрос, насколько совместимы требования по защите персональных данных, установленные европейским регламентом GDPR, с блокчейном.

- Уровень ИТ-инфраструктуры. Это самый понятный уровень, на котором реализуются традиционные механизмы защиты узлов, входящих в распределенный реестр, а также определяется план обеспечения непрерывности для всех участников и план управления коллизиями в блокчейне.

Рисунок 2. Архитектура безопасности блокчейна

Нормативное регулирование

Какие-либо нормативные акты в области регулирования деятельности, связанной с безопасностью блокчейн, на момент написания этого материала отсутствовали. Но так как блокчейн сегодня очень плотно завязан на применение криптографических алгоритмов, то мы должны помнить о ключевых положениях законодательства в области криптографии, действующего в России:

- Регулированием этой области занимается только ФСБ России.
- На разработку решений, использующих криптографию, требуется лицензия ФСБ России.
- Встраивание в существующие системы криптографических подсистем обычно требует согласования с ФСБ.
- ФСБ России считает, что системы криптографической защиты информации подлежат сертификации. Это требование является обязательным для всех государственных информационных систем. Для коммерческих предприятий эта позиция регулятора часто оспаривается юристами, считающими, что обязательная сертификация применяется только в случаях, установленных Правительством или Президентом, а их очень мало.
- Распространение криптографических решений подлежит лицензированию и дополнительному контролю со сторону ФСБ России, например, требуется учет всех покупателей таких средств.
- Если ввозится криптографическое решение из-за границы, то для этого требуется соответствующее разрешение ФСБ, а в ряде случаев и специальная лицензия Минпромторга на ввоз.

Однако надо отметить, что в зависимости от важности проекта, базирующегося на блокчейне, для государства, вопросам нормативного регулирования может быть отведена второстепенная роль или она вообще может не учитываться, как это было сделано, например, при организации уже упомянутого дистанционного электронного голосования за поправки к Конституции. При его реализации не было соблюдено ни одного нормативного акта в области защиты информации, утвержденного ФСТЭК России или ФСБ России.

Квантовые вычисления

Идеи квантовой механики, заложенные в проектируемые сейчас квантовые компьютеры, несут безусловную пользу цифровому бизнесу за счет совершенно иных скоростей проведения вычислений и новых способов коммуникаций. Квантовые вычисления имеют два аспекта, которые важно знать с точки зрения кибербезопасности. Речь идет о квантовой криптографии и квантовом криптоанализе.

В отличие от традиционной криптографии, построенной на математических методах обеспечения целостности и конфиденциальности информации, квантовая криптография использует законы физики и позволяет создать канал связи, который защищен от прослушивания. Квантовый же компьютер, за счет экспоненциального роста вычислительных возможностей, позволяет «взламывать» многие современные системы шифрования, безопасность которых зависит от вычислительной сложности решения ряда математических задач, что в долгосрочной перспективе может нести существенные риски для цифрового бизнеса.

Риски ИБ для квантовой криптографии

На данном этапе квантовая криптография находится на этапе активного экспериментирования и только приближается к этапу практического применения. Поэтому сложно говорить о сформировавшейся картине рисков кибербезопасности для этой технологии – существуют более опасные барьеры для нее, связанные не с кибербезопасностью (физические ограничения, стоимость, требования к окружению и т.п.). Но и говорить об их отсутствии тоже уже нельзя. В 2010-м году уже был продемонстрирован способ атаки на уязвимые реализации двух квантовых криптографических систем от компаний ID Quantique и MagiQ Technologies. Но и устранить данные уязвимости можно было достаточно легко.

Риски ИБ от квантовых компьютеров

Если верить экспертам, на временном горизонте в 7-10 лет, появится действующий квантовый компьютер, который может поставить много вопросов перед используемой сейчас криптографией, делая задачу дешифрования зашифрованного текста вполне реальной. Если у нас есть данные, которые требуют обеспечения для них конфиденциальности и целостности на срок 10 лет и более, то вопрос выбора правильной криптографии для них стоит наиболее остро и квантовые компьютеры могут стать для таких данных вполне реальной угрозой, к которой надо готовиться уже сейчас.

Таблица 2. Уязвимые к квантовым атакам технологии и приложения

Технология	Приложения
PKI	Сертификаты Управление ключами
Электронная подпись	Договора, срок действия которых заканчивается после 2022 года Защищенная электронная почта
Хэш-функции	Контроль целостности Журналы регистрации Парольная защита
Блокчейн	Смарт-контракты Криптовалюты
Безопасность данных	Сохраненные и зашифрованные данные SSL/TLS TPM

С точки зрения квантовых вычислений вся криптография может быть разделена на два типа – квантово-безопасная и квантово-небезопасная. К первой относятся многие симметричные алгоритмы (в т.ч. американский AES или отечественный ГОСТ Р 34.12-2015), но с увеличенной как минимум вдвое длиной ключа (какая длина будет достаточной, кстати, пока неизвестно). А вот криптоалгоритмы, базирующиеся на сложности факторизации целых чисел (например, RSA) или дискретного логарифмирования (например, Эль-Гамаль или эллиптические кривые), не являются квантово-безопасными, в том числе и отечественные ГОСТ Р 34.10-2012 и ГОСТ 34.10-2018. В любом случае, современные криптоалгоритмы, используемые в тех или иных проектах по цифровой трансформации, например, в блокчейне, могут потребовать замены, что сопряжено с выделением дополнительных ресурсов и с дополнительными рисками.

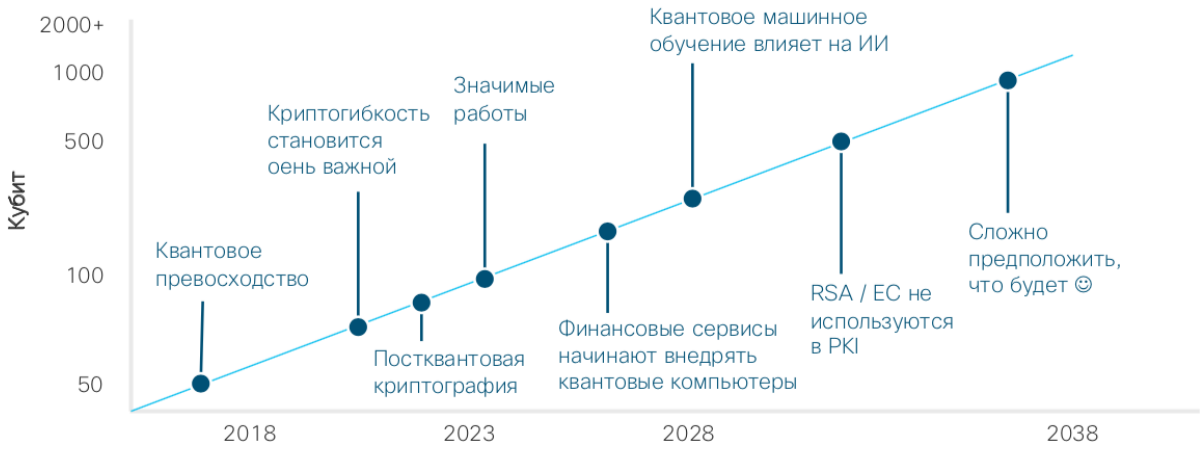


Рисунок 3. Соответствие возможностей квантовых компьютеров и традиционной криптографии

Рекомендации по ИБ

На какие вопросы вы должны будете ответить в своей цифровой стратегии применительно к кибербезопасности квантовых вычислений? Я бы выделил несколько ключевых:

1. Новые способы коммуникаций на базе квантовой криптографии выглядят перспективно, но пока, к сожалению, существующие каналы связи,

поддерживающие эту технологию, ограничены несколькими десятками километров, что позволяет применять их только между офисами в рамках одного здания или города. Эксперименты показывают, что возможно создание канала связи длиной более 100 км. Если вы планируете объединять свои офисы с помощью квантового шифрования, то подходят ли вам такие расстояния?

2. Квантовая криптография достаточно медленная штука и в существующих проектах скорость передачи данных не превышает нескольких десятков килобит в секунду. Согласно исследованиям возможно достижение скорости передачи данных по квантовому каналу до 50 Мбит/сек, что может быть очень мало для проектов по цифровой трансформации. С другой стороны, таких скоростей может быть достаточно для квантового распределения ключей (при условии решения вопроса с длиной канала связи).
3. Квантово-безопасные ли алгоритмы вы сейчас используете? Вероятнее всего ответ будет отрицательный, особенно если речь идет об отечественных алгоритмах. Если это так, то ничего посоветовать тут пока нельзя, - остается ждать, когда ФСБ России разработает и утвердит новые криптографические алгоритмы. Пока же криптографический регулятор утвердил только правила квантового распределения ключей.
4. Где вы используете криптографию? Web-сайт, электронная почта, межофисное взаимодействие, мобильные устройства, бизнес-приложения, удаленный доступ, взаимодействие с облаками… Это всё? А TPM-модуль, встроенный в каждый компьютер и ноутбук? Зачастую мы просто не осознаем масштаб применения криптографии в современном цифровом бизнесе. При рассмотрении актуальности риска квантовых атак необходимо провести всестороннюю инвентаризацию всех систем и используемых ими криптографических алгоритмов.
5. Как долго мы должны обеспечивать конфиденциальность наших данных (каков их жизненный цикл)? Не все зашифрованные данные имеют долговременную ценность и для них по-прежнему будет возможным применение текущих криптоалгоритмов. Например, если вам нужно обеспечивать целостность и конфиденциальность транзакций Интернет-магазина, то от них не требуется длительный «срок жизни» и мы можем не беспокоиться об опасности квантовых компьютеров. Банковские операции, которые требуется хранить в течение нескольких лет, уже могут потребовать задуматься о квантово-безопасной криптографии, но при условии, что такая замена будет экономически целесообразной (потенциальный ущерб должен превышать стоимость перехода на новые технологии). А вот, например, электронные ипотека или кадастры, срок жизни которых измеряется десятилетиями уже не смогут обойтись без механизмов защиты от квантовых атак.
6. Как быстро мы можем обновить существующие средства криптографической защиты (для многих предприятий могут потребоваться на это годы)? Этот вопрос особенно актуален для финансовых организаций, которых, согласно Положению Банка России №382-П, обязали полностью перейти на российские сертифицированные СКЗИ, которые пока не являются полностью квантово-безопасными и в случае осуществления такого перехода, на рубеже 2025-2028 (а Банк России требует завершить переход до 2031-го года) потребуется вновь заменять криптографию на квантово-безопасную, что влетит в «копеечку».
7. Обязаны ли мы применять только сертифицированные СКЗИ или можем рассмотреть вариант с применением постквантовой несертифицированной криптографии? Надо отметить, что постквантовой криптографией сегодня

занимаются не только за пределами нашей страны – например на российской конференции РусКрипто регулярно представляются доклады по гомоморфному шифрованию, изогенным суперсингулярным эллиптическим кривым, криптографии на мультивариативных квадратичных уравнениях и кодах исправления ошибках, а именно эти 4 направления признаны наиболее перспективными в ситуации, когда на рынке появится первый работающий квантовый компьютер. Правда, пока дальше докладов дело не ушло.

8. Постквантовая криптография несовместима с существующими решениями, что потребует разработки соответствующего плана на переходный период и большего внимания к ранее упомянутой cryptoagility (хотя в условиях отсутствия альтернатив стандартизованным отечественным криптоалгоритмам это будет непросто).
9. Представляют ли для вас опасность спецслужбы? Для большинства организаций квантовые вычисления пока выходят за рамки экономически целесообразного приобретения и поэтому очень небольшое количество потенциальных нарушителей (преимущественно из разряда спецслужб) могут их использовать против вас. Поэтому, если вы не включали АНБ, ФСБ, МИ-6 и т.п. в список своих врагов, то и бояться квантовых атак вам пока в обозримом будущем не придется.

Нормативное регулирование

Формально, квантовая криптография не имеет никакого отношения к тому, что попадает под регулирование со стороны ФСБ, так как никаких криптографических преобразований квантовые системы связи не производят. Поэтому и ограничения, описанные в разделе про блокчейн, к квантовой криптографии неприменимы. Некоторым исключением является, пожалуй, только квантовое распределение ключей, которое регулируется «Временными требованиями к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» (ВТ ККС ВРК СКЗИ), утвержденными 20 июля 2017 года.

Искусственный интеллект и машинное обучение

Искусственный интеллект (ИИ) очень неудачный перевод с английского «artificial intelligence», который уже прижился в русском языке, но не отражает реальной сути этой технологии, которая на самом деле не нова (первые работы в этой области можно отнести к середине прошлого века), но именно сейчас она переживает новый виток своего развития, что обусловлено и наличием больших объемов данных для анализа, и новыми задачами, и грядущим появлением квантовых вычислений. С точки зрения кибербезопасности цифровой трансформации искусственный интеллект (хотя лучше все-таки использовать термин «машинное обучение») интересен нам в двух областях:

- Как можно атаковать искусственный интеллект и что можно противопоставить этим атакам?
- Как противодействовать злонамеренному использованию искусственного интеллекта против нас?

Чтобы ответить на эти вопросы, нам нужно вспомнить, что машинное обучение базируется на трех ключевых элементах, которые и могут быть мишенями злоумышленников:

- *Датасет*. Чтобы научить модель распознавать что-то (плохое или хорошее), ей на «вход» надо подать большие объемы данных, называемые датасетом. Это может быть Интернет-трафик, сетевые потоки, логи, почтовые сообщения, активность пользователя, изображения, голосовые данные, отпечатки пальцев и многое другое. Чем больше и разнообразнее обучающие данные, тем точнее будет результат предсказания. Например, чтобы научиться определять СПАМ, нам нужны сотни тысяч и миллионы электронных сообщений для анализа. Чтобы научиться распознавать номера автомобилей, нужны десятки тысяч фотографий таких номеров, чистых и грязных, новых и старых, сделанных под разными ракурсами, в условиях разного освещения и т.п. От качества датасета зависит эффективность машинного обучения – если данных мало, они неполны или некачественны (а то и вовсе в них могут быть специально внесены некорректные данные), то никакая, даже самая лучшая модель машинного обучения помочь будет не в состоянии.
- *Признаки*. Это то, что мы ищем в датасетах. Например, отправитель e-mail, IP-адрес, цвет волос на голове, наличия оружия в руках, автомобильный номер, и т.д. В зависимости от решаемой задачи могут быть сотни различных признаков. Например, у некоторых систем защиты оконечных устройств может быть более 400 признаков – это метаданные, ассоциированные с анализируемым файлом – имя, дата создания, размер, наличие сетевых подключений, нестандартные протоколы, использование определенных вызовов, внесение изменений в файловую систему, разработка под определенную архитектуру, обращения к реестру и т.д.
- *Алгоритмы/модели*. Найти по определенным признакам искомое в датасете можно различными способами, выбор которых зависит от множества параметров. Правильный выбор алгоритма или модели – это всегда баланс между скоростью работы, аккуратностью предсказания и сложностью модели. Поэтому обычно на практике экспериментируют с моделями, выбирая из них лучше всего подходящую для конкретной задачи.

Риски ИБ для искусственного интеллекта

Итак, как можно атаковать искусственный интеллект? Есть несколько точек приложения сил злоумышленников, основными из которых являются две:

- Атака на алгоритм / модель
    - Внесение изменений в алгоритм с целью принятия неверных решений.
    - Подстройка под алгоритм с целью изучения принципов принятия решения и последующего обхода модели.
    - Состязательные атаки с целью генерации данных, которые обманывают модель.
- Атака на датасет
    - Внесение посторонних данных с целью принятия моделью неверных решений.
    - Изменение существующих данных с целью принятия моделью неверных решений.

Но это в теории. На практике мы должны учитывать весь жизненный цикл применения искусственного интеллекта и поэтому нельзя не брать в расчет возможные атаки на специалистов, занимающихся разметкой обучающих данных (для алгоритмов машинного обучения с учителем, supervised learning), а также на систему взаимодействия ИИ с другими

компонентами. Схожая идея должна рассматриваться применительно ко многим прорывным технологиям – не обязательно атаковать сам процесс обучения и принятия решений – достаточно просто подменить вердикт в процессе его передачи. И конечно нельзя забывать про атаки на инфраструктуру, обеспечивающую обучение и промышленную эксплуатацию ИИ (обычно это два разных процесса).

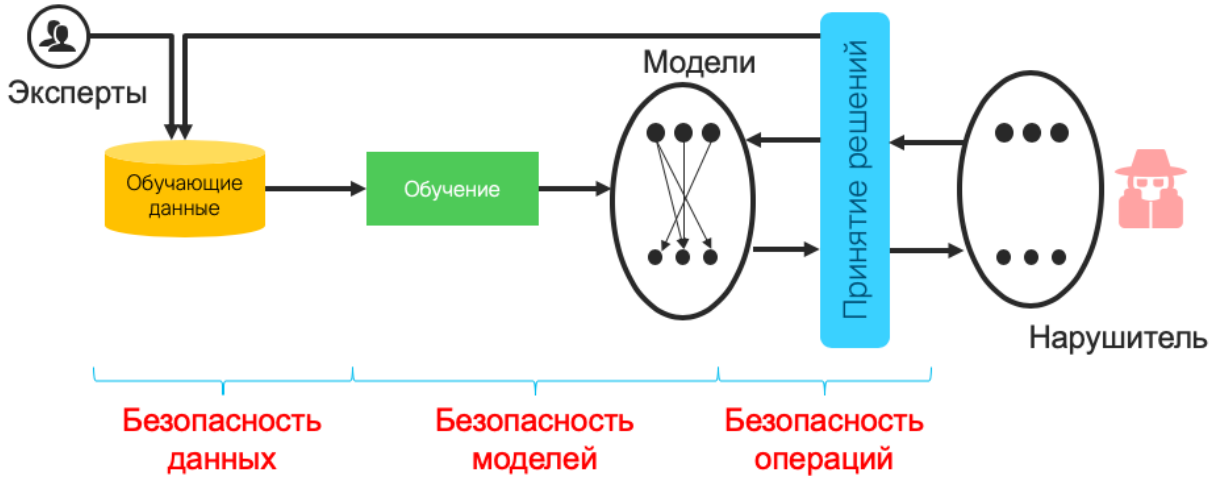


Рисунок 4. Жизненный цикл искусственного интеллекта с точки зрения кибербезопасности

Также не стоит забывать, что целью злоумышленников может быть не только введение ИИ в заблуждение, но и кража самой модели или датасеты, если они являются интеллектуальной собственностью предприятия, дающей конкурентные преимущества в бизнесе. Например, найти сегодня хороший датасет очень непросто и поэтому добыть его можно разными путями. Например, запустить вирусное приложение типа FaceApp, в которое пользователи будут по своей воле загружать фотографии и размечать их, предоставляя разработчикам огромный датасет, содержащий миллионы размеченных изображений. А можно также попробовать заказать кражу датасета, если кто-то его уже собрал для своих проектов.

Риски ИБ от искусственного интеллекта

Злоумышленники тоже начинают применять методы машинного обучения в своей криминальной деятельности – создании вредоносных программ, анализе поведения пользователей, разработке ботов-сборщиков персональных данных, поиске уязвимостей, фишинге, подборе паролей, подмене личности, обходе систем защиты и т.п. Поэтому надо не только противопоставлять таким злоумышленникам также искусственный интеллект, но и задавать вопрос разработчикам вашего ИИ-проекта – «Насколько ваша технология/решение способно распознавать и бороться с атаками со стороны недружественного ИИ?»

Рекомендации по ИБ

Исходя из вышеописанного в стратегию цифровой трансформации стоит включить ответы на следующие вопросы:

- Включены ли обучающие данные для используемых бизнесом систем искусственного интеллекта в перечень защищаемых?

- Если мы используем внешние обучающие данные, то каково их происхождение и насколько мы им доверяем?
- Как мы обучаем системы искусственного интеллекта? Кто имеет к ним доступ и как регулируется этот доступ?
- Учитывает ли наша модель угроз/нарушителя применение искусственного интеллекта злоумышленниками? Сегодня известны примеры применения ИИ со злым умыслом – для поиска уязвимостей, фишинга, подбора пароля, обхода CAPTCHA, подмены личности, обмана биометрии. Готова ли наша система защиты к таким инновационным угрозам?

Нормативное регулирование

Можно ли как-то нормативно регулировать кибербезопасность искусственного интеллекта? Для начала давайте ответим себе на вопрос, а что такое искусственный интеллект и чем он отличается от обычного интеллекта или обычной программы, которую мы можем купить в Интернете или в обычном магазине? Следуя неформальному определению, ИИ – это способ использования компьютеров для выполнения творческих задач, что традиционно считается свойством человека. Но в общем смысле искусственный интеллект пока не существует и поэтому сегодня он имеет очень узкое применение – игра в шахматы, распознавание и классификация образов, синтез человеческой речи и т.п. А как можно законодательно регулировать игру в шахматы или обнаружение болезней на рентгенографических снимках? Или обнаружение компьютерных вирусов с помощью машинного обучения? Искусственный интеллект в данных применения всего лишь позволяет видеть то, что недоступно человеку, или делать это гораздо быстрее, чем мог бы сделать человек.

Но значит ли это, что надо закрывать глаза на возможности, которые дает искусственный интеллект? Конечно, нет. Допустим, плохие парни используют искусственный интеллект, чтобы создавать компьютерные вирусы или программы, которые обходят системы защиты. Это безусловно плохо. Но это плохо и без искусственного интеллекта и такая деятельность уже прекрасно регулируется действующим российским законодательством. А теперь представим, что врач воспользовался искусственным интеллектом, который должен распознавать рак, и интеллектуальная система приняла неверное решение (неважно какое). Это врачебная ошибка и отвечает за нее врач; независимо от того, что ему помогало ее сделать. Врач, не распознавший рак в начале 20-го века и врач, не сделавший это в 21-м, одинаково виноваты и именно им отвечать (если до этого дойдет) за ошибку. В обоих этих случаях в рамках действующего законодательства отвечает человек, который использует искусственный интеллект, который является только помощником. Но есть ситуации, когда интеллектуальная система принимает решение самостоятельно и вот тут начинается самое интересное.

Вспомним недавние печальные истории с беспилотными автомобилями, которые становились причинами дорожно-транспортных происшествий. Именно системы искусственного интеллекта в них, неспособные в определенных условиях (в том числе и специально созданных) распознавать дорожные знаки, препятствия или пешеходов, привели к негативным последствиям. Но кто должен нести ответственность в этом случае и на кого её должно возложить государство? Логичный ответ – на автопроизводителей, если ИИ дал сбой по их вине. Но есть и противоположная точка зрения – коль скоро

автовладелец осознает риск использования беспилотного автомобиля, то именно он и должен нести всю полноту ответственности.

Можно привести аналогию с законом «О персональных данных», в статье 16 которого есть такие пункты: «*1. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных частью 2 настоящей статьи.*
2. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.
3. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.»

Обратите внимание, в данной статье используется схожая идеология. Системе запрещено самой принимать решение без участия человека за исключением ситуации, когда человек понимает и принимает все риски и дает на это письменное согласие. Возможно, схожая норма должна действовать и в случаях применения искусственного человека без участия человека; разве что необходимо добавить пункт об ответственности производителей, если искусственный интеллект наносит ущерб по вине именно разработчика. В случаях, когда искусственный интеллект только помогает человеку, именно последний несет ответственность в рамках действующего законодательства.

В рамках программы «Цифровая экономика» предусмотрена разработка концепции развития искусственного интеллекта, которая по планам должна появиться в пределах одного года. Однако не стоит ждать от нее ничего конкретного и жестко регулирующего. Согласно экспертам Центра компетенций по нормативному регулированию в рамках программы «Цифровая экономика», искусственный интеллект – это не ближайшее будущее и поэтому оно не требует немедленной реакции законодателей. Пока речь может идти о законопроекте о статусе роботов (его даже обещали внести в Госдуму уже в эту осеннюю сессию) и определении сфер возможного применения искусственного интеллекта, требующих регулирования. Но гораздо больше сейчас говорят о том, что пока надо подумать об этических нормах и саморегулировании ИИ. Об этом преимущественно говорит и мировое сообщество, которое предпринимало уже неоднократные попытки разработать некий этический кодекс разработчиков искусственного интеллекта.

Если не рассматривать классические законы робототехники Айзека Азимова и правила «Лиги гуманности» из научно-фантастической пьесы Карела Чапека, то одну из первых попыток предприняла Южная Корея, разработавшая в 2007-м году Этический устав роботов, за которым последовал закон о содействии развитию умных роботов, носящий

скорее рамочный характер, чем описывающий жесткие рамки. Но основные попытки стали предприниматься совсем недавно. Например, Азиломарские принципы искусственного интеллекта (2017 год), который подписало уже около 4000 экспертов по всему миру. Отказ от гонки вооружений (хотя это маловероятно, учитывая использование ИИ в Министерстве Обороны РФ, Агентстве перспективных исследований МинОбороны США и т.д.), ответственность разработчиков, нацеленность на принесение пользы людям и т.п. Достаточно классический набор принципов, который должен применяться к любой новой технологии и особенно к искусственному интеллекту, который Илон Маск назвал угрозой, еще большей, чем даже ядерная война.

Также в 2017-м году руководитель Microsoft Сатья Наделла, предложил 10 законов ИИ, а чуть позже была создана некоммерческая ассоциация Partnership on AI, в которую вошли Microsoft, Facebook, Amazon, Google, Apple, IBM, Nvidia, Intel, PayPal, SAP и другие. Но и в случае с этой инициативой пока рано говорить о каких-то результатах и разработанных правилах. Пока можно говорить о том, что основные усилия направлены на оценку и разработку этических норм в области искусственного интеллекта. Кстати, Google тоже выступила инициатором разработки своих этических принципов (их семь), которых она будет придерживаться при разработке всех своих решений. В той же Германии был принят некий свод этических правил для автопроизводителей, которые работают в области беспилотных автомобилей. Это всего лишь рекомендации, но и это уже неплохо. Тем более, что Германия уже приняла закон, регулирующий вполне конкретную и узкую сферу – дорожное движение. Немецкие законодатели выделили новый класс автотранспортных средств «со значительно или полностью автоматизированной функцией вождения» и разрешили им двигаться по дорогам, но при условии увеличения лимита ответственности для водителей и обязательной установки «черного ящика» для отслеживания всех действий, предпринимаемых автопилотом. Это, кстати, одна из рекомендаций, которой советуют придерживаться эксперты, - фиксация всех действий ИИ (и защита журнала с этими данными), чтобы в случае инцидента можно было понять его причины и отыскать виновного.

Один из лидеров в области искусственного интеллекта – Китай, тоже не имеет законодательства в этой сфере, хотя и занимает по оценкам экспертов первое место по числу инноваций в этой области. В разработанном в Поднебесной плане развития технологий ИИ первые нормативные акты в этой сфере запланированы только на 2020-й год. Европа пока тоже далека от полноценного правового регулирования этой сферы – только в 2016-м году Европарламентом был принят к рассмотрению проект резолюции о правовом статусе роботов, но и он пока касается базовых вещей – классификация роботов, этический кодекс разработчиков, а также их ответственность.

В конце августа 2018-го года в ООН прошли переговоры экспертов более 80 стран и международных организаций, которые должны были определиться с будущим развитием автономных систем вооружений, которые часто называют боевыми роботами. Германия и Франция выступили с инициативой регулирования этой сферы на уровне ООН и важности сохранения человеческого контроля над ней. Россия готова поддержать эту идею, но выступает категорически против юридически обязывающих ограничений (заменить этическими нормами?), ссылаясь на то, что полноценного искусственного интеллекта до сих пор не существует и поэтому регулировать его не надо. Кроме того, Россия считает, что существующее международное право и так способно регулировать так называемые смертоносные автономные системы вооружений.

Такой отказ говорит о том, что и внутри страны мы пока не готовы на юридически обязывающие ограничения в этой сфере (как провести грань между военными и гражданскими разработками в этой сфере?). Однако несмотря на это, в России уже есть определенные наработки в сфере регулирования ИИ и робототехники. Например, в 2016-м году со-основатель Mail.ru Дмитрий Гришин разработал концепцию закона о робототехнике. А в начале 2018-го года в России был представлен проект конвенции по робототехнике и искусственному интеллекту, который хотели рассматривать в Госдуме. Среди ключевых положений этого документа те, что уже озвучивались выше – непричинение вреда человеку и животным, защита от несанкционированного доступа со стороны третьих лиц, фиксация всех действий с помощью «черного ящика», наличие «красной кнопки» для моментального отключения и т.п.

Развитие искусственного интеллекта, который только нащупывает почву для своего развития, по мнению ряда экспертов и организаций может быть сдержано введением избыточного регулирования. Поэтому принимаются нормативные акты, вводящие так называемый экспериментальный режим в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта без особых ограничений. Такой режим, сроком на 5 лет, например, был введен федеральным законом в Москве с 1-го июля 2020-го года. В частности, этот закон позволяет обойти ряд ограничений, установленных законом «О персональных данных» на случаи, в которых обработка персональных данных осуществляется искусственным интеллектом.

Схожую конструкцию, но уже в масштабах всей страны, предлагает реализовать и Министерство экономического развития, которое разработало законопроект, выводящий обработку персональных данных граждан из-под отдельных законодательных норм. В частности, законопроект предлагает вывести обработку персональных данных из-под действия законов «О связи», «О персональных данных» и «Об основах охраны здоровья граждан» в связи с принятием федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (в части развития технологий искусственного интеллекта и больших данных). В том числе, в рамках эксперимента Минэкономразвития предложило разрешить не применять обязательство по соблюдению тайны связи, переписки и телефонных переговоров, а также врачебной тайны. В этом случае требование закона «О персональных данных», Трудового кодекса и иных нормативных правовых актов о получении письменного согласия гражданина на обработку его персональных данных и возможности отозвать такое согласие станет необязательным.

Биометрия

В 2018-м году в России принят закон, подразумевающий создание Единой биометрической системы и разрешающий кредитным организациям (а в перспективе и другим предприятиям) использовать биометрию при удаленной идентификации клиентов. Идея в том, чтобы расширить возможности рядовых граждан и позволить им пользоваться услугами банков, не посещая их офисы. Еще раньше биометрическую идентификацию стали использовать отдельные корпорации для облегчения контроля доступа сотрудников в помещения или к информационным активам. Звучит многообещающе, но необходимо обратить внимание на ряд факторов в области кибербезопасности.

Дело в том, что согласно действующему на тот момент законодательству финансовые организации обязаны были проверять подлинность своих клиентов, заставляя их в отделении предъявлять паспорт и тем самым проходить идентификацию. Но то, что не вызывает вопросов в крупных городах, где мы без усилий можем посетить ближайший офис банка, становится непреодолимым препятствием для удаленных населенных пунктов или ситуаций, когда наше физическое присутствие невозможно (болезнь, отпуск и т.п.). Удаленная идентификация с помощью биометрии решает проблему.

Существует три способа проверки так называемой подлинности человека. Во-первых, мы можем убедиться, что он знает нечто секретное (например, пароль или PIN). Это самый распространенный и недорогой в реализации механизм, который, однако, является и самым незащищенным. Узнать пароль не сложно – человек редко следует правилам выбора надежных паролей и опирается на словарный запас, который составляет несколько тысяч слов, дополненный цифрами и различными спецсимволами. Злоумышленники научились подбирать такие комбинации.

Вторым способом проверки является контроль владения некой неповторимой вещью (например, смарт-картой, ключом или штрих-кодом). Это более надежный, но и более дорогой способ аутентификации. Наконец, третий способ — это проверить, что человек обладает какой-то уникальной физической, биологической, физиологической или поведенческой характеристикой (например, отпечатками пальцев или радужной оболочкой глаза). Именно этот метод сегодня набирает популярность, так как считается, что, помимо удобства для пользователя, он является и более защищенным. Но это не совсем так.

Если у пользователя украли пароль, это неприятно, но не смертельно – его можно заменить. Украденные карта или токен тоже подлежат замене. А вот биометрический фактор уникален. Ну как вы можете поменять отпечатки пальцев, голос, глаза? Кстати, идентифицировать человека можно не только по отпечаткам пальцев, голосу, геометрии лица и руки, а также строению сосудов кисти (рисунку вен), а это самые популярные методы биометрической идентификации, из которых в банках будет применяться пока только два – голос и геометрия лица. Среди других присущих человеку особенностей можно назвать почерк, в том числе и клавиатурный, запах, электроэнцефалограмма мозга и электрокардиограмма сердца, походка, и даже, извините, то место, на котором мы сидим (его геометрия, оказывается, тоже уникальна).

В принципе, биометрия действительно решает многие классические проблемы. Традиционный вариант проверки личности клиента по кодовому слову и т.п. давно уже перестал хоть как-то защищать от мошенников. По данным исследования Opus Research «A New Authentication Paradigm: Call Center Security without Compromising Customer Experience», 65% клиентов банков не нравится процесс проверки по паролю и кодовому слову при звонках в Call Center. 49% клиентов считает, что проверка слишком долгая (от 40 до 90 секунд). 74% хотя бы раз не получили доступа к своим данным из-за того, что не прошли проверку и не смогли подтвердить свою личность стандартным способом. И биометрия может помочь во всех этих случаях, но…

Тут и возникает ловушка сознания, в которую попадают многие. Считая, что биометрия сделает жизнь удобнее и безопаснее, мы начинаем ее активно внедрять, не взвесив все за и против. Вернемся к описанной выше ситуации с кражей биометрических персональных

данных. Единожды «потерянные» голос или данные геометрии лица использовать снова будет невозможно. Разумеется, «потерять» их не так просто: они специальным образом преобразовываются и затем хранятся в специальном хранилище.

Риски ИБ

А что может угрожать биометрическим системам? На помощь приходят фантастические фильмы, в которых плохие парни отрезают пальцы, записывают голос, делают 3D-маски лица или муляжи ладони. Это действительно существующие атаки, но они направлены только на систему считывания биометрических данных, в то время как векторов атак гораздо больше.

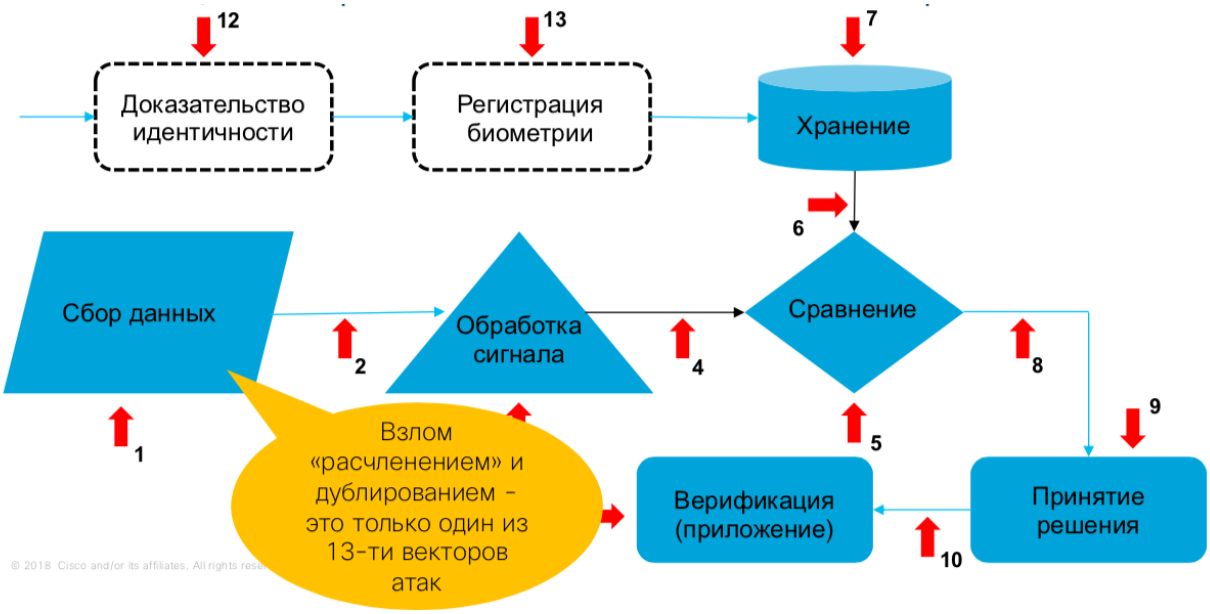


Рисунок 5. Вектора атак на биометрические системы

Например, можно сломать сам считыватель, и что бы ему не предъявляли, он будет принимать или не принимать положительное решение о подлинности человека. Можно вмешаться в работу системы верификации и поменять решение системы на нужное. Еще можно взломать хранилище биометрических профилей и внести новые, а также подменить/уничтожить существующие данные по нужным людям. Это, пожалуй, самый опасный вариант для любой схемы биометрии; так компрометируют разом всех пользователей. Всего существует около полутора десятков способов взломать систему биометрической идентификации и выбор злоумышленниками наиболее удобных из них зависит от конкретной реализации системы и задач, стоящих перед хакерами. Если, например, надо дискредитировать всю систему, то вектор атаки будет направлен на само хранилище биометрических профилей. Если надо заставить систему принять нужное решение, то эффективнее атаковать систему верификации. Если действия злоумышленников направлены на конкретного человека, то тут логичнее всего синтезировать его голос и видео и выдать себя за жертву. Тем более, что сегодня существуют технологии, которые позволяют имея запись голоса любого человека или видео с ним, синтезировать его речь или наложить его лицо на любую видеозапись.

В 2018-м – 2019-м годах набрал популярность проект DeepFake, который «в шутку» позволял «вживлять» в существующее видео фотографию любого человека. В это же время появились исследовательские проекты, которые позволяли синтезировать речь любого

человека всего по 20 минутам записанного ранее голоса, синхронизировать движение губ на видео с произносимыми словами, и объединять все это вместе. Остается только ждать, когда злоумышленники начнут активно создавать «цифровых двойников» и заключать за них договора, получать кредиты, переоформлять недвижимость и т.п.

Если вернуться к Единой биометрической системе, то надо понимать, что биометрия в национальном масштабе очень сильно отличается от корпоративного применения. В таких глобальных проектах необходимо учитывать ряд специфических особенностей, среди которых:

- Количество участников, измеряемое десятками миллионов.
- Отсутствие договоров с пользователями, что может привести к юридическим сложностям в случае каких-либо конфликтов с признанием факта прохождения проверки подлинности.
- Религиозные нюансы, связанные с тем, что в разных религиях могут быть свои ограничения. Самый простой пример: геометрия лица - женщинам в мусульманских регионах нельзя показывать лицо посторонним.
- Недоверие к любым государственным инициативам.
- Национальные проекты ориентированы преимущественно на статическую (фиксированная фотография или заранее записанный голосовой фрагмент или набор слов) и физиологическую (голос, геометрия лица, отпечатки пальцев) биометрию, в то время как современные корпоративные проекты начинают активно переходить на динамические и поведенческие (анализ клавиатурного почерка или анализ поведения человека за компьютером через web-камеру) технологии, дающие больший эффект, большую защищенность и менее заметные пользователю.

Рекомендации по ИБ

В отличие от квантовых компьютеров, которые пока только видны на горизонте, биометрия уже прочно вошла в нашу жизнь и многие компании не только активно используют встроенные в мобильные устройства технологии типа Touch ID или Face ID, но и внедряют самостоятельные решения для идентификации и аутентификации своих пользователей с помощью различных биометрических факторов (голос, геометрия лица, отпечатки пальцев, геометрия ладони и др.). Для многих это не является необходимостью, а скорее демонстрирует «продвинутость» компании, которая может обойтись слишком дорого.

Таблица 3. Виды биометрических факторов

Радужная оболочка глаза	Свайпинг
Голос	Сила нажатия на экране смартфона
Отпечатки зубов	Походка
Геометрия ладони	Форма ягодиц
Отпечатки пальцев	Энцефалограмма головного мозга
Строение сосудов руки	Электрокардиограмма
Геометрия лица	ДНК
Почерк	Запах из рта
Клавиатурный почерк	И т.п.

Какие особенности надо учитывать при решении бизнеса внедрять биометрию? Стоит выделить четыре основных вопроса, к которым надо быть готовым:

- Как мы поступим, если произойдет утечка или компрометация базы биометрических идентификаторов? В отличие от пароля или украденного пропуска мы не можем сменить голос или отпечатки пальцев. Выбранная бизнесом технология позволяет реализовать искажение биометрического фактора (для его замены) или использовать не все факторы (например, два пальца, которые, в случае компрометации, можно заменить оставшимися)?
- Какой временной горизонт допустим при внедрении биометрии? Технологии меняются и дешевеют быстро, а внедрение биометрии на тысячи и десятки тысяч устройств (например, банкоматов) может занять длительное время. А в случае компрометации системы нам, возможно, придется заменять ее на другую, что будет не только долго, но и дорого.
- На какой тип биометрии мы рассчитываем – физиологический или психологический? Первый менее подвержен изменениям с течением времени, чем второй (например, динамика набора текста на клавиатуре), но второй реализовать может быть дешевле. При этом надо учитывать, что сегодня на рынке представлено множество различных технологий биометрии, которые используют разные факторы – от распространенных (голос, лицо, глаза, ладонь) до очень специфичных (походка, ЭКГ, свайпинг пальцами на экране смартфона). На практике обычно используется мультимодальность (комбинация двух и более факторов), обеспечивающая здоровый баланс между уровнем ложных срабатываний (FAR/FRR), стоимостью решения и временным горизонтом.
- Какова наша модель угроз? Дело даже не в том, что обычно рассматривается только одна угроза – подмена биометрического фактора на этапе сбора данных (отрезанные пальцы, муляжи ладони или 3D-маски лица), забывая про остальные 12 векторов (например, можно просто подменить вердикт системы на противоположный и вся система превратится в «тыкву»), описанных выше. Но даже на этапе сбора сегодня появляется немало новых угроз, которые могут кардинально изменить будущее биометрии, которое нельзя не учитывать в стратегии цифровой трансформации. Например, известно немало исследований в области применения нейросетей для обмана биометрических систем. Да, сегодня они пока осуществляются в благих целях (для улучшения системы защиты), но и хакеры могут (и уже делают) воспользоваться полученными результатами и обойти биометрию.

Таблица 4. Перечень угроз для биометрии и мер по их нейтрализации

Элемент системы	Угроза	Мера нейтрализации
Сбор данных	Подмена	Обнаружение «живости» Запрос / ответ
	Использование недоверенного устройства (подмена устройства)	Взаимная аутентификация
	Перегрузка устройства (выведение из строя)	Устройства в защищенном исполнении
Обработка сигнала	Внедрение данных нарушителя	Проверенные алгоритмы
	Замена компонентов	«Подписанные» компоненты

Сравнение	Внедрение данных нарушителя	Проверенные алгоритмы
	Замена компонентов	«Подписанные» компоненты
	Угадывание/перебор (FAR атака)	Проверенные алгоритмы Многофакторность / комбинация биометрических методов
	Манипуляция результатами (рейтингом) сравнения	Защита от отладки
	Hill-climbing (отправка сгенерированных шаблонов и, на основе полученного вердикта от модуля сравнения, генерация модифицированных шаблонов для прохождения успешной проверки)	Защищенный канал Доверенный сенсор (взаимная аутентификация)
Принятие решения	Hill-climbing	Защищенный канал Доверенный сенсор (взаимная аутентификация)
	Манипуляция настройками пороговых значений	Контроль доступа Защита данных
	Манипуляция принятием решения	Защита от отладки
	Замена компонентов	«Подписанные» компоненты
Приложение (верификация)	Вредоносный код	Соответствие стандартам (BioAPI, CBEFF) Подписание кода
Хранение	Компрометация базы данных (чтение биометрического шаблона, замена шаблона, изменение связки)	Защита сервера Контроль доступа к базе данных Шифрование и электронная подпись биометрического шаблона Хранение шаблонов на смарт-картах или иных устройствах
Передача «сырых» данных и передача обработанных данных	Перехват	Защищенный канал передачи
	Повтор	Взаимная аутентификация Подписанные ЭП данные Использование временных меток / Time-to-Live
	«Человек посередине»	Защищенный канал Привязка биометрии к сертификату открытого ключа

	Подбор / перебор	Таймауты / блокировки
Поиск биометрического шаблона	Перехват	Защищенный канал передачи
	Повтор	Взаимная аутентификация Подписанные ЭП данные Использование временных меток / Time-to-Live
	«Человек посередине»	Защищенный канал Привязка биометрии к сертификату открытого ключа
Передача результата сравнения	Hill-climbing	Защищенный канал Доверенный сенсор (взаимная аутентификация)
	Манипуляция результатами (рейтингом) сравнения	Защищенный канал Взаимная аутентификация
	Замена компонентов	«Подписанные» компоненты
Взаимодействие с приложением (верификатором)	Перехват	Защищенный канал
	Манипуляция принятым решением по сравнению	Защищенный канал

Нормативное регулирование

Мы не будем приводить список нормативных актов, которые регулируют применение Единой биометрической системы, а вот перечень документов, которые влияют на корпоративное применение биометрии, приведем:

- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных», требующий письменного согласия на обработку биометрических персональных данных.
- Постановление Правительства РФ от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
- Указание Банка России от 10 декабря 2015 г. №3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных»
- Приказы ФСТЭК России, разрешающие применение биометрической идентификации/аутентификации при построении систем защиты информации.
- А также более 45 национальных стандартов, регулирующих различные аспекты биометрии (среди них ГОСТ Р 58273–2018, ГОСТ Р 54411- 2018, ГОСТ Р ИСО/МЭК 29109, ГОСТ ISO/IEC 2382- 37–2016, ГОСТ Р 58298–2018 и другие).

Технология 5G

Не успели мы насладиться скоростями, которые предоставляет нам технология LTE (4G), как производители задумались о необходимости разработки нового стандарта мобильной связи, в простонародье называемом 5G, который бы предоставлял новые скорости (в 10-20 раз больше, чем текущие сети) и новые возможности, ранее недоступные в ряде сценариев цифровой трансформации (Интернет вещей, беспилотные летательные аппараты и транспорт, видеоаналитика в реальном времени, дополненная и виртуальная реальность и т.п.). С точки зрения безопасности этой технологии, если отбросить санкционную тематику конфликта Huawei и США с союзниками, существуют две диаметрально противоположные точки зрения. Одни эксперты утверждают, что активное внедрение 5G в гораздо большее число критических сервисов (от ядерной энергетики до оповещения в чрезвычайных ситуациях) может повлечь за собой серьезные последствия для бизнеса и общества, если злоумышленники смогут вывести инфраструктуру 5G из строя. Другие эксперты, наоборот, считают риски для 5G преувеличенными.

Риски ИБ

С точки зрения архитектуры сети 5G отличаются от того, как сейчас построены сети мобильной связи 4-го или 3-го поколений, которые строились преимущественно на базе аппаратных решений, выполняющих узкие и вполне определенные задачи (SGSN, GGSN, SBC, BRAS, HLR, HSS и т.п.). Сеть 5G активно использует возможности программного обеспечения и, в частности, программно-определяемых сетей (SDN, Software Defined Network) и виртуализации сетевых функций (NFV, Network Functions Virtualization), которые разворачиваются на базе стандартных коммутаторов, серверов с виртуальными машинами, контейнерами и микросервисами, и систем хранения данных со всеми, присущими им уязвимостями и особенностями обеспечения кибербезопасности.

Например, активное использование программно-определяемых сетей и виртуализации сетевых функций приводит к размыванию границ между различными компонентами сети оператора связи, с гораздо большими возможностями для злоумышленников по атакам на них, которым больше не придется пробираться через физические и логические границы, как это было раньше. А если добавить сюда тот факт, что сети 5G строятся на базе ПО от разных производителей, а качество и, как следствие, защищенность ПО постоянно снижаются, то риски атак на сети 5G возрастают. И бороться с описанными проблемами может только оператор связи, в зоне ответственности которого и находится ядро мобильной сети. Правда, есть у этой проблемы и другая сторона. Виртуализация сетевых функций делает современные мобильные сети более устойчивыми и живучими, так как при правильном проектировании исчезает единая точка отказа, на которую могли быть направлены усилия хакеров.

Снижение времени задержек и рост скоростей 5G требует сдвигать вычислительные возможности как можно ближе к потребителям, что приводит к необходимости строить несколько ядер мобильной сети 5G, что, с одной стороны, также повышает устойчивость системы (отказ одного ядра не сказывается на работоспособности других), а с другой, повышает риски атак на ядро, которое имеет меньше рубежей защиты, чем раньше. И так как оператору связи будет сложно разграничивать критические и некритические компоненты своей сети, то злоумышленнику станет проще проникать в критические сегменты, начиная свою атаку через некритический компонент, приближенный к мобильным потребителям, число которых будет многократно расти (и это будут не только

пользователи мобильной связи, но и миллиарды Интернет вещей, которым 5G откроет второе дыхание).

Еще одним нововведением 5G стала технология нарезки сетевых сервисов (network slicing), в основу которой легла виртуализация сетевых функций и которая позволяет логически разделять сети для различных типов услуг 5G – высококачественное видео, голос, обычный Интернет вещей и для критичных к задержкам приложений, и т.д. Использование единой физической инфраструктуры, поддерживающей нарезку сетевых сервисов, позволяет многократно ее использовать с гибким перераспределением ресурсов между различными услугами 5G. Но за таким преимуществом, которое позволяет снизить не только капитальные, но и операционные затраты, вновь скрывается проблема с ИБ, - отсутствие четких границ и несоблюдение принципа эшелонированной обороны повышает вероятность негативного влияния на предоставляемые сетями 5G сервисы.

Если отвлечься от архитектурных недостатков ИБ в сетях 5G, то необходимо упомянуть и о проблемах ИБ в их реализации. В частности, в уже были выявлены уязвимости в протоколе аутентификации и согласования ключей (AKA), которые позволяют выявить местоположение устройств, подключенных к 5G. Европейское агентство по кибербезопасности в свою очередь предупреждает, что сетям пятого поколения могут быть присущи проблемы ИБ в протоколах сигнализации, которые давно были выявлены в сетях 2G/3G/4G.

Но все описанные выше риски присущи именно ядру сетей 5G, которое находится в управлении оператора связи. В итоге, если не рассматривать среди рисков технологии 5G, которая пока еще не внедрена в России, угрозы со стороны цепочки поставок и зависимость от производителей, а также не брать во внимание описанные выше риски, связанные с SDN и NFV, на которые потребитель повлиять не может, то с точки зрения кибербезопасности у нас остается только одна проблема – взрывной рост числа устройств, подключенных к сети, которые могут быть использованы для проведения различных кибератак, например, рассылки спама. Если это «наши» устройства, из-за уязвимостей или некорректной конфигурации которых хакеры смогли взять их под контроль, то атаки могут быть проведены против других организаций, пользователей и государств. А если устройства чужие, то они, находясь под управлением злоумышленников, могут превратиться в распределенную атакующую сеть, которая может генерировать вредоносный трафик мощностью в десятки и сотни терабит в секунду, что поставит очень остро вопрос организации нейтрализации DDoS-атак.

Рекомендации по ИБ

Для борьбы с описанными угрозами операторы связи должны будут внедрять различные защитные меры, на которые, как уже было сказано выше, потребители повлияет не могут, и им остается только надеяться, что сети 5G будут достаточно защищены. Если же сфокусироваться на том, что могут сделать корпоративные пользователи сетей 5G, то можно выделить 6 ключевых направления по обеспечению кибербезопасности:

- Взаимное доверие между операторской и корпоративной сетью, которое будет достигаться за счет правильной настройки и использования механизмов обоюдной аутентификации.

- Защита от DDoS-атак, которая может быть достигнута внедрением собственных решений по отражению атак «отказ в обслуживании» или приобретению соответствующего сервиса у оператора связи или специализированного провайдера услуг.
- Контроль доступа к IoT (в случае его использования), который может быть реализован за счет правильной сегментации сети Интернета вещей, их настройки безопасности, регулярного обновления программного обеспечения, а также мониторинга различных аномалий, исходящих из данного сегмента.
- Контроль доступа к приложениям и сервисам, использующим сервисы 5G, который должен быть настроен при условии предоставления соответствующих механизмов защиты со стороны поставщиков приложений и сервисов (телемедицина, VR, умный город, беспилотные автомобили, умное энергоснабжение
- Защита корпоративного периметра, которая уже должна быть реализована в компании, и которая не должна делать исключений ни для какого типа подключений, включая и сети 5G.
- Обеспечение приватности данных, которая требуется законодательством множества стран, и которая может быть обеспечена путем заключения соответствующих соглашений (с обязательным контролем их исполнения) с поставщиками услуг на базе 5G.

Технологии мобильной связи 6G

Не успев внедрить сети пятого поколения, некоторые компании, преимущественно из азиатского региона, заговорили о сетях 6-го поколения, в которых скорости по сравнению с 5G будут в 50-400 раз выше, а задержки снизятся в 10 раз. Это позволит предоставлять такие сервисы как иммерсивная дополненная реальность (XR), цифровая репликация или мобильные голограммы. Сдвиг вычислений ближе к потребителю, на уровень периметра мобильной сети, начатый в сетях 5G, и рост скоростей позволит реализовать облачный искусственный интеллект. Пока рано говорить о кибербезопасности сетей 6G, но можно предположить, что в них будут схожие риски, что и в сетях 5G.

Нормативное регулирование

В России пока отсутствует специальные требования по безопасности сетей 5G и 6G, исключая общие требования к операторам связи обеспечивать тайну связи и систему обеспечения оперативно-разыскных мероприятий.

Технология Wi-Fi 6

Технология беспроводных сетей достаточно активно эволюционирует и вот уже в промышленную эксплуатацию начинает внедряться новый стандарт Wi-Fi – 802.11ax, больше известный как Wi-Fi 6. Наверное, не совсем правильно относить этот стандарт к прорывным технологиям, которые лягут в основу цифровой трансформации, так как новый стандарт беспроводной связи стоит рассматривать всего лишь как улучшение текущего стандарта 802.1ac, который не очень хорошо справлялся с тремя сценариями, становящимися все более популярными:

- Хаотичные внедрения Wi-Fi, происходящие, например, в торговых и бизнес-центрах, где каждый арендатор пытается установить собственную точку доступа, мешающую

соседям. Аналогичная проблема возникает и на крупных мероприятиях, когда бесконтрольное использование Wi-Fi начинает создавать помехи в работе.

- Высокая плотность пользователей, приводящая как к снижению пропускной способности беспроводной сети в пересчете на отдельного пользователя, так и к появлению помех в работе.
- Интернет вещей, условием функционирования которого является длительная автономная работа с низким энергопотреблением, что противоречило обычной практике работе беспроводных устройств, потребляющих достаточно много энергии для своей работы и, в условиях автономности, «живущих» не очень долго.

Соответственно новый стандарт Wi-Fi 6 позволяет задействовать новые частоты и более эффективно разделять беспроводной спектр, предоставляет более эффективное энергопотребление, снижает риск коллизий и т.п. В отличие от мобильной связи пятого поколения, рассмотренной ранее, решения на базе стандарта Wi-Fi 6 в гораздо большей степени находятся в зоне контроля корпоративного пользователя, у которых больше возможностей по их защите.

Риски ИБ и рекомендации по их нейтрализации

Новых рисков ИБ стандарт Wi-Fi 6 не несет, так как является обычным улучшением уже привычных нам способов беспроводной связи, риски которых нам прекрасно известны. Речь идет о публичных хотспотах, подключиться к которым может любой желающий, слабых паролях, незащищенном трафике, фальсификации точек доступа и т.п. Отдельно я бы выделил возможность организации атак «отказ в обслуживании» на корпоративные инфраструктуры с взломанных устройств Интернета вещей (схожая проблема есть и в сетях 5G), так как скорости подключения таких устройств возрастают многократно (до теоретических 9,6 Гбит/сек).

Нейтрализация части перечисленных угроз заложена в самом стандарте Wi-Fi 6. Например, использование технологии MU-MIMO (аббревиатура от английского «multi-user, multiple input, multiple output», означающая обеспечение направленности сигнала для конкретного пользователя, минимизируя влияние на других) позволяет снизить риски перехвата данных, так как их передача осуществляется в более узком направлении, чем в прежних стандартах Wi-Fi. Однако для борьбы с большей частью известных угроз был предложен также обновленный и разработанный альянсом Wi-Fi Alliance стандарт WPA3, в котором были улучшены механизмы шифрования (увеличена длина ключа), усилены механизмы аутентификации и защиты от слабых паролей, а также реализована защита управляющих фреймов.

Таблица 1. Отличия механизмов защиты WPA2 и WPA3

	WPA2		WPA3	
	Personal	Enterprise	Personal	Enterprise
Шифрование	AES 128	AES 128	AES 128	AES 192
Аутентификация	PSK	802.1x	SAE	802.1x
Защита управляющих фреймов	Не требовалась	Не требовалась	Обязательно	Обязательно

С практической точки зрения стоит обратить внимание на то, что не все беспроводное оборудование, поддерживающее стандарт 802.11ac (предыдущая версия, также редко упоминаемая как Wi-Fi 5), будет поддерживать Wi-Fi 6, - обновления программного обеспечения или «прошивок» может быть недостаточно. Однако, при замене парка оборудования стандарт WPA3 будет уже встроен в новые беспроводные контролеры и точки доступа. Останется только настроить их для безопасной работы.

Нормативное регулирование

В России пока отсутствует специальные требования по безопасности беспроводных сетей стандарта Wi-Fi 6, исключая общие требования ФСТЭК и Банка России к защите беспроводных технологий, используемых в государственных информационных системах, критической информационной инфраструктуре, обработке персональных данных, переводе денежных средств или иных финансовых сервисах.

Интернет вещей

По данным Cisco к 2020-му году в мире должно было быть подключено к Всемирной сети около 50 миллиардов устройств. Вы представляете какой это поток информации и какие сложности встанут перед организациями с точки зрения кибербезопасности? Позволю себе перечислить только некоторые из них:

- Рост объемов трафика, что потребует более производительных решений по безопасности.
- Отсутствие человека, работающего за прибором в Интернете вещей, что потребует активного использования технологий аутентификации не пользователей, а устройств.
- Миниатюризация устройств, требующая миниатюризации и защитных средств и технологий (снижение объема кода, повышенные требования к автономной работе и т.п.).
- Небольшие порции передаваемой информации, что потребует пересмотра криптографических технологий.
- Огромное число устройств, что потребует пересмотра вопросов распараллеливания обработки трафика и аутентификации такого количества устройств.
- Совершенно новые, ранее непредполагаемые устройства (очки, часы, одежда, кардиостимуляторы, кофеварки, холодильники, сантехника и т.п.), что потребует пересмотра традиционного отношения к объекту защиты.

Готовы ли мы к этим инновациям с точки зрения информационной безопасности? Как мы будем защищать взаимодействие между взаимодействующими через социальные сети людьми? Как мы защитим RFID-метку от направленного на нее негативного воздействия? Как мы отследим целостность информации, передаваемой по сети метеорологических сенсоров? Как, в конце, концов защищать индустриальные системы и системы управления технологическими процессами, которые также стали называть термином «Интернет вещей», добавляя к нему приставку «промышленный» или «индустриальный» (IIoT, Industrial Internet of Things)? Все это требует не просто внимания, но и детальной проработки архитектуры, разработки совершенно новых подходов и средств защиты.

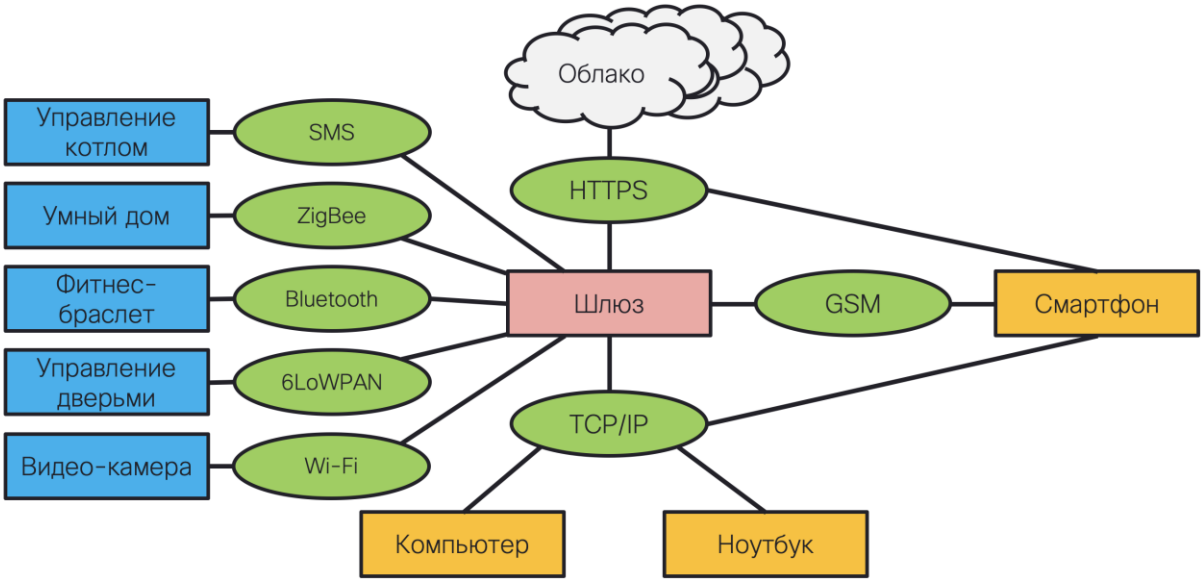


Рисунок 6. Высокоуровневая архитектура Интернета вещей

Сегодня мы сталкиваемся с целым рядом значимых событий, которые отражают становление такой темы как кибербезопасность промышленного Интернета вещей. С одной стороны, ведется много разговоров о таком явлении как Industry 4.0 и Интернете вещей (Internet of Things, IoT), которые вроде как положительно влияют на экономику отдельных отраслей и целых государств, а также улучшают жизнь граждан. В России создают различные ассоциации и даже при Ростехрегулировании создали свой технический комитет ТК194, который и будет заниматься стандартизацией киберфизических систем, в том числе Интернета вещей.

Риски ИБ

Мы видим рост числа атак на промышленные системы, а также использование Интернет-вещей для осуществления противоправных действий. В 2017-м году появился ботнет Mirai. В 2018-м году число IoT-ботнетов многократно увеличилось – «Амнезия», «Hajime», «BrickerBot», «Persirai». При этом не проходит месяца, чтобы какой-нибудь исследователь не заговорил о взломе автомобиля, сантехники, сексуальной игрушки с встроенной видео-камерой, кардиостимулятора, инсулиновой помпы, стелек, холодильника, подключенных к Интернет. И это не говоря о промышленном Интернете вещей, который раньше называли системами промышленной автоматизации, и который ломают сегодня очень активно – Stuxnet, атаки на энергосистему Украины, атаки на канализацию в Брисбене, шифровальщик WannaCry, выведший из строя 5 заводов Renault и попавший на ряд железнодорожных объектов, шифровальшик NotPetya или Neytya, который вывел из строя огромное количество промышленных объектов в Украине.

Недавно исследователи обнаружили новый вредоносный код – CrashOverride, который называют 4-м в истории, созданным специально для промышленных систем (после Stuxnet, BlackEnergy и Havex). Тут надо сразу оговориться, что речь идет об известных вредоносах, которые ориентированы именно на системы промышленной автоматизации и их специфику. Когда мы слышим разговоры о том, что это 4-й пример воздействия на физический мир, не совсем понятно, на чем базируются авторы таких высказываний. Ведь и раньше кибератаки наносили ущерб физическим объектам. Вспомним историю с

закладкой в ПО, украденном советскими разведчиками в США и затем использованном на газопроводе в СССР. Был взрыв и останов работы трубопровода на определенное время. Также, как и история с инсайдером на Игналинской АЭС в 1989-м году, в результате активности которого чуть не было выброса ядерных материалов. Да, в те времена никто не собирал индикаторы компрометации и в современных базах инцидентов нет никаких сигнатур вредоносных файлов. Но это не значит, что тех атак не было и они не повлияли (или не могли повлиять) на физический мир. Да тот же WannaCry, который является исконно офисным «вирусом» сумел немало навредить и промышленным объектам – заводы Renault, поликлиники, вокзал в Франкфурте, завод по производству телекоммуникационного оборудования, логистическая компания Maersk. Примеры можно продолжать, но в любом случае они показывают, что сегодня мир виртуальный и мир физический объединены очень сильно и для воздействий на второй из них из первого не всегда требуются особые знания. Хотя появление CrashOverride показывает, что компетенции злоумышленников растут и можно спрогнозировать увеличения числа специфических для разных отраслей, систем промышленной автоматизации и промышленных протоколов вредоносных программ.

Пример: автомобили

CDO крупной металлургической компании в приподнятом настроении вышел из лифта и направился к своей Audi Q7, стоящей в дальнем углу подземного корпоративного паркинга. Сев за руль и нажав кнопку Start, он с удовольствием прислушался к медленному нарастанию урчащего звука мотора, выдающего в железном коне чистокровную породу. Вырулив в лучах заходящего солнца на Кутузовский проспект, наш CDO втопил педаль газа в пол и меньше чем за 10 секунд стрелка спидометра проскочила отметку в 100 км/час, а еще через некоторое время стрелка прочно обосновалась на отметке в 150 км/час. Ни сигнализация эвакуируемых машин, ни шум дорожных работ не отвлекали CDO от предвкушения наступающего вечера — в компании своей любимой, с бокалом виски в руке, смотря на горящие в камине поленья… Но мечтам не суждено было сбыться. Audi Q7 внезапно и самопроизвольно стал набирать скорость. CDO попытался тормозить, но соответствующая педаль перестала реагировать на нажатия… Перед глазами CDO стали проноситься яркие события прошлой жизни, которые прервал страшный удар в ряд бетонных тумб, защищающих Триумфальную арку…

Прочтя предыдущий абзац, наверное, у вас возник вопрос, а причем тут цифровая трансформация и описанная ситуация. Так сложилось, что автомобиль по своей начинке мало чем отличается от корпоративной сети — в нем есть сеть, есть компьютеры (их роль выполняют контроллеры ECU, управляющие различными функциями автомобиля, — стеклоподъемниками, датчиками температуры, давлением в шинах, ABS, мультимедиа, контролем слепых зон и т.п.), есть выход в Интернет, есть свои хранилища данных…

40% современного автомобиля – это электроника и программное обеспечение. ПО насчитывает несколько миллионов строк кода (даже в космических кораблях их меньше). Объем ПО в премиальных автомобилях достигает 1 гигабайта. Длина кабельной системы в автомобиле составляет до 3 км, а число интерфейсов превышает 3000. Вот только безопасности почему-то в автомобилях нет. И примеров взломов автомобилей за последнее время становится все больше и больше, а модель угроз для железного коня

ширится с каждым днем. Вот только несколько примеров того, что можно сегодня сделать с автомобилем:

- Перехват местоположения
- Блокирование передачи данных о местоположении
- Изменение маршрута движения
- Подмена Point-of-Interest в навигационной системе
- Блокирование/разблокирование дверей
- Блокирование/разблокирование двигателя
- Блокирование передачи сигнала о краже
- Кража контента в развлекательной системе
- Внесение изменений в работу электронных блоков управления (ECU).

Пример: умный дом

Представьте, что вы устанавливаете газовой котел на дачу и продавец вам предлагает систему дистанционного мониторинга и управления котлом по SMS. На словах все выглядит просто потрясающе – у вас появляется возможность отслеживать уровень температуры в помещениях, повышать его или понижать, а также удаленно включать или выключать газовый котел. «А как защищена эта система?» - спросите вы (ну мы надеемся, что вы спросите). «А зачем?» - скорее всего последует недоуменный ответ.

Рядовой продавец не знает, что можно сделать с такой системой дистанционного управления, не обладающей даже зачатками защитных механизмов. Самое первое, что приходит в голову, - отключение котла в зимние морозы, что приведет к промерзанию труб отопления и потенциальному их разрыву (если там залита вода, а не антифриз). А уж если вспомнить про пресловутый Stuxnet, заразивший объект по обогащению ядерного топлива в иранском Натанзе, то обычными SMSками, которые передаются в открытом виде и могут быть подменены, можно нарушить режим работы котла, то включая его, то отключая, что в свою очередь приведет к выходу его из строя и необходимости дорогого ремонта. Если все это вы расскажете продавцу, то он уйдет от вас ошарашенный, а вы лишний раз убедитесь в том, что о безопасности Интернета вещей у нас сегодня мало кто думает.

И это не единственный пример незащищенности умных домов, которые строятся гражданами у себя на загородных участках и в квартирах, а компаниями при проектировании бизнес-центров и элитных жилых домов. Согласно статистике компании HP 100% исследованных ими систем умного дома не требовали сложных паролей для своей настройки. Пять из десяти систем имели проблемы с перехватом данных при их передаче с мобильного устройства, а семь из семи облачных платформ для управления умным домом могли быть легко взломаны.

Пример: кардиостимуляторы и инсулиновые помпы

Знаете ли вы, что Интернет вещей проник даже в такие, казалось бы, далекие от Интернета, вещи как персональные медицинские приборы, например, в кардиостимуляторы или инсулиновые помпы. Что за бред, скажете вы, и ошибетесь. С точки зрения врача и пациента это удобно – можно дистанционно снимать показания приборов. Но проблема заключается в том, что у этих приборов есть не только функции диагностики – еще можно дистанционно менять режим их работы. Например, инсулиновая помпа по команде извне

может впрыснуть диабетику не жестко заданную порцию инсулина, а весь объем лекарства, что приведет к анафилактическому шоку и смерти человека. А некоторые модели кардиостимуляторов оснащены встроенным дефибриллятором, предназначенным для запуска остановившегося сердца. А теперь представьте, что дефибриллятор дал разряд в 800 вольт на работающем «пламенном моторе»? Сердце просто остановится. И это не фантастика – это результаты реальных исследований безопасности медицинских приборов. Недаром американский Минздрав в начале 2015 года выпустил специальные требования по кибербезопасности медицинских устройств. И это не единственные риски в области медицинского Интернета вещей. Если мы используем какие-либо облачные сервисы, которые связаны с используемыми медицинскими приборами (весы, инсулиновые помпы, ингаляторы и небулайзеры, и даже дозаторы таблеток), то у нас появляются риски утечки этих данных, которые могут быть использованы злоумышленниками для шантажа.

Пример: носимые гаджеты

Кардиостимуляторы и инсулиновые помпы с Интернет-подключением – это, к счастью, пока редкость. В отличие от фитнес-браслетов, трекеров и «умных» часов, которые завоевывают все большую популярность среди людей, стремящихся вести здоровый образ жизни. Поэтому они ничтоже сумняшеся доверяют таким устройствам информацию о своем здоровье, о своем местоположении и времени его посещения, о своей сексуальной активности и уровне стресса, и даже о том, когда крепче всего сон (мечта вора-домушника)…

По перечисленной информации уже становится понятно, что основная проблема с безопасностью носимых гаджетов – это приватность. Все упомянутые данные, а также многие другие, могут быть украдены как с самого устройства, так и во время их передачи на мобильное устройство и дальше в облако, а также в самом облачном хранилище. Так уж получилось, что 70% из них передают данные в открытом виде (по исследованию HP), а по статистике компании Symantec 20% такие приложения даже пароли на доступ к облачным хранилищам персональных данных передают в незащищенном виде. 3 из 10 самых популярных умных часов, протестированных HP, позволяли злоумышленникам просто угадать учетную запись и получить несанкционированный доступ к носимому гаджету. Еще более интересное исследование было сделано «Лабораторией Касперского», которая выяснила, что вредоносная программа, установленная на умные часы, может с вероятностью более 90% определять по движению руки пароли и PIN-коды, набираемые на клавиатуре. И это, не говоря уже о том, что вся ваша подноготная продается направо и налево – маркетинговым и рекламных компаниям, страховым и медицинским организациям, а также спортивным производителям. Никаких согласий на обработку персональных данных у владельцев носимых устройств не берут, а на сайтах их производителей обычно не встретишь никакой политики конфиденциальности.

Кстати, на Олимпиаде в Лондоне в 2012-м году в кроссовки легкоатлетов встраивались специальные беспроводные датчики для отслеживания времени в том или ином соревновании. Представьте себе, к чему может привести внесение небольшой задержки или подмена данных, поступающих к судьям. Тут не то, что о золотой медали можно забыть, но и вообще в тройку медалистов не попасть, потеряв не только смысл жизни, но и контракты от богатых спонсоров.

Другие примеры Интернет-вещей

Выше было приведено только несколько примеров Интернет-вещей, имеющих серьезные проблемы с безопасностью. А ведь есть еще сантехника, холодильники, секс-роботы, дороги, парковки, одежда, игрушки, подключенные к Интернет. За термином «Интернет вещей» или даже «Всеобъемлющий Интернет» скрывается очень много разных направлений. Такое разнообразие его применений привело к тому, что до сих пор отсутствует единый стандарт в области взаимодействия Интернет-вещей между собой. В мире сегодня насчитывается свыше 25 (!) различных групп, которые занимаются стандартизацией данного вопроса, — ITU, ISO, IEEE, ETSI, GS1, ANSI, OASIS, IETF, AllSeen, OIC, OMG и т.д. К сожалению, пока они не смогли прийти к взаимопониманию и разработать единый набор спецификаций для использования в разных сферах (может быть это и в принципе невозможно, кто знает). В ноябре 2014-го года ITU-T попробовала аккумулировать в одном документе все работы по стандартизации, которые ведутся в мире. Получился очень весомый документ на 122 страницы, содержащий упоминания свыше 250 (!) различных стандартов (преимущественно в виде проекта) в области Интернета вещей, и с тех пор работа на месте не стояла и появились новые стандарты.

И из всего многообразия этих стандартов только 5 (!) было посвящено вопросам защиты информации. Представьте себе, только 5! С другой стороны, надо признать, что и традиционные средства защиты пока не готовы к работе в Интернете вещей. Ведь тут нет мощных серверов и постоянно подключенных к сети энергоснабжения узлов, на которые можно поставить систему защиты. Миниатюризация, автономность работы, невысокие требования к системным ресурсам… Все это не позволяет обычным антивирусам, системам аутентификации, средствам шифрования и т.п. быть установленными на умные часы, фитнес-браслеты, кофеварки, очки, автомобили и т.п.

И понять такую «слепоту» разработчиков и стандартов, и средств защиты, и новомодных Интернет-гаджетов можно — инцидентов в области Интернета вещей пока еще не было (в массовом порядке), отсутствие спроса со стороны потребителей, отсутствие стандартов взаимодействия, которое не позволяет выработать механизмы защиты… Все это пока приводит к тому, пока безопасность Интернета вещей — скорее дань моде, чем осознанная производителями необходимость. Они больше озабочены выпустить свой продукт на рынок пораньше, чтобы застолбить за собой пальму первенства и захватить большую долю рынка.

Рекомендации по ИБ

В такой ситуации возникает вопрос о том, как защитить современный Интернет вещей? С одной стороны, между ИТ и IoT много общих проблем безопасности, разработано немало стандартов и требований по регулированию специфических вертикалей, мировой рынок решений по ИБ IoT растет, все же он остается фрагментированным и не очень крупным.

Крупные игроки рынка ИБ только-только подступаются к новому сегменту, но используют для этого свои традиционные ИТ-подходы, не всегда работающие в мире IoT. Все дело в том, что оба мира (ИТ и IoT) отличаются по масштабу (миллионы устройств), спектру платформ, специфическим протоколам, воздействию на физический мир, сроку жизни и автономности, встроенности (embedded) и работе в агрессивных средах. Поэтому

использовать привычные нам межсетевые экраны, антивирусы, PKI, системы анализа сетевого трафика в Интернете вещей не получается. Отрасль IoT пока тоже не желает активно заниматься ИБ, исключая крупных поставщиков IoT, уже столкнувшихся с проблемами ИБ в своем оборудовании или попавших под требования регуляторов, как это произошло с медицинскими приборами в США. Вообще сегодня именно инцидент ИБ является драйвером развития отрасли. NetGear запустила программу bug bounty после обнаружения уязвимостей в своем оборудовании, D-Link была оштрафована в январе 2017-го года после множества фактов атак через уязвимости в оборудовании этой компании, американская федеральная торговая комиссия (FTC) запустила соревнование Home Inspector Challenge для выявления проблем с ИБ в IoT-оборудовании.

Учитывая такую неразбериху и многообразие стандартов и сфер применения Интернета вещей сегодня сложно говорить о некоем унифицированном подходе к его безопасности. Разве что сетевой уровень у всех устройств один и тот же и базируется на стеке протоколов TCP/IP, что позволяет начать выстраивать систему защиту IoT именно с этого уровня.

Рисунок 7. Уровни Интернета вещей

Давайте попробуем рассмотреть элементе системы защиты современной Интернет-вещи на примере… умных фонарей, которые сегодня устанавливают не только продвинутые ИТ-компании или университеты в своих кампусах, но и городские администрации, активно внедряющие концепцию умных городов в своих владениях.

Что представляет из себя такой «умный» фонарь? Это просто кишащее различными сенсорами и датчиками устройство, подключенное к корпоративной или ведомственной сети, раздающее Wi-Fi, обрабатывающее персональные данные (иногда и биометрические) и активно общающееся с Интернет и различными облачными сервисами. Вроде бы обычный фонарь, а вроде бы и элемент Интернета вещей. Вроде бы и не сервер с важными данными, и пользователей у фонаря нет, а защиты требует не меньше.

Рисунок 8. Умный фонарь и его компоненты

Начать защиту фонаря, как и любого устройства Интернета вещей, необходимо с четкого определения, куда ему можно подключаться, а куда нет. Особую пикантность этой задаче придет тот факт, что фонарь содержит несколько разных сенсоров, которые передают данные в разные системы – локальные и облачные – сейсмодатчики, датчики дождя, интерком, датчик движения, цифровые вывески и т.п. И из разных систем в фонарь динамически поступают данные, например, из систем управления чрезвычайными ситуациями (в громкоговоритель), из службы безопасности (в интерком) и других. А еще через фонарь находящиеся рядом люди могут получить беспроводной доступ к разным участкам корпоративной сети – работники к внутренним ресурсам, вышедшие покурить гости – только к Интернет. Мы специально взяли в качестве примера столь многофункциональное устройство, чтобы показать особенности и направления обеспечения их ИБ. В реальной жизни большинство Интернет-вещей все-таки имеют одну, максимум, две функции и поэтому их защита будет чуть проще. Но в любом случае нам надо будет ответить на вопрос, что это за IoT-устройство, куда оно может подключаться и что может к нему подключаться. Ответы на эти вопросы лежат в привычной нам плоскости сетевой безопасности.

Пытаться решить задачу контроля такой разнообразной инфраструктуры в лоб, прописывая правила на каждом инфраструктурном устройстве (точке доступа, коммутаторе или маршрутизаторе) по принципу “узлу А разрешить доступ к узлу Б”, можно, но уже на 10-м устройстве мы поймем, что погорячились. Это не только займет время на прописывание и проверку списков контроля доступа, но и снизит производительность сетевых устройств, которые будут вынуждены проверять каждый пришедший фрейм или пакет на соответствие спискам контроля доступа (ACL). А если вспомнить еще про мобильность многих устройств IoT, которые могут находиться в разных местах корпоративной сети или

за ее пределами (и все это в течение одного дня), то задание статических правил не только неэффективно, но и невозможно. В конечном итоге все правила превратятся в классическое “всем разрешено все и всюду”, которое явно не является примером того, к чему стоит стремиться. В итоге мы приходим к контекстной политике доступа, которая опирается не на один атрибут (кто/что), а учитывает множество факторов, отвечающих на следующие вопросы:

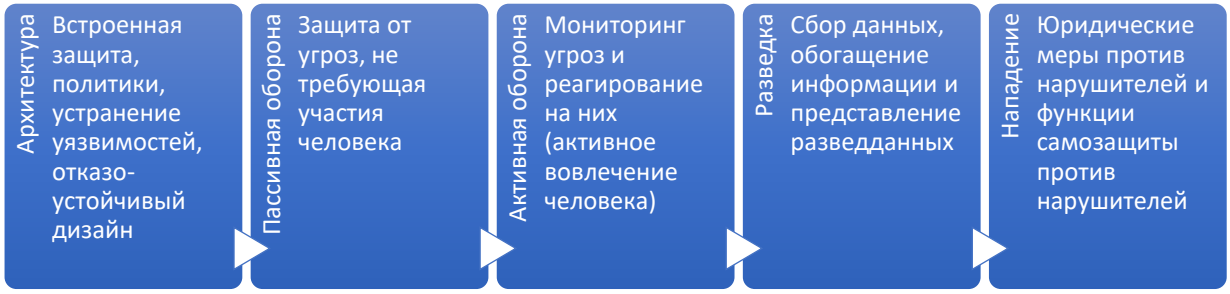
- **КТО** подключается?
- **ЧТО** подключается?
- **КАК** осуществляется подключение?
- **ГДЕ** находится подключаемые IoT-устройство?
- **ОТКУДА** осуществляется доступ?
- **КОГДА** осуществляется доступа?
- **КАКИЕ УСЛОВИЯ** должны быть соблюдены для предоставления доступа?

Кто? Известные пользователи (Сотрудники, продавцы, HR) Неизвестные пользователи (Гости)	**Что?** Идентификатор устройства Классификация устройств (профиль) Состояние устройства (posture)	**Как?** Проводное подключение Беспроводное подключение VPN-подключение
Где / куда / откуда? Географическое местоположение Департамент / отдел SSID / Порт коммутатора	**Когда?** Дата Время	**Другие?** Пользовательские атрибуты Статус устройства / пользователя Используемые приложения

Рисунок 9. Элементы политики контроля доступа Интернета вещей

На самом деле, если посмотреть на эти вопросы более внимательно, то мы поймем, что они же будут применены и к контролю пользователей, а не только устройств Интернета вещей. И это правильно. Не зря многие технологии кибербезопасности сегодня оперируют не понятием «пользователь» или «устройство», а понятием «сущность» или «субъект доступа», что позволяет выстраивать единые политики ИБ, независимо от того, кого или что мы хотим контролировать и защищать. И подтолкнул нас к этому именно Интернет вещей.

Контроль доступа IoT – это только один из элементов защиты, который может и должен быть расширен в рамках одного из 5 последовательных сценариев, позволяющих наращивать защитный потенциал в зависимости от задач стороны защиты и разработанной модели угроз.



Первый сценарий подразумевает правильную архитектуру, то есть базис для системы защиты, частью которого как раз и будет контроль доступа. В случае с Интернетом вещей сюда также попадает сегментирование, управление цепочками поставок оборудования и запчастей, поддержка, устранение уязвимостей, управление патчами и обновлениями и т.п. (разумеется, в тех случаях, когда устройство IoT все это допускает). Т.е. и к защите-то это даже не всегда относится - это именно основа, задающая тон всем последующим сценариям. Обратите внимание, что это наименее затратный, но при этом наиболее эффективный защитный сценарий, который задействует встроенные механизмы ИБ на уровне сетевой инфраструктуры (сегментирование, 802.1x или Port Security, VLAN и т.п.), уровне СУБД, операционных систем и приложений Интернета вещей.

Второй сценарий начинает использовать традиционные средства защиты, но в пассивном режиме. Пассивной защита называется потому, что не требует, ну или почти не требует, постоянного участия человека в процессе защиты. По сути, речь идет об установке различных средств защиты, которые работают в соответствии с заданными, зачастую статическими политиками. К числу таких средств защиты относятся классические межсетевые экраны, системы обнаружения атак, антивирусы, системы контроля доступа (NAC), системы защиты оконечных устройств, например, серверов управления IoT. Разумеется, речь идет не об офисных решениях, а понимающих специфику IoT-инфраструктур – их протоколы, количество IoT-устройств, измеряемых десятками и сотнями тысяч, работу в агрессивных средах, требования по временным задержкам и т.п.

Вернемся к фонарю. Чем он отличается от персонального компьютера, ноутбука или смартфона? Тем, что на него нельзя поставить антивирус или иное средство защиты. Да и от производителя его начинки сложно ожидать, что он будет заботиться о безопасности и внедрять в фонарь механизмы защиты. По крайней мере на этапе завоевания рынка это обычно не бывает – производители, как мы уже упомянули выше, заинтересованы в скорейшем завоевании доли рынка, а не в увеличении времени на разработку и тестирование. Как же быть в такой ситуации? Как защитить то, что нельзя защитить?

В пору вспомнить про социальную рекламу «Если человека нельзя вылечить, это не значит, что ему нельзя помочь». С фонарем, как и любым иным IoT-устройством, ситуация схожая. Если нельзя поставить средство защиты на него, то надо возвести неприступную стену вокруг него. Эту задачу решают системы контроля сетевого доступа, решающие упомянутые выше задачи. Но стена стеной, но даже в них бывают прорехи. Поэтому наша задача заключается в мониторинге происходящего с фонарем и обнаружении следов хакерской или аномальной деятельности. И ту нам на помощь приходит новая технология, ранее не находящаяся в шорт-листе специалистов по ИБ. Речь идет об обнаружении сетевых аномалий. Данные решения работают по знакомому многим ИТ-специалистам принципу – собирают телеметрию NetFlow (или sFlow, IPFIX, NetStream) с имеющегося сетевого оборудования – коммутаторов, маршрутизаторов, точек беспроводного доступа (а даже фонарь, подключенный к Интернет, не может миновать этих устройств), и накладывают на них специальные алгоритмы, призванные искать в собранной телеметрии следы несанкционированной деятельности, обнаружив которую можно дать команду средствам контроля сетевого доступа купировать угрозу, не давая ей распространяться по внутренней сети предприятия. Ведь часто угроза попадает в сеть минуя периметр и установленные на нем межсетевые экраны и системы предотвращения вторжения. Через точку доступа на фонаре любой гость может подключиться к внутренней сети и попробовать натворить плохих дел. Системы обнаружения аномалий превращают сетевую

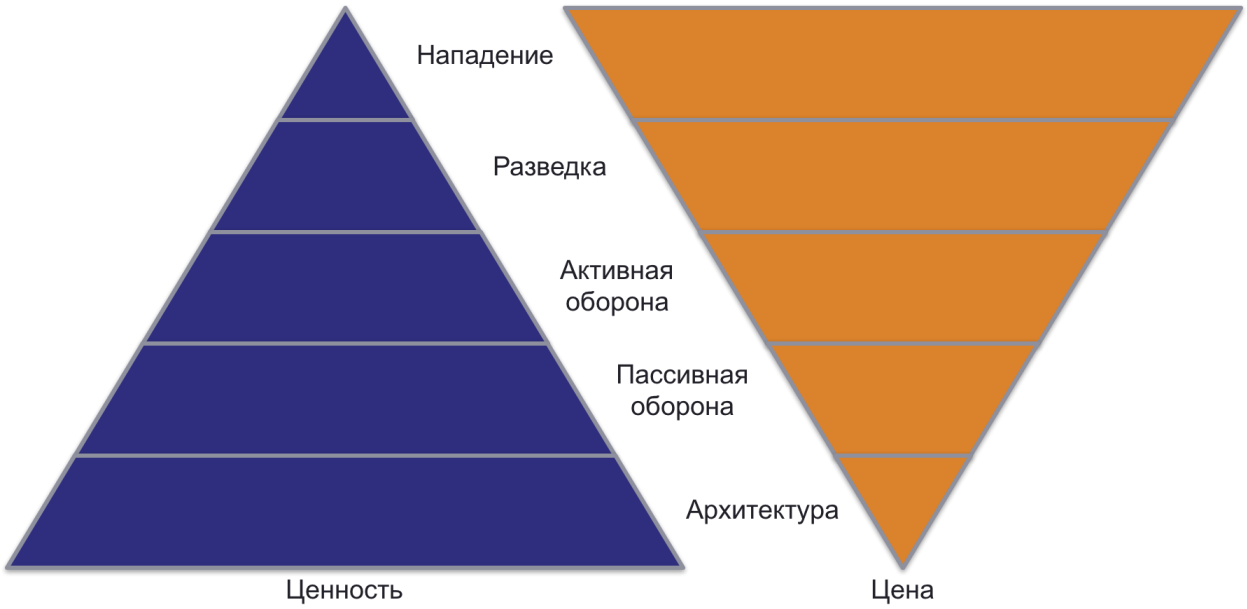
инфраструктуру в распределенную систему защиты, тем самым защищая сделанные инвестиции в сетевое оборудование, которое теперь не только передает трафик из точки А в точку Б, но и занимается его анализом и контролем; в тои числе анализируя и трафик от фонаря и других Интернет-вещей.

Аналогичную задачу, но уже в Интернет (например, для IoT-устройств, подключенных через сети 5G или Wi-Fi 6, развернутый оператором городского Wi-Fi), решают системы мониторинга DNS-трафика, который по статистике используется 93% вредоносных программ для скрытия своей активности – загрузки новых модулей и обновлений, получении команд от управляющих серверов, утечки украденной информации. Как мониторить IoT-устройства, не находящиеся под сенью средств защиты периметра? DNS является по сути единственным источником информации, который можно и нужно взять под контроль.

Переходя от разграничения доступа к мониторингу, мы реализуем следующий сценарий, который подразумевает активное вовлечение человека в процесс защиты. Именно на этом уровне начинается проведение пентестов инфраструктуры Интернета вещей, внедрение систем мониторинга аномальной активности, систем управления логами и другого инструментария для управления инцидентами, подразумевающего непрерывное участие высококвалифицированного персонала, который способен обнаруживать то, что пропускается традиционными средствами сетевой безопасности. Сюда же относится и анализ вредоносного кода. Иными словами, к инструментам второго уровня добавляется аналитика и активное вовлечение человека.

Четвертый сценарий (хотя грань между 3-и м 4-м достаточно условна) подразумевает высший пилотаж - выстраивание процессов Threat Intelligence и Threat Hunting, в рамках которого разрозненные следы несанкционированной активности, обнаруженные на предыдущем этапе, аккумулируются в индикаторах компрометации (IoC), в бюллетенях и отчетах об угрозах, в формализованном описании угроз, которые можно распространять широкой общественности, в том числе и в рамках специально созданных центров распределения информации об угрозах (ISAC, CERT, CSIRT или ГосСОПКА).

Пятый сценарий отражает получающую большее распространение сдвиг от оборонительной тактике к наступательной. Обычно на этом этапе идентифицируются не просто атаки, а уже сами атакующие, против которых затем реализуются различные действия – возбуждение уголовного преследования, перехват управления командными серверами C&C, разделегирование вредоносных доменов и т.п. Это нечастый сценарий, который применяется скорее на государственном уровне или монополистами, имеющими соответствующие возможности и ресурсы для нападения на атакующих.



Очевидно, что чем дальше от первого сценария мы отходим, тем больше ресурсов (временных, людских, финансовых) нам требуется для защиты Интернета вещей (на самом деле и защита корпоративной сети будет подчиняться тем же правилам). При этом уровень защитных возможностей будет возрастать непропорционально сделанным затратам. Надо ли всем стремиться попасть реализовывать самый последний, или хотя бы предпоследний сценарий обеспечения ИБ Интернета вещей? К счастью, нет. Многие, закрепившись на втором уровне, так на нем и остаются, не сталкиваясь с потребностью идти дальше. Им не нужны никакие SOCи, CSIRTы и другие аналитические подразделения. Им не нужны посменно работающие группы аналитиков и специалистов, реагирующих на инциденты. Их устраивает автоматическая защита, даруемая межсетевыми экранами, системами обнаружения вторжений и антивирусами, а то и встроенными в IoT-устройства возможностями. А все почему? Да потому, что они не сталкиваются с угрозами, требующими серьезной аналитики и присутствия человека. Иными словами, они борются с традиционными нарушителями, не относящимися к иностранным спецслужбам или кибертеррористам.

Поэтому сегодня сценарий пассивной ИБ - это как раз удел большинства предприятий, внедряющих Интернет вещей, не сталкивающихся с целенаправленными угрозами. Зачем им тогда тратить деньги на избыточный и редко используемый на практике сервис? А вот для крупных корпораций, военных и ряда государственных структур, использующих системы потребительского или промышленного Интернета вещей, одними только, пусть и популярными и разрекламированными, средствами защиты не обойтись. Нужны еще инструменты для непрерывного мониторинга и люди, способные правильно пользоваться этими инструментами. Или, как вариант, в условиях нехватки квалифицированного персонала возможно переложить эту задачу на внешних подрядчиков.

По существующим оценкам до 60% организаций сегодня реализуют в той или иной степени детальности первый, архитектурный сценарий (при этом в своих офисных сегментах такие организации вполне возможно реализуют уже третий, а то и четвертый сценарии). Еще 30% осуществляют переход ко второму сценарию, внедряя специализированные, но все еще пассивные средства защиты Интернета вещей. И только единицы начинают присматривать для своих IoT-инфраструктур третий и четвертый описанные сценарии. Однако рост числа

специализированного вредосного кода и атак (Stuxnet, BlackEnergy, Havex, Crash Override, Mirai, Amnesia и т.п.) должно изменить эти пропорции в самое ближайшее время.

Большие данные

Объем появляющихся и требующих обработки данных сегодня катастрофически растет и можно предположить, что рост проектов по цифровой трансформации только усилит этот рост, превратив его в экспоненциальный. Это приводит многие предприятия к мысли о смене парадигмы хранения и обработки данных, которые уже далеко не всегда сосредотачиваются в реляционных базах данных, расположенных в корпоративных центрах обработки данных. Современные технологии, среди которых искусственный интеллект, 5G, Интернет вещей и многие другие, уже не ограничены работой только со структурированными данными, сосредоточенными в одном месте. Сегодня вполне обычной становится практикой применения наряду с традиционными СУБД Oracle, Teradata или IBM, систем на базе Hadoop или SAP HANA, хранения их в различных облаках, а обработки как в них или централизованных хранилищах, так и в рамках распределенных инфраструктур, а также на пользовательских устройствах в рамках туманных вычислений. Все это можно назвать концепцией Больших данных (Big Data), которая не может быть реализована в рамках какого-то одного продукта или производителя. Иными словами, Большие данные – это высокопроизводительные, высокоскоростные и разнообразные информационные активы, которые требуют экономически эффективных, инновационных форм обработки информации для расширения понимания и оперативного принятия решений.

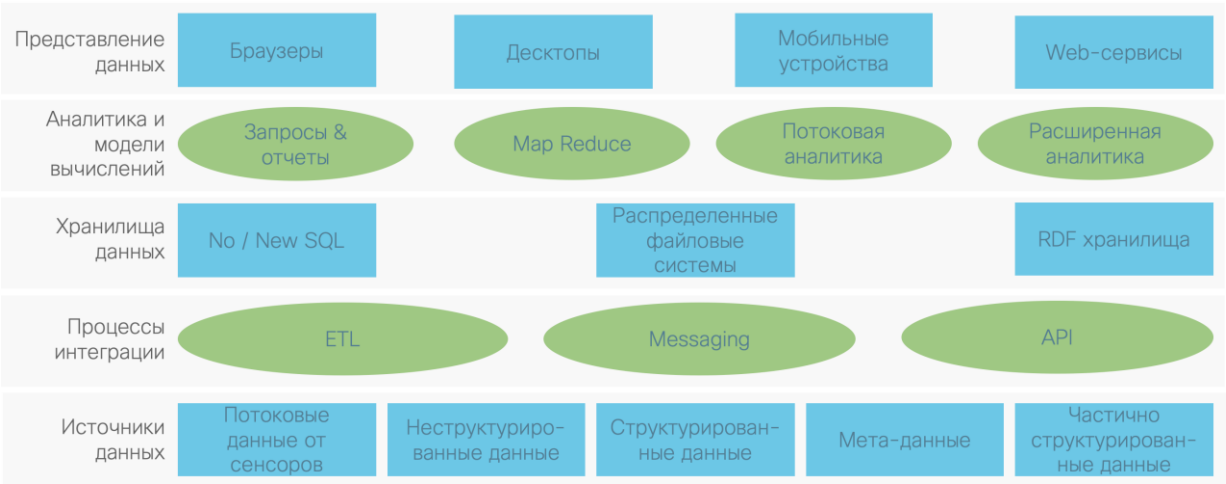


Рисунок 10. Архитектура Больших данных

Кстати, Большие данные могут быть использованы и для целей кибербезопасности, например, в таких приложениях как обнаружение аномалий, обнаружение мошенничества и др., но это выходит за рамки данной главы.

Риски ИБ для Больших данных

Учитывая, что Большие данные – это не один продукт или технология, а совокупность совершенно разных элементов, включающих себя и различные типы хранилищ данных, и способы их представления или обработки, разнообразные источники и форматы данных, а также способы коммуникаций и взаимодействия между ними, составить модель угроз для них достаточно непросто. В реальных проектах обычно такая модель угроз создается

исходя из конкретных используемых решений. Но если все-таки попробовать сгруппировать все угрозы для Больших данных, то можно выделить 5 групп:

- Прослушка / перехват / кража данных
- Повреждение / потеря данных
- Злоупотребления
- Юридические угрозы
- Организационные угрозы.

В каждой из категорий может своя дополнительная классификация и таксономия угроз, привязанные к уровням архитектуры Больших данных. Например, утечка данных может произойти как в их хранилище, так и в процессе передачи, а последняя, в свою очередь, может произойти как в рамках доступа по API, так и в рамках передачи по протоколу HTTP. Вредоносный же код может воздействовать как на устройства сбора данных или системы управления базами данных, так и привести к простою инфраструктуры обработки или представления данных. Таким образом, учитывая количество уровней и компонентов архитектуры Больших данных (а также взаимосвязей между ними), становится понятным, почему так сложно разработать целостную модель угроз для этой концепции. Одна из попыток это сделать была предпринята Европейским агентством по сетевой и информационной безопасности ENISA, которое выпустило серию из нескольких документов, посвященных безопасности Больших данных, и один из них был посвящен именно модели угроз, фрагмент которой (сам документ содержит более 60 страниц) представлен ниже.

Прослушка / перехват / кража	Юридические	Организационные	Повреждение / потеря	Злоупотребления
«Человек посередине»	Утечка данных	Нехватка компетенций	Уничтожение записей	Нелицензионное ПО
Утечка через Web API	Нарушение контрактных обязательств	Банкротство третьей стороны	Потеря устройств	Социальный инжиниринг
Кража носителя	Интеллектуальная собственность	Неверные бизнес-процессы	Потеря у третьей стороны	Вредоносный код
	Персональные данные		Фальшивые данные	Целевые атаки
	Запрос спецслужб		Результат пентеста	Кража Identity

Рисунок 11. Фрагмент модели угроз Большим данным

Риски ИБ от Больших данных

Основным риском от обработки Больших данных сегодня считается нарушение приватности. Государства и крупный бизнес все чаще собирает данные о своих гражданах и пользователях, об их поведении и используемых ими сервисах и продуктах. Несоблюдение мер защиты собранной информации будет приводить к утечками, которые уже сейчас становятся проблемой номер 1 в информационной безопасности.

Рекомендации по ИБ

Понимая всю сложность очерчивания границ Больших данных и многообразие угроз для них, становится понятным и вся сложность с обеспечением их безопасности, которая сопровождается множеством пока еще нерешенных сложностей, среди которых:

1. Распределенная инфраструктура. Хорошим и популярным примером такой инфраструктуры является Hadoop, который изначально разрабатывался для управления большими объемами данных в доверенной среде. Поэтому безопасность не стояла на повестке дня у разработчиков Hadoop и очень долгое время в нем не было никаких серьезных механизмов защиты, а существующие были по умолчанию отключены.
2. Нереляционные хранение. Схожая картина с NoSQL базами данных, которые не имеют достаточного арсенала защитных возможностей, которые обычно реализуются через промежуточное ПО (middleware).
3. Хранилища. В концепции Больших данных хранение может осуществляться на разных уровнях архитектуры, что определяется требованиями бизнеса и производительности. Высокоприоритетные данные могут храниться во флеш-хранилищах, в то время как редкоиспользуемые данные могут по-прежнему располагаться на жестких дисках или иных типах накопителей. Таким образом, при организации Больших данных придется реализовывать не одноуровневую, а многоуровневую защиту и выбирать соответствующие уровням хранения технологии. Например, шифрование флеш-накопителей не должно быть медленнее скорости чтения/записи, что может быть непросто реализовать, если ограничиваться только решениями на базе отечественной криптографии.
4. Большие скорости. Этот атрибут Больших данных также накладывает свой отпечаток на обеспечение их безопасности, так как сегодня многие средства защиты являются не встроенными, а наложенными – на сети, на базы данных, на пользовательские компьютеры, на сервера, на облака и т.п. Любое такое решение вносит задержки, которые могут быть критическими для обработки Больших данных.
5. Оконечные устройства. Так как Большие данные распределены по большому числу оконечных устройств, то необходимо быть уверенными в подлинности и отсутствии компрометации таких устройств, что очень остро ставит вопрос об аутентификации компонентов инфраструктуры Больших данных.
6. Достоверность данных. Напрямую с предыдущим вопросом связана и самая «больная тема» современной науки о данных – их достоверность. Подмена источника данных или внесение изменений в сами данные в процессе их сбора или передачи могут поставить под сомнение всю концепцию Больших данных. Поэтому так важно иметь метаданные («данные о данных»), которые, сопровождая основные данные, помогают определить и определенным образом гарантировать их происхождение. И анализ этих метаданных должен происходить на очень высоких скоростях, чтобы в реальном времени выявлять любые нарушения. В противном случае высока вероятность принятия решений на неверных данных, что может повлечь за собой различные негативные последствия.
7. Контроль доступа. Как и в обычных ИТ-решениях контроль доступа является основой основ информационной безопасности, так как мы должны быть уверены в тех, кто получает доступ к Большим данным, их компонентам, и результатам работы с ними. Учитывая множество уровней архитектуры Больших данных и зоопарк производителей решений для них, создание унифицированной и сквозной политики контроля доступа становится очень непростой задачей.
8. Мониторинг безопасности. Сегодня стало модным строить центры мониторинга и реагирования на инциденты ИБ, которые консолидируют миллионы и миллиарды

ежедневно получаемых событий безопасности, по которым делается вывод о наличии или отсутствии вмешательств в работу корпоративной или ведомственной инфраструктуры (часто такой мониторинг сам по себе построен на базе Больших данных). Но, как правило, такой мониторинг ограничен периметром, рабочими станциями пользователей, сетевым оборудованием и ключевыми серверами, расположенными внутри ЦОДа. Мониторинг облачных сред уже является непростой задачей для многих служб кибербезопасности. А уж мониторинг кибербезопасности распределенной инфраструктуры Больших данных тем более.

9. Интеллектуальный анализ данных (data mining). Это сердце любого проекта по Большим данным, которое позволяет выявлять зависимости и закономерности, на базе которых бизнес принимает управленческие решения. Поэтому так важно обеспечивать не только защиту алгоритмов интеллектуального анализа данных от внесения несанкционированных изменений или кражи (да, сами алгоритмы могут представлять собой интеллектуальную собственность и интерес для конкурентов), но и контролировать доступ к результатам этого анализа. Учитывая, что решения Data Mining – это обычно еще один уровень архитектуры Больших данных со своими технологиями и программными решениями, появляется еще одна, не всегда интегрируемая с другими, задача обеспечения безопасности.

Надо признать, что сегодня отсутствует целостное решение для защиты Больших данных и в каждом конкретном случае приходится строить свою собственную систему обеспечения их кибербезопасности, что является нетривиальной задачей; особенно в отсутствие квалификации у многих специалистов по ИБ, ранее несталкивавшихся с описанными выше проблемами. Кроме того, многие из современных решений ИБ изначально разрабатывались для совершенно иных задач и архитектур и не предназначены для защиты распределенной многоуровневой инфраструктуры, на которой построены Большие данные. Поэтому сегодня защита Больших данных строится преимущественно на встроенных в отдельные компоненты механизмах или специализированных надстройках, разработанными обычно теми же производителями, что и основное решение. Например, для защиты Hadoop можно задействовать как не очень богатые, но все-таки существующие механизмы типа контроля доступа к файлам, прозрачное шифрование, разделение на зоны безопасности, а можно воспользоваться надстройкой Apache Accumulo, представляющей более высокий уровень защиты данных.

Где-то, например, при мониторинге инцидентов ИБ, можно использовать уже известные решения (те же SIEM-платформы для сбора и обработки событий безопасности). Как было уже сказано выше, Большие данные сегодня – это множество разных технологий, в том числе и описанных ранее в этой главе. Поэтому рекомендации по защите Интернета вещей или облачных вычислений подойдут и для Больших данных. Но в каких-то сферах работы с ними нам еще только предстоит узнавать о новых защитных решениях и технологиях. Например, гомоморфное шифрование, уже упомянутое в разделе про квантовые технологии. Оно может помочь не только сделать шифрование более стойким для квантовых компьютеров, но и помочь решить проблему конфиденциальности в Больших данных, так как оно позволяет осуществлять обработку зашифрованных данных без их раскрытия. К сожалению, сегодня существует проблема с производительностью таких решений, непозволяющая применять их в практической деятельности.

Что же касается нейтрализации рисков нарушения приватности при работе с Большими данными, то на каждом этапе жизненного цикла данных (от сбора до использования)

необходимо, с помощью организационных или технических мер, реализовывать следующие ключевые принципы – минимизация, агрегирование, скрытие, информирование, разделение и контроль.

	Этап жизненного цикла	**Ключевой принцип**	**Реализация**
1	Сбор данных	Минимизация	Сбор нужного / удаление ненужного
		Агрегирование	Локальная анонимизация / обезличивание
		Скрытие	Антитрекинг, шифрование, маскирование, защищенная передача
		Информирование	Уведомление пользователей
		Контроль	Механизмы выражения согласия, персональное хранилище и т.д.
2	Анализ данных	Агрегирование	Анонимизация / обезличивание
		Скрытие	Гомоморфное шифрование, анализ при сохранении приватности
3	Хранение данных	Скрытие	Шифрование, AAA и др.
		Разделение	Распределенное / децентрализованное хранилище
4	Использование данных	Агрегирование	Анонимизация / обезличивание, анализ качества и происхождения данных
5	Все этапы	Защита / Демонстрация	Автоматические политики, их внедрение, и оценка соответствия

У Больших данных большое будущее, так как общепризнанным является факт наличия серьезных перспектив у умной аналитики, построенной на большом объеме структурированных и неструктурированных данных, получаемых из разных источников. А это значит, что число проектов Больших данных будет только расти, как и число атак на них, что потребует более внимательно относиться к сохранности и приватности данных.

Нормативное регулирование

В России на момент написания данной главы отсутствовало нормативное регулирование Больших данных, хотя отдельные регуляторы, например, Роскомнадзор, считает вполне допустимым применять требования законодательства «О персональных данных» к рассматриваемой области. Однако ввиду того, что очень часто Большие данные имеют дело с обезличенной информацией, на которую закон «О персональных данных» не

распространяется, предпринимаются различные попытки кодифицировать работу с Большими данными. В частности, существует не менее двух законопроектов, продвигаемых различными ассоциациями и объединениями так называемых операторов Больших данных, которые могут быть внесены в Государственную думу и приняты в качестве федеральных законов. Также есть законопроект, который вносит поправку в закон «О персональных данных», которая позволяет с его помощью регулировать процесс обезличивания и обработку обезличенных данных, которые и могут быть отнесены к Большим данным. Если соответствующие поправки будут приняты, то организации, имеющие дело с Большими данными, получат нормы регулирования, схожие с теми, которые в России применяются к персональным данным. Среди них – регистрация в качестве оператора Больших данных, получение согласия на обработку обезличенных данных и т.п. Требований по технической защите Больших данных в России пока нет и нам неизвестно о планах по их разработке.

С другой стороны, многие эксперты утверждают, что применение к Большим данным норм законодательства о данных персональных приведет к невозможности применения Больших данных в деятельности бизнеса и государства. Поэтому, как было сказано в разделе про искусственный интеллект, Минэкономразвития разработало законопроект, который позволит лицам, занимающимся разработкой и внедрением цифровых инноваций, включая и Большие данные, осуществить их практическое применение и проверить их полезность в условиях отказа от ограничений, установленных нормативными правовыми актами, без риска их нарушения.