Инновации устройств IoT, беспилотных моделей в проблематике безопасности обмена данными. Обзор

Галина Морозоватая

По прогнозам аналитической компании IDC, в 2025 году количество пользователей Интернета вещей превысит численность населения планеты Земля на 80 миллиардов подключённых устройств. Большая часть пользователей применяет их в быту; варианты новейших устройств бесконечно разнообразны: позволяют не только прогнозировать сны, дистанционно управлять процессами жизнедеятельности человека, но даже отслеживать температуру тела коровы в хлеву фермера. Воплощённые инновационные идеи сокращают затраты времени на контроль параметров, однако по тем же причинам возникает проблема безопасности, рисков утечки конфиденциальной информации через протоколы обмена данными. В статье рассматриваются варианты аутентификации IoT в интеллектуальной сетевой архитектуре и авторизации (разрешения взаимодействия) для повышения информационной безопасности.

Интернет вещей и не только

Термин «Интернет вещей» (Internet of Things, IoT) означает совокупность объектов с электронным приводом и адаптером, подключённых к Интернету и обменивающихся цифровыми данными; впервые был использован в 1985 году. В наше время Интернет вещей представляет собой инструментарий, программируемый посредством приложений с возможностью передачи данных не только через Интернет, но и через другие сети, включая «домашние»: локальные и даже нейросети, как частный случай методов распознавания образов, дискриминантного анализа. Между тем обучение нейронных сетей – это многопараметрическая задача нелинейной оптимизации и перспективное направление в структурном подходе (моделировании) естественного интеллекта с помощью компьютерных алгоритмов. Нейронные сети не программируются в привычном смысле этого слова, они обучаются. Возможность обучения – одно из главных преимуществ нейронных сетей перед традиционными алгоритмами. На рис. 1 представлен схематичный вид «ежедневных» взаимосвязанных объектов в системе «Умный дом».

Рис. 1. Схематичный вид «ежедневных» взаимосвязанных объектов в системе «Умный дом»

По доступной статистике, на конец 2022 года в мире насчитывается более 20 млрд устройств IoT. Оборудование поистине разностороннее: датчики, в том числе окружающей среды, приводы, гаджеты, устройства или машины, встроенные в мобильные устройства, промышленное оборудование для разных сфер высокотехнологичной деятельности, включая медицинскую. Популяция устройств IoT, где буквально сталкиваются физический и цифровой миры, экспоненциально растет. Устройства IoT созданы для обмена информацией, они повышают производительность труда и уровень комфорта в жизни. Из-за разнообразия системно интегрированных в сеть электронных устройств, их различных возможностей, мест и способов развёртывания возникает проблема безопасности сохранности данных, включая персональные. В то же время с развитием НТП совершенствуется переоценка биологической активности человеческого мозга. Несмотря на совершенствование интегральных технологий, искусственный интеллект (ИИ) пока не способен решать нелинейные и неформализованные задачи сопоставимо с человеком. Мозг человека и некоторых животных во многих случаях работает в разы эффективнее. Причина в качественных архитектурных различиях между электронным процессором и мозгом живых существ, при этом такое объяснение опирается на не изученные в полной мере возможности передачи информации в мозгу. Так или иначе, готового эффективного решения для создания идеальной искусственной нейронной сети всё ещё нет [2]. В той же публикации для сведения представлена структура искусственного нейрона.

В 2022 году московский студент написал и защитил диплом с помощью нейросети. Этот факт пока не означает, что типичная система высшего образования однозначно несостоятельна, но сие способствует модернизации цифровых технологий в образовательной

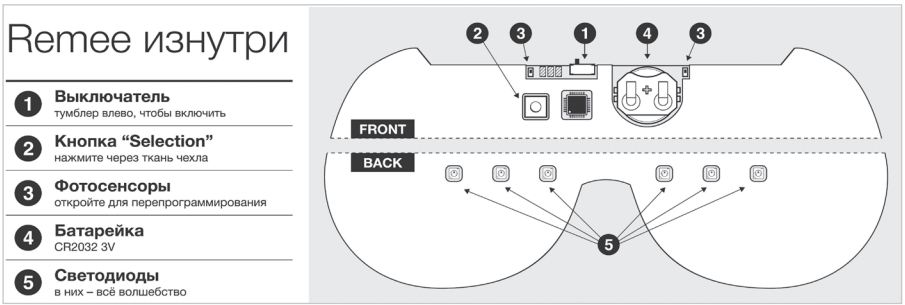

Рис. 2. Схематичная иллюстрация электронного устройства Remee – маски «Палантир» для релаксации

среде и инициирует исследования в области алгоритмов взаимодействия с нейросетью. Всё-таки много фактов свидетельствует о том, что за нейросетями будущее. Неслучайно ещё в октябре 2019 года президентом России принята «Национальная стратегия развития искусственного интеллекта на период до 2030 года».

Современное состояние и перспективы сетей

Предметы повседневного обихода в системе IoT, такие как «умные розетки», элементы освещения, замки, датчики движения, подключаются к глобальной сети и создают большой массив данных в объёмах, сопоставимых с сотнями зеттабайт, притом что 1 ЗБ эквивалентен 1 млрд ТБ или одному триллиону гигабайт. Только 1% данных, генерируемых при подключении к IoT, используется для обучения или прогнозирования [2]. Отсюда можно сделать три основополагающих вывода: есть большие перспективы развития направления, дальнейшего совершенствования ИИ, возможно появление ещё большего количества сетей на основе IoT, существует проблема утечек данных при несанкционированном доступе в сеть. Можно ли заявить об этом, как о новостной проблематике? Вряд ли. Интернет-сайты давно собирают сведения о пользователях посредством фиксации запросов и генерации файлов cookie. Ведущие компании – производители оборудования (к примеру, Samsung) собирают и анализируют агрегированные данные об интересах и предпочтениях пользователей смарт-телевизоров, затем ориентируются на них при разработке приложений, наполнении контентом своих сервисов, размещении рекламы, выбирая при этом лучшее время суток для её восприятия. К примеру, Fitbit, анализируя данные в облачном хранилище, полученные от браслета, знает, сколько и как тренируется пользователь оборудования, каков режим сна и состояние здоровья – всё это предполагает возможности опосредованного влияния. По сути, речь идёт об анализе не только предпочтений и состояния физического здоровья, но и мыслей клиентов, то есть об определённом уровне контроля над ними или, по крайней мере, попытках установления такого контроля.

Элементы нейросети и майнд-машин, интегрированные в IoT

Мозг человека считается одним из наименее изученных органов, загадочная и непредсказуемая деятельность которого способна удивлять даже светлые умы планеты. Когда с развитием НТП и открытием магнитно-резонансной томографии появились новые возможности для изучения функциональности мозга, активности отдельных участков при выполнении разного вида деятельности, были разработаны совершенно уникальные электронные приборы по стимуляции мозга.

Использование приборов стимуляции мозга теперь применяют не только в медицинских целях, но и в качестве несертифицированных электронных устройств-помощников – в быту. В Москве магазин, реализующий «майнд-машины», постоянно работает с 2006 года и по сей день. Типичные примеры таких девайсов представлены ниже. Это направление связано с «киборгизацией» – разработкой и внедрением в жизнь людей новой технической реальности, включающей создание и функционирование кибернетических организмов и роботов-антропоидов с элементами ИИ. На основе изучения нейросетей предполагается улучшать память и способность к обучению, бороться с вредными привычками, бессонницей, поднимать настроение, делать отдых более качественным.

Прибор для осознанных сновидений представляется маской из мягких материалов, которая одевается на

Рис. 3. Внешний вид устройства «Доктор ТЭС-03» для транскраниальной электростимуляции мозга

глаза перед сном. Конструктивная схема устройства представлена на рис. 2. Прежде всего, это электронная система личностного развития и релаксации, предназначенная для самопознания и самосовершенствования, модели которой могут быть интегрированы в IoT. Данный тип электронных устройств не относится к медицинским приборам. Лечебно-восстановительные эффекты проявляются опосредованно, через активацию центральных нервных механизмов, регулирующих вегетативные функции, психическую и двигательную активности, эмоции и поведение через повышение неспецифической резистентности организма. Встроенный внутри маски электронный процессор имеет датчики, реагирующие на движение глаз в фазе быстрого сна, сигнализирующее о начале сновидений. Производитель сообщает, что полёт ваших фантазий и желаний не имеет границ. Вы можете реализовать все свои несбыточные мечты: полететь на Луну, подержать за руку известную личность, избавиться от страха высоты, стоя на краю пропасти, одним словом, делать всё, что невозможно в реальной жизни [3]. Маска «Палантир» предназначена для медитации с открытыми глазами. Помогает концентрации зрения и обеспечивает спокойный сон – вплоть до глубокой медитации и ауто-психокоррекции [5].

Устройство «Доктор ТЭС-03», представленное на рис. 3, – прибор для

Рис. 4. Электронное устройство DreamStalker Ultra

транскраниальной электростимуляции мозга. Частота тревожных сновидений линейно и статистически связана с риском снижения когнитивного восприятия среди взрослых и людей среднего возраста, а также с риском деменции. Причём деменция – не первое заболевание, на которое могут указывать кошмарные сновидения. Связь тревожных снов с болезнью Паркинсона установлена давно. Приблизительно 5% взрослых испытывают кошмары еженедельно, а еще 12–40% ежемесячно. Эффект устройства основан на взаимодействии нейронов (мозга) под воздействием слабой стимуляции электрическим током. Разработчики предложили решение в виде нейроинтерфейсов (интерфейс «мозг–компьютер») – происходит обмен информацией между мозгом и внешним устройством: ПК, смартфоном, экзоскелетом, бытовыми приборами, инвалидной коляской или даже искусственными органами чувств. Все эти устройства конфигурируются в системе IoT.

Ночной сон человека делится на циклы длительностью примерно 90 минут каждый. Каждый цикл подразделяется на фазы. В первом цикле сна фаза со сновидениями длится всего несколько минут. С каждым последующим циклом её длительность возрастает. Длительность глубокого БДГ-сна, наоборот, уменьшается с каждым циклом. Программируя последовательность бесконтактного воздействия на нейроны мозга, можно регулировать продолжительность сна и влиять на сновидения. Подробнее об этом изложено в [3].

По мере старения организма относительная доля глубокого сна и сна со сновидениями уменьшается. Так, возрастные изменения приводят к появлению чувства «недосыпания» и сонливости в дневное время. В улучшении самочувствия может помочь «генератор сна» с оригинальным музыкальным сопровождением (посредством стереонаушников) по технологии бинауральных ритмов и фазированного «розового шума». Технология аудиовизуальной стимуляции помогает контролировать психоэмоциональное состояние без медикаментов, без воздействия посторонних установок и внушений и без формирования зависимости. Таковы технические средства с условно новыми возможностями, значительно расширившимися с интеграцией в систему IoT.

Устройства полезны для улучшения памяти и интеллектуальных функций, повышения физической и умственной работоспособности, для активизации процессов обучения и творческих возможностей, коррекции психоэмоциональных состояний. Кроме того, помогают при реабилитации после тяжелых физических и эмоциональных нагрузок, коррекции психофизиологических состояний в спорте, нивелировании эффекта дисинхроноза при перелётах в другой часовой пояс. Опытные пользователи рекомендуют перед применением электронных приборов для релаксации на основе звуковых и световых эффектов, какими являются майнд-устройства, естественным образом выспаться в течение 4-5 часов, а затем применять девайс. Внешний вид устройства DreamStalker Ultra для осознанных сновидений представлен на рис. 4.

Аналоговые сигналы с датчика поступают на интегрированный АЦП микроконтроллера с разрядностью 12 бит. Увеличение разрядности АЦП даёт возможность более точно отслеживать малейшие изменения сигнала на входе, то есть качественно реагировать на состояние пользователя. Устройство имеет встроенный модуль Wi-Fi, работающий в режиме точки доступа. Управление настройками и функциями производится через интернет-браузер. Если сравнительно недавно аудио- и видеотехнологии использовались для создания информационно-развлекательных систем, то теперь разработчики РЭА уделяют внимание интерфейсам «человек–машина» и системам безопасности.

Проблемы безопасности сетей и связи самоуправляемых транспортных средств

Самоуправляемые транспортные средства – ещё одна область, реализация которой потребует совершенствования сетей связи нового поколения 5G и 6G. Электромобили оснащаются сенсорами, считывающими многофакторную информацию, в том числе о дорожной обстановке: ближайших транспортных средствах, погодных условиях, состоянии асфальта, дорожных знаках и др. Так, на новых автомобилях Tesla Motors устанавливают не менее 8 видеокамер, обеспечивающих обзор 360° на дистанции до 250 метров, и не менее 12 усовершенствованных ультразвуковых датчиков, определяющих объекты вокруг электромобиля и расстояния до них. Раньше та же фирма задействовала «автопилот», который «умел работать» при участии человека. Теперь на основе полученных данных управление поездкой можно осуществлять в автоматическом режиме. Создание полноценного беспилотного автомобиля, в том числе грузового, – один из самых захватывающих вызовов технологической мысли начала XXI века по всему миру.

В США появилась перспектива массового производства дорожных «беспилотников», которые могут обмениваться информацией друг с другом, с объектами дорожной инфраструктуры, их системы не обособлены. «Открытость» системы делает беспилотные электромобили уязвимыми для перехвата управления – та же проблема, что и в сетях IoT, но на ином уровне. В 2015 году через Интернет хакер вошел в систему управления автомобилем Jeep Cherokee и попытался управ-

Рис. 5. Беспилотный электромобиль фирмы Loxo

Рис. 6. Вид электрокара с открытым кузовным отсеком

лять им. После этого система обмена информацией, получившая название V2V (англ. «vehicle-to-vehicle» – «от средства к средству»), и её связь с GPS были усовершенствованы. Ещё 10 февраля 2016 года национальное управление по безопасности движения на автострадах США (англоязычная аббревиатура NHTSA) сообщило, что с точки зрения закона компьютер, управляющий автомобилем вместо человека, может считаться водителем [6]. Разумеется, это значительный шаг вперед в правовом поле и юридический прецедент.

А пока на дорогах Швейцарии представлен первый в Европе коммерческий беспилотник для доставки товаров из магазинов и почты. Он уже появился на дорогах и проходит испытания, но пока не сертифицирован. Внешний вид транспортного средства без водителя представлен на рис. 5.

Автономный шаттл интегрируется в IT-инфраструктуру компании-ретейлера, предлагает трансформируемый грузовой отсек и по габаритам подходит для разных задач. Конструкция реализована на дюралюминиевой платформе-скейтборде, оснащённой четырьмя ступичными электромоторами; без подзарядки проезжает до 110 километров. Самый быстрый дорожный «беспилотник» в Швейцарии способен одновременно доставлять 64 посылки общей массой 320 килограммов. Причём минимальная погрузочная высота в 0,4 метра облегчает доступ к отсеку для людей в инвалидных колясках [5]. Вместо датчиков-сенсоров с вращающейся частью электрокар использует комбинацию из радара, лидара, сонара, камеры и вычислительного алгоритма. Это даёт обзор 360° как шаттлу, так и дистанционно присматривающему за

Рис. 7. Иллюстрация полностью управляемого автономного режима электромобиля

ним оператору. Грузовой отсек «беспилотника» легко трансформировать под конкретные задачи. На внешнюю панель кузова выведены кнопки экстренной остановки (блокировки), которые важны на случай нештатных ситуаций. Такие шаттлы были замечены в конце 2022 года также в Эстонии.

Один из крупнейших разработчиков графических ускорителей и процессоров компания NVIDIA Corporation продемонстрировала возможности открытой платформы Driveworks Alpha 1 для беспилотных машин [6]. Платформа Driveworks Alpha 1 – это аппаратное и программное решение для разработчиков с целью конфигурирования сопутствующей РЭА для беспилотных ТС для качественного ориентирования на дороге и сверхбыстрого реагирования на изменение дорожной ситуации, причём ПО намерены обновлять каждые 2 месяца. Этим шагом, кроме совершенствования ПО, также достигается цель обеспечения защиты от несанкционированного дистанционного проникновения в систему связи шаттла и «центра». На основе перспективного решения разрабатываются автомобили Baidu, nuTonomy, Volvo, TomTom и даже автобусы WEpods. Основное же направление пока «грузовое»: доставка малогабаритных заказов из магазина, служб доставки, почты. На рис. 6 представлен вид электрокара с открытым кузовным отсеком.

Уязвимость интерфейса внешнего доступа

Тем не менее уязвимыми пока являются не только беспилотные гибридные и электромобили, но и традиционные автомобили с беспроводным интерфейсом доступа к ДВС (в том числе через ODBC-порт). Безопасность протоколов коммуникаций встроенного оборудования является актуальной проблемой как для разработчиков из России, так и для зарубежных. Многие из подобных транспортных средств используют аппаратное обеспечение: камеры, радары и лидарные датчики, способные поддерживать полностью автономное вождение. На рис. 7 представлена иллюстрация человека в кабине электромобиля, который «отдыхает» от управления.

Хотя прогноз обещает быстрый прирост числа автономных ТС, пока продажи беспилотных автомобилей остаются крайне низкими. Повсеместно ещё не приняты нормативные акты, позволяющие легально эксплуатировать автономные транспортные средства. Логично, что производители не готовы вкладывать большие средства в разработку моделей, которые не могут в обозримом будущем выйти на рынок. Ещё одним ограничивающим фактором является стоимость сенсорного оборудования. К 2026 году стоимость датчиков, необходимых для обеспечения автономного вождения, станет на 25% ниже, чем в 2022 году. Но и при таком снижении цена останется относительно высокой. Это означает, что в текущем десятилетии автономные функции будут доступны для автомобилей премиум-класса и транспортных средств, принадлежащих крупным автопаркам [6]. Так или иначе, проблемы безопасности в сетях связи и управления, будь то IoT или шифрованный сигнал для электромобиля с использованием GPS и сотовой связи, имеют общее начало.

Защита данных и аспекты безопасности конфигурации IoT

Если говорить об IoT даже небольшой домашней сети, создающей коллекцию устройств многоцелевой среды, задействованы принтеры, цифровые видеорегистраторы, IP-камеры и другие бытовые электронные устройства, в том числе с конфигурацией B2B. Рассмотрим потенциальные риски, связанные с управлением безопасностью устройств IoT. Защитник устройств AWS IoT упрощает аудит конфигураций, аутентификацию устройств, обнаружение аномалий и получение предупреждений для обеспечения стабильной работы. Поскольку устройства IoT подключены к глобальной сети, их можно «взломать», как и любое устройство с доступом к сети Интернет. Производители выпускают большое количество устройств IoT, чтобы не отставать от спроса, а безопасность продукта представляется второстепенной, заботой пользователя на манер сентенции «спасение утопающих – дело рук самих утопающих». В обиход введён специальный термин – «концентрация атаки», как сумма различных факторов, когда неавторизованный пользователь может получить доступ к данным. С одной стороны, минимум подключённых к IoT электронных устройств способствует их безопасности, и наоборот, увеличение количества устройств IoT означает, что риски несанкционированного доступа к информации расширяются с каждым новым устройством, подключённым к Интернету. Электронные устройства собирают и записывают в память, в том числе облачную, конфиденциальные данные, сохраняют доступ и обмениваются данными в потоковом режиме. По условной аналогии со сбором файлов cookie в Интернете получивший доступ к массивам имеет возможность «ознакомиться» со всем происходящим в офисе или доме. К примеру, доступ к принтеру позволит просмотреть всё, что было «отправлено на печать» или отсканировано в течение длительного времени. Сегодня для интернет-трафика популярен условно передовой протокол обмена данных IPv6, предлагающий пул 128-битных адресов для назначения устройствам. Это настолько огромный массив данных, что каждому атому на поверхности планеты Земля можно присвоить уникальный адрес, и притом останет-

ся 99% её неиспользованных возможностей. Пока всё работает, такая взаимосвязанность удобна. Но каждое из устройств является «точкой» входа в корпоративную сеть и потому – рисковый фактор. Несмотря на то что обработка данных в конфигурации IoT подпадает под действие «Общего регламента по защите данных» (GDPR), большинство производителей устройств IoT не продают продукты с высоким уровнем безопасности в формате «конфиденциальность по умолчанию», а ориентируются, прежде всего, на доступную и востребованную среду – «ширпотреб». За последние годы, по статистике, использование IoT-устройств в DDoS-атаках не уменьшается. На этом фоне «недостижимого Монблана» существуют решения для формирования стратегии безопасности данных IoT. Предлагается объединить IT-инфраструктуру (распределённую, неизменяемую или эфемерную конфигурацию) в единую частную сеть с тем, чтобы обеспечить безопасную связь между развёрнутыми устройствами IoT и инфраструктурой, которая контролирует (аккумулирует и хранит) полученные данные. Один из таких вариантов – OpenVPN Business VPN, Access Server в качестве решения для обеспечения безопасности Интернета вещей [1].

Риски IoT и сетей на их основе

Ещё одна проблема безопасности данных связана с уязвимостью бесключевого доступа через Bluetooth без проверки криптографических подписей на прошивке и на устройстве. Хакерам достаточно найти или получить данные для входа в учётную запись в Интернете. Если удаётся проникнуть в сеть и получить доступ к одному из её элементов (устройств), то злоумышленник получает доступ ко всем устройствам сети. Используя учётные данные, пройдя аутентификацию в сети, можно считывать видео с камер видеонаблюдения и получать доступ к сохранённым записям любого из клиентов в системе. В том числе осуществить несанкционированное изъятие персональных данных пользователей или организаций, переместив массив в облачное хранилище или на сервер, зарегистрированный даже в другом государстве. Закрыть же доступ к сети при попытках завладеть данными или DDoS-атаках с дефектом RCE OMIGOD не всегда возможно оперативно.

Методики защиты данных в IoT предполагают изменение (администрирование) учётных записей. Ещё в 2018 были году известны случаи, когда линейка маршрутизаторов D-Link поставлялась с закодированными учётными данными по умолчанию; зная это и обладая достаточной компетенцией, можно изменить прошивку и извлекать затем конфиденциальные данные из потока информации. Большинству устройств бытового назначения в системе IoT недостаёт сложности учётных данных по умолчанию, шифрования, двухфакторной аутентификации и надёжного восстановления пароля. Эти уязвимости в системе безопасности могут привести к тому, что хакеры получат лёгкий доступ к устройствам и корпоративным сетям – ситуация с повышенным риском, поскольку даже анонимный пользователь имеет возможность запустить JavaScript в пользовательской среде и выполнить произвольные команды в ОС маршрутизатора. Отсюда понятна необходимость регулярной смены

аутентификационных данных пользователем сети. Упрощённые программные проверки безопасности при входящих соединениях – ещё один рисковый фактор. Устройства, которые когда-то были безопасными, с развитием технологий становятся полностью уязвимыми для кибератак и утечек данных.

Отсутствие аутентификации при каждом доступе даёт преимущества потенциальным злоумышленникам, действующим в режиме активного мониторинга сети. Вместо этого необходима тройная аутентификация: кодирование сертификатов в обновлении прошивки и с функцией обновления ПО системы безопасности. С одной стороны, обновление является рисковым фактором, который пользователь не контролирует: мало ли куда могут уходить данные при активации нового обновления, но, с другой стороны, встроенные средства управления мобильными приложениями и защиты от вредоносного ПО предполагают поддержку производителя ПО с аналитикой в дистанционном формате угроз в режиме реального времени, а это мотивирующий экономический фактор для производителя, ибо он не заинтересован терять клиентов–потребителей. Таким образом, при отсутствии иных, лучших возможностей контроля трафика и рисковых факторов кражи данных уместно доверить это производителю ПО. А также озаботиться регулярной сменой оборудования раз в 2-3 года. А пока по статистике 5-6 наборов паролей позволяют онлайн-злоумышленникам получить доступ к 10% подключенных устройств IoT. 15% пользователей не меняют пароли устройств по умолчанию, отчего стал реальным сценарий, когда злоумышленник, оставаясь неизвестным, дистанционно через сеть управляет климат-контролем в офисе. В такой ситуации остаётся только радикальный выход: отключить конкретное устройство как от IoT сети, так и от питания электросети 230...240 В.

Проблемные вопросы интерфейса

Для улучшения кибербезопасности специалисты (OWASP) не рекомендуют применять устройства IoT без функции изменения «пароля по умолчанию». Даже если устройство не позволяет изменить пароль (Amazon Alexa, Google Hub), возможным решением станет усиление безопасности в точке подключения (маршрутизатор, модем). Используйте самый длинный пароль или парольную фразу, разрешённую системой паролей. С помощью мнемоники для запоминания сложных паролей применяют самые длинные из возможных паролей. К примеру, в «Книге рекордов Гиннесса» зарегистрировано самое длинное слово на финском языке – lentokonesuihkuturbiinimoottoriapumekaanikkoaliupseerioppilas, означающее ученика-помощника младшего офицера-механика по турбинам реактивных самолетов в силах обороны Финляндии. Почему бы не использовать нечто по аналогии? Если устройство не шифрует сообщения при отправке по сети к облачным службам, а при трансляции данных через Wi-Fi запускает HTTP-сервер (для приёма учётных данных в сеть), соединение посредством VPN улучшает безопасность. VPN с шифрованием трафика данных позволяют устанавливать безопасные удалённые сетевые подключения из любого места. Тогда авторизованные устройства IoT становятся безопасным элементом частной сети.

Выбор правильного протокола безопасности аутентификации и авторизации зависит от протокола связи, который сеть использует для идентификации ПК и защиты данных. Из основных известны три типа протоколов безопасности данных в системе IoT: распределённый односторонний, распределённый двухсторонней связи и централизованный по трёхстороннему подключению. Первый – для соединений между устройствами, которым требуется безопасность, но не постоянный мониторинг; как следует из названия, только одна сторона аутентифицирует себя для другой; способствует авторизации с помощью сохранённых сертификатов и удостоверений. Второй метод взаимной связи для коммерческой передачи конфиденциальных данных требует, чтобы устройства аутентифицировали друг друга посредством цифрового идентификатора перед обменом данными. Третий протокол – централизованное трёхстороннее подключение – устраняет задержку аутентификации за счёт регистрации устройств на центральном сервере; подходит для постоянно подключённых устройств или устройств доступа по требованию. Тут используется централизованный сервер или доверенное стороннее приложение, которое распространяет сертификаты аутентификации устройств IoT и управляет ими.

Большинство современных IoT-устройств обновляют ПО прошивки автоматически посредством беспроводных OTA-технологий. Это очень удобно, но одновременно является рисковым фактором безопасности сети. Чтобы уменьшить его влияние, рекомендуется осуществить резервное копирование устройств IoT перед обновлениями, предусмотрев процедуру восстановления в случае сбоя обновления. Наряду с отсутствием аутентификации и авторизации, слабым шифрованием и фильтрацией входных и выходных данных небезопасные сетевые службы являются проблемой как для предприятий, так и для частных сетей. Типичные и известные способы несанкционированного входа в сеть подразделяются:

- на Wardriving – поиск сетей Wi-Fi, в том числе дистанционно из припаркованного автомобиля, с ноутбука или мобильного устройства;
- Evil Twin Attacks – открытые точки доступа Wi-Fi, созданные хакером для доступа к сообщениям пользователей;
- Wireless Sniffing – использование программного или аппаратного обеспечения для прослушивания сообщений, передаваемых по беспроводной сети.

Из простых решений для противодействия несанкционированному доступу в сеть рекомендованы: ограничение доступа к сети для авторизованных пользователей путём фильтрации адресов управления доступом к среде (MAC); сокрытие уникального «имени» идентификатора набора услуг (SSID); применение двойного брандмауэра: один в беспроводной сети (на основе маршрутизатора или модема), второй на беспроводных устройствах (на основе хоста) практикуют для дополнительной защиты трафика и данных. Интерфейсы, конфигурированные в IoT: web-интерфейс, серверный API, облачное хранилище данных, мобильное устройство взаимодействуют. При обнаружении проблемы уязвимости в одном элементе системы она подвергается опасности целиком. Отсюда важно регулярное обновление ПО точки доступа.

Выводы. Перспективы сетей с IoT

Сфера продуктов, подключаемых к Интернету в режиме реального времени, будет значительно расширена в ближайшие годы. На промышленном уровне для снижения издержек внедряются интеллектуальные системы обеспечения жизнеобеспечения: освещения и регулирования мощности отопления, вентиляции, кондиционирования и охлаждения воздуха (ОВКВ). Подключённые в сеть камеры B2B для наблюдения в офисах, «умные замки», конфигурированные в СКУД с выходом на облачное хранилище, и многие другие при каждом подключении получают собственный IPv6-адрес. Но есть слабые стороны IoT, которые рекомендуется учитывать. Утечки данных, атаки программ-вымогателей и другие угрозы безопасности – ожидающая нас печальная действительность, если не подготовиться и не принять превентивных мер. Усиление защиты устройства – не один шаг или действие, а процесс. Процесс многофакторной защиты устройств уменьшает уязвимости, которые могут использовать хакеры на уровнях хоста, приложения, операционной системы и пользователя, причём каждый уровень требует уникального метода безопасности. Важен эффективный механизм идентификации устройства, когда серверы с помощью аутентификации отличают действующую точку IP- и MAC-адресов от несанкционированного. Уникальный идентификатор каждого устройства IoT позволяет отслеживать его постоянно для защиты сети. Так, можно удалённо проверить устройство, используя инфраструктуру открытого ключа (PKI), связать устройства с сертификатами «открытого ключа» от центров сертификации. Другими мерами являются управление паролями, использование нестандартных конфигураций, а также обновление прошивки и исправлений с отключением ненужных протоколов, служб и портов. Подкреплённые аутентификацией, авторизацией с защищёнными протоколами для устройств и маршрутизацией, такие методы снижают риски несанкционированной потери данных в нейросетях и, в частности, в IoT. Среди ключевых IT-трендов 2023 года переход к платформенным решениям: от идеологии импортозамещения IT-продуктов к формированию отечественной платформы, замещающей импортное ПО. Наработанный опыт интеграции продуктов в единую систему позволяет двигаться в направлении к технологическому суверенитету.

Литература

1. Уязвимость IoT для кибербезопасности. URL: https://openvpn.net/blog/iot-device-vulnerability/.
2. *Сведе-Швец В.Н.* Разработка 3D фотон-электронной матричной нейросетевой реконфигурируемой платформы для высокопроизводительной обработки информации. URL: https://www.soel.ru/online/razrabotka-3d-foton-elektronnoy-matrichnoy-neyrosetevoy-rekonfiguriruemoy-platformy-dlya-vysokoproiz/.
3. Майн-машины. Описание технологии и каталог. URL: https://mindmachine.ru/catalog/shop/.
4. *Кашкаров А.П.* Как преодолеть творческий кризис? Ростов н/Д: Феникс, 2015. 321 с.
5. Первый в Европе коммерческий беспилотник для доставки товаров. URL: https://motor.ru/news/loxo-07-12-2022.htm.
6. Беспилотные ТС (мировой рынок). URL: https://www.tadviser.ru/index.php/.
7. Управление безопасностью устройств IoT. URL: https://aws.amazon.com/iot-device-defender.
8. DreamStalker Ultra. Простое вхождение в осознанный сон. URL: https://mindmachine.ru/catalog/shop/dreamstalker-ultra/.