Интернет приходит на заводы и фабрики

Интернет, как всем известно, родился в научной среде, точнее говоря, на стыке науки и военных технологий. Принципы, по которым создавалась сеть Интернет, впервые были применены в ARPANET, построенной в 1969 г. по заказу Управления перспективных исследовательских проектов Министерства обороны США, работы по созданию сети финансировались из бюджета Министерства обороны США. Спустя годы Интернет перерос научную среду и начал захватывать просторы обыденной человеческой жизни, очень скоро превратившись во «всемирную помойку» данных. Затем уже коммерческие структуры (сначала массмедиа, потом ритейлеры, рекламщики и пр.) осознали, что эта «помойка» может приносить бизнесу «золотые яйца» каждый божий день.

Сегодня мы переживаем новый этап развития Интернета, когда он, наконец-то, дорос до серьезной работы – до стадии Интернета вещей (IoT) и Промышленного Интернета вещей (IIoT). Третье десятилетие XXI века, как это понятно уже сейчас, станет эпохой расцвета сетей нового типа, в которых машины будут общаться и управлять машинами. Одним из мощных драйверов данного направления являются беспроводные сети, среди которых особое место, безусловно, занимают радиосети нового типа LPWAN (LowPower WAN), работающие на нелицензируемых (т. е. общедоступных) радиочастотах. Эта технология стала главной темой первого в этом году номера журнала Connect.

Не секрет, что приход Интернета на производство поставил предприятия перед очень непростой проблемой: как обеспечить безопасность (и не только данных, но и всего производственного процесса), когда заводам и фабрикам приходится открывать двери своих КБ и офисов во Всемирную паутину, населенную бесчисленным количеством хакеров и злоумышленников всех видов и типов? Одной из важнейших тем здесь, несомненно, является безопасность работы автоматизированных систем управления технологическими процессами критически важных объектов. Эти вопросы мы решили обсудить с руководителем одного из ведущих российских системных интеграторов в области ИБ Леонидом Ухлиновым, вице-президентом АО НИП «Информзащита».

Информационная безопасность АСУ ТП КВО также стала главной темой статьи Владимира Акименко, руководителя Центра кибербезопасности критических инфраструктур, АО «ЭЛВИС-ПЛЮС». Анализ нарушений работоспособности объектов электроэнергетики вследствие кибератак дан в материале Владимира Карантаева, к. т. н., руководителя направления кибербезопасности АСУ ТП компании «Ростелеком-Солар», и Владислава Карпенко, старшего аналитика направления кибербезопасности АСУ ТП компании «Ростелеком-Солар». О безопасном обслуживании технологического оборудования рассказал в своей статье Максим Кононенко, начальник отдела технических решений защиты информации, ДИТ АМТ-ГРУП.

В рубрике «Панорама» читатели найдут обзоры 22-го Большого Национального форума информационной безопасности «Инфофорум-2020», конференции PGConf.Russia, организованной компанией Postgress Pro, и форума SAP Digital Exchange 2020.

С уважением,
Дмитрий ШУЛЬГИН,
Connect

ИНТЕРВЬЮ НОМЕРА

4 **Леонид УХЛИНОВ:** «Система защиты не должна искажать характеристик работы АСУ ТП»
Интервью с вице-президентом АО НИП «Информзащита»

9 Государственные задачи ИБ на «Инфофоруме-2020»

КОНФЕРЕНЦИЯ

11 Анализ нарушений работоспособности объектов электроэнергетики вследствие кибератак
Владимир КАРАНТАЕВ, к. т. н., руководитель направления кибербезопасности АСУ ТП компании «Ростелеком-Солар»
Владислав КАРПЕНКО, старший аналитик направления кибербезопасности АСУ ТП компании «Ростелеком-Солар»

13 Оптимизация подходов к выбору мер по защите промышленных объектов КИИ от угроз безопасности информации на основе БДУ ФСТЭК России
Владимир АКИМЕНКО, руководитель Центра кибербезопасности критических инфраструктур АО «ЭЛВИС-ПЛЮС»

ПАНОРАМА

17 Будни импортозамещения на конференции PGConf.Russia

18 Банки в роли провайдеров госуслуг
Такую перспективу обсуждали на XX форуме iFin-2020 в Москве

20 Как добиться космического успеха вместе
Итоги конференции SpaceCom Digital Russia 2020

22 Atos на грани возможного
Презентация высокопроизводительного сервера для периферийных вычислений BullSequana Edge

ТЕМА НОМЕРА

24 LoRaWAN как надежная и безопасная технология связи
Андрей ЭКОНОМОВ, участник технического комитета LoRa Alliance, к. ф.-м. н.

31 Стандартизация и сертификация LoRaWAN
Никита УТКИН, председатель ТК 194 «Кибер-физические системы», руководитель программ АО «РВК»

35 LoRaWAN: один из путей Интернета вещей
Александр ГОЛЫШКО, независимый эксперт, к. т. н.

40 LoRaWAN в разрезе безопасности
Олег ПЛОТНИКОВ, директор центра Промышленного Интернета, компания «Интерсвязь»

44 Круглый стол с экспертами
LoRaWAN в мире Интернета вещей

47 Технологическое погружение в эпоху данных
Итоги технологической конференции SAP Digital Exchange 2020

БИЗНЕС, ТЕХНОЛОГИИ, УПРАВЛЕНИЕ

48 Имитационное моделирование в промышленности
Андрей АККУРАТОВ, технический консультант по решениям SIMULIA, Dassault Syst mes

51 Захват мира, фаза 2
Десятая версия ПО для резервного копирования от Veeam

ИНФОКОММУНИКАЦИИ

52 «Легкие» сети
Дмитрий ЛИТОВЧЕНКО, сетевой инженер CompTek

56 Российское телеком-оборудование
Алексей БОЛДИН, директор по взаимодействию с госорганами, компания RDP.RU

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

60 Безопасное обслуживание технологического оборудования
Максим КОНОНЕНКО, начальник отдела технических решений защиты информации ДИТ «АМТ-ГРУП»

ЭКСПЛУАТАЦИЯ

64 Цифровое пространство устройств печати: от управления инфраструктурой к управлению рабочей средой
Валерий КУЗЬМИЧ, руководитель отдела маркетинга и стратегических программ департамента аутсорсинга документоемких процессов компании Xerox Евразия

Леонид УХЛИНОВ:

«Система защиты не должна искажать характеристик работы АСУ ТП»

За последнее время российские законодатели существенно обновили правовые акты, связанные со сферой информационных технологий. Одной из важнейших тем здесь, безусловно, является безопасность работы автоматизированных систем управления технологическими процессами критически важных объектов (АСУ ТП КВО). Эти вопросы будут обсуждаться на конференции «Информационная безопасность АСУ ТП критически важных объектов», организованной Издательским домом «КОННЕКТ». В преддверии нашего форума мы решили побеседовать с Леонидом Михайловичем Ухлиновым, вице-президентом АО НИП «Информзащита», руководителем одного из ведущих системных интеграторов в области ИБ.

– Каково, по вашим оценкам, положение отрасли информационной безопасности в российской и мировой экономике? Какие новые тенденции помогают АО НИП «Информзащита» продвигаться на этом высококонкурентном рынке?

– Отрасль информационной безопасности за последние пять лет получила достаточно серьезное развитие, причем как в мире, так и в Российской Федерации. В первую очередь необходимо отметить,

что существенно повысилась интеллектуальная составляющая всех систем автоматизации. Автоматизация бизнес-процессов, роботизация, применение искусственного интеллекта, внедрение Интернета вещей – все эти новые технологии требуют параллельного развития средств информационной безопасности.

Сегодня возрастает понимание руководителями компаний необходимости внедрения решений по информационной безопасности как инструментов, которые защищают сам бизнес, а не только информационные системы. Кроме того, идет активное развитие нормативной базы, причем можно наблюдать параллельное развитие как международных норм по информационной безопасности, так и национальных законов и подзаконных актов, которые регламентируют все аспекты информационной безопасности в России.

Следование всем этим тенденциям и определяет ближайшие перспективы развития для «Информзащиты», поскольку наша компания – довольно специализированное предприятие. Мы работаем на рынке уже 25 лет и занимаемся исключительно вопросами информационной безопасности. Именно в этой сфере компания располагает всеми необходимыми компетенциями.

Одно из важнейших для компании направлений развития – Security Operations Center (IZ:SOC), причем развиваем его в сторону SOCaaS (Security Operations Center as a Service – «SOC как услуга»). Мы создали у себя один из лучших в России центров управления безопасностью. Помимо мощной технической инфраструктуры и целого ряда уникальных методик, в «Информзащите» собрался уникальный коллектив, который способен решать задачи по мониторингу инцидентов информационной безопасности, проведению расследований этих инцидентов и выработке рекомендаций для наших клиентов, каким образом им в дальнейшем избежать утечки информации либо других киберугроз.

Мы формировали свой продуктовый портфель в течение длительного времени и сегодня можем позволить себе участие в комплексных проектах под ключ.

Мы создали у себя один из лучших в России центров управления безопасностью.

– Какие новые продукты появились в ассортименте вашей компании за прошедшие два года? Чем вы руководствуетесь при наполнении продуктового портфеля?

– Прежде всего потребностями рынка и теми запросами, которые получаем от заказчиков. Мы формировали свой продуктовый портфель в течение длительного периода времени и сегодня можем позволить себе участие в комплексных проектах под ключ.

Сегодня мы готовы предоставить заказчику систему управления ролевыми моделями, в которую входит все, что связано с регламентацией доступа к ресурсам предприятия, к функциям информационных систем, включая контроль деятельности администраторов информационной безопасности.

Еще одна интересная новинка – система управления безопасностью конфигураций. Как мы знаем, любая информационная система не является неким фиксированным продуктом, который не меняется после ввода в эксплуатацию. Изменению подвержены все системы, в том числе и системы защиты, поэтому отслеживание конфигураций, тех или иных угроз и формирование понимания новых киберугроз, связанных с изменением конфигураций, становится важной задачей, особенно для людей, которые занимаются развитием ИТ-инфраструктуры и систем безопасности.

За последнее время АО НИП «Информзащита» также разработала новые решения в области платформы безопасной аутентификации и авторизации пользователей. Естественно, эти решения в большей степени интересны для таких сфер, как облачные структуры, облачные конфигурации. В ближайшее время будем выводить эти решения на рынок.

Перспективной новинкой является автоматизация деятельности органа криптозащиты, который имеется в любой серьезной организации, располагающей криптографическими системами защиты информации как каналов передачи данных, так и внешних носителей. Автоматизация всей деятельности по управлению ключами, по регистрации устройств, по взаимодействию с регуляторами, отслеживание временных интервалов по смене ключей – все это покрывается нашим новым решением. Мы создали его с использованием ресурсов центра разработки программного обеспечения компании.

Все перечисленные направления в АО НИП «Информзащита» развиваются с целью усилить наши конкурентные преимущества на рынке информационной безопасности.

– По мнению многих экспертов, главным драйвером развития рынка ИБ сейчас является Закон № 187-ФЗ «О безопасности КИИ». Вы согласны с этим утверждением? Какие услуги АО НИП «Информзащита» предлагает в помощь клиентам по реализации требований названного закона?

– Закон № 187-ФЗ «О безопасности КИИ», безусловно, драйвер развития рынка информационной безопасности, но я бы не сказал, что главный, поскольку он охватывает лишь критическую информационную инфраструктуру, не покрывая остальных аспектов информационной безопасности.

А разве программа цифровой трансформации экономики России не является мощнейшим драйвером ИБ? Этот национальный проект охватывает все сферы экономики страны. Забыть о кибербезопасности при переходе на цифровые технологии означает забыть об эффективности трансформации. Рынок намного сложнее, и мы видим гораздо больше потребностей в области информационной безопасности, чем в сфере критической инфраструктуры.

Если просмотреть все подзаконные акты, которые изданы регуляторами по реализации Закона № 187-ФЗ, то мы увидим, что все начинается с аудита ИТ-инфраструктуры и ресурсов, с категоризации, с выявления критичных ресурсов по защите информации, затем уже дело доходит до создания систем защиты, их внедрения и обслуживания. АО НИП «Информзащита» предоставляет заказчикам полный спектр услуг – от тестов на проникновение и выявление возможных каналов утечки, создания моделей угроз до проектирования и внедрения систем защиты, а также их обслуживания.

– На каком этапе сейчас находится реализация требований Закона № 187-ФЗ в российской промышленности? Как вы оцениваете уровень защищенности российских промышленных предприятий по результатам проделанной работы?

– Работа по реализации требований находится на начальном этапе. Закон № 187-ФЗ принят два года назад, но сегодня выполнены работы в основном по категорированию объектов критической инфраструктуры. Дальнейшая работа, как правило, упирается в сложно решаемую проблему: предприятию необходим бюджет, причем достаточно большой, для того, чтобы система защиты соответствовала той категории, которую определили на начальном этапе работ.

На мой взгляд, настал момент перейти от желания выполнить все требования закона с минимальными затратами к обеспечению реальной безопасности критической инфраструктуры предприятия. Просто отчитаться перед ФСТЭК в том, что категорирование завершено и что-то сделано в области разработки моделей угроз, – это лишь самое начало процесса. Главная задача – создать систему защиты, которая будет соответствовать современным технологиям. Зачастую компании, которые работают на этом рынке, указывают в своих материалах следующее: «Мы обеспечим выполнение текущих требований регулятора». Это неправильно! Наша компания стоит на других позициях: «Мы обеспечиваем безопасность критической инфраструктуры, а не только оформляем необходимые документы и формуляры для регулятора».

> Главная задача – создать систему защиты, соответствующую современным технологиям.

До выхода Закона № 187-ФЗ уровень информационной безопасности предприятий был гораздо ниже сегодняшнего. Однако требуемый уровень безопасности объектов критической инфраструктуры еще не достигнут – мы только на пути к этому.

– Переходя к более узкой тематике АСУ ТП: насколько проекты в области информационной защиты промышленных сетей востребованы сейчас на российском рынке? Для каких АСУ ТП особенно сложно организовать полноценную защиту?

– Безопасность АСУ ТП обсуждается с момента появления таких систем, хотя повышенное внимание к этому сектору стало уделяться в последние пять лет. Особенность всех проектов, связанных с безопасностью АСУ ТП, заключается в том, что для построения их защиты необходимо привлекать специалистов исключительно по АСУ ТП, поскольку в этих системах применяются внутренние технологические протоколы.

Особенности обычных информационных систем всем хорошо известны, и все они давно уже стандартизованы. Конечно, стандартизация существует и в секторе АСУ ТП, однако протоколы разные, потому и последовательность применения средств защиты, и их состав значительно отличаются от того, что имеется для обычных ИС.

Ключевая особенность этих проектов заключается в следующем: необходимо сохранить все характеристики работы АСУ ТП при внедрении средств защиты. Поясню на простом примере: в информационных системах, если мы поставим межсетевой экран, который будет генерировать задержку доставки пакета до рабочего места клиента длительностью 2–3 секунды, никто этого просто не заметит. А теперь представьте себе систему управления ядерного реактора: задержка в долю секунды при поднимании и опускании стержней может привести к катастрофе планетарного масштаба. Поэтому система защиты не должна искажать характеристик работы АСУ ТП как объекта

защиты. Мы должны обеспечить минимальное вмешательство в работу оборудования при сохранении максимального контроля над безопасностью объекта.

Не все способны выполнить такую ювелирную работу: специалист по информационной безопасности не всегда в деталях и тонкостях понимает функционал той или иной системы управления. Поэтому мы создали в своей компании Центр промышленной безопасности, в который набрали специалистов по АСУ ТП – уникальных экспертов, в том числе из числа наших «воспитанников». Это результат сотрудничества «Информзащиты» с российскими вузами, с производителями АСУ ТП, со многими вендорами на российском рынке.

Мы имеем большое наследие еще со времен СССР, когда АСУ ТП создавались на заводах местными специалистами – эти люди ушли, документации на предприятиях нет, и сегодня никто не знает, на каких принципах работают их системы автоматизации. Прежде чем заниматься защитой информации в такой среде, приходится изучать оборудование предприятия, выяснять, как именно работает АСУ ТП.

– Какие рекомендации можно дать компаниям, которые в процессе категорирования обнаружили у себя значимые объекты КИИ? Какие механизмы защиты им стоит внедрить в первую очередь?

– Исходя из опыта реализации таких проектов, хотелось бы особо выделить один из механизмов – сегментацию объектов информационной инфраструктуры по уровню защищенности. Речь идет об изоляции объектов с необходимостью наиболее высокой степени защиты и о выделении демилитаризованных зон.

Второй важный аспект – мониторинг работоспособности ИТ-инфраструктуры, той инфраструктуры, которая обеспечивает работоспособность и реализацию всех бизнес-процессов, а также мониторинг событий информационной безопасности, включая реагирование на инциденты и оперативное расследование инцидентов. Все это требует создания SOC.

Далее, обязательно создание службы информационной безопасности либо, если это невозможно по ряду причин (отсутствие бюджета, невозможность расширения штатной структуры), заключение

сервисного договора на обслуживание, аутсорсинг со специализированными организациями.

– Какие проекты по внедрению российских продуктов были для вашей компании наиболее поучительны? Как вы оцениваете уровень зрелости российских промышленных предприятий по реализации проектов в области информационной безопасности?

– Нам, разумеется, больше всего интересны комплексные проекты. Мы должны учитывать существующий ландшафт информационной безопасности. Когда мы приходим в какую-то компанию или крупную структуру, обычно там присутствуют средства защиты как от российских, так и от зарубежных вендоров, и нам доставляет особое удовольствие показать по завершении проекта заказчику, что мы сохранили его инвестиции в имеющиеся средства защиты, добавив к ним лишь те функции, которые были ему максимально необходимы для обеспечения безопасности. Понятно, что каждого заказчика волнует эффективность потраченных денег, и в этом отношении мы придерживаемся строгих принципов: заказчик не должен слышать от нас, что все, что у него было раньше, нужно снести и построить новую систему с нуля. Мы стараемся по максимуму сохранить все, что было, и добавить наши новые знания, новые возможности. Именно в этом мы видим свое конкурентное преимущество.

Что же касается уровня зрелости российских промышленных предприятий, то сейчас информационная безопасность там гораздо выше, чем несколько лет назад. За последние годы, что отрадно отметить, заметно выросла компетенция заказчиков: все видят необходимость внедрения решений ИБ, понимают терминологию, у большинства заказчиков выделены специалисты, которые занимаются защитой информационных ресурсов.

Нам удалось создать коллектив единомышленников, которые способны решать любые задачи.

– Насколько в целом успешной, на ваш взгляд, оказалась стратегия импортозамещения в области информационной безопасности? Остались ли области, где российских продуктов по-прежнему не хватает?

– Традиционно наши отечественные разработчики были сильны в средствах криптозащиты, поскольку российская криптография базируется на мощной математической школе. Если вы сегодня посмотрите публикации форумов по криптографии, то найдете множество российских трудов, которые легли в основу тех или иных решений, – это и криптографические протоколы, и квантовая криптография, и многое другое.

Однако все, что касается решений, связанных с интеллектуальным насыщением систем защиты (не просто зашифровать данные, а сделать систему управляемой, адаптивной, провести интеграцию средств выявления инцидентов со средствами решения инцидентов), то наши зарубежные коллеги стали заниматься этими вопросами раньше. Мы на сегодняшний день еще не достигли такого состояния, когда можно было бы говорить о 100%-ном замещении всех средств защиты.

Безопасность промышленных систем мы рассматриваем в качестве одного из перспективных направлений роста нашего бизнеса.

– В каком направлении планирует развиваться ваша компания в области защиты промышленных систем? Как будет совершенствоваться ассортимент используемых вами продуктов и развиваться партнерская политика?

– Прежде всего я хотел бы сказать, что безопасность промышленных систем мы рассматриваем в качестве одного из перспективных направлений роста нашего бизнеса. Три года назад был создан Центр промышленной безопасности, и сегодня он уже вышел на хорошие объемы заказов. Но самое главное – нам удалось создать коллектив единомышленников, которые способны решать любые задачи, в том числе связанные с защитой АСУ ТП в сложных условиях производства.

Мы делаем большие инвестиции в тестовую базу: сегодня у нас более 150 стендов, на которых можно смоделировать любую систему и любую ситуацию, связанную с управлением производственными процессами. Наша компания ориентируется на более глубокое партнерство с производителями технологий и программного обеспечения, анализирует интересные тренды на производстве, в частности внедрение робототехники.

Таким образом, будущее АО НИП «Информзащита» – повышение интеллектуальной составляющей проектов. ■

Государственные задачи ИБ на «Инфофоруме-2020»

В Москве 30 и 31 января 2020 г. прошел 22-й Большой Национальный форум информационной безопасности «Инфофорум-2020». В поисках оптимальных решений по противодействию киберугрозам и минимизации киберрисков в условиях цифровизации на «Инфофорум» прибыли представители федеральных и региональных органов власти, органов местного самоуправления, ведущих российских и международных ИТ-компаний, образовательных и научных центров. Организаторами «Инфофорума-2020» выступили: Комитет Государственной Думы РФ по безопасности и противодействию коррупции, аппарат Совета Безопасности РФ, Ассоциация Национальный форум информационной безопасности «Инфофорум».

В этом году Большой Инфофорум поддержали ФСБ России, МВД России, Министерство обороны России, ФСТЭК России, ФСО России, МЧС России, Минкомсвязи России, Россвязь, Роскомнадзор, Минэкономразвития России, Минэнерго России, Минтранс России, Минфин России, Центральный Банк РФ, некоторые другие федеральные министерства и ведомства, правительство Москвы, правительства других субъектов Российской Федерации, а также Секретариат и Парламентская ассамблея ОДКБ, секретариат ШОС. Они прислали на форум своих представителей, которые приняли активное участие в обсуждении важнейших проблем международной информационной безопасности.

«Инфофорум-2020» открылся Пленарным заседанием: «Информационная безопасность России в условиях глобального информационного общества и цифровой экономики». Также в двухдневную программу «Инфофорума-2020» вошли 17-я церемония награждения профессиональной премией в области информационной безопасности «Серебряный кинжал», 12 тематических заседаний, выставочная экспозиция «Информационная безопасность граждан, бизнеса и государства» и другие мероприятия.

Организаторы «Инфофорума-2020» включили в повестку темы, которые являются на сегодняшний день устойчивыми трендами для сферы информационной безопасности. Среди них и традиционные темы, которые волнуют всех, такие как безопасность критической информационной инфраструктуры, безопасность Интернета, противодействие киберпреступности, методы анализа и реагирования на компьютерные инциденты. И новые – такие как информационная безопасность связи пятого поколения (5G), Интернета вещей, технологий искусственного интеллекта, облачных технологий и технологий управления данными. Также в этом году «Инфофорум-2020» предложил и совершенно новый тематический тренд в сфере ИБ. Это блок вопросов, выделенных под названием «Лаборатория социальных проблем информационной безопасности». Сюда вошли вопросы цифровой идентичности и информационной безопасности и защиты интересов личности в цифровой среде, а также вопросы развития цифровой культуры и культуры информационной безопасности граждан, начиная с самого юного возраста.

Кроме того, Николай Мурашов, заместитель начальника НКЦКИ, рассказал о проекте российского мультисканера – его создание предусмотрено в федеральном проекте «Информационная безопасность». В настоящее время работа ведется ФСБ России во взаимодействии с заинтересованными организациями. Прототип мультисканера будет запущен в опытную эксплуатацию в 2021 г. Это позволит гражданам и юридическим лицам повысить уровень защиты своей информации, опираясь на лучшие практики российских компаний по противодействию вредоносному программному обеспечению, исключить необходимость обращения к зарубежным антивирусным ресурсам.

В 2020 г. планируется создание специального ресурса, предназначенного для взаимодействия граждан и организаций с уполномоченными органами в целях оперативной передачи данных о признаках противоправных действий в области информационных технологий, компьютерного мошенничества, навязанных услуг операторов связи, фишинговых схем. В настоящее время ведется активная работа Генеральной прокуратуры России во взаимодействии с МВД России, ФСБ России, Роскомнадзором, Следственным комитетом России, Банком России и другими заинтересованными органами власти при тесном сотрудничестве с бизнес-сообществом в рамках рабочей группы АНО «Цифровая экономика» по разработке концепции и технических требований к указанному ресурсу, а также по сбору предложений

по внесению изменений в законодательство.

В рамках «Инфофорума-2020» обсуждению названной инициативы была посвящена отдельная панельная дискуссия «Правовой ландшафт информационной безопасности. Проблематика преступлений в цифровой среде против граждан, бизнеса и государства», которая прошла под председательством директора по направлению ИБ АНО «Цифровая экономика» Николая Зубарева. На ней было отмечено, что специализированный ресурс предполагается создать как один из суперсервисов под названием «Прием обращений граждан в правоохранительные органы онлайн». Причем создание спецресурса является ключевым параметром национального проекта «Цифровая экономика РФ», утвержденного Советом при Президенте РФ по стратегическому развитию и национальным проектам.

Еще одной темой, обсуждаемой на «Инфофоруме-2020», была Государственная единая облачная платформа (ГЕОП) и планы по переводу в нее государственных информационных систем (ГИС). Эта работа будет проводиться в рамках Положения об эксперименте по переводу в ГЕОП информационных систем и ресурсов ФОИВ и ГВФ (Постановление Правительства РФ от 28.08.2019 № 1114). В процессе эксперимента предполагается изучение возможностей по переводу 49 информационных систем из девяти ФОИВ в гособлако. Завершить эксперимент планируется до конца текущего года, а в начале следующего будут подготовлены поправки к законодательству для перевода в ГЕОП всех государственных информационных систем.

Тема экспериментов с ГЕОП и его защиты активно обсуждалась на «Инфофоруме-2020». В частности, директор департамента развития архитектуры и координации информатизации Минцифры Василий Слышкин отметил, что сейчас государство поддерживает более 800 ресурсов, которые содержат информацию объемом более 80 Пбайт, и в ближайшие годы ожидается удвоение этого объема. Сейчас эта важная для функционирования «электронного государства» информация располагается на собственной инфраструктуре ведомств, которые не всегда имеют компетенции по организации ее надежного и безопасного хранения. Потому и возникла инициатива по переносу ГИС в ГЕОП, для которого можно будет обеспечить и надежность путем резервирования, и защиту за счет центров реагирования на инциденты.

Тему продолжил Игорь Ляпунов, вице-президент ПАО «Ростелеком», который отметил, что сейчас объекты КИИ (к ним относятся ГИС) атакуют уже не отдельные хакеры, а спецслужбы других государств. Для них характерен более жесткий стиль атаки, предполагающий разработку профессионального атакующего ПО, специально созданного под конкретную среду исполнения и имеющего микромодульную архитектуру с возможностью загрузки различных новых функций и обновлений по требованию из командного центра. Обнаружить присутствие таких вредоносов с помощью стандартного ПО практически невозможно, к тому же на финальном этапе злоумышленники применяют стандартные инструменты удаленного управления, которыми пользуются администраторы систем. Обнаружить подобную активность весьма сложно, но можно, если знать, куда смотреть. Однако профессиональные нападающие очень быстро затирают следы своего присутствия в системе. Чтобы заметить подобное вмешательство, служба безопасности объекта КИИ должна работать непрерывно и быть высокопрофессиональной. Естественно, отдельные ФОИВ защиту такого уровня обеспечить не могут – это лучше делать централизованно, на уровне государства в целом.

В настоящее время «Ростелеком» создает систему раннего обнаружения атак на уровне операторской инфраструктуры. Она позволяет выявить подозрительную активность еще в инфраструктуре провайдера услуг доступа, до того как атака будет проведена против клиента. На уровне оператора подозрительное использование IP-протоколов можно заметить лучше, поэтому компания планирует предлагать услуги по раннему предупреждению атак для своих клиентов, особенно из числа субъектов критической инфраструктуры. «Ростелеком» распоряжением № 2667-р назначен одним из основных исполнителей по переносу в ГЕОП ресурсов таких ведомств, как Минтруд России, Минюст России, «Ростехнадзор», «Росимущество», ГФС России, «Росархив» и Фонд социального страхования. Переносом ресурсов «Росгвардии» и ФТС России в гособлако будет заниматься ФГБУ НИИ «Восход». На «Инфофоруме» были озвучены планы по переводу в гособлако системы ЕИИС «Соцстрах», принадлежащей ФСС России, резервирования ЕАИС таможенных органов и почтовой системы «Росгвардии».

Эксперимент по переводу 49 ГИС в ГЕОП продлится до конца текущего года. По его результатам должны быть подготовлены требования по переносу других ГИС в ГЕОП, а также требования для других облачных операторов – сведения о них будут занесены в реестр аккредитованных поставщиков облачных услуг. Результаты этой работы должны быть утверждены на уровне законодательных актов. Кроме того, ФГБУ НИИ «Восход» должен разработать систему управления ГЕОП и рабочее место государственного служащего для подключения к ГИС, перенесенным в ГЕОП, с использованием программ из реестра отечественного ПО. В результате, по мнению Василия Слышкина, до 80% всех ГИС должно быть портировано в ГЕОП. Это позволит повысить надежность и безопасность функционирования российского «электронного государства». ■

Анализ нарушений
работоспособности объектов электроэнергетики вследствие кибератак

Владимир КАРАНТАЕВ,
к. т. н., руководитель направления кибербезопасности АСУ ТП компании «Ростелеком-Солар».

Владислав КАРПЕНКО,
старший аналитик направления кибербезопасности АСУ ТП компании «Ростелеком-Солар».

Введение

Цифровизация электроэнергетической отрасли является одной из приоритетных задач по цифровизации энергетики России [1]. Существуют два подхода к решению поставленной задачи: «Концепция. Цифровая трансформация 2030» от ПАО «Россети» [2] и «Цифровой переход в электроэнергетике России» от Национальной технологической инициативы Энерджинет [3]. Обе концепции декларируют использование информационно-коммуникационных технологий как основу коренного изменения в работе отраслевых компаний. Однако положительные стороны цифровизации могут быть нивелированы растущими рисками нарушения устойчивости работы объектов электроэнергетики вследствие кибератак.

Обозначенная проблема была изучена экспертами «Лаборатории кибербезопасности АСУ ТП» «Ростелеком-Солар» в рамках инициативной научно-исследовательской работы «Анализ нарушений работоспособности объектов электроэнергетики в результате деструктивных воздействий компьютерных атак» [4].

Методология исследования

Основная задача настоящего исследования – формирование инструментария для моделирования сценариев кибератак, вызывающих последствия на физическом уровне. Для анализа был взят перечень аварий из постановления Правительства Российской Федерации [5]. Область исследования [4] была ограничена рассмотрением электроустановок переменного и постоянного тока и воздействующих на них систем управления и защиты.

Следующим этапом было исследование технологических причин каждой аварии.

Архитектуры объектов электроэнергетики, в частности цифровых подстанций (ЦПС), в НИР [4] были взяты из стандарта организации ПАО «Россети» [6]. Полученная информация используется для выполнения следующего этапа исследования – рассмотрения воздействия вторичных подсистем на первичное оборудование, для чего устанавливается взаимосвязь управляющих воздействий подсистем и технологических нарушений.

После анализа отраслевой специфики электроэнергетики исследование НИР [4] переходит к рассмотрению классических для области информационной безопасности вопросов, в частности к моделированию угроз и нарушителя (МУиН). Для решения этой задачи были использованы материалы «Методики определения угроз безопасности информации в информационных системах» [7] и приказа ФСТЭК России № 236 [8].

На основе методики [7] было проведено исследование модели нарушителя кибербезопасности объекта электроэнергетики и сделан вывод, что нарушитель может быть как внутренним, так и внешним, ему достаточно обладать средним потенциалом, чтобы создать реальную угрозу нарушения работы технологического объекта.

В исследовании кибератаки были классифицированы по типам компьютерных инцидентов, возникающих на компонентах подсистем, соответствующих типизации из приказа [8]. В рамках НИР [4] принимается, что создание этих инцидентов является локальной целью нарушителя. Такое

допущение требуется для формирования взаимосвязи кибератак и компонентов вторичных подсистем, на которые они могут быть направлены. По сути, в НИР [4] синтезирована информация, необходимая для исследования сценариев кибератак с физическими последствиями.

Результаты НИР

На последнем этапе НИР [4] используется информация, полученная на предыдущих этапах, для демонстрации исследования сценариев кибератак. В итоге рассмотрено около десяти различных сценариев, которые, по мнению авторов исследования, могут иметь место в реальной ситуации.

В НИР [4] показано, как реализация угроз информационной безопасности во вторичных системах может приводить к авариям (реализации угроз кибербезопасности объекта электроэнергетики). Наиболее значимым практическим результатом авторы считают возможность сделать следующий вывод: **нарушение устойчивости функционирования объектов электроэнергетики с высоким уровнем цифровизации вторичных систем вследствие воздействия на них кибератак возможно**.

По результатам исследования было установлено, что к наиболее ответственным с точки зрения защиты от кибератак относятся следующие вторичные системы:

- система релейной защиты и автоматики (РЗА);
- автоматизированная система управления технологическим процессом (АСУ ТП);
- система специального автоматического управления и регулирования (САУ, САР);

Релейная защита выполняет функции ликвидации и локализации повреждений оборудования технологических объектов, отключая поврежденное оборудование от сети. Автоматика разделена на противоаварийную и режимную. Противоаварийная автоматика является системой, которая необходима для предотвращения системных аварий, а режимная автоматика направлена на поддержание нормального функционирования электрической сети.

АСУ ТП необходима для выполнения функций автоматизированного управления объектом, повышения наблюдаемости его состояния. Также АСУ ТП дает возможность удаленного оперативного управления из центров управления сетями (ЦУС) или диспетчерских центров (ДЦ).

САУ и САР используются для управления динамическим оборудованием, которое осуществляет регулирование электрических параметров электросетей.

Перечисленные системы нуждаются в наиболее надежной защите – как наложенными средствами защиты информации для систем в целом, так и механизмами безопасности, встроенными в интеллектуальные электронные устройства (ИЭУ), которые составляют эти системы. РЗА, АСУ ТП, САУ имеют возможность оказывать непосредственное влияние на работу технологического объекта, а деструктивные воздействия, направленные на эти системы, могут привести к массовым отключениям потребителей, повреждению силового оборудования, выходу электрических параметров за допустимые пределы и т. д., что, в свою очередь, может повлиять на надежность электроснабжения потребителей и системную надежность Единой энергосистемы России в целом.

В настоящее время проводятся исследования по созданию базы знаний для экспертной системы по оценке влияния деструктивных воздействий компьютерных атак на объекты электроэнергетики. Предполагается, что база знаний будет воспроизведена с помощью семантических технологий и представлена онтологической моделью. Онтология, лежащая в основе базы знаний, позволит установить семантические связи между техниками, тактиками злоумышленников и авариями объекта электроэнергетики, которые могут произойти вследствие кибератак. ■

Литература

1. *Кулапин А.И. Ведомственный проект Минэнерго России «Цифровая энергетика». М., 01.10.2018.*
2. *ПАО «Россети». Концепция. Цифровая трансформация 2030. М., 2018.*
3. *Холкин Д.В. и Княгинин В.Н. Цифровой переход в электроэнергетике России. М.: Энерджинет, 2017.*
4. *Карпенко В., Карантаев В., Парьев С. и др. Анализ нарушений работоспособности объектов электроэнергетики в результате деструктивных воздействий компьютерных атак. М.: Ростелеком Солар, 2019.*
5. *Правительство Российской Федерации. Постановление № 846 от 28 октября 2009 г. «Об утверждении правил расследования причин аварий в электроэнергетике» (в ред. Постановлений Правительства РФ № 996 от 05.12.2011, № 1114 от 17.10.2015, № 525 от 10.06.2016).*
6. *Стандарт организации ПАО «Россети» СТО 34.01-21-004-2019 «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110–220 кВ и узловых цифровых подстанций напряжением 35 кВ», 29.03.2019.*
7. *ФСТЭК России. Методика определения угроз безопасности информации в информационных системах. 2015.*
8. *ФСТЭК России. Приказ № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (в ред. приказа ФСТЭК 22 декабря 2017 г.).*

Оптимизация подходов

к выбору мер по защите промышленных объектов КИИ от угроз безопасности информации на основе БДУ ФСТЭК России

Владимир АКИМЕНКО,
руководитель Центра кибербезопасности критических инфраструктур, АО «ЭЛВИС-ПЛЮС»

Положения Федерального закона № 187-ФЗ от 26.07.2017 и принятых в соответствии с ним нормативных правовых актов устанавливают порядок определения требований и мер защиты объектов критической информационной инфраструктуры (КИИ) от угроз безопасности информации. Требования к составу и выбору мер защиты установлены приказом ФСТЭК России № 239 от 25.12.2017 (239-П).

Этот документ определяет порядок выбора мер по обеспечению безопасности значимых объектов КИИ, который включает:

а) определение базового набора мер по обеспечению безопасности значимого объекта (на основе установленной категории значимости объекта);

б) адаптацию базового набора мер по обеспечению безопасности значимого объекта;

в) дополнение адаптированного набора мер по обеспечению безопасности объекта дополнительными мерами (при необходимости).

Базовый набор мер по обеспечению безопасности значимого объекта КИИ подлежит адаптации в соответствии с угрозами безопасности информации (УБИ), признанными актуальными для рассматриваемого объекта КИИ. При адаптации базового набора мер каждой актуальной угрозе, включенной в модель угроз, сопоставляется мера или группа мер, обеспечивающих блокирование одной или нескольких УБИ или снижающих возможность ее реализации, исходя из условий функционирования значимого объекта КИИ. В случае если базовый набор мер не позволяет обеспечить блокирование (нейтрализацию) всех актуальных УБИ, в него дополнительно включаются меры защиты, приведенные в 239-П. Однако этот порядок формально не допускает возможности использования для обеспечения безопасности объекта КИИ набора мер защиты менее адаптированного базового набора. То есть дополнительные меры защиты применять можно, а уменьшать набор мер защиты менее базового набора – нельзя.

Структура состава обобщенных ОВ

Рис. 1.

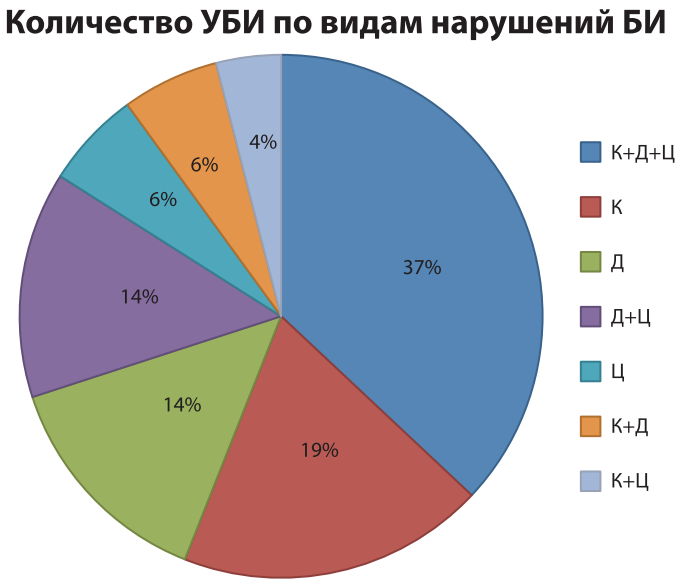


Рис. 2.

При моделировании УБИ для объектов КИИ ФСТЭК России предписывает (239-П, п. 11.1) в качестве исходных данных использовать банк данных угроз (БДУ), ведение которого осуществляется с 2015 года (bdu.fstec.ru).

Можно предположить, что базовый набор мер по обеспечению безопасности значимых объектов КИИ, включенный в 239-П, определялся на основе типовых моделей угроз безопасности информации, построенных с учетом лучших мировых практик, в том числе и с учетом угроз безопасности информации (БИ), включенных в БДУ ФСТЭК России.

В рамках настоящей статьи рассматривается сравнение набора мер защиты, определенных на основе анализа полного комплекса УБИ из БДУ ФСТЭК России, применимых для типовой структуры АСУТП, с минимально необходимым (базовым адаптированным) набором мер, определенным в соответствии с требованиями 239-П.

Как известно, УБИ рассматривается на основе цепочки: Источник угрозы (И) – Объект воздействия (ОВ) – Уязвимость (У) – Способ реализации угрозы (Р) – Последствия (П) (нарушение конфиденциальности (К), доступности (Д), целостности (Ц)).

В качестве источников УБИ в БДУ рассматриваются в основном антропогенные источники – нарушители. Нарушители характеризуются своей мотивацией и потенциалом. Анализ источников угроз показывает, что доля угроз, которые могут быть реализованы только нарушителем с высоким потенциалом, составляет всего 5%. Соответственно исключение подобных типов источников угроз несущественно влияет на состав рассматриваемых угроз.

Бессистемность в обозначении объектов воздействия в БДУ

Рис. 3.

Рис. 4.

(одни и те же, по сути, объекты называются в БДУ по-разному, например: оборудование указывается и как техническое средство, и как аппаратное обеспечение, и как сервер, АРМ, облачный сервер и т. п.) вызывает сложности при анализе угроз. Если обобщить приведенные понятия, то можно выделить группы объектов, указывающие на возможную цель воздействия нарушителя (рис. 1). Структура обобщенных объектов воздействия показывает, что основным объектом нарушения БИ выступает программное обеспечение (микропрограммное, системное, прикладное, сетевое, программное обеспечение гипервизора).

Как правило, в промышленных системах к технологической информации не предъявляются требования по обеспечению конфиденциальности, в связи с чем угрозы нарушения конфиденциальности могут быть признаны неактуальными, их доля может составлять до 20% от общего числа угроз (рис. 2), включенных в БДУ (за исключением угроз, направленных на получение доступа к аутентификационной информации).

Реализация УБИ возможна при наличии определенных факторов (уязвимостей), используя которые нарушитель может реализовать угрозы. Анализ сценариев реализации УБИ, указанных в БДУ, показывает, что основным способом реализации большого количества угроз является эксплуатация уязвимостей/«слабостей» программного обеспечения как общесистемного, так и микропрограммного, сетевого, прикладного и ПО гипервизора (рис. 3). Причем подобные «слабости»

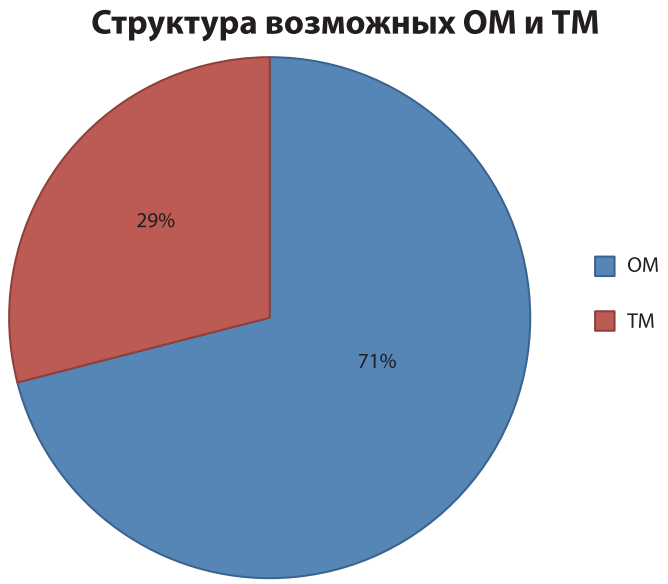


Рис. 5.

Доля возможных мер парирования УБИ по БДУ в общем количестве базовых мер, определенных 239-П

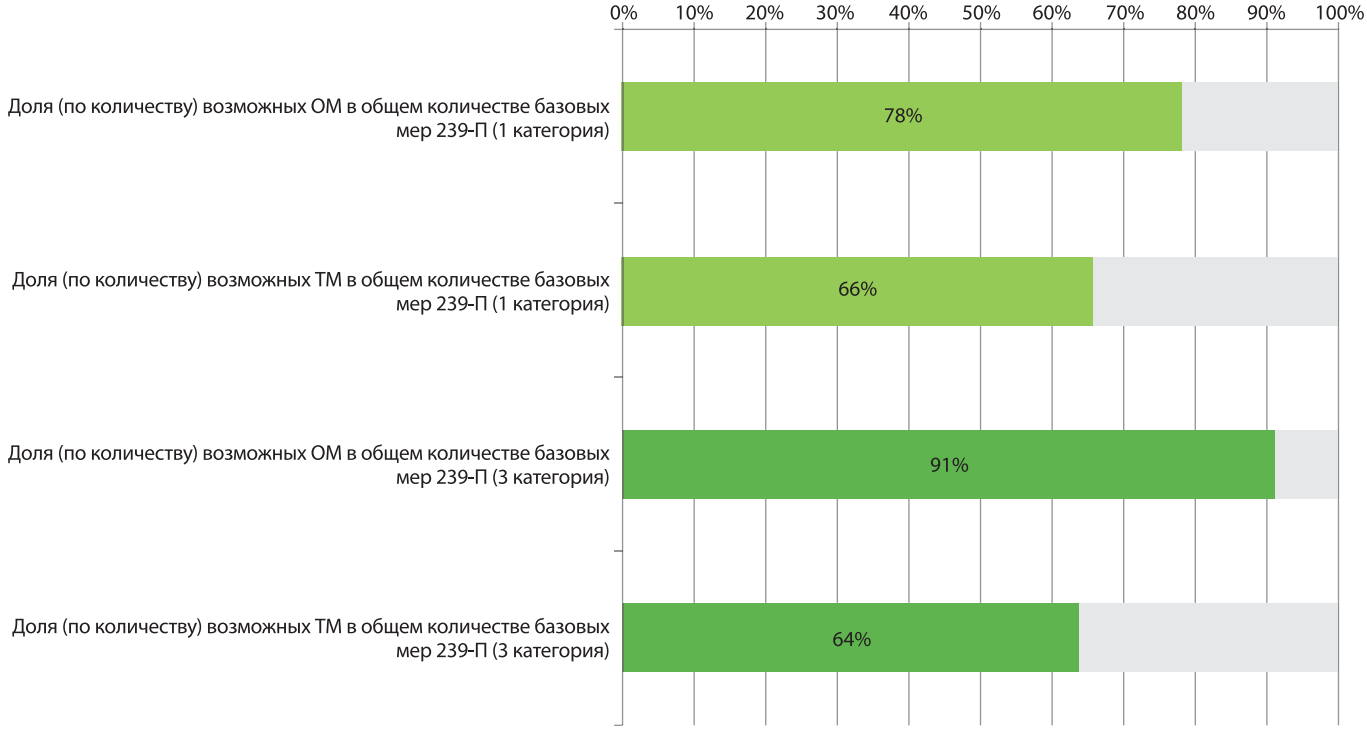


Рис. 6.

обусловлены не только нарушениями конфиденциальности или целостности обрабатываемых данных, но и нестабильной работой приложений, сбоями, некорректной обработкой данных, отсутствием защиты от ошибочных действий пользователей и другими функциональными уязвимостями.

Выбор мер парирования УБИ предполагает знание не только общей структуры средств автоматизации и порядка функционирования объекта КИИ, но и понимание модели обработки и хранения информации, потоков данных, технологий обработки и обмена данными между компонентами системы, а также знание механизмов защиты от возможных угроз нарушения безопасности информации. Указанные обстоятельства предъявляют достаточно высокие требования к квалификации работников, осуществляющих анализ и выработку возможных мер парирования актуальных угроз безопасности информации.

Рассмотрев возможные способы и механизмы нейтрализации указанных выше факторов и проведя их ранжирование, можно получить возможный перечень мер (рис. 4), обеспечивающих блокирование (снижение вероятности реализации) УБИ, указанных в БДУ.

При этом количество возможных технических мер защиты составляет примерно третью часть всех предполагаемых к внедрению мер (рис. 5). Они достаточно понятны, широко применяются в информационных системах как корпоративного, так и промышленного сегментов (средства межсетевого экранирования, антивирусная защита, средства управления доступом, регистрация событий, резервное копирование и восстановление).

Существенный вклад в нейтрализацию угроз вносят организационные меры, связанные с определением требований по защите, регламентацией процессов обеспечения и контроля безопасности объектов КИИ и установлением ответственности за обеспечение и нарушение правил безопасной работы с информационными ресурсами и средствами объекта КИИ.

Сопоставляя возможные меры парирования УБИ, входящие в БДУ, с базовым набором мер, определенным 239-П, а также учитывая предположения и ограничения, которые были указаны в настоящей статье, можно сделать вывод, что набор базовых мер, определенный 239-П, превышает состав мер, которые необходимы для парирования УБИ, включенных в состав БДУ (рис. 6).

Настоящий анализ может говорить о возможности оптимизации состава мер обеспечения безопасности объектов КИИ, установленного 239-П, путем проведения моделирования УБИ и выбора необходимых мер их нейтрализации.

При этом следует не забывать, что ответственность за соблюдение требований по обеспечению безопасности объектов КИИ несет субъект КИИ. ■

Будни импортозамещения
на конференции PGConf.Russia

Импортозамещение постепенно переходит в стадию реализации: на различных мероприятиях уже рассказывают о переводе крупных информационных систем на российские разработки. Больше всего таких примеров можно было отметить на прошедшей в начале февраля конференции PGConf.Russia, организованной компанией Postgress Pro, которая является разработчиком отечественной СУБД Postgres Pro и оказывает услуги коммерческого сопровождения проектов на основе СУБД PostgreSQL. В частности, о переходе на российское ПО рассказали Федеральное казначейство, АО «ВНИИЖТ» и «БАРС Груп», где речь шла в основном о переводе именно базы данных с Oracle на PostgreSQL.

Одним из важных факторов перевода государственных информационных систем на российские продукты стало Постановление Правительства от 8 июня 2018 г. № 658 «О централизованных закупках офисного программного обеспечения, программного обеспечения для ведения бюджетного учета, а также программного обеспечения в сфере информационной безопасности» и принятый в рамках его исполнения приказ Минкомсвязи № 725 «Об утверждении формы и порядка представления в 2019 году информации о потребности, формирования потребности в осуществлении централизованных закупок офисного программного обеспечения и программного обеспечения в сфере информационной безопасности», с помощью которого ведомство собрало информацию по потребностям ФОИВ в двух типах программного обеспечения.

Надо признать, что сбор информации от ведомств занял практически целый год, и только 17 декабря 2019 г. состоялся сам аукцион. Причем он был разбит на три отдельных лота, для каждого из них были предложены собственные решения. В результате конкурса два лота для ФНС и других ведомств получила компания «Ланит», один лот для Федерального казначейства – компания «Софтлайн проекты», которая будет поставлять «Р7-Офис» для 40 тыс. пользователей – это подтвердил в своем выступлении на круглом столе Александр Албычев, заместитель руководителя Федерального казначейства.

Федеральное казначейство уже в течение двух лет занимается миграцией на российские продукты своих государственных информационных систем (их у него шесть) – и еще 20 дополнительных ИС. В качестве базовых компонентов ведомство рассматривает технологии Linux, PostgreSQL и 1С-fresh. Причем по последнему пункту Федеральное казначейство назначено оператором централизованной закупки бухгалтерского ПО для ФОИВ. Уже сейчас ведомство ведет бухгалтерский учет для 35 ФОИВ, в этом году планируется добавить оставшиеся 11 органов. Казначейство рассчитывает войти в ГЕОП как один из его операторов с собственной инфраструктурой.

История переноса базы данных АО «ВНИИЖТ» на отечественную платформу, которую рассказал на PGConf.Russia Анатолий Афиногенов, заместитель директора научного центра – начальник отдела разработки программного обеспечения института, оказалась довольно драматической. Институт занимается ежедневным составлением расписаний грузовых перевозок для РЖД. Для переноса использовался набор сценариев подобной миграции Ora2Pg, однако после него, естественно, код хранимых процедур пришлось доделывать вручную. Работали над проектом три человека. Тем не менее, специалисты института не только добились аналогичной с Oracle производительности, но и превысили ее.

Аналогичной работой, но более систематически занимались в компании «БАРС Груп» (г. Казань) Александр Кварацхелия, архитектор программного обеспечения, и Александр Чирков, архитектор ПО. В их проекте хранимых процедур оказались тысячи, поэтому даже ручная доработка процедур после сценариев Ora2Pg была бы слишком накладной. Поэтому они разработали универсальный транслятор с использованием транслятора Antlr4 (ANother Tool for Language Recognition). Причем вся система была реализована на PHP в виде веб-микросервисов. Компании также удалось справиться с переносом всех своих приложений, хотя количество программистов, которые были задействованы в работе, было существенно больше. Таким образом, практически все наиболее нагруженные приложения СУБД можно переносить на PostgreSQL, что обеспечивает процесс импортозамещения в части переноса баз данных на российские решения. ■

Банки
в роли провайдеров госуслуг

В Москве состоялся XX Международный форум «Электронные финансовые услуги и технологии» (iFin-2020), организованный Ассоциацией российских банков и компанией «АйФин Медиа». В нем приняли участие разработчики программного обеспечения и оборудования, консалтинговые и сервисные компании, предлагающие решения для финансового рынка. Интерес к мероприятию обусловлен масштабными изменениями, происходящими в сфере банковского обслуживания и смежных сегментах по инициативе регулятора, стремлением финтехкомпаний представить технологичные решения для оказания массовому клиенту широкого спектра услуг, в том числе дистанционных.

Развитие биометрической системы эксперты называют одной из тем, интерес к которой шагнул за пределы сферы финансовых институтов. В роли оператора этой системы, отвечающего за строительство соответствующей инфраструктуры, предоставление на ее базе сервисов и обеспечение требований безопасности, выступает «Ростелеком». Из доклада на форуме директора по развитию проектного офиса «Единая биометрическая система» компании «Ростелеком» Тимура Шаповалова стало известно, что в настоящее время 227 банков по всей стране собирают биометрические данные (фотография лица и запись голоса) в Единую биометрическую систему (ЕБС). Услуга, доступная гражданам в 13 тыс. отделений банков, находящихся в 1048 городах, занимает не более пяти-шести минут. Ряд банков уже реализовали кейсы, позволяющие дистанционно открыть счет. Предварительно сдав биометрические данные в любом банке, можно стать клиентом другой финансовой организации без необходимости посещения ее отделения.

В настоящее время реализуются пилотные проекты по внедрению возможностей ЕБС в различных сегментах, что, как ожидается, упростит доступ к государственным и муниципальным услугам через МФЦ, порталы, городские онлайн-сервисы, а также на ряд социальных объектов. Наряду с этим прорабатывается возможность использования ЕБС для организации удаленного судопроизводства.

Приняты в первом чтении законопроекты, расширяющие возможности применения ЕБС на другие отрасли. Сейчас в стадии согласования с федеральными органами исполнительной власти норма о праве МФЦ осуществлять сбор биометрических образцов в единую систему. В июле текущего года начнет действовать норма об использовании ЕБС для получения облачной квалифицированной электронной подписи. В декабре вступят в силу поправки в законодательство о нотариате, разрешающие нотариусам оказывать услуги клиентам, прошедшим идентификацию через ЕБС. В выступлении директора по развитию проектного офиса «Единая биометрическая система» были представлены различные сценарии идентификации гражданина с использованием мобильного приложения «Биометрия».

Примечательно, что архитектура ЕБС позволяет подключить использование и иных помимо лица и голоса биометрических модальностей (радужная оболочка, сетчатка глаза, палец, геометрия кисти руки, рисунок вен, силуэт или походка). Эксперты отмечают низкую точность таких модальностей, как походка или силуэт. Однако их можно использовать в комбинации с другими. Например, если лицо человека оказалось закрыто шляпой или газетой, то в этот промежуток времени его можно идентифицировать по походке либо силуэту.

По мере развития цифрового общества возрастает значение цифрового банкинга. Об этом шла речь в выступлении директора по продажам компании «АйСимплЛаб» Алексея Колесникова, который заострил внимание аудитории на направлениях, актуальных для банков с точки зрения повышения лояльности клиентов и увеличения доходов. Государство заинтересовано в том, чтобы банки, выполняющие обязательства по сбору биометрических данных, будучи доверенной средой, являлись провайдерами госуслуг. Прогнозируется, что финансовые учреждения будут играть ключевую роль во взаимодействии государства и общества по цифровым каналам.

Чтобы соответствовать инициативам регулятора и рассчитывать на получение прибыли, банкам предстоит перестраивать бизнес-процессы работы с клиентами, которым можно будет предлагать услуги не только банковского

характера. Для этого нужна гибкая мультифакторная платформа дистанционного банковского обслуживания (неограниченная по функционалу и каналам взаимодействия). Кроме того, банк должен взять на себя роль провайдера небанковских продуктов, сервисов и осуществлять свою деятельность там, где удобно клиенту.

В рамках проектов, расширяющих возможности финансовых учреждений, клиенту можно предоставлять от лица банка услуги, за которыми он идет в другие многофункциональные кабинеты. Но банк может дополнить такой инструмент своими «фишками» и сервисами, предложив клиенту, например, доступ к услугам Пенсионного фонда, Бюро кредитных историй. Как ожидается, на эти сервисы клиенты будут подписываться. В регионах формируется интерес к подобным услугам. В частности, региональные банки на базе своих отделений открывают рабочие места МФЦ. «Клиенты приходят в банк за получением госуслуг. Эта тенденция может быть подхвачена и развита цифровыми банками», – полагает эксперт.

Несмотря на активное продвижение дополнительных услуг, финансовые транзакции останутся основным банковским функционалом, который совершенствуется по мере развития системы быстрых платежей (СБП), B2B переводов. Сервис СБП позволяет физическим лицам мгновенно (в формате 24×7) переводить деньги по номеру мобильного телефона себе или другим лицам независимо от того, в каком банке открыты счета отправителя либо получателя средств. На форуме отмечалось, что классические переводы с использованием реквизитов карты и переводы через СБП будут дополнять друг друга.

Банки не перестают думать о привлечении новых клиентов, в частности представителей малого бизнеса. И одна из проблем состоит в том, что обеспечить лидогенерацию (маркетинговая тактика поиска потенциальных клиентов по контактным данным) «холодными» звонками становится все труднее. Входящие звонки вызывают раздражение,

абоненты пользуются спам-фильтрами. Банки переключились на формирование входящих заявок, оптимизируют труд операторов. Помощниками в подобных случаях являются готовые программные инструменты, в частности SaaS-решения, позволяющие автоматизировать и настроить работу операторов. Преимущества такого ПО в том, что оператор не теряет время на дозвон и занят исключительно общением с потенциальными клиентами.

Современные технологии искусственного интеллекта, роботизации активно проникают и в этот сегмент решений, о чем рассказала на форуме коммерческий директор сервиса «Скорозвон» Дилара Музафарова. Обработку звонков на первой линии планируется поручить роботам. Они успешно справляются с классификацией входящих заявок и переводом звонка на более профильную вторую линию. Преимущества очевидны: если с помощью облачного сервиса «Скорозвон» оператор может провести 300 разговоров за 12-часовую смену, то робот справится с такой же нагрузкой за две-три минуты.

Атмосфера на XX форуме «Электронные финансовые услуги и технологии» располагала к тому, чтобы проследить основные этапы развития отрасли на примере конкретных решений, направлений и компаний. Этот прием использовал в своем выступлении, посвященном новым территориям онлайн-банкинга для юридических лиц, заместитель директора по развитию сервиса Faktura.ru Владимир Михайлов. За два десятилетия одноименная мультибанковская платформа превратилась в экосистему. Поначалу сервис развивался от потребностей банков. Теперь, когда компания нарастила внутренние экспертные компетенции, дав рынку возможность оценить себя, сервис предлагает банкам рекомендации, как развивать онлайн-банкинг.

Одна из рекомендаций состоит в необходимости сегментировать клиентскую базу. Разработанный для конкретного сегмента набор инструментов обеспечит возможность таргетировать продуктовые предложения. В рамках планов развития сервисов с использованием технологий машинного обучения компания намерена дать возможность интеллектуального подбора маржи в зависимости от профиля клиента.

Резюмируя выводы одной из дискуссий, посвященных трендам развития электронного банкинга в 2020 г., генеральный директор «АйФин Медиа» Андрей Бурдинский на правах модератора заметил, что в форуме приняли участие компании, которые стимулируют развитие финансовых технологий в России. Сегодня разработчики услуг и решений зачастую отталкиваются не от запросов рынка, которые неочевидны или плохо формализованы, а от идей авторов инноваций, берясь за их воплощение, несмотря на то что попутно приходится формировать спрос. ■

www.connect-wit.ru

Как добиться космического успеха вместе

29 января в выставочном центре «Крокус Экспо» прошла конференция SpaceCom Digital Russia 2020. На протяжении последних лет в рамках деловой программы форума CSTB проводилась секция «Мультисервисные спутниковые сети и VSAT». Это мероприятие переросло прежний формат, поэтому было принято решение провести отдельную конференцию.

Михаил Глинка, директор Департамента продаж операторских и корпоративных решений ГП КС, выступил с докладом на тему «Современные системы спутниковой связи в Ku- и Ka-диапазонах, основные результаты работы в 2015–2019 гг. Перспективная система спутниковой связи на ВЭО «Экспресс-РВ».

ФГУП «Космическая связь» создало в Ku-диапазоне три сети спутниковой связи. Первая сеть VSAT на базе оборудования iDirect Evolution была введена в эксплуатацию в 2009 г.: она состоит из пяти центральных коммутационных станций, размещенных в трех центрах космической связи; в сети iDirect Evolution работает сейчас более 1000 станций; суммарная пропускная способность сети составляет 350 Мбит/с; ежемесячный объем передаваемых данных – 14,61 Тбайт.

Вторая сеть VSAT (включает в себя две подсети) работает на оборудовании Hughes HN. Первая подсеть введена в эксплуатацию в 2015 г.: в ней работает более 1100 станций; суммарная пропускная способность подсети составляет 114,5 Мбит/с; ежемесячный объем передаваемых данных – 13,47 Тбайт. Вторая подсеть введена в эксплуатацию в 2017 г.: в ней работает более 100 станций; суммарная пропускная способность подсети составляет 46,5 Мбит/с; ежемесячный объем передаваемых данных – 0,34 Тбайт.

Третья сеть VSAT на базе оборудования MCTAPUHP-200 введена в эксплуатацию в 2019 г.: она состоит из пяти центральных коммутационных станций, размещенных в трех центрах космической связи; в сети VSAT MCTAPUHP-200 работает более 100 станций; суммарная пропускная способность составляет 68,3 Мбит/с; ежемесячный объем передаваемых данных – 2,1 Тбайт.

Совместный проект ГПКС и Eutelsat в Ka-диапазоне частот был запущен на территории России в 2012 г. с использованием емкости Ka-SAT. Используемая платформа – Viasat SurfBeam 2. В настоящее время в этой сети работает не более 1100 станций (в 2015 г. было 6000 станций). Суммарная пропускная способность сегмента сети на территории России составляет 5,1 Гбит/с; ежемесячный объем передаваемых данных – 13,59 Тбайт.

Спутниковая система высокоскоростного доступа (ССВД) в Ka-диапазоне частот – это бриллиант в короне ГП КС. Восточный фрагмент сети введен в эксплуатацию в 2015 г., западный – в 2016 г. В сети работает более 16 000 станций; суммарная пропускная способность системы составляет 12 Гбит/с; ежемесячный объем передаваемых данных – более 410 Тбайт (290 Тбайт в восточном сегменте и 120 – в западном); среднемесячное потребление трафика на один терминал – 28,9 Гбайт в восточном сегменте, 23,3 Гбайт – в западном; распределение абонентских устройств в ССВД – 66% в восточном сегменте, 34% – в западном.

Михаил Глинка также представил информацию, касающуюся основных показателей сетей связи Ku/Ka-диапазонов по состоянию на октябрь 2019 г. Так, общее количество земных станций спутниковой связи составляет 19,4 тыс., из них: в сетях Ku-диапазона – 2,3 тыс. станций; в сетях Ka-диапазона – 17,1 тыс. станций. Суммарная пропускная способность созданных сетей связи достигает 17,7 Гбит/с, из них: в сетях Ku-диапазона – 0,57 Гбит/с; в сетях Ka-диапазона – 17,1 Гбит/с. Суммарный объем ежемесячного трафика, генерируемого сетями связи, составляет 454,11 ТБ, из них: в сетях Ku-диапазона – 30,52 ТБ; в сетях Ka-диапазона – 423,59 ТБ.

Говоря о проекте системы спутниковой связи на ВЭО «Экспресс-РВ», Михаил Глинка отметил, что общая пропускная способность системы составит 4,4 Гбит/с. При этом обеспечивается возможность работы абонентских терминалов с антенной диаметром 60–70 см со скоростью до 80 Мбит/с на прием.

Андрей Лобанов, руководитель группы эксплуатации Технического департамента МОКС «Интерспутник», рассказал о проекте OpenTeleport, который был создан в сотрудничестве с государственными и частными партнерами со всего мира. Платформа OpenTeleport обеспечивает быстрый поиск информации о необходимых услугах и оборудовании

по всему миру с помощью интерактивной карты (более 15 фильтров помогают сузить поиск). Сейчас платформа позволяет направлять запросы об оказании следующих вдов услуг: спутниковое вещание; передача данных; VSAT; подвижная спутниковая связь; VNO; TT&C; мониторинг качества спутниковой связи.

Можно создать личный кабинет, чтобы отслеживать ранее направленные запросы, или же стать поставщиком и разместить свои телепорты на сайте. На OpenTeleport также имеется раздел продажи нового и подержанного оборудования.

Андрей Бурашников, директор направления «Телекоммуникации» компании «Теком», выступил с докладом на тему «Телепорт под контролем». Он представил ЦИСУСС «NB XT EM» – инструмент контроля использования ресурсов и планирования развития технологической сети связи.

Основными предпосылками внедрения решения ЦИСУСС от компании «Теком» Андрей Бурашников назвал: наличие большого парка разнородного оборудования, необходимость единого централизованного контроля, необходимость единых обобщенных критериев оценки состояния оборудования, необходимость автоматического формирования унифицированных отчетов и автоматизации регламентов эксплуатации оборудования.

Работу пленарной сессии завершил Максим Самсонов, первый заместитель генерального директора GS Labs, выступивший с докладом на тему «Опыт разработки и внедрения системы гибридной доставки контента». Он представил три варианта гибридной доставки контента: нишевое решение (на примере курорта в Камбодже и российской воинской части на Северной Земле); резервирование канала; улучшение сервиса вместе с улучшением доступа к Интернету.

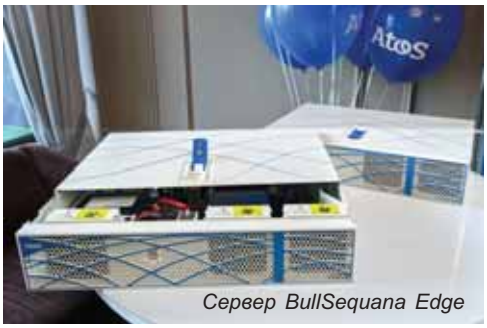
После перерыва состоялась дискуссия на тему «Digital SpaceCom – цифровое перерождение», в ходе которой эксперты отрасли обсуждали, как трансформируются спутниковые коммуникации в новой цифровой реальности. В качестве центральных спикеров дискуссии выступили: Константин Ланин, глава представительства Hughes Network Systems в России и СНГ; Виктор Стрелец, научный консультант ФГУП «НИИР»; Даниил Нирман, руководитель направления «Спутниковый Интернет», «Триколор»; Алексей Величко, руководитель отдела продаж ООО «Евтелсат Нетворкс», и Максим Самсонов, первый заместитель генерального директора GS Labs.

Из многих фраз, прозвучавших в ходе дискуссии, нам хотелось бы особо отметить одно откровенное высказывание Константина Ланина, который заявил о том, что на сегодня производители спутникового оборудования уже подошли к стоимостному пределу, ниже которого они просто не могут опуститься, так что ожидать снижения цен на абонентское оборудование нет смысла: «Существующие технологии изготовления микросхем и печатных плат в ближайшие годы не позволят нам снизить цены в разы, как этого хотят операторы спутниковой связи, – это реальность, с которой всем придется смириться».

После дискуссии участники конференции получили возможность задать вопросы в ходе публичного интервью с Мартином Джарольдом, вице-президентом GVF – глобального некоммерческого объединения спутниковой индустрии, основанного в 1997 г. со штаб-квартирой в Лондоне. Главный вывод, который мы можем сделать по итогам выступления мистера Джарольда, заключается в том, что основополагающим драйвером развития спутниковой связи на ближайшие годы станут аппараты ультравысокой пропускной способности (до 1 Тбит/с).

Работа конференции завершилась бизнес-игрой #SpaceQuest: «Как добиться космического успеха вместе», в которой приняли участие эксперты российского рынка спутниковых коммуникаций. ■

Atos на грани возможного

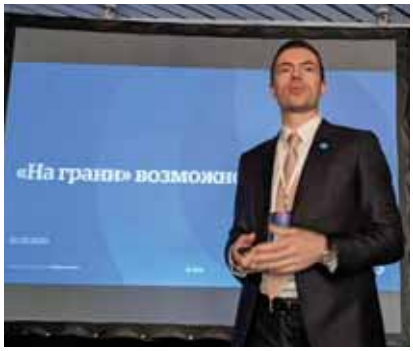


Сервер BullSequana Edge

20 февраля в Москве компания Atos провела презентацию высокопроизводительного сервера для периферийных вычислений BullSequana Edge. Сервер предназначен для использования в средах промышленного Интернета вещей и призван отвечать на вызовы Индустрии 4.0, в условиях которой IoT-данные необходимо обрабатывать и анализировать в режиме реального времени. В роли основного докладчика выступил Роман Гоц, директор Департамента большие данные и безопасность (BDS), ООО «Атос АйТи Солюшенс энд Сервисез». Он рассказал об инновационных технологиях и архитектуре, позволяющих в защищенном режиме управлять IoT-данными и обрабатывать их в непосредственной близости от источника, что обеспечивает высокую скорость работы. Приглашенный эксперт Atos Бенуа Кушон проанализировал возможности и преимущества решения BullSequana Edge при работе с приложениями на основе AI.

Ключевыми преимуществами сервера BullSequana Edge являются: безопасность и конфиденциальность – и данные, и сам сервер защищены посредством современной системы обеспечения безопасности; почти мгновенная реакция системы – данные обрабатываются в режиме реального времени; автономность – уменьшенная зависимость заказчика от доступности облачных сред, ЦОД и сетевых подключений, обеспечивается бесперебойная работа приложений в случае нестабильного подключения к сети, данные могут передаваться по радиоканалу, по GSM или Wi-Fi; интерактивность – данные из разных источников и разного формата могут анализироваться в реальном времени; экономическая выгода – снижение расходов на создание инфраструктур ЦОД и сетей.

Сервер BullSequana Edge на данный момент поддерживает три основные модели использования. Искусственный интеллект: Atos Edge Computer Vision обеспечивает углубленное извлечение и анализ «отличительных особенностей» (люди, лица, эмоции, поведение) для выполнения по результатам анализа действий в автоматическом режиме. Эта модель использования



Роман Гоц

Бенуа Кушон

поддерживает различные интеллектуальные камеры, например для видеонаблюдения, для согласованной работы в реальном времени и отслеживания действий без их нарушения. Большие данные (Big Data): Atos Edge Data Analytics позволяет компаниям оптимизировать свою работу с помощью прогнозирующих и директивных решений, Data Analytics основывается на базе озер данных, что делает данные достоверными и практичными. Atos Edge Data Container – это универсальное контейнерное решение может работать в периферийных системах и выступает в качестве децентрализованной ИТ-системы (от одной серверной стойки до целого контейнерного центра обработки данных). Оно может работать автономно за пределами сред центров обработки данных и без необходимости функционировать локально.

Серверы BullSequana Edge уже доступны для заказа – их можно приобрести в виде отдельного решения или совместно с программной платформой, включая Atos Edge Computer Vision и Edge Data Analytics, или в виде контейнерной системы Atos Edge Data Container. Сервер BullSequana Edge прошел IoT-сертификацию Microsoft Azure. Серверы Edge в максимальной конфигурации обладают следующими характеристиками: процессор Intel Xeon D-2187NT; 512 ГБ ОЗУ; 2 × SSD 960 ГБ; порты 2 × 1 GbE + 2 × 10 GbE; GPU 2 × Nvidia T4 16 ГБ; беспроводные соединения – Wi-Fi, Bluetooth, LoRaWAN, 3G/4G. ■

Есть такая технология! Сети LoRaWAN в мире и России

LoRaWAN
как надежная и безопасная технология связи

Андрей ЭКОНОМОВ,
участник технического комитета LoRa Alliance, к. ф.-м. н.

В настоящее время в большинстве развитых стран мира в дополнение к мобильной связи активно развиваются радиосети нового типа – Интернета вещей (IoT) класса LPWAN (LowPower WAN), работающие на нелицензируемых (общедоступных) радиочастотах. В Российской Федерации с этой целью выделен диапазон 868 МГц (частоты 864–869,2 МГц), в котором уже построены сети как общемирового стандарта LoRaWAN, так и локальных спецификаций, например XNB и NB-Fi.

Базовые характеристики LoRa/LoRaWAN

По состоянию на начало 2020 г. именно стандарт LoRaWAN является драйвером развития направления IoT (Internet of Things) во всем мире и используется в качестве основного инструмента для управления критически важной инфраструктурой, транспортом, а также производством, здравоохранением, муниципальным и сельским хозяйством. И это далеко не пилотные проекты, например, в России уже более 10 тыс. уличных светильников управляются сетью LoRaWAN АО «ЭР-Телеком Холдинг».

Конференции, посвященные технологии LoRaWAN, собирают тысячи участников со всего мира, например ежегодная The Thing Conference в Нидерландах. В LoRa Alliance входит более 500 компаний, среди которых можно назвать мировых гигантов – Google, Alibaba, Orange, CISCO, NEC и IBM, а также отметить трех участников из России – «ЭР-Телеком», МТТ и «Лартех».

Спецификация LoRaWAN развивается с 2015 г.: LoRa – это сокращение от слов Long Range («дальнее действие»). Беспроводные сети базируются на методе модуляции радиоинтерфейса LoRa, запатентованном Semtech Corporation, и на открытом протоколе LoRaWAN, разработанном исследовательским центром IBM Research в партнерстве с Semtech Corporation.

К отличительным особенностям стандарта LoRaWAN следует отнести [2]:

- помехоустойчивую модуляцию, относящуюся к классу ЛЧМ (линейно-частотной модуляции), в англоязычной терминологии – CSS (Chirp Spread Spectrum), что позволяет уверенно принимать сигнал от абонентских устройств на уровнях ниже уровня шума;
- длительную работу абонентских устройств без подзаряда батарей (до десяти лет от одного аккумулятора типа «АА»);
- существование трех классов абонентских терминалов с разными скоростями отклика на сообщения от сети и уровнями энергопотребления;
- автоматический роуминг между сетями разных операторов;
- возможность дистанционного обновления программного обеспечения абонентских терминалов

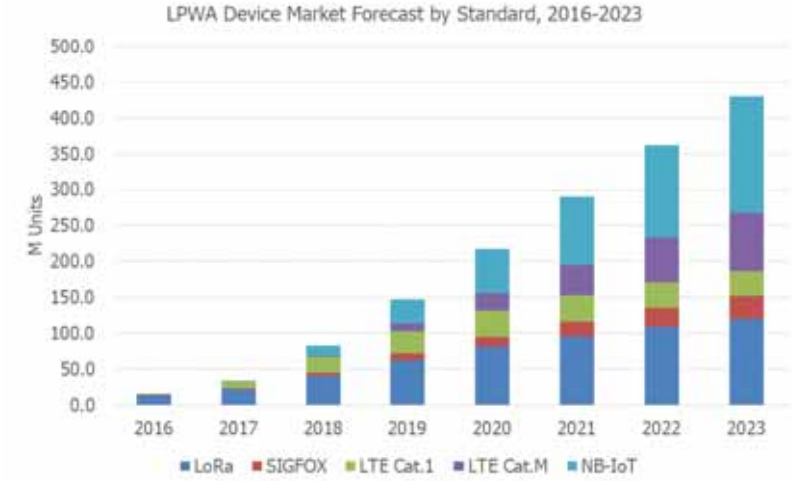


Рис. 1. *Статистика и прогноз поставок абонентских устройств IoT 2016–2023 гг. (в млн штук, по данным LoRa Alliance)*

через радиоэфир (технология FUOTA – Firmware Upgrade Over The Air);
- опцию беспроводного репитера с батарейным питанием для покрытия подвалов и экранированных помещений;
- режим вещания Multicast (одновременный прием одного сообщения несколькими датчиками);
- мультилатерационную геолокацию, позволяющую определять координаты абонентского терминала с точностью до 200 м без использования GPS-приемника.

Сегодня нередко можно столкнуться с утверждениями, что беспроводные системы связи в общедоступных диапазонах частот якобы не способны обеспечивать уверенную связь из-за неконтролируемых помех. На самом деле в нелицензируемых диапазонах для средств радиоэлектронной связи (РЭС) действуют даже более строгие правила, чем в лицензируемых. В частности, в полосе 868 МГц согласно [3] ограничены: во-первых, излучаемая мощность (на большинстве каналов – не более 25 мВт), во-вторых, время нахождения в эфире (как правило, не более 1%). Причем наказания за нарушения указанных величин точно такие же, как и за несанкционированное вещание на лицензируемых частотах. Так что любые радиосистемы гражданского назначения вне зависимости от способа выделения спектра – по стандартным процедурам (лицензионный) или по упрощенным (нелицензионный) – могут пострадать от преднамеренных радиопомех. Однако это в равной мере незаконно, и способы борьбы с такими помехами известны и одинаково доступны всем пользователям радиоспектра.

Ключевое преимущество работы в нелицензируемом диапазоне частот, особенно в отечественных реалиях, – это дешевизна и быстрота развертывания сети.

Целевая область применения технологии LoRa/LoRaWAN в системах IoT:
- автономные устройства без внешнего электропитания;
- устройства, генерирующие малые потоки данных;
- устройства, сравнительно редко выходящие в эфир;
- территории, покрытие на которых необходимо развернуть быстро и с минимальными затратами.

Таким образом, несмотря на возможный быстрый рост технологии NB-IoT, конкурирующей с LoRaWAN, последняя, по мнению большинства аналитиков отрасли, в перспективе сохранит значимую долю мирового рынка, что подтверждает прогноз поставок абонентских устройств IoT [4] (рис. 1).

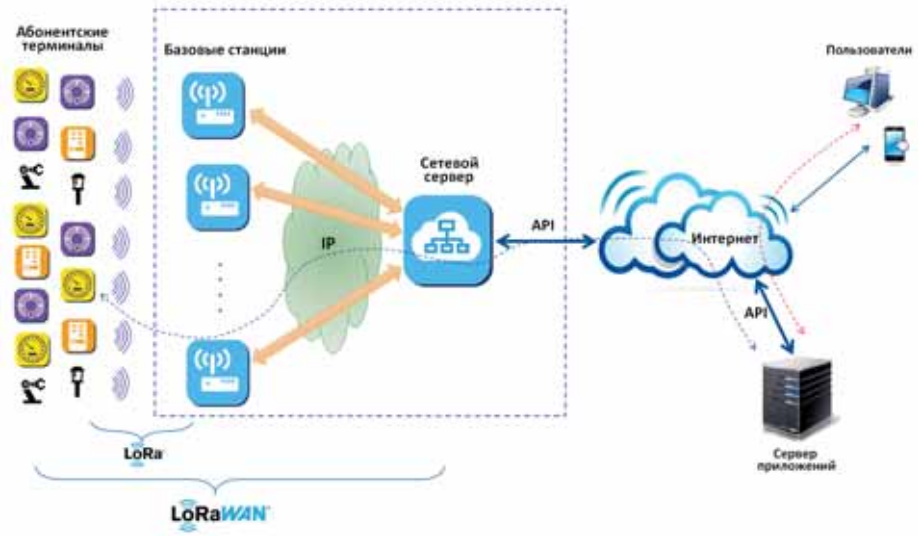


Рис. 2. *Архитектура сети LoRaWAN*

Описание архитектуры сети LoRaWAN

Сеть LoRaWAN состоит из следующих элементов: абонентские терминалы, базовые станции (шлюзы), сетевой сервер и сервер приложений (рис. 2).

Абонентский терминал представляет собой обобщающее наименование для сенсоров, датчиков, счетчиков, актуаторов и радиомодулей IoT, устанавливаемых на стороне пользователя. Стандарт LoRaWAN [2] определяет следующие классы терминалов (см. таблицу).

Таблица. Классы терминалов LoRaWAN

Класс устройства	Формат работы
A	Сеанс связи инициирует терминал. Его основная задача – передавать данные от устройства к сети; прием данных возможен только сразу после передачи – терминал открывает два окна приема. Терминалы класса A применяются в приложениях, где передача данных от сети возможна только как ответная реакция на получение данных от конечного устройства и требуется максимальное время работы от автономного источника питания.
B	В дополнение к ресурсам класса A здесь появляется возможность по расписанию принимать данные от сети, т. е. сеанс связи может быть инициирован как устройством, так и сетью. Терминалы класса B используются в случаях, когда прием данных от сети требуется, но не моментально, а по назначенному заранее расписанию (например, раз в 32 сек). Тем самым соблюдается баланс между скоростью реакции устройства на внешнюю команду и его энергопотреблением.
C	Устройства класса C постоянно готовы принимать данные от сети – прием данных прекращается только во время передачи данных самим устройством. Таким образом, сеанс связи, как и для устройства класса B, может быть инициирован и устройством, и сетью. Терминалы класса C применяются в приложениях, где быстрота реакции на команду, полученную от сети, важнее экономии электропитания, а также в тех кейсах, где устройству необходимо получать через IoT-сеть большие объемы данных.

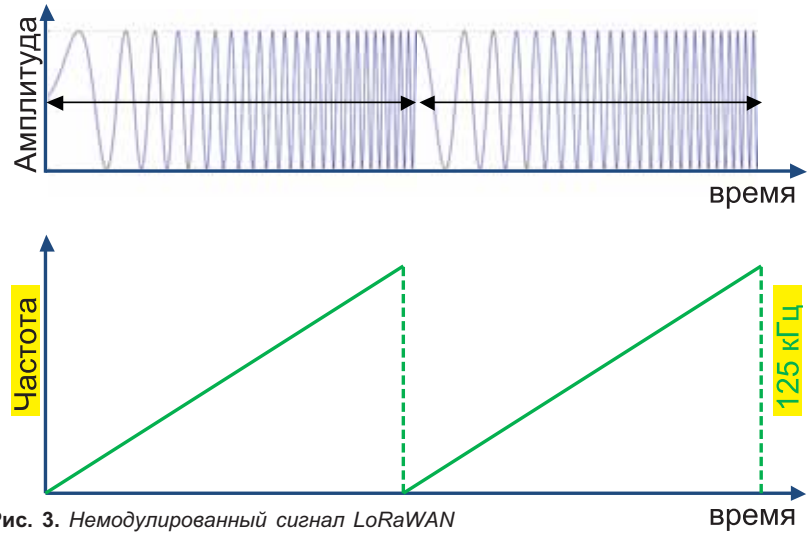


Рис. 3. *Немодулированный сигнал LoRaWAN*

Базовая станция – типовое понятие для многих радиосистем, в том числе и для радиосетей IoT. Применительно к сети LoRaWAN (как и во многих других радиосетях) базовая станция (БС) выполняет функции сопряжения и взаимодействия радиосети с абонентским терминалом и концентрации нагрузки с группы терминалов, поэтому в документации LoRa Alliance она именуется шлюзом и/или концентратором. Тем не менее обычно в текстах используется более широкое и общепринятое понятие «базовая станция».

Сигнал от одного терминала может приниматься несколькими БС. Совокупность базовых станций оператора связи обеспечивает территорию радиопокрытия сети и прозрачную двунаправленную передачу данных между конечными устройствами и сетевым сервером. Базовая станция оснащена приемно-передающей антенной (секторной или всенаправленной – омни), а также (опционально) GPS/ГЛОНАСС-антенной для прецизионной синхронизации внутренних часов и определения точных координат приемно-передающей антенны.

Сетевой сервер представляет собой программно-аппаратный комплекс (ПАК), управляющий радиосетью, контролирующий радиосеть и выполняющий маршрутизацию пакетов данных от абонентских терминалов до соответствующих серверов приложений.

- **Управление радиосетью**. Сетевой сервер сети LoRaWAN выбирает БС для передачи сообщений в направлении «вниз» (downlink), принимает решения о необходимости изменения скорости передачи данных для каждого терминала, мощности передатчика, контролирует заряд батарей конечных устройств, шифрует данные и т. п.
- **Контроль радиосети** включает в себя функции мониторинга, сбора статистики и аварийного информирования.
- **Маршрутизация**. Каждый пакет данных, отправляемый абонентским терминалом, имеет в своем составе уникальный идентификатор DevAddr, а на сетевом сервере хранится запись о соответствии DevAddr и URL сервера приложений, которому предназначена информация от терминала (датчика). На основании этого соответствия сетевой сервер выполняет маршрутизацию пакета до сервера приложений, где и происходит его дальнейшая обработка приложением сервис-провайдера.

Сервер приложений – это платформа, которая выполняет первый уровень шифрации/дешифрации и обработку данных, получаемых от терминалов и направляемых к ним. Помимо работы с данными сервер приложения может управлять терминалами с уровня приложения, например, переводить их в режим работы другого класса, управлять опцией адаптивной передачи данных, Multicast и т. п.

Особенности радиопротокола LoRaWAN

Модуляция LoRa базируется на импульсах линейно-частотной модуляции (ЛЧМ) (Chirp Spread Spectrum – CSS) (рис. 3). В отличие от систем Sigfox, XNB и NB-Fi, использующих для связи узкую полосу в 100 Гц и фазовую модуляцию, данные в сетях LoRaWAN передаются датчиками в полосе шириной 125 кГц, т. е. более чем в 1000 раз шире.

Каждое устройство стандарта LoRaWAN излучает сигнал с изменяющейся частотой (см. рис. 3). Модуляция LoRaWAN заключается в обрыве цикла на одной из промежуточных частот (рис. 4) и новом его начале, именно это и кодирует передаваемый символ. Всего существует 128 возможных различных частот обрыва цикла в каждом частотном канале (шириной, напомним, 125 кГц), а значит, один ЛЧМ-импульс кодирует 7 бит данных.

Поскольку частота сигнала LoRaWAN меняется в диапазоне 125 кГц, узкополосная помеха практически не оказывает влияния на успешность декодирования сигнала LoRaWAN. Еще одно преимущество, вытекающее из особенности модуляции LoRaWAN, – устойчивая работа на движущихся объектах (поездах, автомобилях и т. п.), поскольку доплеровский сдвиг частоты заметно не влияет на успешность передачи сигнала.

И последнее. Модуляция и канальное кодирование LoRaWAN позволяют осуществлять прием полезной информации даже при отрицательных значениях отношения сигнал/шум (SNR до –20 дБ). Кодирование (не путать с шифрованием) – это добавление к передаваемым пользовательским данным избыточной (контрольной) информации для повышения

вероятности успешного приема. Степень избыточности определяется соотношением CodeRate (CR) вида 4/5, означающим, что на каждые 5 бит передаваемой информации 4 бита – полезные данные и один – контрольный бит. От значения CodeRate зависит скорость передачи полезной информации. В LoRaWAN используются CodeRate от 4/5 до 4/8.

В целях экономии заряда батарей абонентских устройств и емкости сети датчики системы LoRaWAN выходят в эфир на одном из восьми частотных каналов [1] без предварительной синхронизации с сетью, в отличие от, скажем, GSM, где каждому абоненту сеть выделяет на время разговора персональный таймслот на определенном частотном канале. Это создает вероятность внутрисетевых коллизий: вдруг две двери откроются одновременно, и соответствующие сенсоры выйдут в эфир в один и тот же момент на одном частотном канале? Примет ли сеть сигнал от них, или они заглушат друг друга, или один заглушит другой?

Стандартом LoRaWAN [2] определены так называемые Spreading Factor (SF) – коэффициенты расширения спектра. Спецификацией [1] их предусмотрено всего шесть – от SF7 до SF12. SF – это «скорость» изменения частоты в ЛЧМ-импульсе: чем выше SF, тем медленнее меняется частота (рис. 5). Изменение SF на единицу означает увеличение длительности импульса в два раза. Для SF7 и полосы 125 кГц длительность импульса минимальна и составляет 1,024 миллисекунды.

Чем больше значение SF, тем медленнее передаются данные, но тем выше способность системы распознать их без ошибок: время передачи одного сообщения в сетях LoRaWAN составляет от 0,2 до 2,5 сек. SF каждому абонентскому устройству назначает сетевой сервер (NS – Network Server) по алгоритму ADR (Adaptive Data Rate – адаптивная скорость передачи данных) на основании измерений отношения сигнал-шум (Signal-to-Noise Ratio – SNR), выполненных базовой станцией. Если абонентские терминалы находятся в разных радиоусловиях относительно базовой станции (например, один – рядом с БС, другой – далеко, или одно устройство – у окна квартиры, второе – за капитальной стеной), то передавать данные они будут с разными SF и интерферировать друг с другом не будут, даже в случае наложения сигналов друг на друга по времени на одном частотном канале. Ведь в силу разных скоростей изменения частоты у передатчиков с разными SF такие устройства будут представлять друг для друга лишь узкополосную помеху, что, как уже было сказано, легко компенсируется канальным кодированием.

А что будет, если базовая станция примет одновременные сообщения от двух устройств с одинаковым SF? Возникнет коллизия: либо одно, либо оба сообщения будут потеряны в результате интерференции. Однако это произойдет только на одной базовой станции, в то время как сигнал от каждого абонентского устройства LoRaWAN в профессионально спланированной и грамотно построенной сети принимают минимум три БС – именно такое количество базовых

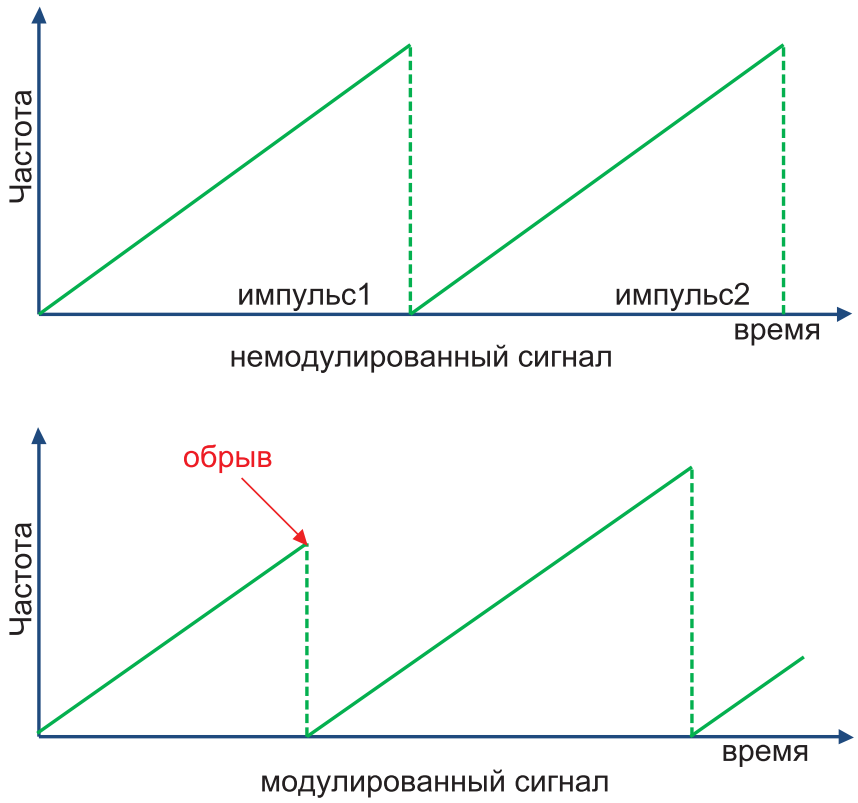


Рис. 4. *Модулированный сигнал LoRaWAN в сравнении с немодулированным*

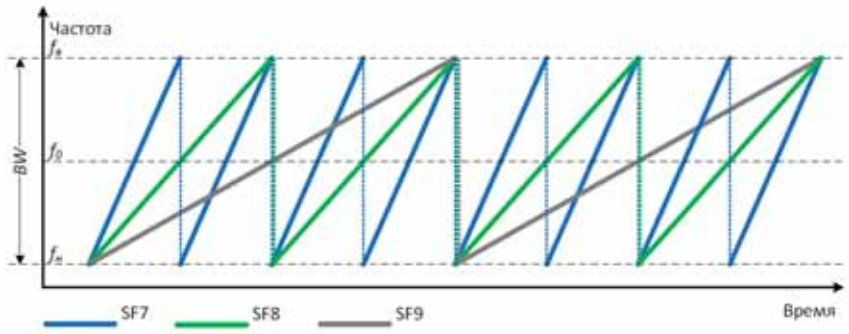


Рис. 5. *Модулированный сигнал LoRaWAN в сравнении с немодулированным*

станций необходимо для корректной работы опции геолокации методом TDoA. И если на одной БС возникнет коллизия, то прием сообщений успешно пройдет через другие базовые станции. В сетевом сервере LoRaWAN даже существует специальный таймер (длительностью 250 мс), чтобы дождаться, пока сообщение от определенного абонентского устройства будет получено всеми возможными БС с целью выбрать среди них наилучшую (с точки зрения SNR) на тот случай, если потребуется отправка сообщения от сети к датчику (подтверждение приема или MAC-команда).

В исследовании [5], проведенном компаниями MachineQ и Semtech, установлено, что восемь восьмиканальных БС LoRaWAN за сутки в состоянии принять один миллион сообщений от абонентских устройств. А если надо больше? Ответ простой – нужно увеличивать количество базовых станций. Ведь в отличие от сотовых систем связи базовые станции LoRaWAN не ведут постоянного вещания пилотных (как в LTE) или широковещательных (как в GSM) сигналов, так что установка новых БС не приводит к повышению внутрисетевой интерференции. Основную часть времени БС LoRaWAN работают на прием, а режим передачи включается лишь в редких случаях отправки команды управления или подтверждения приема на абонентское устройство. Также для покрытия помещений можно использовать репитер LoRaWAN (его спецификация на данный момент находится на финальном утверждении в техническом комитете LoRa Alliance). Репитер позволит улучшить (т. е. уменьшить номер) SF для сообщений, отправляемых indoor-датчиками, что снизит вероятность коллизий, поскольку, как уже было отмечено, сообщения с низким SF передаются многократно быстрее, чем сообщения с высоким SF.

Обеспечение безопасности передаваемых данных

В сети IoT LoRaWAN используется многоуровневая система безопасности передачи данных (рис. 6).

Первый уровень. AES-шифрование на уровне приложения (End-to-End, т. е. между абонентским терминалом и клиентским сервером приложений) с помощью 128-битного переменного сессионного ключа Application session key (AppSKey). Такой ключ шифрования хранится в абонентском терминале и на сервере приложений – он недоступен оператору сети (доступ к AppSKey есть только у клиента – владельца сервера приложений). Формирование сессионного ключа AppSKey происходит параллельно в абонентском терминале и на стороне сети в процессе активации терминала – через эфир AppSKey не передается.

Второй уровень. AES-шифрование и проверка целостности сообщений на сетевом уровне (между абонентским терминалом и сетевым сервером) с помощью 128-битного переменного сессионного ключа Network session key (NwkSKey). Такой уровень шифрования используется для защиты передаваемых сигнальных команд на MAC-уровне, а также для вычисления MIC (Message Integrity Code) в целях проверки целостности данных, передаваемых на радиоинтерфейсе. NwkSKey хранится в абонентском терминале и на сетевом сервере и недоступен клиенту (доступ к NwkSKey имеется только у оператора сети связи – владельца сетевого сервера). Формирование сессионного ключа NwkSKey также происходит параллельно в абонентском терминале и на стороне сети в процессе активации терминала – через эфир NwkSKey не передается.

Третий уровень. Стандартные методы аутентификации и шифрования интернет-протокола (IPsec, TLS и т. п.) при передаче данных по транспортной сети между узлами сети – базовая станция, сетевой сервер, Join-сервер, сервер приложений.

По команде приложения или сетевого сервера в любой момент возможен переход на новую

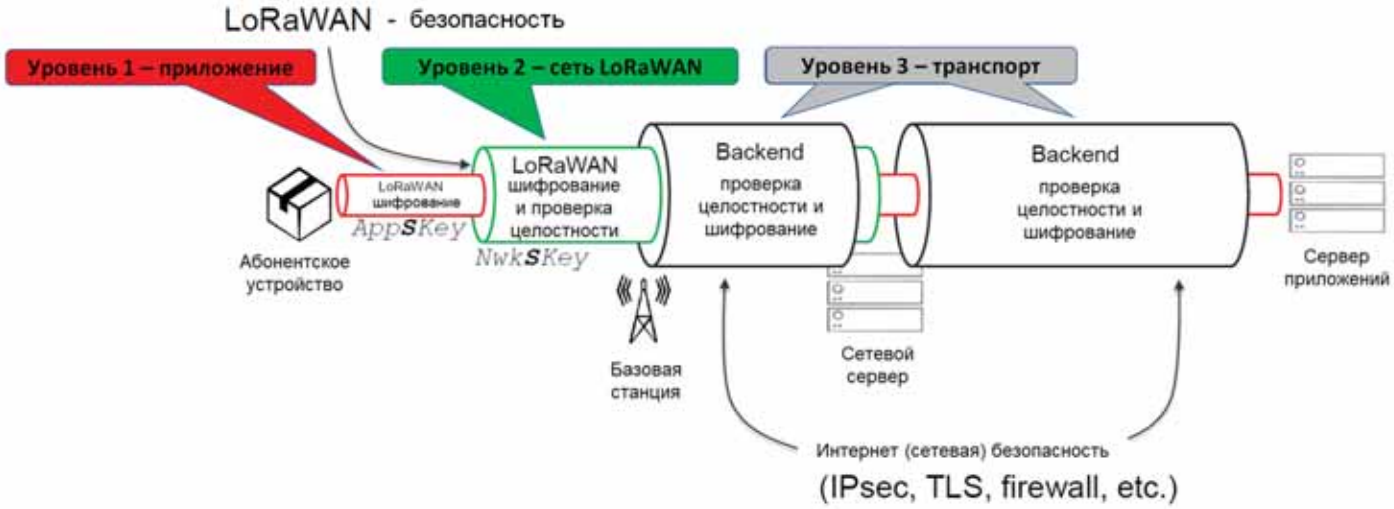


Рис. 6. *Общая схема безопасности данных в сети LoRaWAN*

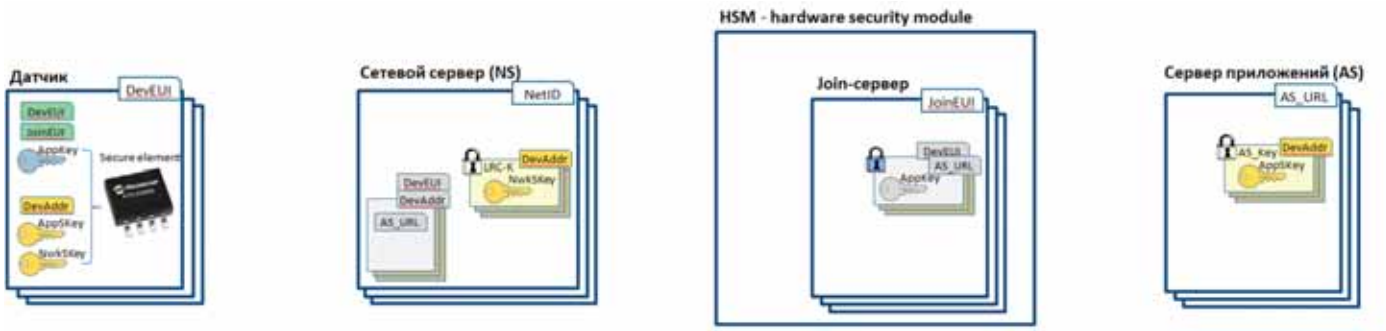


Рис. 7. *Схема хранения ключей шифрования*

сессию с генерацией нового комплекта ключей шифрования, что делает бесполезными старые ключи. Также есть возможность установки периодической генерации нового комплекта ключей NwkSKey и AppSKey.

В версии стандарта LoRaWAN V1.0.x [2] формирование сессионных ключей на стороне сети производится на сетевом сервере (NS), однако в версии V1.1 [6] для этих целей определяется выделенный сервер (так называемый Join-сервер) (рис. 7). Join-сервер может быть дополнительно защищен отдельным аппаратным модулем безопасности HSM (Hardware Security Module).

В этом случае для безопасной передачи сгенерированных сессионных ключей между серверами, а также хранения их на сетевом сервере и сервере приложений внедряются дополнительные ключи: AS_Key – для ключа AppSKey и LRC_K – для ключа NwkSKey.

На абонентском устройстве ключи шифрования опционально могут защищаться специальным аппаратным элементом безопасности Secure element (например, микроконтроллером Microchip ATECC608A), что исключит их компрометацию в случае физического воздействия на терминал.

Внедрение аппаратных средств защиты в сети и на терминале делает бесполезными попытки перехвата сессионных ключей при передаче их между серверами и попытки взлома серверов или абонентских устройств в целях извлечения сессионных ключей.

Рассмотренные мероприятия создают условия и для защищенного роуминга данных – безопасной авторизации датчиков в гостевой сети и защищенной передачи данных «домашнему» серверу приложений из «гостевой» сети.

В целях дополнительной защиты процесса генерации сессионных ключей Join-сервер может быть физически вынесен на территорию клиента или производителя устройств (рис. 8). В этом случае даже сотрудники оператора не смогут получить доступ к сессионным и корневым ключам шифрования абонентского терминала.

Несмотря на то что в России не требуется обязательная сертификация средств кодирования (шифрования) при передаче сообщений, не составляющих государственную тайну, по требованию заказчика используемые в стандарте LoRaWAN уровни шифрования AES-128 могут быть дополнены одним из стандартизованных в РФ алгоритмов, входящих в семейство ГОСТ Р 34.10-2012 [7], ГОСТ Р 34.11-2012 [8], или по алгоритму «Кузнечик» – согласно ГОСТ Р 34.12-2015 [9] и ГОСТ Р 34.13-2015 [10].

Для этого при производстве абонентских терминалов LoRaWAN предлагается устанавливать в них дополнительный микроконтроллер СКЗИ (средства криптографической защиты информации), сертифицированный ФСБ России и соответствующий требованиям, предъявляемым к шифровальным средствам класса КС3 (дистанционное банковское обслуживание, электронный документооборот в государственном секторе и т. д.). В качестве такого микроконтроллера могут быть использованы, например, микропроцессоры MIK51SC72D или MIK51AD144D отечественного производства компании «Микрон», сертифицированные ФСТЭК и ФСБ России, имеющие небольшие размеры (около 14 мм²) и малое энергопотребление.

Схема безопасности данных в сети LoRaWAN с дополнительным уровнем СКЗИ представлена на рис. 9.

Ключ шифрования уровня СКЗИ, например SubSKey (согласно ГОСТ Р 34.12-2015 [9]), прошивается в абонентский терминал LoRaWAN при производстве, как и корневой ключ уровней

Рис. 8. *Возможные сценарии размещения Join-сервера*

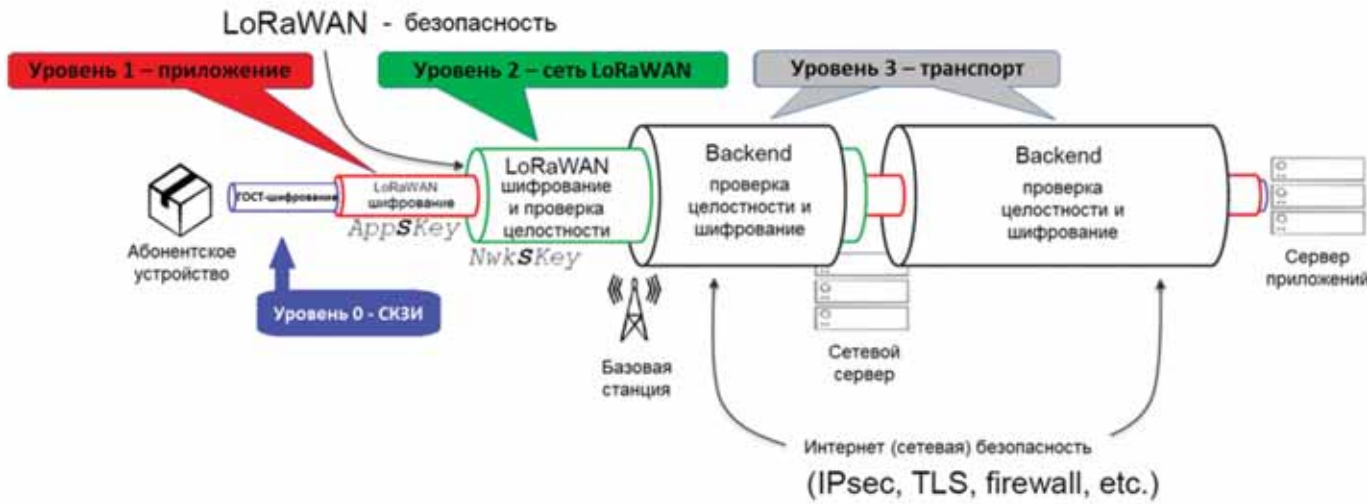


Рис. 9. *Схема внедрения отечественной СКЗИ в структуру шифрования данных сетей LoRaWAN*

шифрования 1–2 LoRaWAN, либо внедряется в терминал LoRaWAN вместе с микроконтроллером СКЗИ при введении терминала в эксплуатацию (с помощью специального слота). Дешифрация данных уровня СКЗИ выполняется на территории заказчика сервером приложений после дешифрации уровня приложения сессионным ключом AppSKey. Ключ шифрования SubSKey передается клиенту вместе с датчиком непосредственно самим производителем абонентского терминала и недоступен сотрудникам оператора сети LoRaWAN.

В завершение нашего обзора обобщим критерии безопасной передачи данных в сетях IoT и способы, которыми они реализуются в сети стандарта LoRaWAN.

End-to-End конфиденциальность пользовательских данных на уровне приложения – AES-шифрование с помощью сессионного ключа AppSKey.

Взаимная идентификация устройства и сети – процесс авторизации терминала при первичном подключении к сети (или по специальной команде о повторе авторизации).

Проверка целостности данных при передаче на радиоинтерфейсе – вычисление MIC-кода на основе сессионного ключа NwkSKey.

Конфиденциальность сигнальной информации (управляющих команд) – AES-шифрование MAC-команд с помощью сессионного ключа NwkSKey.

Безопасное хранение идентификаторов абонентского устройства и его полномочий – внедрение аппаратного элемента безопасности Secure element в абонентский терминал и защита HSM-модулем Join-сервера.

Оперативное устранение найденных уязвимостей на сетевой стороне и на абонентских терминалах – дистанционная смена ПО абонентских терминалов через эфир с помощью специфицированного LoRa Alliance механизма FUOTA (Firmware Upgrade Over The Air) [11] и установка обновлений на сетевой сервер и сервер приложений.

Возможность использования отечественных СКЗИ для критической инфраструктуры (КИ) – внедрение дополнительного, «нулевого» уровня End-to-End шифрования по сертифицированным ФСБ РФ алгоритмам. ■

Литература

1. *LoRaWAN 1.0.3 Regional Parameters, 2018.*
2. *LoRaWAN Specification, Version V1.0.3, 2018.*
3. *Решение ГКРЧ № 18-46-03-1 от 11.09.2018. О выделении полос радиочастот, внесении изменений в решения ГКРЧ и продлении срока действия решений ГКРЧ.*
4. *LoRaWAN Members Meeting. Tokyo, 2018.*
5. *Ross Gilson, Michael Grudsky. LoRaWAN capacity trial in dense urban environment, 2018.*
6. *LoRaWAN 1.1 Specification, 2018.*
7. *ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи, 2012.*
8. *ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. 2012.*
9. *ГОСТ Р34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. 2015.*
10. *ГОСТ Р 34.13–2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. 2015.*
11. *LoRa Alliance, FUOTA Process Summary Technical Re 1 commendation TR002 v1.0.0, 2019.*
12. *Извещение по вопросу использования несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети Интернет. ФСБ РФ. 2016.*

Стандартизация и сертификация LoRaWAN

Никита УТКИН,
председатель ТК 194 «Кибер-физические системы», руководитель программ АО «РВК»

Регулирование Интернета вещей (Internet of Things – IoT), Промышленного Интернета (Industrial Internet of Things – IIoT) и сенсорных сетей (Wireless sensor network – WSN) является одним из ключевых направлений в деятельности Технического комитета по стандартизации № 194 «Кибер-физические системы». Именно для этой работы в рамках Технического комитета была институционализирована Рабочая группа «Интернет вещей».

История вопроса

За последний год комитетом «Кибер-физические системы» совместно с рыночными игроками и объединениями, среди которых достойное место занимает профильная для тематики Интернета вещей рыночная ассоциация АИВ («Ассоциация участников рынка Интернета вещей»), было инициировано к разработке более 70 национальных стандартов, заметная часть которых имеет непосредственное отношение к Интернету вещей, Промышленному Интернету и сенсорным сетям.

Началом видимой части работы комитета стало утверждение в феврале 2019 г. первого предварительного национального стандарта Интернета вещей – ПНСТ 354-2019 «Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi)», который был разработан при участии ООО «Телематические решения», АО «Российская венчурная компания» (АО «РВК»), Фонда развития интернет-инициатив (ФРИИ), АИВ и НП «Русское биометрическое общество».

Таким образом, стандарт NB-Fi (Narrow Band Fidelity) стал первым утвержденным в России стандартом Интернета вещей и был введен в действие в апреле 2019 г. Можно сказать, что именно с этого месяца и стартовала его официальная апробация. Заметным преимуществом стандарта стало то, что в его основу заложена полностью российская технология, которая позволяет создавать беспроводные сети обмена данными между множеством модемов с одной стороны и множеством базовых станций – с другой. Кроме того, эта технология уже на практике доказала возможность ее применения в масштабных проектах.

Вопреки предположениям рынка о том, что указанный стандарт станет единственным

Кибер-физические системы

Технический комитет №194 «Кибер-физические системы» был создан приказом Федерального агентства по техническому регулированию и метрологии № 507 от 21 марта 2018 г. (ранее – приказ Федерального агентства по техническому регулированию и метрологии № 642 от 27 марта 2017 г.) для осуществления деятельности по нормативно-техническому регулированию (стандартизации) целого ряда цифровых технологий, включая Интернет вещей.
Коллегиальный орган выступает платформой для развития цифровой экономики и Национальной технологической инициативы (НТИ) за счет разработки стандартов цифровых технологий для новых перспективных рынков. Комитет объединяет ведущие научные и общественные организации, технологические компании, некоммерческие организации разработчиков оборудования и программного обеспечения. Среди его участников «Газпром нефть», «Ростелеком», «РУССОФТ», «Лаборатория Касперского», МГТУ им. Н.Э. Баумана, НИУ ВШЭ, МГУ и др.
В состав ТК № 194 «Кибер-физические системы» входит более 100 организаций. Возглавляет Технический комитет в должности председателя Никита Уткин, руководитель программ Российской венчурной компании.

www.tc194.ru

и монопольным, а другие технологии беспроводных сетей, такие как LoRaWAN и NB-IoT, которые уже используются во многих регионах страны, могут попасть под запрет, практически сразу после утверждения стандарта NB-Fi ТК «Кибер-физические системы» вынес на публичное обсуждение другие стандарты Интернета вещей, в том числе проект предварительного национального стандарта (ПНСТ) «Протокол беспроводной передачи данных для высокоемких сетей на основе сверхузкополосной модуляции радиосигнала» (Open Ultra-Narrowband – OpenUNB), разработанный Центром компетенций НТИ на базе Сколтеха, а также ПНСТ «Информационные технологии. Интернет вещей. Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением», прошедший предварительное рассмотрение в АИВ. Именно за сложным названием последнего и стоит российская версия стандарта сетевого протокола и системной архитектуры сети LoRaWAN (Long Range Wide Area Networks).

Стандартизация LoRaWAN в России

В чем его специфика и зачем он был инициирован к разработке? Как уже отмечено, стандарт определяет сетевой протокол и системную архитектуру сети LoRaWAN, оптимизированные на национальном уровне для мобильных и стационарных конечных устройств с батарейным питанием. Его отличительными особенностями являются высокая энергоэффективность, возможность передачи данных на большие расстояния, способность поддерживать двунаправленную связь, а также гибкая адаптация полосы пропускания. Особое внимание разработчики уделили тому, чтобы стандарт поддерживал российские криптографические алгоритмы, что позволяет обеспечивать необходимый уровень безопасности передачи данных.

В базовой конфигурации сеть LoRaWAN имеет топологию типа «звезда» (star topology), в которой шлюзы ретранслируют сообщения между конечными устройствами и центральным сервером сети, что также нашло отражение в стандарте. Сервер сети маршрутизирует пакеты с каждого устройства на соответствующий сервер приложений, т. е. устройства (датчики, счетчики и сенсоры) взаимодействуют с базовой станцией напрямую. Такая система построения сети хорошо зарекомендовала себя в мире при создании систем городских и региональных масштабов.

Для нас было весьма важным, что к разработке проекта национального стандарта в этой сфере присоединился широкий круг игроков рынка, в том числе АО «ЭР-Телеком Холдинг», ООО «Лартех Телеком», концерн «Гудвин» и ОАО «МТТ».

Публичное обсуждение проекта национального стандарта продолжалось в течение трех месяцев. Следующей важной вехой в работе над ним стала международная конференция «Регулирование цифровых технологий», которая прошла осенью в Санкт-Петербурге. Это мероприятие собрало более 250 международных экспертов с площадок Международной организации по стандартизации (International Organization for Standardization – ISO), Международной электротехнической комиссии (International Electrotechnical Commission – IEC), Международного союза электросвязи (International Telecommunication Union – ITU), Института инженеров электротехники и электроники (Institute of Electrical and Electronics Engineers – IEEE) и др. Конференция была приурочена к проведению первого в России заседания подкомитета ISO/IEC в области Интернета вещей (ISO/IEC SC 41 Internet of Things and related technologies).

В ходе подготовки к этому мероприятию во взаимодействии с LoRa Alliance был отдельно проработан вопрос определения статуса российского стандарта LoRaWAN. В результате представленный предварительный национальный стандарт (ПНСТ) был поддержан международными экспертами во главе со специалистами LoRa Alliance в качестве полноценного протокола семейства LoRaWAN и одобрен к использованию в качестве региональной спецификации для российского рынка LoRaWAN RU.

Многие рыночные партнеры охарактеризовали данную ситуацию как «win-win» («выгодно обеим или всем сторонам»), поскольку проект стандарта учитывает специфику российского законодательства и в то же время совместим с международным протоколом LoRaWAN, развивающимся при участии международной организации LoRa Alliance.

Сертификация LoRaWAN в мире

На международном уровне сертификация оборудования LoRaWAN проходит в рамках аккредитованных лабораторий LoRa Alliance. Стоит отметить, что сертификация является не обязательной, принять в ней участие могут только члены LoRa Alliance.

Для целей добровольной сертификации LoRa Alliance выпускает и систематически обновляет «Требования к сертификации конечных устройств», где изложены минимальные требования, которым конечное устройство должно соответствовать, прежде чем оно сможет использовать соответствующий сертификационный ярлык LoRaWAN Certified Device. Чтобы обеспечить соответствие конечных устройств этим требованиям, LoRa Alliance назначает реестр авторизованных испытательных центров для сертификационных испытаний LoRaWAN в соответствии со своими спецификациями. После проведения необходимого сертификационного тестирования конечного устройства результаты сертификации публикуются на сайте LoRa Alliance вместе с набором протестированных функций.

Целью сертификации LoRa Alliance является подтверждение того, что конечное устройство отвечает функциональным требованиям спецификации протокола LoRaWAN.

Для сертификации LoRa Alliance не обязательно, чтобы конечное устройство соответствовало всем нормативным требованиям, но необходимо понимать, что они потребуются перед продажей или введением в эксплуатацию продукта и/или сервиса в соответствующем регионе.

Для сертификации LoRa на данный момент также не обязательно проводить какие-либо тесты производительности на конечном устройстве. Операторы сети могут запросить эту информацию у производителя конечного устройства из семейства LoRa Alliance.

Членство в LoRa Alliance

Таким образом, производитель устройства, которому необходима сертификация LoRa должен:

- быть членом LoRa Alliance;
- использовать один из аккредитованных испытательных центров LoRa Certification для проведения тестов функциональных протоколов.

По завершении тестов результаты будут представлены на сайте LoRa Alliance. И если устройство прошло все обязательные тесты, LoRa Alliance выдаст соответствующий сертификат – LoRa Certification.

Функциональный тест LoRaWAN

Функциональный тест проверит соответствие конечного устройства спецификации LoRaWAN, а сертификат LoRa Certification будет соответствовать конкретному выпуску спецификации LoRaWAN.

Некоторые функции LoRaWAN являются необязательными для прохождения процедуры сертификации, однако список всех дополнительных функций, которые были успешно протестированы, будет включен в результаты сертификационных испытаний.

Тестовый стенд состоит из персонального компьютера, работающего в качестве сетевого сервера LoRa, подключенного к стандартному шлюзу LoRa. Тестируемое конечное устройство (The End Device under test – DUT) помещается в защищенный от радиочастот контейнер и подключается к испытательному шлюзу через радиосвязь. Компьютер с сетевым сервером LoRaWAN и сервером приложений управляется посредством набора тестовых сценариев, которые будут тестировать определенные функции LoRaWAN.

Чтобы полностью протестировать конечное устройство, тестируемый девайс должен запустить тестовое приложение (в тестовом режиме), работающее поверх уровня MAC, отключить все ограничения рабочего цикла и приостановить свое обычное прикладное программное обеспечение.

Во время испытания протокол обмена проверяется путем передачи тестовых сообщений. Так же проверяется корректность использования протоколов шифрования. Радиомагнитная совместимость устройств в ходе такого тестирования не проверяется.

Органы по сертификации

Перечень решаемых задач:

- сбор документации, предоставляемой организациями, заинтересованными в сертификации своей продукции;
- лабораторные испытания образцов продукции;
- анализ протоколов лабораторных испытаний;
- принятие квалифицированного решения о регистрации сертификата либо отказе;
- ведение базы данных (реестра) с занесением в нее информации о новых сертификатах соответствия;
- выдача аккредитации исследовательским лабораториям, специализирующимся на опытах с образцами продукции;
- работа с апелляциями.

Испытательные лаборатории

Перечень решаемых задач:

- проведение сертификационных испытаний и подготовка протоколов сертификационных испытаний.

Сертификация Интернета вещей в России

За процессом стандартизации неминуемо следует сертификация, и на этой «поляне» ряд преимуществ получает тот, кто первый занялся содержательной работой на фазе стандартизации – «открылся» перед рынком и начал формировать вокруг себя партнерскую экосистему.

Очевидно, что вся сертификация Интернета вещей в России находится в зачаточном состоянии. В этом есть и положительные, и отрицательные моменты: все заботы и достижения в данной области еще впереди.

С учетом международных практик можно с уверенностью сказать, что сертификация систем Интернета вещей – актуальный и востребованный тренд при условии обеспечения должного уровня прозрачности. Поэтому формирование на национальном уровне полноценной системы сертификации в области Интернета вещей – вопрос времени.

Следует отметить, что национальная система сертификации может быть как обязательной, так и добровольной.

Какой в общих чертах должна быть система сертификации? В нее должны войти орган по сертификации и испытательные лаборатории, аккредитованные Федеральной службой по аккредитации («Россакредитация») в соответствии с требованиями законодательства Российской Федерации.

Крайне важно, чтобы в испытательных лабораториях можно было проверить все стандартизированные на национальном уровне протоколы Интернета вещей: искажения и перегибы в пользу отдельных стандартов должны быть исключены.

В части криптографической защиты информации, шифрования и электромагнитной совместимости должны использоваться либо уже действующие, либо создаваемые лаборатории. Таким образом, каждый из вопросов сертификации должен быть адресован в лабораторию с соответствующим профилем.

Гармонизация с международными стандартами и национальная специфика

Что касается сертификации LoRaWAN в России, то очевидно, что она должна опираться на два элемента равносильной важности: гармоничность ключевых инженерных требований с международной сертификацией LoRaWAN (чтобы не потерять ключевое достижение интероперабельности) и учет региональной специфики, отраженной в тексте проекта предварительного национального стандарта.

Верным принципом сертификации в России, согласно региональной спецификации LoRaWAN RU, может стать отсутствие привязки процесса сертификации тестируемого конечного устройства к факту членства организации в LoRa Alliance.

Для этого необходимо активизировать работу российских экспертов как на площадках ISO/IEC, так и в профильной рабочей группе LoRa Alliance – в LoRa Alliance Technical Committee Regional Parameters Workgroup. ■

Программный комплекс управления средой виртуализации «Брест» от ГК Astra Linux сертифицирован Минобороны России

Группа компаний Astra Linux сообщила об успешной сертификации программного комплекса управления защищенной средой виртуализации «Брест» по требованиям безопасности информации Министерства обороны России. ПК «Брест» на основе операционной системы специального назначения Astra Linux Special Edition – одно из первых средств управления виртуализацией, получивших сертификат МО России на применение в информационных системах предприятий ОПК и других организаций ведомства, обрабатывающих конфиденциальную информацию, в том числе составляющую государственную тайну до уровня «совершенно секретно». Программный комплекс «Брест» реализует управление виртуальными инфраструктурами любой сложности с использованием всего спектра средств защиты информации операционной системы специального назначения Astra Linux Special Edition и обеспечивает работу виртуальных машин в условиях дискреционного и мандатного управления доступом. В круг задач, решаемых ПК «Брест», входят централизованное управление кластерами виртуализации, масштабирование и обеспечение их отказоустойчивости, создание защищенной среды виртуализации рабочих столов (VDI) и серверов архитектуры x86-64, виртуализация сетей, хранилищ, миграция работающих виртуальных машин между узлами кластера виртуализации, групповое создание виртуальных машин из шаблонов, построение защищенных облачных решений. «Для нас как компании-разработчика сертификация ПК «Брест» по требованиям безопасности информации Минобороны России – знаковый момент. Мы шли к этому несколько лет. Тем заказчикам, кто работает с гостайной и чьи ИТ-инфраструктуры должны проходить аттестацию в системе Минобороны России, важно было получить сертифицированный программный продукт для управления виртуализацией. Теперь возможности таких предприятий в части совершенствования информационных систем серьезно расширятся», – отметил директор по инновациям ГК Astra Linux Роман Мылицын. Для организаций, информационные системы которых должны соответствовать требованиям безопасности по линии ФСТЭК России, ГК Astra Linux разработала вторую версию «Бреста» с расширенным функционалом и оперативными обновлениями. Программный комплекс управления средой виртуализации «Брест» имеет уникальную и оптимальную архитектуру, которая была достигнута за счет переноса средств защиты информации на уровень операционной системы, поэтому сам программный комплекс сертифицировать во ФСТЭК России нет необходимости.

www.astralinux.ru

Мне нравится, когда цветок или пучок травы растет сквозь щель в бетоне. Это, черт возьми, героически.

Джордж Карлин

LoRaWAN:
один из путей Интернета вещей

Александр ГОЛЫШКО,
независимый эксперт, к. т. н.

Все только начинается… Интернет вещей (IoT/IIoT – Internet of Things/Industrial Internet of Things), связывающий различные устройства для взаимодействия друг с другом, – очередная Big Thing нашего времени, без которой трудно представить будущее цивилизации. Эти устройства подключаются к сети Интернет не затем, чтобы сидеть в социальных сетях, а чтобы оперировать данными, генерируемыми быстро растущим цифровым миром.

Девятый вал IoT-устройств

Прогрессивному человечеству вскоре придется столкнуться как минимум с десятками миллиардов подключенных устройств из пула IoT и информационным обменом с огромным количеством датчиков (например, систем ЖКХ), в том числе датчиков, внедренных в производственные процессы различных «киберфизических систем», рассредоточенных по значительной площади.

Разумеется, существующие сети сотовой (мобильной) связи могут обслужить IoT/IIoT, но одно дело, когда речь идет о десятках тысяч устройств M2M (Machine-to-Machine), другое – когда о десятках миллиардов (как свидетельствуют многочисленные прогнозы). Так, если на один жилой дом из 300 квартир приходится 1500 счетчиков ЖКХ (электричество, газ, тепло и два на воду) с крайне дешевым трафиком от низкоскоростной телематики, то это может полностью забрать ресурс пропускной способности ближайшей базовой станции (например, LTE), ничего не оставив людям.

Другая существенная проблема – энергопотребление. Многие терминальные устройства будут вынуждены работать от батареек, но технические характеристики сетей сотовой связи не позволят делать это дольше нескольких дней. Низкое энергопотребление вообще является критическим условием для 80% случаев использования IoT в «умных» счетчиках, носимой электронике, смарт-парковках и т. п. Кроме того, стоит отметить, что простота установки и небольшой размер потери в случае кражи – тоже немаловажные факторы для массовой технологии.

Ну а если обратиться к стоимости услуг мобильной связи, то для хоть и надежной, но низкоскоростной передачи данных она также будет великовата. В целом же канал связи в 5 Мбит/с не нужен, чтобы раз в сутки передать, сколько кубов воды набежало по каждой квартире. Сенсоры и датчики год от года становятся все «умнее», в частности благодаря использованию технологий искусственного интеллекта. Растут требования предприятий к сервисам IoT. Заказчиков интересуют доступность инструментов, низкая стоимость обслуживания, простота развертывания и пр.

Беспроводная передача данных

Многочисленные разработки технологий беспроводной передачи данных в виде Wi-Fi, Bluetooth, Z-Wave, Zigbee и т. п. умеют решать задачи IoT-коммуникаций лишь в пределах одной «вещи» или одного человеческого тела, одного помещения. В результате поиска чего-то экономичного для IoT/IIoT появилось сразу несколько технологий, которые стали дальнейшим развитием так называемой энергоэффективной глобальной сети дальнего радиуса действия – Low Power Wide Area Network (LPWAN), ориентированной на низкоскоростную передачу данных и вариант сети мобильной связи, стандартизованный 3GPP.

На данный момент существует несколько десятков стандартов для сетей IoT/IIoT – часть из них универсальны, другие приспособлены решать ограниченный круг задач.

LoRa Alliance™

LoRaWAN 1.1 Regional Parameters

Poland	433.05–434.79 MHz	EU433
	863–873 MHz	EU863–870
	918–921 MHz	Other
Portugal	433.05–434.79 MHz	EU433
	863–870 MHz	EU863–870
Qatar	433.05–434.79 MHz	EU433
	868–868.6 MHz	EU863–870
	868.7–869.2 MHz	EU863–870
	869.4–869.65 MHz	EU863–870
	869.7–870 MHz	EU863–870
Romania	433.05–434.79 MHz	EU433
	863–870 MHz	EU863–870
Russian federation	866–868 MHz (Licensed)	RU864–870
	864–865 MHz	RU864–870
	868.7–869.2 MHz	RU864–870
	433.075–434.75 MHz	EU433
	916–921 MHz (Licensed)	Other
Salvador	915–928	AU915–928, AS923
Saudi Arabia	863–870 MHz	EU863–870
	433.05–434.79 MHz	EU433
Senegal		None

Требования IoT-приложений настолько разнообразны, что все случаи использования LPWAN не могут быть охвачены единой технологией. В связи с этим появились стандарты для узкополосных IoT-устройств NB-IoT (Narrow Band IoT) в сетях LTE; для расширенного GPRS-покрытия (EC-GPRS или EC-GSM-IoT) и межмашинных LTE-соединений eMTC (встречаются также названия LTE-M, LTE-MTC, LTE Cat.M1). Все эти технологии предусматривают работу в лицензируемом диапазоне радиочастот (как и все системы сотовой связи), что означает необходимость получения соответствующих разрешений.

LoRa и LoRaWAN

Для работы в нелицензируемых диапазонах радиочастот 868/915 МГц (Европа/США) разработаны соответствующие технологии, и наиболее часто встречается среди них LoRa (сокращение от Long Range – т. е. это сеть масштаба района или города, а не квартиры или офиса). Аббревиатура LoRa обозначает лишь вид модуляции, а протокол канального уровня носит имя LoRaWAN. В настоящее время многие компании строят сети на основе этой технологии либо включили ее в свои ближайшие планы благодаря надежности и открытости. Сегодня при передаче данных в LPWAN используются два подхода:

- широкополосное кодирование на увеличенных битовых скоростях для борьбы с более высоким уровнем шума в приемнике – это подход LoRa в сетях LoRaWAN;
- сужение полосы спектра в целях снижения уровня помех на приемнике – это узкополосный подход, который применяет технология «СТРИЖ».

Одним из главных достоинств LoRaWAN является то, что это открытый стандарт, над чем успели поработать радиоинженеры. Таким образом, если мы строим сеть, отвечающую стандартной спецификации, и у нас есть стороннее устройство, соответствующее спецификации, оно сможет работать в данной сети.

В 2008 г. патент на технологию LoRa получила компания Cycleo (Франция), а в 2012 г. ее приобрела компания Semtech (США). LoRa использует собственный метод модуляции, основанный на технологии расширения спектра (Spread Spectrum Modulation) и вариацию линейной частотной модуляции (Chirp Spread Spectrum), при которой данные кодируются широкополосными импульсами. Такое решение в отличие от технологии прямого расширения спектра (как, например, в сетях мобильной связи CDMA)

делает приемник устойчивым к нестабильности частоты, что позволяет использовать недорогие кварцевые резонаторы в тактовом генераторе.

Своих «мозгов» эти чипы LoRa не имеют – они управляются по SPI (Serial Peripheral Interface) от внешнего контроллера. Топология сети – «звезда», дальность – от нескольких километров в плотной городской застройке до 30–50 км прямой видимости. Скорость передачи данных – до 250 кбит/с (уменьшается с увеличением расстояния). Количество устройств – до 5 тыс. штук/км². Максимальный размер сети ограничен пропускной способностью канала центрального приемника, который должен успевать проводить радиообмен со всеми подключенными к нему устройствами.

Как работает LoRa

Алгоритм функционирования LoRa следующий: базовая станция (БС) анализирует эфир в заданном диапазоне частот, и когда она получает запрос от какого-либо из терминальных устройств, то отвечает ему на частоте обращения. Ширина канала при этом составляет 125 кГц (в стандарте предусмотрены 250 и 500 кГц, но в России их обычно не используют), максимальная скорость – чуть более 5 кбит/с. В зависимости от состояния эфира выбирается оптимальный набор параметров связи. За это отвечает SF (spreading factor – целое число, которое в стандарте может принимать значения от 7 до 12) – коэффициент, к которому привязываются параметры передачи и приема. Чем выше SF, тем лучше помехозащищенность линии, но тем ниже скорость передачи информации и тем больше времени в эфире занимает передача (например, максимальная помехозащищенность при SF = 12, при этом время пакета в эфире составляет 2,466 секунды, а скорость – 292 бит/с). Чем больше терминальных устройств будет работать через базовую станцию, тем больше времени в эфире они займут. Поэтому при хороших радиоусловиях SF будет меньше. Растет скорость – падает время передачи.

Пакеты принимаются базовой станцией (в архитектуре LoRa ее именуют шлюзом). Обрабатывает пакеты сетевой сервер, который отвечает за управление всеми шлюзами: он решает, через какой шлюз общаться с датчиком, если датчик «слышно» через несколько шлюзов. Полезную информацию из принятых пакетов обрабатывает сервер приложений, где происходит расшифровка показаний от датчиков и сенсоров. Эта информация в заранее установленной форме передается либо в биллинг, либо в интерфейс потребителю, либо куда-то еще.

Из приведенных LoRa Alliance радиочастот для работы в РФ используются 1,5 МГц нелицензируемого спектра: 864–865 МГц и 868,7–869,2 (защитный интервал между каналами должен составлять 75 кГц). Мощность сигнала – не более 25 мВт.

Реальные возможности LoRa

Разумеется, необходимо трезво оценивать технологию и ее возможности. LoRa устойчиво работает на грамотно построенной сети, но ни о какой десятикилометровой дальности (порой заявляемой) говорить нельзя – ее можно обеспечить лишь в чистом поле без внешних помех. В городских условиях дальность связи составляет 2–3 км. К тому же LoRa никогда не достигнет одновременно значений 10 км и 5 кбит/с (либо другое). Как свидетельствуют те, кто уже развертывал сети LoRa, ее оборудование не любит:

- размещение на малых высотах;
- плохие антенны и некачественный монтаж;
- оборудование GSM-900, находящееся в непосредственной близости.

Важная характеристика LoRaWAN – безопасность, которая в стандарте реализуется с помощью двух ключей. Любой пакет шифруется ключом сетевого сервера и сервера приложений. Относительно слабым моментом этого метода является то, что ключи либо заданы изначально (метод ABP), либо генерируются в момент активации устройства (OTAA). Получается, что они будут использоваться вечно (ABP) либо до переактивации устройства (OTAA). Даже в последнем случае счет может идти на месяцы. Хотя истории пока не известны примеры взломов LoRaWAN, в стандарте уже появилась спецификация, позволяющая решить проблему со старыми ключами.

С учетом сравнительно небольшой полосы радиочастот, выделенной под нелицензируемые радиосети, для широкополосной связи вероятность коллизий с сигналами от подобных устройств (других аналогичных сетей) всегда выше. И эту ситуацию невозможно компенсировать улучшенным кодированием. Результат – резкое снижение дальности стабильной работы такой системы: устройства, находящиеся на предельно дальней дистанции, уже не будут «услышаны».

Кроме того, особенностью принимающих станций LoRa является то, что они не могут демодулировать более чем восемь пакетов одновременно. При этом они могут определить принадлежность пакета только после демодуляции. То есть станция LoRa принимает все пакеты, а «свои» выделяет уже потом. Но любой пакет данных даже из «чужой» сети, принятый «своей» станцией, блокирует получение любого «своего» пакета на этом же канале до тех пор, пока он не будет полностью принят, что создает понятные проблемы в случае одновременной работы в одной зоне сразу нескольких подобных сетей. Таким образом, любой желающий может вполне легитимно, отправляя с восьми LoRa-модемов произвольные данные без остановки, заблокировать все восемь каналов в любой сети LoRa в любом городе. Станция будет вынуждена принимать пакеты, идущие от «чужих» модемов, в ущерб пакетам из «своей» сети. Собственно говоря, от перечисленных недостатков

и постарались избавиться разработчики платформы LPWAN «СТРИЖ» – за счет некоторого ухудшения других технических характеристик.

Система «СТРИЖ»

Когда речь идет о стоимости той или иной системы связи, следует иметь в виду, что она часто является коммерческой тайной и зависит от количества заказываемого оборудования, однако в любом случае открытые стандарты имеют своим следствием серьезный рост конкуренции, а за ним – снижение стоимости. В свою очередь, проприетарные системы с ограниченным (а чаще уникальным) количеством поставщиков несут с собой не только лучшие технические характеристики, но и соответствующие дополнительные риски.

На физическом уровне для передачи сигнала в системе «СТРИЖ» используются модуляция DBPSK (относительная/дифференциальная/двоичная фазовая манипуляция) и сравнительно узкая полоса радиосигнала. Такой подход уменьшает количество устройств, способных работать в определенном частотном диапазоне. Зато в полосе 125 кГц, которая требуется LoRa для кодирования одного канала, посредством узкополосного метода можно получить до 1250 каналов. А значит, можно использовать до 1250 устройств «СТРИЖ» без ухудшения характеристик вместо одного устройства LoRa.

Устройства с широкополосными сигналами при одновременной работе в одном канале позволяют добиться защиты от помех на уровне 10–20 дБ. Трансиверы, применяемые «СТРИЖ», обеспечивают до 65 дБ защиты от помехи на соседнем канале – 45 дБ разницы по сравнению с LoRa, что дает большое преимущество надежности и помехоустойчивости связи в реальных условиях. При большом времени передачи система становится уязвимой к помехам от других устройств, работающих в той же полосе.

Технология NB-IoT

Начиная со спецификации Release 14 3GPP, в сотовой связи много внимания уделяется вопросам описания и детализации параметров радиоинтерфейса 5G, обеспечивающего максимально точное пространственное позиционирование и широкополосные коммуникации в реальном времени и с крайне малой задержкой сигнала (менее 1 мс) от мобильных объектов – автомобилей, дронов и пр. Возникает чувство, будто IoT создавался специально под технологии 5G (как еще продать 5G на мировом уровне?), а технологии 5G – соответственно под IoT. Пока 5G – больше «в уме», у мобильной индустрии уже есть технология NB-IoT. Это принципиально новая разработка, хотя и предусматривающая интеграцию с сетями LTE и применяющая сходные технологии.

NB-IoT использует несущую шириной 200 кГц, которая может быть расположена в каком-либо свободном диапазоне, внутри каналов GSM (как в EC-GSM), внутри канала LTE (как в eMTC) или в защитном интервале между каналами LTE. Частотный диапазон может быть любым из тех, что определены для сетей LTE с частотным разделением каналов (LTE FDD). В канале «вниз» используется технология множественного доступа OFDMA, в канале «вверх» – SC-FDMA.

Следует заметить, что в реальной жизни базовая станция должна не только поддерживать одновременную работу многих тысяч устройств IoT, но и обеспечивать их подключение наилучшим образом независимо от качества покрытия. В результате технология NB-IoT поддерживает широкий диапазон скоростей передачи данных. Достижимая скорость передачи данных зависит от качества канала связи (отношения сигнал/шум), а количество подключенных устройств – от выделенных ресурсов (пропускной способности). В канале «вниз» все устройства имеют одну и ту же энергетику радиоканала и могут одновременно принимать сигналы с базовой станции. В канале «вверх» каждое устройство имеет собственный энергетический потенциал, что может быть использовано для мультиплексирования трафика. При этом создаваемый совокупный сигнал от нескольких устройств (и соответственно их мощность) будет больше, чем у одного устройства. Да и в реальных условиях во многих местах устройства NB-IoT будут ограничены уровнем собственных сигналов, а не пропускной способностью сети. Такие устройства способны сконцентрировать свою излучаемую мощность в узкой полосе радиочастот без потери производительности, освободив при этом полосу пропускания для других устройств.

Чтобы получить такую возможность, в NB-IoT вместо коллективного канала (общего блока ресурсов) со скоростью передачи данных до 250 кбит/с предусмотрено использование поднесущих частот с полосой пропускания 15 кГц (эффективная полоса пропускания общего канала NB-IoT – 180 кГц) и скоростью передачи данных до 20 кбит/с. В свою очередь, терминальные устройства могут использовать одну или нескольких

> LoRa устойчиво работает на грамотно построенной сети, но ни о какой десятикилометровой дальности (порой заявляемой) говорить нельзя.

поднесущих в восходящей линии связи. Более того, используемые ими радиочастоты могут быть упакованы даже ближе друг к другу за счет уменьшения ширины полосы поднесущих до 3,75 кГц. Это обусловливает необходимость выделения части из них в качестве защитных интервалов в целях предотвращения интерференции с поднесущими с шириной полосы 15 кГц, что может привести к потере производительности.

Таким образом, технология NB-IoT, вобравшая в себя все сетевые достижения мобильной индустрии, обеспечивает большую зону обслуживания, низкое энергопотребление, возможности быстрой модернизации существующей сети, обещает длительный (до десяти лет) срок службы батареи, низкую стоимость терминала, простоту развертывания (plug & play), а также высокую надежность и безопасность. Обещанные разработчиками 50 тыс. устройств IoT на сектор базовой станции – тоже не фантастика. Кроме того, предполагается, что существенная переработка протоколов канального уровня позволит снизить стоимость устройства NB-IoT по сравнению с LTE Cat.M1 на 90%.

Что лучше для IoT?

Учитывая начальную стадию освоения IoT и всего сказанного выше, у специалистов может возникнуть закономерный вопрос: какая из технологий развертывания IoT лучше? У экспертов на этот счет свое мнение.

Прежде всего, раз уж сеть NB-IoT относится к сотовой связи, то устройства, работающие в ней, должны «просыпаться» и синхронизироваться с сетью, и каждый сеанс синхронизации отнимает у аккумулятора устройства заряд энергии. В свою очередь, асинхронная отправка данных в сети LoRaWAN подразумевает передачу только тогда, когда эти данные есть. В остальное время устройство «спит» и энергия не расходуется. Ранее эксперты ассоциации GSMA провели множественные тесты работы LPWAN, в результате которых выяснилось, что автономность LoRaWAN-устройств в три-пять раз выше, чем у девайсов, работающих в других LPWAN.

Разумеется, NB-IoT – более эффективный протокол IoT с высокими скоростями передачи информации, что важно для быстрых приложений, требовательных к времени задержки и регулярному приему/отправке сообщений. Однако для многих случаев передачи телематики устройствам LoRaWAN вполне достаточно скорости передачи данных в 11 кбит/с. При этом требования к пропускной способности сигнала, обозначенные 3GPP, составляют 180 кГц, а LoRa необходимо 125 кГц.

NB-IoT обеспечивает лучшее покрытие в сложных городских условиях, однако производительность сети будет избыточной в пригородных или сельских районах. Покрытие LoRaWAN остается относительно устойчивым вне зависимости от условий местности, и для развертывания такой сети требуются более низкие инвестиции.

Технология LoRa может использоваться как операторами, работающими в секторе мобильной связи, так и не имеющими отношения к этой сфере. Сети NB-IoT – принадлежность операторов мобильной связи и не являются фрагментами корпоративных сетей, тогда как LoRa подходит для этого. Крупные предприятия относительно просто смогут создавать гибридные модели IoT с сетью LoRa.

Средняя стоимость терминального оборудования LoRaWAN составляет 8–10 долл., что в два раза ниже, чем для модулей NB-IoT/LTE, но, как отмечалось, все зависит от масштабов закупок. И если речь идет о сотнях тысяч, то может быть всякое. Несомненно, затраты на развертывание с нуля LoRaWAN значительно ниже, чем NB-IoT, но эти сети работают поверх уже существующей инфраструктуры 4G/LTE (т. е. основные инвестиции уже сделаны), а введение на них опции NB-IoT может обеспечиваться программным образом, благодаря использованию в современном оборудовании сотовой связи технологии SDR (Software Define Radio).

Кроме того, стоит отметить, что лицензируемые диапазоны радиочастот свободны от помех, а нелицензируемые – нет. И даже при отсутствии внешних помех системы связи LPWAN могут просто мешать друг другу.

Экосистема LoRa пока значительно шире экосистемы NB-IoT. Ну а поскольку для IoT в целом все только начинается, следует понимать, что отстающие пока от сетей LPWAN сети NB-IoT будут стремительно развернуты, как только индустрия мобильной связи почувствует действительно массового потребителя. А потом наступит время специально созданных для поддержки IoT сетей 5G. Конечно, применительно к индустрии мобильной связи всегда останется актуальной фраза: «Носорог очень плохо видит, но при его весе это не его проблема».

Российские проекты

Тем не менее заслуживают уважения отечественные проекты развертывания сетей LoRaWAN. В частности, 1 сентября 2018 г. «ЭР-Телеком Холдинг» объявил о запуске сети IIoT в 52 городах Российской Федерации.

Реализуется крупный LoRaWAN-проект по внедрению в Забайкальском крае АСУЭ на 90 тыс. точек учета. Есть и многие другие. Надеемся, что, во-первых, все они сумеют освоить определенные ниши зарождающегося рынка IoT, во-вторых, LoRaWAN и NB-IoT смогут сосуществовать друг с другом, обслуживая разные сегменты глобальных IoT-рынков.

Однако если терминальные устройства IoT разовьют свой искусственный интеллект до такой степени, что начнут сидеть в социальных сетях, всех нас будет ждать очередная трансформация соответствующего рынка вместе с его инфраструктурой. И тогда все начнется сначала. ■

По материалам:
iot.ru, nag.ru, habrahabr.ru, strij.tech, isup.ru, tadviser.ru

LoRaWAN
в разрезе безопасности

Олег ПЛОТНИКОВ,
директор центра Промышленного Интернета, компания «Интерсвязь»

Технология беспроводной передачи данных – LoRa – используется на российском рынке уже давно и перестала быть диковинкой. Свои сети развернули несколько десятков операторов, заявляются даже два федеральных игрока. Однако у заказчиков LoRa до сих пор остаются сомнения в ее безопасности. В этой статье мы не будем касаться темы надежности передачи, а попробуем непредвзято рассмотреть вопрос информационной безопасности, причем не просто радиоканала LoRa как модуляции, а именно стандарта канального уровня LoRaWAN.

Активация LoRaWAN

Технология LoRa (Long Range), разработанная французской компанией Semtech, ориентирована на передачу небольших объемов данных огромным количеством устройств, т. е. LoRaWAN не предназначена для передачи больших объемов данных от одного устройства. Более того, стандарт это прямо запрещает через специальный параметр – duty cycle, который определяет максимальное время нахождения оконечного устройства в эфире, оно равно 1%. Речь в дальнейшем пойдет о спецификации версии 1.02-1.03, хотя самая свежая спецификация на сегодняшний день – 1.1, но она почти не внедрена на местах.

Для начала рассмотрим первоначальную регистрацию устройства в сети. В LoRaWAN этот процесс называется активацией. Ниже приведен список необходимых нам терминов. Если немного запутаетесь – можете возвращаться сюда и сверяться. Возвращаться наверняка придется, так как аббревиатуры многих терминов очень похожи. Кроме того, в описании приведены аналогии, чтобы вы понимали, с чем можно сравнить тот или иной термин. Точные аналогии подобрать не всегда возможно, потому не судите эту колонку слишком строго (рис. 1).

Активация в LoRaWAN может производиться по воздуху (Over-the-Air-Activation – OTAA) или по преднастройкам оператора (Activation by Personalization – ABP).

По воздуху

В случае активации по воздуху на радиомодуле должны быть заданы три параметра: его уникальный идентификатор (DevEUI), идентификатор сервера (AppEUI) и ключ сервера (AppKey). Со стороны сервера также должны быть получены следующие параметры: идентификатор радиомодуля,

Параметр	Значение	Аналогия/Физический смысл
DevEUI (Device Extended Unique Identifier)	Уникальный идентификатор устройства. Не должен повторяться вообще	Что-то вроде MAC-адреса
AppEUI (Application Extended Unique Identifier)	Уникальный идентификатор сервера	Наш логин для входа на сервер при первом соединении
AppKey (Application Key)	Ключ сервера	Это не пароль от логина выше. Он шифрует ответы сервера при активации. Аналогию придумать не удалось
DevAddr (Device Adress)	Уникальный адрес устройства в пределах сети. В разных сетях может повторяться	Что-то вроде «серого» IP-адреса
NwkSKey (Network Session Key)	Сессионный ключ сетевого сервера	Шифрует обмен пакетами между радиомодулем и сетевым сервером после активации
AppSKey (Application Session Key)	Сессионный ключ сервера приложений	Шифрует обмен пакетами между радиомодулем и сервером приложений после активации
MIC (Message Integrity Code)	Код целостности сообщения	Контрольная сумма сообщения

Рис. 1. *Расшифровка терминологии, используемой в LoRaWAN*

Size (bytes)	8	8	2
Join Request	AppEUI	DevEUI	DevNonce

Рис. 2. *Формат запроса к серверу join_request*

идентификатор сервера и ключ. То есть сервер должен изначально знать то устройство, которое попытается к нему присоединиться. Если мы знаем идентификаторы и ключи сервера, но наш DevEUI не внесен в его базу данных, то соединение не состоится. Тем не менее сервер будет «слушать» все устройства и принимать их пакеты, однако не сможет расшифровать и не будет отвечать таким устройствам.

При первоначальном включении радиомодуль отправляет в эфир пакет join_request с запросом на подключение на одной из трех заранее оговоренных частот присоединения. Этим пакетом он запрашивает, есть ли поблизости сеть, которая его «узнает». На рис. 2 приведен состав пакета join_request. Как видим, он содержит те самые DevEUI и AppEUI, а также DevNonce.

DevNonce – величина случайная. Сервер хранит ее в памяти и, если придет join_request с таким же DevNonce, как один из предыдущих, данный запрос проигнорирует. Это сделано для защиты от атаки повторения, когда злоумышленник может записать запрос на активацию, а потом повторить его со своего устройства. Кстати, защитой от подобной атаки могут похвастаться далеко не все стандарты IoT.

AppKey в данном сообщении напрямую не используется, но через него считывается контрольная сумма MIC в конце кадра. Этот ключ понадобится нам чуть дальше, в ответном сообщении сервера – join_accept. Причем запрос join_request передается в незашифрованном виде.

Положительный ответ сервера (join_accept) поступит в том случае, если серверу известны AppEUI и DevEUI, а также нет совпадения по полю DevNonce и проблем с контрольной суммой MIC. Иначе ответа не последует. Если все проверки пройдены, то сервер генерирует ответное сообщение join_accept (рис. 3).

Для взаимодействия с устройством сервер передает клиентскому оборудованию два сессионных ключа – сетевого взаимодействия с сервером (NwkSKey) и взаимодействия с приложением (AppSKey). Вместе с другой информацией они шифруются ключом шифрования сервера AppKey и отправляются радиомодулю. Далее все сообщения шифруются этими двумя сессионными ключами, что приводится в качестве аргумента защищенности LoRaWAN.

На самом деле ситуация с шифрованием сложнее. Если в пакете имеются данные для приложения и MAC-команды для сервера, то шифрование действительно выполняется двумя ключами. Пакет только с MAC-командами, которые не требуют от сервера обращения к приложению, ключом приложения уже не шифруется. Пакет с данными NwkSKey не принимает непосредственного участия в шифровании, но участвует в подсчете контрольной суммы и влияет на ее результат. Следует отметить, что NwkSkey и AppSKey уникальны для каждого отдельного клиента сети LoRaWAN.

Два ключа используются для дополнительного уровня защиты, чтобы сервер мог расшифровать только те послания, что адресованы ему, т. е. MAC-команды. Приложение в таком случае увидит лишь полезную составляющую пакетов – сами передаваемые данные. Нужно это для того, чтобы разделить уровни сети и приложения, поскольку сервер чаще всего будет стоять у провайдера, а вот приложение вполне может быть размещено у клиента. Двойное шифрование затрудняет провайдеру анализ содержания пакета, предназначенного для приложения.

Помимо двух ключей в join_accept по OTAA есть еще одна важная информация – расширенный список частот (CFList). Напомним, что изначально радиомодуль знает только три частоты, на которых он может работать. После активации ему передаются дополнительные частоты для выхода на связь, что очень удобно, если точно неизвестно, в какой сети будет работать устройство. Можно договориться, что во всех сетях три частоты (+RX2) будут всегда совпадать, остальные пять – на усмотрение провайдера. С увеличением количества нелицензируемых частот в поддиапазоне 868 это вдвойне актуально.

Преднастроенные устройства

Чтобы не заниматься активацией по воздуху, в LoRaWAN используется упрощенная процедура, когда сессионные ключи сразу зашиваются в радиомодуль и изначально прописаны со стороны провайдера. Радиомодуль сразу готов к работе. К сожалению, это не всегда удобно для большой сети, а также если устройства и сеть принадлежат различным компаниям. Кроме того, в данном случае нельзя менять частоты передачи динамически. Обычно такая процедура применяется в тестовых сетях, когда заранее известно, что с сервером могут происходить метаморфозы.

Size (bytes)	3	3	4	1	1	(16) Optional
Join Accept	AppNonce	NetID	DevAddr	DLSettings	RxDelay	CFList

Рис. 3. *Формат положительного ответа сервера join_accept*

Следует отметить: режим ABP устойчивее к атаке клонирования, но плата за такую устойчивость слишком высока.

Криптоанализ

Итак, основная нагрузка по шифрованию ложится на сессионные ключи сетевого сервера и сервера приложений. Рассмотрим их более подробно.

Главная претензия критиков стандарта LoRaWAN заключается в том, что при активации устройства в сети появляются два ключа, которые могут месяцами и даже годами не меняться, пока не произойдет реактивация устройства. В нормальных условиях радиомодуль активировали и забыли, так что срок жизни ключа в три-четыре года – вполне реальная перспектива. Собственно говоря, от установки до исчерпания заряда батарейки.

Насколько надежны наши ключи? Спецификация сообщает, что они соответствуют загадочному RFC4493. Что это такое? Это алгоритм шифрования, более известный как AES-CMAC. Мы не будем погружаться в дебри криптографии и ограничимся общим пониманием картины (рис. 4).

Принцип AES-CMAC примерно такой: шифруемое сообщение разбивают на 128-битные блоки (M1, M2, … Mn). Каждый блок шифруется отдельно AES-ключом. Причем при шифровании второго блока помимо ключа используется результат шифрования первого. А при шифровании третьего – результат второго и (косвенно) первого. Такая цепочка усложнений.

Насколько надежен этот принцип? Весьма надежен. Алгоритм вышел больше десяти лет назад. С тех пор на него провели множество различных атак и в конце концов в теории доказали, что его таки можно взломать. Проблема в том, что для взлома понадобится широкая выборка пакетов – несколько тысяч. Тогда есть шанс понять, что же внутри зашифрованных блоков.

Сможет ли злоумышленник с нужными знаниями получить данную выборку, если мы говорим про перехват пакетов LoRaWAN? Давайте прикинем. Пусть пакеты передаются раз в час. За месяц от радиомодуля уйдет 720 пакетов – маловато для взлома. Для реальной угрозы понадобится очень терпеливый злоумышленник, который будет месяцами писать пакеты. И то не факт, что он сможет взломать алгоритм, чтобы получить заветные ключи. Не забудем, что такое терпение надо будет проявлять в отношении каждого клиентского устройства отдельно. Кроме того, напомним, что передача пакетов раз в час – это ОЧЕНЬ часто. На практике промежутки намного больше – часов шесть, а то и раз в сутки.

Но даже эта призрачная возможность сейчас закрыта после выхода спецификации 1.1, где реализованы команды реактивации и запроса join_server. Понятие «дырявости» – это вообще удел открытых стандартов. Когда есть огромное сообщество, которое под микроскопом изучает все уязвимости, то они находятся быстро. И в этом преимущество открытого подхода. При очередной модернизации стандарта разработчики точно знают, на что смотреть в первую очередь. У проприетарных стандартов такой возможности нет, и их внутренние проблемы либо остаются известны только в среде разработчиков, либо вообще находятся уже в процессе эксплуатации в самый неподходящий момент.

В итоге получаем, что угроза безопасности скорее иллюзорна. Где-то в глубокой теории взлом произвести можно, но на практике вряд ли. Теперь помножим на ценность полученной информации. Станет ли наш злоумышленник месяцами писать пакеты, чтобы узнать показания счетчика? Маловероятно.

```
+-----+          +-----+          +-----+
| M_1 |          | M_2 |          | M_n |
+-----+          +-----+          +-----+
   |                |                |    +--+
   |        +---->(+)        +---->(+)<-|K1|
   |        |       |        |       |    +--+
+-----+     |    +-----+     |    +-----+
|AES_K|     |    |AES_K|     |    |AES_K|
+-----+     |    +-----+     |    +-----+
   |        |       |        |
   +-------+        +-------+
```

Рис. 4. *Упрощенная схема шифрования по алгоритму AES-CMAC*

Возможен ли взлом?

Хорошо, расшифровать пакеты злоумышленнику будет проблематично. А как насчет возможности удаленно ввести в заблуждение сервер или организации атаки на отказ в обслуживании – DoS? Рассмотрим несколько наиболее популярных техник атаки на радиосети.

Атака повторения

В случае атаки повторения злоумышленник записывает сообщение от устройства (без расшифровки) и позже передает его в эфире, «прикидываясь» устройством. Такая атака не будет успешной, поскольку в каждом пакете есть контрольная сумма, привязанная к счетчику пакетов, т. е. следующий пакет, даже с тем же содержимым, должен иметь другую контрольную сумму.

DoS преамбулами

Преамбула – это часть сообщения, которая «привлекает»

внимание сервера. Что-то вроде «слушай, сейчас будет сообщение». Атака заключается в забивании эфира преамбулами, в результате чего сервер будет все время ждать какого-то сообщения и не получать его. Реальный пакет в такой ситуации может просто не пройти. Это классический SYN-flood, с которого начинались первые DoS-атаки на IP-сети. И вот тут, увы, LoRaWAN сдает позиции. Сервер прослушивает все пакеты в эфире, поэтому он весьма чувствительно реагирует на подобные атаки. Справедливости ради надо отметить, что такой болезнью страдают не только LoRaWAN, но практически все радиопротоколы.

Глушение

Передача в эфир мощной помехи на рабочих частотах – более простой способ DoS-атаки. Заглушить можно любую радиосвязь: вопрос в соотношении мощностей передатчиков полезного сигнала и помехи. У LoRaWAN очень хорошие показатели работы в шумном эфире, технология может работать даже ниже уровня шума. Но физику никто не отменял, и ощутимая помеха, особенно рядом с базовой станцией или устройством, вызовет потерю пакетов.

Человек посередине

Еще более сложная атака, когда между сервером и устройством вклинивается злоумышленник. Он перехватывает пакеты от устройства, а на сервер отправляет уже измененную информацию. И наоборот. Для проведения такой атаки в рабочей сети злоумышленник должен знать сессионные ключи и идентификаторы устройства. Их еще надо раздобыть (возвращаемся к разговору выше). Теоретически при наличии только идентификаторов можно попробовать вклиниться в момент активации, т. е. ввести в заблуждение и сервер, и клиентское устройство.

Но тут две проблемы. Первая – нужно точно знать момент активации, умудриться перехватить join-пакеты с обеих сторон и не дать им пройти по маршруту. Непростая задача в условиях, когда устройства активируются в зоне действия легальной базовой станции. Да и персонал провайдера может заподозрить что-то неладное по косвенным признакам. Например, по уровню сигнала от устройства или явному несоответствию приходящих данных. Второй вариант – добраться до устройства и произвести его переактивацию. Это уже ближе к реальности, и все равно внеочередные запросы на реактивацию могут насторожить инженеров провайдера. В общем, чисто технически это осуществимо, но требует высокой квалификации и хорошего оборудования, а также точного понимания логики работы не только технологии, но и инженеров провайдера.

Клонирование

Создание клона устройства – частный случай атаки человека посередине. В предыдущем случае мы вводим в заблуждение как сервер, так и оконечное устройство. В случае клонирования обманывать будем лишь сервер. Нужно устройство со всеми теми же идентификаторами, что и легальный терминал. Кроме того, режим активации должен быть выбран OTAA. Проводим активацию клона, сервер считает, что у нас переактивировалось оригинальное устройство и обновляет сессионные ключи. Готово. Клон теперь воспринимается сервером и приложением как легальный источник данных, а настоящее устройство сервер перестает слышать, поскольку стирает его сессионные ключи. Старый терминал продолжает слать пакеты, но сервер их уже не воспринимает из-за устаревших сессионных ключей.

Тут есть две тонкости. Во-первых, нужно откуда-то взять набор идентификаторов легального устройства для клона. Во-вторых, некоторые производители добавляют в оконечные устройства оригинальную защиту, не предусмотренную спецификацией. Например, если терминал слишком долго не слышит ответов от сервера, то он запрашивает реактивацию. И вот тут сервер будет игнорировать уже сообщения клона.

Плюс – внимательность инженеров на сервере, которые должны заметить слишком частые запросы на реактивацию устройства. Клон может повести себя не так, как оригинальное устройство, что тоже должно вызвать подозрения.

К примеру, у нас есть специальная проверка на большой выборке данных: водосчетчик шлет данные, а мы записываем их в базу. В какой-то момент вклинился злоумышленник и начал нам отправлять заниженные показания. Если в момент вклинивания очередной пакет с показаниями от водосчетчика будет меньше, чем предыдущий, то сработает триггер: «Счетчик начал мотать назад». Генерируется аварийный акт и назначается разбирательство «руками инженера», вплоть до выезда на место.

Не знаю, как у других, но подозреваю, что не одни мы такие умные, и большинство серверов крупных провайдеров также обложены проверками.

Заключение

Итог. Любой стандарт, любой канал связи можно взломать. Особенно беспроводной. Это всегда вопрос ресурсов и времени. Если вам говорят, что технология совершенна и никто не может ее взломать, – не верьте. Либо кривят душой, либо сами не знают про какую-нибудь уязвимость. Другой вопрос, когда изначально ясно, какие ресурсы потребуются для взлома. Тогда можно оценить, стоит ли овчинка выделки. Обычное соотношение цена/качество является основой для реальной информационной безопасности. Очевидно, что через LoRaWAN не будут передавать данные, которые могут заинтересовать ЦРУ или МОССАД, – спецслужбы с большими финансовыми возможностями. А месяцами слушать пакеты, чтобы узнать показания водосчетчика, причем без гарантии успеха – удел весьма странного и терпеливого злоумышленника. Такого еще поискать в наших широтах. ■

Круглый стол

LoRaWAN
в мире Интернета вещей

В круглом столе принимают участие

Александр ГОЛЫШКО,
независимый эксперт, к. т. н.

Никита УТКИН,
председатель ТК 194 «Кибер-физические системы», руководитель программ АО «РВК»

Андрей ЭКОНОМОВ,
участник технического комитета LoRa Alliance, к. ф.-м. н.

Многие эксперты рынка информационных технологий, как в мире, так и в России, считают LoRaWAN одним из драйверов развития Интернета вещей. LoRaWAN уже сегодня используется в качестве основного инструмента для управления критически важной инфраструктурой (КИ), транспортом, производством, здравоохранением, муниципальным и сельским хозяйством. Конференции и форумы, посвященные тематике LoRaWAN, собирают тысячи участников со всего мира. Мы попросили экспертов высказать свою точку зрения по ключевым проблемам, связанным с дальнейшим развитием и продвижением технологии LoRaWAN в России.

Какими преимуществами обладает LoRaWAN в сравнении с другими беспроводными технологиями (ZigBee и пр.)?

Александр ГОЛЫШКО

Оперативность развертывания, высокая энергоэффективность, доступность и появление стандартизации. Именно поэтому сети LoRaWAN будут лидировать на настоящем этапе развития Интернета вещей.

В будущем возможно включение в пул сетей доступа 5G. Но об этом в терминах реальных проектов говорить пока рано.

Никита УТКИН

LoRaWAN строится и развивается на российском рынке за счет вполне понятных преимуществ: потенциально высокой энергоэффективности и потенциально высокой дальности передачи данных, что при достаточной обеспеченности энергоемкостью устройств в сети LoRaWAN позволяет им работать в автономном режиме довольно продолжительное время.

Важным фактором распространения технологии LoRaWAN является и то, что для ее развертывания не требуется получения лицензий на использование частот.

Андрей ЭКОНОМОВ

LoRaWAN – это открытый стандарт, разрабатываемый мировым Hi-Tech-сообществом. В LoRa Alliance уже входят представители таких компаний, как Google, IBM, Orange, Cisco, ARM, Alibaba, что позволяет развивать технологию с использованием наиболее

передовых решений. Благодаря этому в стандарте LoRaWAN присутствуют современные опции, например обновление ПО датчика через эфир, мультикаст, LoRa-геолокация абонентских устройств, LoRa-репитер, многоуровневое шифрование данных и т. д.

Что относится к главным недостаткам LPWAN-сетей? Можно ли ожидать в ближайшем будущем коррекции слабых мест этой технологии?

Александр ГОЛЫШКО

Основной недостаток LPWAN-сетей сегодня – работа в относительно небольшом нелицензированном диапазоне радиочастот, где обязательно будут помехи при высокой плотности работы систем разных владельцев. К тому же несложно получить помеху со стороны конкурентов или каких-нибудь радиохулиганов. Все это создает проблемы с обеспечением качества связи.

Никита УТКИН

За обозначенные в ответе на первый вопрос преимущества, которые весьма востребованы в реалиях построения распределенных сетей Интернета вещей, как и при любой другой альтернативной технологии, приходится платить. В случае с технологией LoRaWAN этой расплатой являются невысокая установленная скорость передачи пакетов данных и работа исключительно с небольшими их объемами.

Кроме того, необходимо учитывать, что построение сетей LoRaWAN может приводить к дополнительным затратам на создание инфраструктуры.

В каких областях применение технологии LoRaWAN наиболее перспективно?

Александр ГОЛЫШКО

В малом и среднем бизнесе: по сбору показаний датчиков и счетчиков в сфере ЖКХ, автостоянках и «умных» (smart) жилищах, а также в здравоохранении (внутри лечебных учреждений).

Никита УТКИН

С учетом всех преимуществ и недостатков технологии LoRaWAN неудивительно, что изначально решение LoRaWAN было позитивно принято рынком именно для формирования сетей промышленного Интернета (IIoT), применяемых в первую очередь для диспетчеризации промышленного оборудования, промышленных конструкций и сооружений.

Однако в наши дни коммерческая эксплуатация технологии LoRaWAN продвигается не только в индустриальном секторе, но и для функционирования линейки «умных» (smart) городских устройств.

Андрей ЭКОНОМОВ

Это «умный город» (smart city), «умное здание» (smart building), геолокация с низким энергопотреблением и все объекты, где нет электропитания или где прокладка провода недопустима из-за специфики объекта, например: контейнеры, прицепы, путепроводы, технические помещения, места установки датчика с технологическими ограничениями…

Нужно ли создавать в России общенациональную стратегию развития LPWAN (в рамках программы «Цифровая экономика») или лучше отдать это на откуп частным компаниям?

Александр ГОЛЫШКО

Как показывает опыт, малый и средний бизнес расцветает, если его вообще не трогать. И наоборот… Не хватает нам еще и в этой области бюрократию разводить.

Никита УТКИН

По отношению к большим и статусным документам национального уровня у рыночных игроков всегда присутствует подсознательный страх: вопрос упирается в равномерность учета возможных альтернатив, некорректную приоритизацию задач, а также сроки разработки подобных документов.

Кроме того, нередко такие документы страдают излишней гуманитарной описательностью, непомерным размером и отсутствием конкретики. Между тем реальная их ценность, как и деятельности, связанной с их разработкой, заключается в возможности прохождения ключевых развилок развития рынка Интернета вещей в равноправном диалоге частного бизнеса и государства.

Если уж и заниматься созданием общенациональных стратегий, то делать это следует не в отдельном сегменте LoRaWAN, а по всему Интернету вещей, уделяя внимание всем существующим альтернативам и принципиальным развилкам.

Какой смысл вкладывается в LoRaWAN (проект предварительного национального стандарта появился только в 2019 г.), когда существует альтернатива в виде NB-IoT (первая рабочая версия спецификации 3GPP была представлена еще в июне 2016 г.)?

Александр ГОЛЫШКО

А зачем, например, мы катаемся на велосипедах и самокатах, если есть общественный транспорт, личные авто и пр.? К тому же ниша для альтернативы должна еще созреть, когда появятся потребности в «окучивании» больших объемов и пространств за относительно небольшие деньги.

Никита УТКИН

Я глубоко убежден в том, что на российском рынке должны быть созданы условия для того, чтобы «росли все цветы»: и LoRaWAN, и NB-IoT. А уже далее российский рынок сам проголосует рублем за то, что окажется лучше и эффективнее.

Некоторые рыночные игроки вообще не рассматривают для себя возможность поставить все на одну лошадь, умело балансируя между несколькими альтернативными решениями. Вопрос лишь в одном: для того чтобы иметь полноценное право на развитие, необходимо выполнить обязательства по полному раскрытию перед рынком, а лучший метод для этого – раскрытие полной спецификации в национальном стандарте.

Такой путь во взаимодействии с нашим Техническим комитетом уже избрали для себя сторонники NB-Fi, LoRaWAN, OpenUNB, идут обсуждения по поиску лучшего варианта для раскрытия NB-IoT. Одним словом, раскрытие перед российским рынком всего семейства стандартов Интернета вещей – исключительно вопрос времени, причем весьма недалекого.

Андрей ЭКОНОМОВ

В среде операторов (включая и владельцев NB-IoT-сетей) такой вопрос не стоит, поскольку в больших, сложных проектах технологии взаимно дополняют друг друга, что обусловлено различными техническими особенностями решений.

Большинство аналитиков сходятся во мнении, что для LoRaWAN останется существенная рыночная доля, даже если все сотовые операторы мира включат в своих сетях NB-IoT. Во-первых, устройства LoRaWAN всегда будут дешевле девайсов NB-IoT – уже в силу более простой схемотехники. Во-вторых, нелицензируемый диапазон, особенно в отечественных реалиях, позволяет быстро и относительно дешево развертывать сети LoRaWAN там, где нет и не предвидится покрытия NB-IoT (удаленные технологически площадки – карьеры, буровые установки, железнодорожные и автомобильные магистрали).

Как обстоят дела с проблемой кибербезопасности в сетях LoRaWAN?

Александр ГОЛЫШКО

В нашем мире вообще нет ничего кибербезопасного, кроме отсутствия Интернета.

Другой вопрос – нужна ли кому-то информация из большинства таких сетей, если они не касаются производства, финансов и обеспечения той же самой безопасности? А они в большинстве своем и не касаются.

Андрей ЭКОНОМОВ

У LoRaWAN – наивысшая степень безопасности передачи данных среди всех LPWAN-технологий. Она включает в себя: многоуровневую систему шифрования (в том числе End-to-End), безопасные генерацию и хранение ключей шифрования (как на устройстве, так и на стороне сети), возможность обновления ПО уже установленных датчиков через эфир в целях устранения найденных уязвимостей. ■

Технологическое погружение в эпоху данных

19–20 февраля в Москве, в Центре цифрового лидерства SAP, состоялась очередная технологическая конференция SAP Digital Exchange 2020. Пленарная сессия была посвящена инструментам построения интеллектуального предприятия. Представляя решения компании и технологическую платформу для бизнеса, топ-менеджеры SAP SE рассказали о трансформации технологий в глобальную эпоху данных, преимуществах цифровизации взаимодействия с клиентами и на примерах пояснили, у кого выше шансы выиграть на рынке в условиях экономики впечатлений.

Технологическая конференция SAP Digital Exchange 2020 стала третьей по счету, при этом она впервые проводилась отдельно от Форума SAP, который в текущем году состоится 23 апреля. По словам генерального директора SAP CIS Андрея Филатова, решение о проведении конференции в феврале принято неслучайно. SAP предлагает много новинок, продолжает развивать свои решения. И чем раньше компания расскажет о них, тем раньше заказчики начнут пользоваться современными продуктами.

Год назад SAP представила на рынке концепцию интеллектуального предприятия. Речь идет не о наборе продуктов, а о путешествии, под которым понимается непрерывное движение вперед. В подобном случае важнее подход, позволяющий под другим углом зрения посмотреть на бизнес и с использованием современных технологий получить от бизнеса нечто недоступное ранее.

Нередко о SAP упоминают в контексте ERP-системы для автоматизации бизнес-процессов. По мере проникновения цифровых технологий на первый план вышла задача по извлечению данных из этих процессов. Сегодня в компании предпочитают говорить о реализации не ERP-системы, а цифрового ядра. SAP S/4HANA служит основой для построения интеллектуального предприятия.

При обсуждении темы облачных технологий на пленарной сессии говорилось о недоверии к ним. Службы безопасности не приветствуют применение решений на базе облачных технологий. В этом плане Россия не отличается от других стран, где тоже есть консервативно настроенные заказчики. Тем не менее облачные технологии продолжают развиваться, увеличивается объем их реализации.

В конце прошлого года компания SAP CIS заключила соглашение с Минкомсвязи РФ о создании совместного акселератора для стартапов. Из 107 компаний, подавших заявки, вендор отобрал десять. В рамках системы акселерации специалисты SAP помогут этим стартапам развивать предложенные ими решения.

Наряду с этим SAP CIS в роли посредника продолжает активировать взаимодействие бизнеса и высших учебных заведений. К настоящему времени действует 25 лабораторий с ведущими вузами страны, в том числе региональными. Бизнес ставит перед студентами цифровые задачи, компания предоставляет технологии, обеспечивает консультации архитекторов, других специалистов. Такой подход на практике зарекомендовал себя как эффективный способ продвижения инноваций.

В текущем году в SAP CIS намерены реализовать еще один проект – Marketplace SAP в России. Среди его преимуществ – централизованный доступ к решениям партнеров на платформе вендора, снижение затрат, повышение гибкости и скорости внедрений.

На пленарной сессии конференции выступили вице-президенты и руководители таких направлений SAP SE, как SAP S/4HANA, «Платформа и технологии», Intelligent Robotic Process Automation, «Управление продуктами и индустриальное развитие». Большое внимание в этих презентациях было уделено тенденциям технологического развития в глобальную эпоху данных, которые находятся в разных средах и работают по различным правилам. В том и заключается основная сложность их применения с выгодой для бизнеса.

Использование интеллектуальных технологий позволяет не только моделировать, автоматизировать, но и переосмыслить бизнес-процессы. В частности, сегодня компания предлагает инструменты роботизированной автоматизации процессов, а также искусственного интеллекта для преобразования бизнес-процессов предприятия. Потребность современных компаний в роботизированной автоматизации объясняется необходимостью оптимизации процессов и ресурсов, уменьшения доли ручных операций, повышения удовлетворенности клиентов.

На конференции неоднократно подчеркивалось, что любые технологические новинки и подходы к их внедрению в различных индустриях реализуются в целях повышения лояльности и управления клиентским опытом. ■

www.connect-wit.ru

Имитационное моделирование в промышленности

Андрей АККУРАТОВ,
технический консультант по решениям SIMULIA, Dassault Systèmes

Место инструментов симуляции в жизненном цикле создания и обслуживания изделий и работе предприятий.

При создании сложных технических объектов, таких как самолеты, автомобили, высотные здания нестандартного вида, нефтеперерабатывающие заводы и другие, на всех этапах проектирования зачастую внедряются нестандартные новые решения. В этом случае проверки на прочность, комфорт и качество изделия выполняются расчетными инструментами, которые в производственной части применяются для оптимизации технических процессов.

Яркий пример – аддитивные технологии, так называемая 3D-печать, позволяющая с помощью средств моделирования полностью воссоздать производственный процесс в виртуальной среде. Мы виртуально выстраиваем деталь, которую планируется напечатать, и определяем потенциальные дефекты и искажения, которые могут проявиться в процессе печати. Коррекция потенциальных несовершенств в цифровом формате позволяет с первого раза получить деталь требуемых параметров и качества. Таким образом, мы минимизируем затраты – материал на изготовление детали, рабочее время технолога и станка – и быстрее получаем готовый продукт. В этом основная цель инструментов моделирования – сокращение времени и стоимости разработки, уменьшение количества натурных испытаний, обеспечение безопасности и высокого качества изделий.

Всеобщее моделирование

В целом можно заключить, что место инструментов симуляции, иными словами имитационного моделирования, в жизненном цикле разработки – между конструкторской и проектной деятельностью и технологической частью. Необходимость в таких инструментах возникает уже после разработки структурной части, но еще до отправки спроектированных изделий в производство или на монтаж – именно тогда нужно провести верификацию данных конструкторских решений, чтобы соблюсти условия прочности, безопасности, долговечности и др.

Средства имитационного моделирования в настоящее время используются во всех научных направлениях: обеспечение прочности (прочность, усталость, трещиностойкость), гидро- и аэродинамика (воздушные, жидкостные потоки); в сферах, связанных с электромагнитными явлениями, задачами теплопередачи и др. Требования относительно качества конечного продукта, а вместе с ними и сложность инженерных задач неуклонно растут во всех сферах: например, автомобили, которые выпускались 20–30 лет назад и выпускаются сегодня, с технологической точки зрения отличаются довольно существенно. То же самое в строительстве сложных технических объектов, таких как высотные здания оригинального дизайна в сейсмоопасной зоне. Такое здание должно полностью соответствовать ряду критериев безопасности, в частности, должна быть решена сложная задача прогрессивного разрушения.

Принципы работы остались аналогичными, но необходимость внедрения новых деталей, таких как турбированные двигатели, потребовала инновационного подхода. Таким решением стали расчетные инструменты, позволяющие с большой точностью проектировать продукты высокого качества, которые будут работать на заданном уровне, с заданным качеством, в заданный срок.

При использовании методов имитационного моделирования важно провести качественную верификацию построенных моделей. В настоящее время она осуществляется путем конечных натурных испытаний. Разумеется, цель использования расчетных инструментов в том, чтобы уменьшить количество таких испытаний

до нуля, но, к сожалению, она пока не достигнута. Точность расчетов за последние годы значительно возросла, удалось сократить количество испытаний, и в некоторых областях расчетные результаты принимают в качестве сертификационного материала, однако далеко не повсеместно.

В будущем, с появлением усовершенствованного расчетного программного обеспечения возможно проектирование без прототипирования (zero-prototipe): когда мы проектируем изделие, рассчитываем параметры, проводим виртуальные испытания и они становятся сертификационной частью.

Основное назначение инструментов симуляции в том, чтобы руководство предприятия могло использовать результаты расчетов при принятии решений. Такие инструменты помогают проверять, подтверждать и обеспечивать заявленные свойства продукта, выпускать максимально сложные и качественные товары по высочайшим стандартам, достигать экономической эффективности производства, максимально сокращать сроки проектирования и количество натурных испытаний. Значимость инструментов симуляции в инфраструктуре управления современным производством растет из года в года по мере повышения требований к качеству продукции и сложности технических объектов.

Классификация решений

Существует несколько классификаций. Первая – по научным направлениям: это структурный анализ (прочность, усталость, трещиностойкость), гидрогазодинамика (все, что касается исследования потоков, газовых или жидкостных), электромагнетизм, многотельное моделирование (multibody simulation).

Вторая классификация основана на моделировании процессов на макро- и микроуровне. На микроуровне имитируется поведение материала вплоть до молекулярной ступени. На макроуровне изучается характер детали, моделируется поведение сборок с несколькими деталями, соединенными между собой.

Третья классификация – это отдельно стоящие и сопряженные расчеты, когда одновременно производится расчет, например, прочности и гидрогазодинамики. Яркая иллюстрация – аэроупругость, при которой структурные изменения конструкции влекут за собой изменение аэродинамических характеристик, а изменение аэродинамических характеристик, в свою очередь, меняет результаты структурного анализа.

Инструменты бренда SIMULIA нашей компании охватывают все классификации и научные направления. Dassault Systèmes помимо непосредственно расчетных инструментов предоставляет руководству предприятий возможность отслеживать связи между расчетами, конструкторскими разработками и технологическими решениями на базе платформы 3DEXPERIENCE. Благодаря платформе топ-менеджмент может принимать оптимальные решения на основе ряда полученных результатов.

Потребности

Расчетные инструменты будут эффективны для всех компаний – разработчиков негабаритной продукции, а также тех, кто предоставляет сервисное обслуживание, однако в России в этой сфере они пока редко используются. При этом даже у одного производителя инструментов моделирования есть целый набор продуктов, каждый из которых нацелен на решение комплексных и нестандартных задач в различных отраслях. Например, одно решение может быть создано для расчетов структурной прочности (усталости или трещиностойкости), другое – моделирует гидрогазодинамические процессы, третье – выполняет все виды расчетов для исследования электромагнитных явлений.

В частности, требования безопасности в аэрокосмической отрасли крайне высоки, поэтому точность и надежность расчетов не должны ставиться под сомнение. Среди наших заказчиков есть и Boeing, и Airbus – крупнейшие производители самолетов, а также производители авиационных двигателей, относящихся к самым сложным объектам, разработанным человеком за всю историю.

Имитационное моделирование необходимо и в горнодобывающей отрасли. Геомеханические исследования очень сложны, и в мире не так много расчетных инструментов, которые на высоком уровне могут выполнять сложное моделирование за короткий срок. Есть решения, которые позволяют сократить моделирование и механический расчет нефтяного месторождения в несколько раз. Кроме того, решениями для имитационного моделирования пользуется множество заказчиков из шинной индустрии, судостроения, медицины.

Расчетные инструменты наиболее эффективны в проектировании сложных технических объектов: они позволяют уменьшить как сроки, так и стоимость проектирования. Для окупаемости любому производителю важно, чтобы в течение гарантийного срока ему не пришлось тратиться на обслуживание изготовленного продукта. Тем не менее следует понимать, что не всегда подобные решения окупаются напрямую. Например, коммерческий успех ABAQUS объясняется его сильным математическим аппаратом, позволяющим решать задачи, которые требовали бы совместного использования сразу нескольких интегрированных между собой инструментов.

Заключение

При рассмотрении тенденций развития инструментов для имитационного моделирования не стоит жестко разделять мировой и российский рынки: вероятно, в определенных сферах производства российские разработчики действительно отстают от зарубежных, но в целом следуют ведущим трендам. Основная тенденция сегодня как в России, так

и за рубежом – совершенствование математического аппарата для повышения точности и качества результатов. Кроме того, прослеживается тренд на интеграцию различных расчетных инструментов в единые платформы и даже в один интерфейс. Также все чаще производители объединяют решения с системой PLM и расширяют функционал для выполнения мультифизических задач. Появляется множество возможностей для сопряженных расчетов, которые позволяют совместно выполнять структурный расчет и многотельное моделирование для получения более высокого результата.

В целом конкуренция на рынках производственных продуктов и программного обеспечения обостряется, все компании стараются нарастить количество клиентов. Российские производители пока проигрывают зарубежным по причине того, что не привыкли активно вкладываться в развитие расчетных инструментов и выделять средства на их поддержку. Тем временем такие инвестиции приняты у зарубежных компаний и крайне важны. Во-первых, эти средства окупаются за счет выпуска наиболее совершенного продукта. Во-вторых, позволяют производителям экономить на сервисном обслуживании: им не приходится выполнять гарантийные обязательства, соответственно они не задействуют персонал и производственные мощности, сокращая расходы. Благодаря этому компания обретает хорошую репутацию и доброе имя, что, в свою очередь, дает возможность выпускать более дорогие и сложные изделия, поскольку потребители уверены в качестве, удобстве и надежности товаров.

Некоторые российские разработчики постепенно наращивают арсенал расчетных инструментов и инвестируют в их поддержку, но конкурировать с зарубежными лидерами индустрии, разумеется, пока еще сложно. Например, некоторые решения нашей компании имеют историю развития и выполнения прикладных задач продолжительностью около 40 лет, и новым продуктам непросто нарастить аналогичный функционал, экспертизу и репутацию. ■

Новое программное обеспечение позволяет исключить ручное программирование и осуществлять 3D-печать за считаные минуты

ABB добавила функцию 3D-печати в свой программный продукт RobotStudio, предназначенный для моделирования и офлайн-программирования. Это позволит всего за 30 минут программировать роботов ABB для аддитивного производства. Новый модуль для 3D-печати добавлен в RobotStudio в рамках пакета PowerPac. Он позволяет исключить ручное программирование и ускорить производство прототипов. PowerPac поддерживает различные процессы, такие как сварка или печать гранулированным пластиком или цементными смесями, и идеально подходит для небольших объемов печати материалов с высокой смешиваемостью. Традиционные методы программирования многоосевых систем для 3D-печати подразумевают трудоемкий и утомительный процесс подготовки траекторий с миллионами точек. Благодаря модулю 3D Printing PowerPac любой стандартный дизайн, предложенный программой слайсером, можно «перевести» в среду моделирования ABB и программный код робота. Это позволяет оператору переходить от CAD-моделей к 3D-печати в течение получаса. По данным исследовательской компании Markets and Markets, индустрия 3D-печати интенсивно растет. Ожидается, что к 2024 г. она достигнет 34,8 млрд долл., в частности благодаря разработке новых материалов для 3D-печати промышленного уровня. «Наше программное обеспечение дает пользователям упрощенный и более быстрый процесс 3D-печати. Вкупе с высокой производительностью наших роботов это позволит более эффективно изготавливать высококачественные 3D-печатные объекты для самого разнообразного применения в промышленности», – рассказал Стивен Уайатт, глава отдела цифровых продуктов ABB Robotics

www.abb.ru

Захват мира, фаза 2

Десятая версия ПО для резервного копирования от Veeam

Международная компания Veeam объявила о выпуске новой, уже десятой по счету версии своего флагманского продукта Availability Suite – решения для защиты данных от потери в виртуальных средах. Система позволяет делать резервные копии виртуальных машин и восстанавливать их в случае необходимости в другой виртуальной среде в рамках одного облака. Именно ориентированность технологий Veeam на облачные конфигурации и позволила компании стать лидером на рынке решений для резервного копирования данных в облачных средах VMware, Hyper-V и S3, оставив позади производителей классических решений для резервного копирования.

По словам нового регионального директора Veeam в России, СНГ, Украине и Грузии Владимира Клявина, выход в лидеры на рынке систем резервного копирования является только первой фазой, в которой компания работала по классической методике продаж бессрочных лицензий. Компании удалось убедить 375 тыс. заказчиков в том, что их продукт может просто работать и гарантировать быстрое восстановление работоспособности облачных приложений и сервисов. В результате оборот компании уже перевалил за миллиард долларов.

Теперь компания приступает к реализации фазы 2 своего плана по захвату мирового рынка резервного копирования, который подразумевает синергию с цифровизацией и переход от традиционных бессрочных лицензий на модель подписки на уровне оператора сервиса. С этой целью компания создает единую платформу резервного копирования и защиты данных для облачных, виртуальных и физических сред, что поможет облачным провайдерам предлагать своим клиентам различные варианты обеспечения защиты их данных. Естественно, в рамках второй фазы компания планирует расширить взаимодействие с операторами облачных сервисов и системными интеграторами.

Причем новая версия продукта позволяет пользоваться резервной копией данных, например, для их анализа, что может пригодиться владельцам больших данных. Veeam опубликовала API для разработчиков таких приложений, с помощью которого можно организовать доступ к архивным данным. Это позволит активно использовать резервную копию данных в бизнесе. При этом компания предлагает даже для облачных сервисов систему защиты от шифровальщиков – неудаляемые копии. Система резервного копирования в течении некоторого времени не удаляет резервные копии и автоматически проверяет целостность данных и структур файлов и не дает их уничтожить даже администраторам ресурса. Это позволит в случае нападения вируса шифровальщика или перехвата злоумышленниками контроля над облачным сервисом откатить систему до момента его проникновения в систему и сохранить накопленные к тому моменту данные.

Кроме того, компания предложила технологию «мгновенного» восстановления цифровых сервисов – виртуальные машины сервиса запускаются очень быстро, но до восстановления накопленных данных их функционал будет несколько ограниченным. Данные в системе появятся по мере загрузки их из резервной копии. Такие решения очень полезны в эпоху цифровой экономики, поскольку позволяют сохранить работоспособность цифровых сервисов даже в случае нападения вымогателя. Благодаря таким разработкам сервисы резервного копирования должны стать частью системы информационной защиты цифрового предприятия.

Хотя компания была организована русскими инженерами, но ее программное обеспечение не находится в реестре отечественного ПО. Veeam изначально создавалась как международная и на текущий момент имеет офисы разработки в Санкт-Петербурге и Праге. Общее количество сотрудников в настоящее время составляет около 4,5 тыс человек по всему миру, и в ближайший год компания рассчитывает нанять еще около 1 тыс. Отсутствие привязки к российскому реестру позволило владельцам компании продать ее инвестиционному фонду Insight Partners за 5 млрд долл. – сейчас сделка находится на этапе подтверждения всеми регулирующими органами. После ее завершения компания окончательно станет американской, что позволит усилить ее позиции в том числе и на американском рынке. В этом случае ее продукция, скорее всего, будет распространяться по всему миру. В результате руководство компании рассчитывает удвоить оборот в самое ближайшее время, т. е. достигнуть оборота в 2 млрд долл. ■

«Легкие» сети

Дмитрий ЛИТОВЧЕНКО,
сетевой инженер, CompTek

Аббревиатура Li-Fi (Light Fidelity) используется (по аналогии с привычной всем Wi-Fi) для обозначения двунаправленной высокоскоростной беспроводной технологии. Термин Li-Fi был придуман Харальдом Хаасом – профессором Эдинбургского университета. Этот вид передачи данных использует видимый свет в открытом пространстве без волновода как канал связи в отличие от радиоволн в сетях Wi-Fi. Таким образом, Light Fidelity принадлежит к коммуникационным технологиям VLC (Visible Light Communication – связь по видимому свету).

Связь по свету

Li-Fi – это высокоскоростные сети, использующие инфракрасный (ИК) диапазон спектра и диапазон видимого излучения. Изначально развитие Li-Fi предполагалось в рамках IEEE 802.15.7, однако рабочая группа по этому стандарту прекратила свою работу.

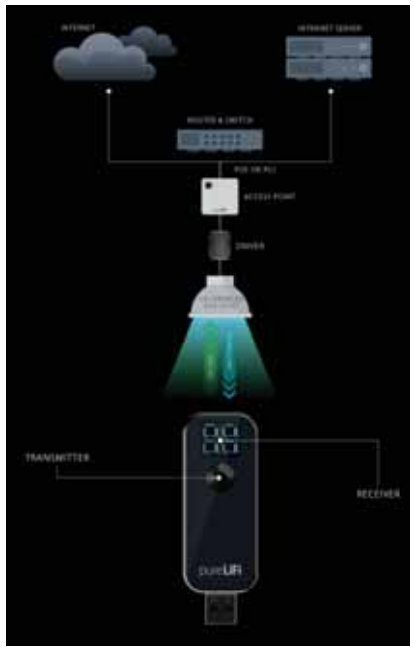
Максимальная канальная скорость, определенная в стандарте, составляет 96 Мбит/с. Для раскрытия полнодуплексной передачи с помощью света потребовались новые решения и новые стандарты. Все существующие на данный момент на рынке решения используют проприетарные технологии.

Исследователи работают над более эффективными методами модуляции сигнала для Li-Fi-сетей и предлагают различные «обертки» из стека протоколов, которые добавляют модель каналов, защиту от интерференции, описывают связь с сетевыми протоколами и интеграцию в существующие сети беспроводной связи.

Отметим также, что дальнейшая стандартизация Li-Fi ведется рабочей группой IEEE 802.11bb (не путать с 802.11b). Более 20 лет стандарт 802.11 описывал локальные беспроводные сети (WLAN), работающие в радиочастотном диапазоне, а теперь он расширил круг своих интересов и до видимого излучения.

Схема Li-Fi-сети

Рассмотрим наиболее распространенную схему Li-Fi-сети, предлагаемую известными производителями оборудования.



Точка доступа Li-Fi подключается в локальную сеть, а ее интерфейс для взаимодействия со светодиодами подсоединяется к светильнику. Для загрузки (Downlink – канал связи от светильника к клиентскому устройству) используется диапазон видимого излучения, для Uplink (канал связи от клиентского устройства к светильнику) – ИК-диапазон.

Для этого светильник должен быть оборудован ИК-приемником либо необходимо монтировать точку доступа с интегрированным ИК-приемником рядом со светильником. В качестве клиента выступает совместимый с USB 2.0 адаптер, который подключается к ноутбуку или планшету. Современные решения предусматривают роуминг между сотами (светильниками), которые находятся в одной подсети.

Текущее состояние рынка Li-Fi

Индустрия Li-Fi сегодня представлена следующими значимыми вендорами: PureLiFi, Signify, Oledcomm, VLNComm, Panasonic.

PureLiFi

Эта компания готова предложить полноценное решение для Li-Fi-сети, состоящее из точки доступа (PureLiFi XC Access

Point) и абонентского устройства (PureLiFi XC Station), совместимого с USB 2.0.

Последнее поколение устройств, выпущенное в 2018 г., называется XC и способно обеспечивать связь на скорости до 43 Мбит/с полного дуплекса. При этом драйверы для абонентского устройства есть под все популярные ОС: Windows 10, Mac OS, GNU/Linux.

Особенности точки доступа:

- одна точка поддерживает до восьми одновременно подключенных клиентов;
- возможность изменения мощности светового потока без потери передачи данных;
- поддержка широкого спектра светильников;
- проприетарный протокол роуминга;
- WPA2-Personal/WPA2-Enterprise аутентификация.

Signify

Компания Signify предлагает набор решений под общим названием Trulifi, которые разработаны как для сетей типа «точка – многоточка», так и «точка – точка».

Система Trulifi может быть легко интегрирована в существующую инфраструктуру светильников, однако есть возможность приобрести светильники от производителя с интегрированными оптическими трансиверами. Заявленная скорость для сетей «точка – многоточка» и «точка – точка» составляет 150 Мбит/с и 250 Мбит/с соответственно.

Trulifi поддерживает роуминг, также заявлена возможность одновременного просмотра до 30 FullHD видео с одной точки доступа.

Решение состоит из оптического трансивера Trulifi-6002 Plug-In Optical Transceiver, Li-Fi-совместимых светильников и USB клиентского устройства.

Oledcomm

Основное решение, предлагаемое компанией, – LiFiMax

Trulifi-6002

Trulifi клиентское устройство

Интеграция Trulifi абонентского устройства в спинку кресла в транспорте

LiFiMax Access Point

LiFiMax Dongle

Access Point и LiFiMax Dongle. Заметим, что в этом решении отсутствуют светодиодные светильники, а в качестве основного приемопередающего устройства используется точка доступа, работающая в ИК-диапазоне. Точка доступа поддерживает 16 одновременных соединений и обеспечивает Downlink до 100 Мбит/с.

Также на основе Li-Fi компанией Oledcomm создано решение GEOLiFi – система позиционирования устройств. Компоненты решения:

- GEOLiFi совместимые светодиодные светильники;
- GEOLiFi передатчик;
- GEOLiFi планшет с интегрированным фотосенсором (Android);
- приложение позиционирования для планшета.

VLNComm

Эта компания предлагает светодиодные светильники собственного производства LumiNex со встроенной точкой доступа и ИК-приемопередатчиком, а в качестве клиента выступает Lumi Stick – совместимый с USB 2.0 адаптер.

Точка доступа поддерживает до 15 одновременных соединений и обеспечивает Downlink и Uplink на скорости 70 и 60 Мбит/с соответственно. Для передачи от точки доступа к клиенту могут использоваться как светодиоды, так и ИК-интерфейс, т. е. передача данных возможна при выключенном освещении.

Panasonic

Panasonic использует технологию LinkRay, основанную на Li-Fi. LinkRay работает только в одну сторону – смартфон считывает информацию. Такая схема передачи схожа с распознаванием QR-кодов. LinkRay позволяет обычному смартфону считывать ID, которые передаются светодиодными передатчиками (дисплеи, указатели, точечные светильники производства Panasonic). Чтобы считать ID, на смартфоне необходимо установить приложение LinkRay и навести камеру на источник излучения.

Производитель подтверждает совместимость многих моделей смартфонов (https://panasonic.net/cns/LinkRay/#LinkRaySupport), например, практически все современные модели от Apple совместимы.

Основным преимуществом LinkRay перед QR-кодами, которые распознает камера смартфона, является возможность считывания ID с большего расстояния и в местах с высокой плотностью людей. После того как ID (чаще всего это ссылка на сторонний ресурс) будет получен с помощью LinkRay, дальнейшая передача данных происходит другими доступными клиентскому устройству методами (Wi-Fi, мобильная сеть).

LinkRay предполагается применять в торговых центрах, на выставках и для навигации на транспорте.

Преимущества технологии

Li-Fi работает в частотном диапазоне видимого и ИК-излучения. Из этого следует два значимых плюса. Li-Fi не интерферирует с устройствами, работающими в сантиметровом диапазоне, т. е. с Wi-Fi. Другими словами, Li-Fi-сеть и подключенные клиенты не будут занимать среду передачи Wi-Fi и замедлять работу сети. Кроме того, использование видимого излучения открывает возможности для высокоскоростной передачи, так как частотный спектр видимого излучения значительно шире (почти на шесть порядков), нежели спектр, выделенный под Wi-Fi-устройства.

Современные решения позволяют осуществлять передачу данных даже при отсутствии освещения, что достигается либо путем снижения мощности светового потока светодиодов до уровня, когда человеческий глаз не распознает свет, но передача данных возможна, либо с помощью ИК-интерфейса.

Шум от сторонних источников, например от солнца, не сказывается на работе Li-Fi. PureLiFi заявляет о стабильной работе клиентского устройства при освещенности в 77 тыс. люксов, что сопоставимо с работой под прямыми лучами солнца в ясный день.

Li-Fi приписывается много достоинств, но являются ли они конкурентными? Рассмотрим это на следующих примерах.

Высокая скорость передачи

Из имеющихся сегодня на рынке решений максимальную скорость передачи предлагает Signify – до 150 Мбит/с при подключении к точке доступа одного клиента. Приблизительно такая же скорость достигается при использовании Wi-Fi-сети, состоящей из точки доступа и клиентского устройства и работающей на канале 40 МГц с поддержкой двух пространственных потоков.

Безопасность

Свет не проходит через стены, поэтому к Li-Fi-точке доступа нельзя подключиться из соседней комнаты или удаленно собрать передаваемый трафик. Хотя это и является преимуществом, существующие Li-Fi-продукты используют набор протоколов безопасности WPA2-Personal/WPA2-Enterprise – тот же самый протокол, который применяется в Wi-Fi. Такой набор протоколов успешно обеспечивает безопасность Wi-Fi-сети и позволяет делать ее столь же защищенной, как и проводное подключение.

Простота внедрения

Наличие большого количества светильников не означает простоту внедрения Li-Fi. Имеющиеся решения можно разделить на две группы: светильник уже имеет встроенную точку доступа Li-Fi; точка доступа подключается отдельно к каждому совместимому светильнику. В первом случае необходимо монтировать целый парк новых светильников, во втором – точки доступа в надежде, что светильники будут совместимы (иначе см. первый случай).

Уменьшение нагрузки на Wi-Fi-сети

Поскольку технология Wi-Fi насчитывает более двух десятков лет, на рынке труда много квалифицированных инженеров, которым хорошо известны принципы проектирования Wi-Fi-сетей для условий высокой плотности пользователей. Комплексный и последовательный подход к проектированию Wi-Fi-сети снимает необходимость в увеличении ее емкости с помощью Li-Fi.

Низкие задержки

Li-Fi обещает низкие задержки при передаче данных. Производитель VLNComm сообщает о задержках в сети, построенной на их оборудовании, менее 1 мс. Столь низкие задержки при передаче данных – очень интересная особенность, применение которой пока сложно найти. Самые требовательные к задержкам и их вариациям приложения – голос и видео – успешно передаются в Wi-Fi и мобильных сетях. Более того, чаще всего то, что называют требовательным к задержкам, на самом деле требовательно к их равномерности, что еще сильнее уменьшает необходимость в этом «преимуществе».

Li-Fi безопасен для использования в медицине и авиации

Это действительно так, однако сети Wi-Fi также не создают помех медицинскому оборудованию (ни в диапазоне 2.4 ГГц, ни в 5 ГГц), потому что работают в другом диапазоне частот. Сервис Wi-Fi на борту гражданского самолета уже не вызывает удивления и предлагается большинством крупных авиаперевозчиков, потому что бортовое оборудование сейчас может быть успешно изолировано от интерференции с сетями Wi-Fi.

Недостатки Li-Fi

Приемопередатчики на клиентских устройствах

Во всех существующих реализациях клиентское устройство расположено на горизонтальной поверхности, сенсор с углом обзора в 100–120° направлен в потолок. Смартфон при эксплуатации значительно меняет свое положение в пространстве, поэтому необходимо интегрировать в его корпус более одного сенсора для уверенного приема сигнала в различных положениях.

Экспертами рассматриваются различные варианты установки сенсора на клиентское устройство, которое на протяжении экспериментов находится в положении как при телефонном разговоре (см. статью https://mentor.ieee.org/802.11/dcn/18/11-18-1236-01-00bb-ieee-802-11bb-reference-channel-models-for-indoor-environments.pdf). Понятно, что в таком положении хватит и одного сенсора на верхней кромке смартфона, однако понадобится еще как минимум два сенсора на фронтальной и тыльной сторонах устройства для работы на горизонтальной поверхности.

> Li-Fi обещает низкие задержки при передаче данных.

Отсутствие клиентских устройств

Главный минус сетей Li-Fi вытекает из отсутствия весомых конкурентных преимуществ и нишевости данной технологии.

Стандартизация

Рабочая группа по 802.11bb предлагает изменения в стандарте 802.11, которые позволят реализовать передачу в видимом диапазоне излучения. Для этого необходимо пересмотреть физический и канальный уровни передачи данных.

На канальном уровне вносятся изменения в метод доступа к среде (в HCF), а также рассматривается вопрос пересекающихся зон покрытия сервиса Li-Fi и Wi-Fi и роуминга. На физическом уровне предлагается использовать ортогональное частотное разделение каналов с множественным доступом (OFDMA), известное из LTE и Wi-Fi 6 (802.11ax).

Текущая версия стандарта – 0.1. То есть процесс работы начался сравнительно недавно, и нам еще представится возможность увидеть дальнейшие метаморфозы сетей Li-Fi. ■

Российское телеком-оборудование

Алексей БОЛДИН,
директор по взаимодействию с госорганами, компания RDP.RU

Ни для кого не секрет, что российская промышленность в сфере производства телекоммуникационного оборудования в настоящее время отстает от Запада (США и Европы) и Востока (Китая, Японии, Южной Кореи). И в этой ситуации есть два пути развития: смириться с существующим положением вещей и просто пользоваться зарубежными технологиями или пытаться наверстать отставание и заместить зарубежные аналоги.

Выбор сделан

Первый путь (пользоваться зарубежными телекоммуникационными технологиями) имеет целый ряд недостатков, связанных с национальной безопасностью, включая и зависимость от Запада, и уязвимость в случае конфликта из-за наличия незадекларированных возможностей зарубежного оборудования и т. д.

С учетом вектора внешней политики, определенного руководством нашей страны, первый путь для России однозначно не подходит, что подтверждается, в частности, большим количеством целевых программ, задача которых – поддержать российских производителей в сфере телекоммуникаций. Такие программы инициируются на всех уровнях государственной власти и, кроме того, государственными корпорациями.

Основной государственной программой в этой сфере является «Цифровая экономика Российской Федерации», утвержденная распоряжением Председателя Правительства № 1632-р от 28 июля 2017 г. Указанная программа затрагивает широкий спектр изменений в различных отраслях российской экономики. Для ее реализации необходимо продвинутое «цифровое пространство», которое может быть построено на современном телекоммуникационном оборудовании.

Пути решения проблемы

Согласно документу значительное отставание в развитии цифровой экономики от мировых лидеров объясняется пробелами нормативной базы и неблагоприятной средой для ведения бизнеса и инноваций и, как следствие, низким уровнем применения цифровых технологий бизнес-структурами.

Чтобы стимулировать российских производителей, делается ставка на импортозамещение. В целях реализации этого пункта «Цифровой экономики» был создан Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий, в обязанности которого входят анализ и проработка возможных изменений в существующей нормативной базе.

Одновременно с этим государство выделяет средства на разработку определенных видов товаров, перечень которых утверждается. Деньги выделяются ежегодно на возмещение части затрат на разработку или в виде грантов.

Законодательные инициативы

Что касается изменения нормативно-правовой базы, то в настоящее время уже принят целый ряд документов, направленных на стимулирование российских производителей в сфере информационных технологий.

Так, в ноябре 2015 г. было утверждено Постановление Правительства № 1236, устанавливающее запрет на закупку зарубежного программного обеспечения государственными и муниципальными структурами. Особо подчеркнем, что это постановление было утверждено еще до программы «Цифровая экономика», а команда, которая работала над ним, вошла в состав Центра компетенций. Также стоит отметить активное участие самих разработчиков в создании постановления.

Был сформирован Реестр отечественного программного обеспечения и утверждены соответствующие параметры. Теперь при осуществлении закупок программного обеспечения для государственных и муниципальных нужд заказчик должен приобретать в первую очередь ПО из Реестра, а в случае отсутствия нужного ПО необходимо писать обоснование о невозможности закупки российского софта. Несмотря на то что заказчики идут на различные ухищрения, чтобы пользоваться привычным зарубежным ПО, продажи российских компаний в этой области значительно выросли.

В плане программирования Россию никак нельзя считать отстающей: многие российские программы используются по всему миру и имеют огромный успех.

Российский телеком

По этому же пути решили пойти и с телекоммуникационным оборудованием. В июле 2019 г. Правительство Российской Федерации утвердило Постановление № 878, устанавливающее приоритет оборудования российского происхождения при закупках для обеспечения государственных и муниципальных нужд. Был создан единый Реестр российского радиоэлектронного оборудования, объединивший в себе ранее действующие реестры: телекоммуникационного оборудования, которому присвоен статус российского, и реестр по Постановлению № 719 от 17 июля 2015 г.

Кроме того, с сентября 2016 г. действует Постановление Правительства № 925, которое предусматривает ценовой приоритет в 15% российского оборудования при закупках госкомпаниями по Федеральному закону № 223 «О закупках товаров, работ, услуг отдельными видами юридических лиц» от 18 июля 2011 г.

Таким образом, при закупках ИТ-оборудования в соответствии с Федеральным законом № 44 от 05.04.2013 (ред. от 27.12.2019) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», если были поданы два и более предложения с оборудованием из единого Реестра радиоэлектронного оборудования, то должны быть отклонены все заявки с предложением иностранного оборудования. По Федеральному закону № 223 при закупках ИТ-оборудования российское оборудование из Реестра оценивается по цене «предложение минус 15%».

Распоряжение от 26.12.2019 дополняет Постановление Правительства № 878 только в части ВОЛС, которые в постановлении не затрагиваются, поскольку они не относятся к радиоэлектронному оборудованию. Оптические кабели российского производства широко распространены, так что в этом смысле ценность распоряжения минимальна.

Если говорить о возможности использования российского оборудования в КИИ, то в ФЗ № 187 понятие КИИ размыто. По идее к КИИ относится любая сеть связи, что означает необходимость принуждать частный бизнес к выполнению указанного закона, а инструмент воздействия не прописан. Исходя из определения Закон «О суверенном Интернете» можно отчасти отнести к реализации КИИ, но в ФЗ № 90 КИИ не упоминается.

Проблемы развития импортозамещения

Итак, российские производители получили мощную господдержку: нормативную (см. вышеуказанные документы) и денежную – ежегодно выделяются миллиарды рублей. Вроде бы импортозамещение должно в России идти полным ходом, однако все пошло не так, как планировалось, особенно в отношении телекоммуникационного оборудования.

Во-первых, попасть в Реестр не так просто. Компания RDP.RU знает это не понаслышке: в нашем портфеле есть оборудование, которому присвоен и в дальнейшем подтвержден статус ТОРП (телекоммуникационное оборудование российского происхождения), например EcoNAT, EcoDPI, EcoRouter 216. Чтобы не допустить в Реестр зарубежных производителей, экспертным советом проводится тщательная проверка заявителей.

Во-вторых, даже если оборудование попало в Реестр и собрано на российской компонентной базе, его характеристики могут заметно уступать зарубежному оборудованию, а цена может оказаться выше. С 2021 г., чтобы попасть в Реестр, необходимо использовать микропроцессоры российского производства, но именно в технологиях производства процессоров Россия сильно отстала от Запада и Востока.

С учетом того, что заказчик не очень заинтересован работать с незнакомым оборудованием, ему не составит большого труда написать такое обоснование или указать в закупке такие характеристики, по которым российские телеком-продукты просто не пройдут. На наш взгляд, проблема заключается именно в незаинтересованности заказчика закупать российский продукт. Поэтому необходимы законы, которые будут стимулировать государственные и муниципальные органы, осуществляющие закупки.

Еще одна проблема – несогласованность развития бизнеса в сфере телекоммуникации. Чтобы разработать качественный процессор, требуются время и вложения, причем весьма существенные. Но прежде чем вкладываться, разработчик должен быть уверен, что его инвестиции окупятся. Кроме того, необходимо написать встроенное программное обеспечение, что тоже делается не быстро и стоит денег. Потом нужно найти разработчика телекоммуникационного оборудования или серверных платформ, которые закупят у него процессор.

Производителям последнего, прежде чем покупать российский процессор, также требуются гарантии, что готовый продукт будет востребован: ведь с начала разработки прошло немало времени и технология могла устареть. К тому же новый процессор нельзя просто так поставить – и все заработает: придется переписать софт, протестировать и отладить его работу. На это также уйдет много времени. Затем следует пройти процедуру вхождения в Реестр, которая может затянуться из-за необходимости предоставления большого комплекта документов и т. д.

Оценивая такой порядок действий и учитывая, что технологии развиваются очень быстро, российский разработчик обычно решает, что игра не стоит свеч.

Мобильные сети пятого поколения

Согласно Концепции создания и развития сетей 5G/IMT-2020 в Российской Федерации, утвержденной приказом Минкомсвязи России № 923 от 27.12.2019, в главе 4 определены требования высокого уровня по построению сетевой инфраструктуры 5G/IMT-2020, с учетом виртуализации сетевых элементов и функциональности SDN/NFV.

Таким образом, в России ставка делается прежде всего на ПО, с помощью которого реализуются сетевые функциональные возможности. В соответствии с мировой тенденцией передовые вендоры сетевого оборудования акцентируются на разработке именно программного обеспечения, тем самым упрощая «железную» составляющую.

При наличии у нас универсальной платформы – высокопроизводительного сервера, в зависимости от установленного на нем программного обеспечения он сможет выполнять функции маршрутизатора, а также CG-NAT (Carrier-Grade Network Address Translation – трансляция сетевых адресов операторского класса), BRAS (Broadband Remote Access Server – маршрутизатор широкополосного удаленного доступа), DPI (Deep Packet Inspection – технология глубокого анализа пакетов) и др. или даже все вместе. Поэтому у нас неплохие шансы наверстать отставание по части телекоммуникационного оборудования, функции которого можно реализовать виртуально.

Если в России будет качественное ПО, пусть даже пока работающее на иностранном «железе», при появлении отечественного производительного оборудования нам останется только портироваться на него, что не представляет большой проблемы.

Однако именно в этом вопросе нормативная база в России сильно устарела и предпосылок к ее быстрому исправлению пока нет. Дело в том, что российский заказчик сегодня не разделяет телекоммуникационное оборудование на «железо» и ПО, а воспринимает его в целом и соответственно размещает закупки на программно-аппаратный комплекс.

По этой причине разработчик не получает необходимой поддержки своего продукта (по Постановлению № 1236) и пытается попасть в Реестр радиоэлектронного оборудования, где к нему предъявляются жесткие требования, применяемые к производству, а не к разработчику ПО.

Таким образом, компаниям, специализирующимся на ПО, приходится перестраивать свою работу. А с учетом того, что в России пока нет высокопроизводительного сервера, удовлетворяющего требованиям Реестра, разработчик программного обеспечения лишается и этой поддержки.

Зачем нужны консорциумы

В сложившейся ситуации становится очевидным, что российским производителям необходимо объединяться в консорциумы, куда входили бы разработчики всех составляющих конечного продукта, а также сам госзаказчик – потребитель создаваемого российского телекоммуникационного оборудования.

Между ними должны быть подписаны соответствующие соглашения, гарантирующие востребованность разработок. Таким объединениям проще получить государственные субсидии и взаимодействовать с органами государственной власти в своих интересах, лоббировать необходимые изменения в нормативно-правовой базе.

Цифровая безопасность России

Еще одно направление, на которое выделяются большие средства бюджета, – цифровая безопасность страны. Госорганы, отвечающие за эту область, понимают, что в настоящее время ставку стоит делать на софт.

Последний год запомнился большим количеством изменений в законодательных актах, связанных с защитой информации. Было утверждено множество подзаконных актов, направленных на уменьшение зависимости российского цифрового пространства от зарубежных партнеров.

В ближайшее время планируется ввести целый ряд запретов на применение иностранного ПО в программных аппаратных комплексах, закупаемых по № 44-ФЗ, № 223-ФЗ, и отдельно – на использование иностранного ПО на значимых объектах критической информационной инфраструктуры. К таким программам относятся межсетевые экраны, системы обнаружения и предотвращения вторжений, системы мониторинга сетей и др.

***

Подводя итог, еще раз подчеркнем, что производителям не стоит ждать, что государство решит все их проблемы. Российским компаниям необходимо участвовать в обсуждениях, отстаивать свои права, объединяться и активно продвигать свою продукцию. ■

В России будут разработаны стандарты в области ИИ в здравоохранении

В 2020 г. в России будут разработаны первые редакции национальных стандартов в области искусственного интеллекта в здравоохранении. Координировать разработку будет Технический комитет по стандартизации «Искусственный интеллект» (ТК 164), созданный на базе РВК.

В соответствии с перспективным планом работы Технического комитета до 2027 г. планируется разработать около 50 стандартов в области искусственного интеллекта в здравоохранении по отдельным направлениям, включая общие требования и классификацию систем ИИ в клинической медицине, лучевую и функциональную диагностику, системы дистанционного мониторинга, гистологию, системы поддержки принятия врачебных решений, реконструкцию изображений в диагностике и лечении, большие данные в здравоохранении, медицинские системы аналитики и прогнозирования, образовательные программы в здравоохранении.

Редакции первых шести национальных стандартов будут подготовлены уже в 2020 г., среди них:

- Системы искусственного интеллекта в клинической медицине. Часть 1. Клинические испытания;
- Системы искусственного интеллекта в клинической медицине. Часть 2. Программа и методика технических испытаний;
- Системы искусственного интеллекта в клинической медицине. Часть 3. Применение менеджмента качества к дообучаемым программам. Протокол изменения алгоритма;
- Системы искусственного интеллекта в клинической медицине. Часть 4. Оценка и контроль эксплуатационных параметров дообучаемых алгоритмов;
- Системы искусственного интеллекта в клинической медицине. Часть 5. Требования к структуре и порядку применения набора данных для обучения и тестирования алгоритмов;
- Системы искусственного интеллекта в клинической медицине. Часть 6. Общие требования к эксплуатации.

В целях координации работ по унификации и стандартизации требований к системам ИИ в здравоохранении, а также установки сертификационных требований к медицинским изделиям приказом Росстандарта в составе ТК 164 создан подкомитет «Искусственный интеллект в здравоохранении» (ПК01/ТК164). Подкомитет образован на базе Центра диагностики и телемедицины. Его возглавил главный внештатный специалист по инструментальной и лучевой диагностике Департамента здравоохранения Москвы и Минздрава России по ЦФО, директор Центра диагностики и телемедицины, д. м. н., профессор Сергей Морозов.

Технический комитет «Искусственный интеллект» создан в 2019 г. по инициативе РВК при поддержке Минпромторга РФ и Росстандарта. Работы по стандартизации в области ИИ в ключевых отраслях экономики будут проводиться ТК 164 в соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 г. Она предусматривает создание единых систем стандартизации и оценки соответствия технологических решений, разработанных на основе искусственного интеллекта, развитие международного сотрудничества по вопросам стандартизации и обеспечение возможности сертификации продукции, созданной на основе ИИ.

https://www.rvc.ru/

Infinidat перешагнул рубеж в шесть эксабайт общего объема хранения

Infinidat, поставщик мультипетабайтных решений для хранения данных, объявляет о преодолении отметки в шесть эксабайт поставленной емкости по всему миру. Переход от пяти эксабайт к шести менее чем за полгода отражает быстрый рост рынка больших СХД с высокой доступностью и успех Infinidat в предоставлении критически важных решений высокого качества.

Общий объем поставленной емкости Infinidat больше, чем суммарно у восьми ведущих производителей флеш-массивов в 2019 г. Infinidat поставил более одного эксабайта менее чем за шесть месяцев – это означает рост быстрее на 50%, чем девять месяцев назад. Ожидается, что сохраняющийся спрос на системы петабайтного масштаба ускорит рост количества клиентов и внедрения СХД Infinidat.

Системы хранения InfiniBox были разработаны для удовлетворения потребностей заказчиков, поскольку объем данных, которые пользователи производят и хранят, продолжает расти с двузначной скоростью. Клиенты из разных отраслей, как небольшие, так и крупные, уменьшили эксплуатационные расходы и повысили производительность персонала, консолидировав большое количество массивов хранения в InfiniBox.

https://infinidat.com/ru

Безопасное обслуживание
технологического оборудования

Максим КОНОНЕНКО,
начальник отдела технических решений защиты информации ДИБ АМТ-ГРУП

Функционирование промышленного предприятия сегодня трудно представить без автоматизированной системы управления производственными и технологическими процессами (АСУ ТП). Обеспечение защиты информации, обрабатываемой в АСУ ТП, предупреждение умышленного или неумышленного вмешательства в штатную и запланированную ее работу, исключение несанкционированного доступа к конфиденциальной информации становятся необходимой частью любого технологического процесса.

Техпроцесс безопасности

Повышение уровня автоматизации промышленных предприятий средствами современных информационных, телекоммуникационных и технологических систем, усложнение АСУ ТП, а также переход к необслуживаемым объектам и удаленному управлению по-новому ставят задачу надежного и безопасного функционирования объектов с точки зрения обеспечения информационной безопасности внедряемых информационных технологий.

Одной из главных проблем обеспечения защиты технологического оборудования является организация его безопасного обслуживания. В большей или меньшей степени функционирование производственных линий требует подключения оператора для администрирования оборудования и программного обеспечения. Некоторые категории пользователей системы – разработчики, подрядчики, производители оборудования – также часто прибегают к удаленному подключению для решения стоящих перед ними задач.

Безопасность в промышленных сетях означает в основном поддержание работоспособности всех компонентов АСУ ТП, поэтому три базовые цели, на достижение которых изначально была направлена информационная безопасность, – конфиденциальность, целостность и доступность – хотя и остаются прежними, но в контексте систем промышленной автоматики и контроля приоритетность их меняется. В рамках определенных требований к эксплуатации отдельных компонентов и АСУ ТП в целом значение доступности самой по себе или в сочетании с целостностью перевешивает значение конфиденциальности.

Защита технологического сегмента

Материалом для настоящей статьи послужил реализованный проект по разработке и внедрению системы информационной безопасности для крупного территориально распределенного промышленного предприятия, производственный процесс которого управляется более чем сотней АСУ ТП. При проектировании системы информационной безопасности были учтены требования действующих редакций приказов ФСТЭК России № 31 от 14.03.2014 г., № 235 от 21.12.2017 г. и № 239 от 25.12.2017 г.

Первым этапом построения защиты любой АСУ является ее исследование, в ходе которого выявляются наиболее распространенные проблемы защиты:

- использование слабых паролей;
- незакрытые возможности удаленного подключения;
- некорректные настройки оборудования;
- возможность бесконтрольного подключения в промышленную сеть из корпоративной сети.

Промышленная сеть на крупном предприятии традиционно реализована как распределенная по функциям система, которая взаимодействует через компьютерную сеть, построенную на коммутаторах. Для организации быстрого обмена коммутаторы работают на уровне L2 модели Open System Inter

connection (OSI) и оперируют MAC-адресами, т. е. анализировать трафик и тем более его блокировать по определенным правилам они не в состоянии. В промышленной сети широко распространены SCADA-серверы, программируемые логические контроллеры, датчики и исполнительные механизмы, осуществляющие мониторинг, контроль и управление технологическим оборудованием. В силу разнообразия технических средств для обеспечения безопасности промышленной сети необходимо контролировать трафик сразу на нескольких уровнях модели OSI.

При выработке решения проблем промышленного заказчика нужно учитывать и требования по обеспечению непрерывности технологических процессов, а также финансовые и технические возможности заказчика.

Сегментация

Ключевая задача большинства проектов по обеспечению информационной безопасности АСУ ТП заключается в отделении промышленной сети от корпоративной, причем последняя имеет и подключение к Интернету. При решении данной задачи основными инструментами обеспечения информационной безопасности являются:

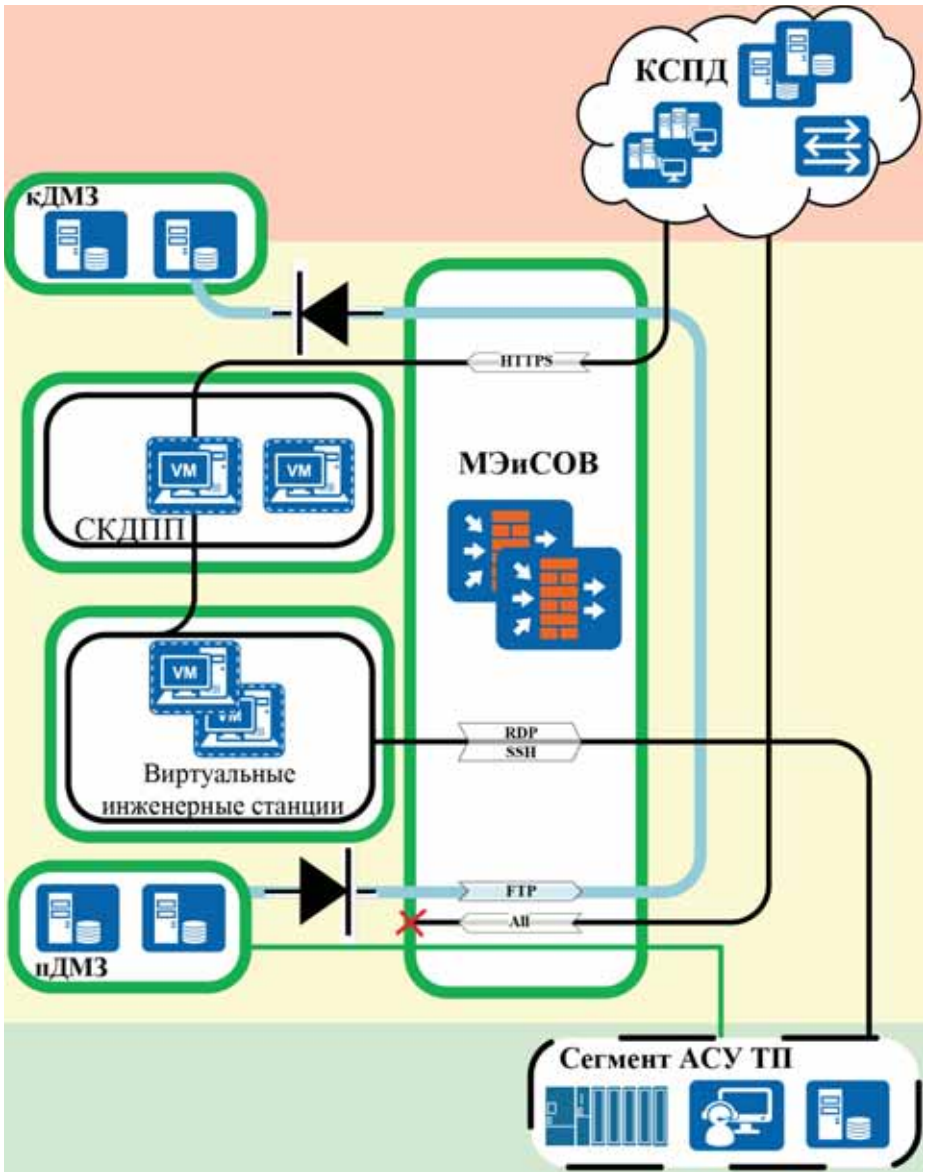
- межсетевые экраны (МЭ);
- системы обнаружения вторжений (СОВ);
- однонаправленные шлюзы;
- системы контроля действий привилегированных пользователей (СКДПП);
- регистрация событий безопасности.

Предложенную схему организации системы информационной безопасности иллюстрирует рисунок.

Межсетевой экран

Межсетевой экран служит для отделения промышленной сети не только от корпоративной, но и от внешних сетей. Этот инструмент позволяет, в частности, компенсировать такой недостаток промышленного оборудования, как использование в нем устаревших версий операционных систем и иного программного обеспечения, которое невозможно обновить без нарушения какого-либо технологического процесса. Межсетевой экран не позволяет обращаться к такому оборудованию напрямую из корпоративной сети, доступ разрешен только через специально контролируемые инженерные рабочие станци.

Для этого доступ из корпоративной сети в промышленную сеть организован через специальный сегмент в виде демилитаризованной зоны (ДМЗ) согласно рекомендациям стандарта NIST 800-82. Демилитаризованная зона организуется по принципу ограничения прямого взаимодействия корпоративной и технологической сетей, при этом создаются две ДМЗ: промышленная ДМЗ (пДМЗ) для сбора и обработки информации с компонентов АСУ ТП и корпоративная ДМЗ (кДМЗ), куда передаются сводные данные мониторинга технологического оборудования из пДМЗ, доступные пользователям, находящимся в корпоративной сети.



Система обнаружения вторжений

Система обнаружения вторжений (СОВ) обеспечивает анализ команд, проходящих через периметр промышленной сети, а также предотвращает нарушения в функционировании технологических процессов из-за специфических угроз информационной безопасности путем инспектирования трафика на предмет наличия в нем признаков вредоносной активности на различных уровнях модели OSI.

гарантирует отсутствие обратной связи. Прокси-серверы обеспечивают связь с внешними системами в сегментах пДМЗ и кДМЗ и организуют однонаправленный транспорт данных между собой. На принимающей стороне в сегменте пДМЗ прокси-сервер выступает в роли сервера данных (используется получение данных по протоколу FTP), на передающей стороне прокси-сервер выступает в роли клиента.

Обеспечивая однонаправленную выгрузку копии трафика

Большинство проектов по обеспечению информационной безопасности АСУ ТП заключаются в отделении промышленной сети от корпоративной.

Однонаправленный шлюз

Дополнительно для передачи информации из пДМЗ на серверы в кДМЗ устанавливается однонаправленный шлюз (диод). Он позволяет передавать информацию с помощью протоколов прикладного уровня в одном направлении и, как правило, представляет собой аппаратно-программный комплекс, который обеспечивает организацию каналов однонаправленной передачи данных на физическом уровне и безопасную выгрузку данных из критических систем, в этом случае из промышленной в корпоративную сеть, посредством управления межсетевыми потоками.

Для решения такой задачи диод разворачивается в виде следующей схемы: два прокси-сервера и аппаратное устройство однонаправленной передачи данных. Передача трафика через диод возможна только в одном направлении, так как гальваническая развязка как АСУ ТП, так и отдельных подсистем безопасности, диод дает возможность операторам и администраторам контролировать события, происходящие в промышленной сети, находясь в корпоративной сети, и гарантированно исключает возможность любого негативного информационного воздействия из корпоративной сети.

СКДПП

Управление производственным оборудованием и технологическим процессом, администрирование и обеспечение средств информационной безопасности в промышленной сети осуществляются в соответствии с принятым регламентом исключительно персоналом этой сети с АРМ операторов АСУ ТП. Для предотвращения нарушения работоспособности АСУ ТП и утечки конфиденциальной информации существует необходимость контроля действий пользователей, обладающих, по сути, неограниченными правами. Дополнительным средством обеспечения безопасности АСУ ТП является использование СКДПП. Под привилегированными пользователями в данном случае подразумеваются лица, которым разрешено использовать автоматизированную систему вопреки общей политике безопасности и которые могут получить доступ к защищаемой информации без явного разрешения владельца активов. К привилегированным пользователям относятся, например, инженеры отдела эксплуатации АСУ ТП. Привилегированный пользователь может быть как законным пользователем (принадлежать к персоналу предприятия), так и посторонним лицом, похитившим чужую учетную запись и пытающимся непосредственно или с помощью имеющихся у него технических и программных средств получить доступ к информационным ресурсам и инфраструктуре сети предприятия. При этом доступ непривилегированных пользователей из корпоративной сети в промышленную необходимо закрыть. Многие СКДПП не могут противостоять попыткам привилегированного пользователя нанести ущерб АСУТП и информационным ресурсам. Главная задача такого типа систем заключается в фиксации действий злоумышленников, которая может быть использована и как доказательная база при расследовании инцидентов.

СКДПП обеспечивает единую точку входа, управляет аутентификацией и авторизацией привилегированных учетных записей, протоколирует действия таких пользователей в системе для последующего контроля и анализа. Решение по СКДПП может быть реализовано в виде программного средства в системе виртуализации. Для доступа в промышленную сеть используются виртуальные

инженерные станции. Система фиксирует в специальном журнале трафик сессий, не внося изменений в саму сессию, записывает видеопоток для графических сеансов, клавиатурный ввод пользователя, запущенные фоновые процессы, окна. При необходимости имеется возможность просмотра журнала событий, восстановления и анализа действий привилегированных пользователей.

Регистрация событий безопасности

Упомянутые средства защиты, конечно же, не являются достаточными для создания полноценной системы информационной безопасности АСУ ТП, поскольку есть еще средства идентификации, аутентификации и управления доступом, анализа защищенности, криптографической защиты каналов связи, антивирусной защиты и многие другие. Они, а также описанные выше средства защиты были интегрированы в систему регистрации событий безопасности (SIEM).

Организация защиты

Решение задачи безопасного обслуживания АСУ ТП было бы неполным без внедрения комплекса организационных мер, включающих разработку комплекта политик, инструкций и регламентов, должностных обязанностей, консультирование и обучение персонала и иных мер. Необходимо учитывать, что первоочередным фактором в обеспечении безопасности всегда являются внимательность и ответственное поведение персонала предприятия.

Непосредственное внедрение системы информационной безопасности на предприятии проводится поэтапно на основании согласованного с производственными отделами плана, разработанного в целях безопасного обслуживания непрерывных технологических процессов. При этом учитываются результаты испытаний как отдельных средств и подсистем, так и системы защиты в целом. В рамках испытаний выполняется проверка полноты и качества реализации системой информационной безопасности своих функций в различных условиях функционирования – для этого существуют и требования регуляторов к системе обеспечения защиты, и лучшие мировые практики.

Важной задачей внедрения средств защиты на крупном предприятии является обеспечение масштабирования предложенного решения. Обычно на пилотном внедрении все работает отлично, а при массовой защите большого количества АСУ ТП возникают нюансы. Один из вариантов масштабирования - создание дополнительных сегментов для новых АСУ ТП на МЭ и контроль межсетевого взаимодействия между ними. Сегмент может быть создан один для всей АСУ ТП, но более правильным вариантом и в тоже время более сложным является подход когда мы уменьшаем площадь атаки при проникновениях в сеть путем создания отдельных сегментов для программируемых логических контроллеров (ПЛК), для АРМ операторов и для SCADA-серверов.

Заключение

Специфика системы информационной безопасности АСУ ТП требует от исполнителей на этапе разработки глубокого понимания технологических процессов, знания систем автоматизации и промышленного оборудования, на этапе внедрения – минимального влияния на производство и максимального использования встроенных механизмов защиты. Процедуры обслуживания АСУ ТП, в том числе внедрения систем защиты, сами по себе представляют значительную опасность, поскольку требуют согласованного изменения состояния многих элементов технологического оборудования и зависят от безупречного выполнения определенных последовательностей автоматических операций, а также согласованных действий технологического персонала и специалистов по информационной безопасности.

Создание систем защиты информации – сложная и ответственная задача. Предложенные в статье подходы к созданию системы информационной безопасности, обеспечивающей выполнение основных производственных и технологических процессов, позволяют повысить эффективность защиты ядра производственной системы, обеспечив через комплекс технических и программных средств, а также организационных мер непрерывность работы в круглосуточном режиме производственной АСУ ТП. ■

Сегментация сети – один из важнейших инструментов защиты информации, который позволяет уменьшить площадь атаки при проникновениях в сеть.

Цифровая интеграция устройств печати:

от управления офисной инфраструктурой к управлению рабочей средой

Валерий КУЗЬМИЧ,
руководитель отдела маркетинга и стратегических программ департамента аутсорсинга документоемких процессов, компания Xerox Евразия

По мере развития мобильных и облачных технологий изменяются методы работы и трансформируется понятие рабочего места. По оценкам Quocirca, к 2025 г. более половины офисных работников станут мобильными. Этот тренд совпадает с интересами работодателей. Стремясь к большей гибкости, они сокращают офисные площади и расходы на ИТ. Компании формируют экосистему для удаленной работы географически распределенных и мобильных сотрудников, которым требуются постоянный доступ к информации, возможности обмена ею и обработки в любом месте с любого устройства. Ускорение бизнес-процессов зависит от того, насколько успешно решаются задачи перевода работы с документами в цифровое пространство.

Происходящие изменения определяют и вектор развития офисных устройств. Термин «многофункциональные устройства» (МФУ) до недавнего времени указывал на способность устройств не только наносить изображение на бумагу, но и выполнять ряд других функций по работе с документами: сканировать, отправлять по электронной почте или факсу.

Сегодня платформа офисного устройства по аналогии со смартфонами позволяет создавать и устанавливать приложения, функциональность которых ограничена только воображением. По сути, данное устройство становится офисным терминалом или своего рода бизнес-ассистентом, который расширяет спектр операций с документами. Благодаря такому терминалу можно находить документы в сети или в облаке, вводить бумажные версии и извлекать из них значимую информацию, переводить на другие языки, отправлять по списку адресатов, задавать последовательность их обработки в рамках того или иного рабочего процесса. С помощью приложений можно получить справочную информацию о состоянии устройства, расписании рейсов и погоде или, например, заказать пиццу. Наряду с этим бизнес-ассистенты сохранили полезную функцию печати.

Современные офисные устройства, наделенные дополнительными возможностям, становятся важным элементом цифровой экосистемы компании, интегрированным в бизнес-процессы.

Трансформация услуг по управлению печатной инфраструктурой

Изменения рабочей среды и развитие офисных технологий оказывают влияние на наполнение услуг, которые до недавнего времени были сконцентрированы на управлении печатными процессами и офисной техникой. Задачи, связанные с оптимизацией парка, снижением издержек, управлением печатными процессами, остаются приоритетными для компаний. Вместе с тем более глубокая интеграция устройств в рабочие процессы, подключение к сети и обеспечение их доступности для удаленных и мобильных сотрудников диктуют новые требования к услуге и расширяют ее границы в таких направлениях, как безопасность, аналитика, цифровизация и облачные технологии. При реализации комплексного подхода объектами услуги становятся не только печатные устройства и процессы, но и рабочая среда, что подразумевает создание оптимальной инфраструктуры и эффективных рабочих мест, повышение производительности труда сотрудников, надежную защиту документов, устройств и данных.

Безопасность

По данным исследования Quocirca Global Print Security, опубликованного в феврале 2019 г., 73% компаний обеспокоены угрозами безопасности в сфере документооборота. При этом лишь 24% участников опроса уверены в том, что их инфраструктура надежно защищена.

Комплексный подход сервис-провайдера к безопасности рабочей среды направлен на обеспечение защиты устройств, документов и данных. Безопасность устройств реализуется с помощью встроенных решений (например, McAfee и Cisco), которые используют механизмы предотвращения, выявления и отражения киберугроз.

Человеческий фактор по-прежнему – одна из главных причин утечек данных. Большую роль в корпоративной безопасности играет ограничение доступа к данным и документам, в том числе отправляемым на печать. Услуги по управлению рабочей средой могут включать в себя разработку и внедрение политик и процедур в области безопасности, внедрение решений по ограничению прав доступа к документам, позволяющих контролировать содержание распространяемых и печатаемых документов, реализующих технологию pull-printing, которая защищает от несанкционированного доступа к документам, отправленным на печать.

Аналитика

Эффективность решений, принимаемых при проектировании рабочей среды, внедрении тех или иных технологий, существенно повышается, если они основаны на результатах анализа объективных данных, которые могут быть получены по результатам аудита, выполненного на уровне устройств, пользователей, документов и рабочих процессов. На основе такой информации разрабатываются программы оптимизации, которые помогают сделать рабочую среду более эффективной и контролируемой, дают возможность принимать оптимальные решения и достигать целевых бизнес-показателей.

Например, анализ жизненного цикла документа позволяет выявить неэффективные процессы и предложить их цифровые альтернативы, в том числе реализуемые с помощью приложений. По результатам мониторинга и анализа печатных работ пользователей можно разрабатывать как индивидуальные рекомендации, так и инициативы на уровне компании по формированию ответственного отношения к печати. Например, решение Xerox Print Awareness Tool конвертирует информацию об объемах печати в аналитику, отражающую уровень потребления электроэнергии, данные о выбросах углекислого газа в атмосферу, количестве деревьев, необходимых для производства использованной бумаги. Применение такого инструмента позволяет внедрять программы в области устойчивого развития, создавать позитивную мотивацию у сотрудников для сокращения необязательных отпечатков.

Цифровизация

Еще одно фокусное направление в рамках услуг по управлению рабочей средой – оптимизация и автоматизация трудоемких процессов. Что это значит на практике? Известно, что бумажный документ – самый «медленный» носитель информации. Ускорить процессы ее ввода и обработки можно, если перевести документ в цифровой вид на раннем этапе. Офисный бизнес-ассистент с установленным специализированным приложением позволяет эффективно организовать сканирование документов, категорировать, выполнить первичную обработку (извлечь значимые данные или присвоить атрибуты) и маршрутизировать для последующих операций в рамках соответствующего процесса. Разработка таких приложений и процессов тоже может быть частью услуги.

Благодаря цифровизации в рамках аутсорсинга американская компания Morrell Group ускорила комплектацию и отправку продуктов, добилась 25%-ного снижения издержек и исключила ошибки при отгрузке. Это стало возможным в результате применения печатных устройств с интеллектуальными функциями и специально разработанного приложения, которое переводит обработку документов в цифровой формат.

Облачные технологии

Чтобы лучше учитывать потребности распределенных и мобильных сотрудников, сервис-провайдер может сформировать масштабируемую ИТ-инфраструктуру на основе облачных платформ и инструментов. Такой подход позволяет оптимизировать ресурсы и упростить работу ИТ-специалистам.

Удобный персонализированный доступ в любое время из любого места повышает производительность труда.

При этом автоматизацию бизнес-процессов ускоряет интеграция бумажного и цифрового документооборота на всех этапах: от создания контента до его преобразования и хранения. В частности, благодаря переходу на аутсорсинг с применением облачных технологий британское фермерское хозяйство The Tomato Stall сократило время планирования и свело к минимуму количество ручных операций. Для этого компания стала использовать сервис планирования маршрутов, который автоматически формирует маршрутные листы, экономя рабочее время логистов.

***

Задачи, которые можно ставить перед сервис-провайдером, не ограничиваются уменьшением затрат на печать. Заказчики могут рассчитывать на комплекс услуг по проектированию и поддержанию интеллектуальной рабочей среды, обеспечивающей максимальную эффективность рабочих мест, повышение производительности и безопасность. Одно из основных преимуществ такой среды – способность быстро адаптироваться к меняющимся потребностям бизнеса и сотрудников. ■

The world of information technology
Connect. WIT
мир информационных технологий
январь–февраль 2020

ПОДПИСКА 2020

ГАРАНТИЯ СВОЕВРЕМЕННОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ

Внимание!

Редакционную подписку на журнал Connect вы можете оформить в редакции

Общество с ограниченной ответственностью «ИД КОННЕКТ»
ООО «ИД КОННЕКТ»
Тел.: (495) 925-1118

Платежные реквизиты получателя:
р/сч № 40702810900000030157
БИК 044525555
к/сч № 30101810400000000555
ПАО «Промсвязьбанк» г. Москва

Через сайт в Интернете: http//www.connect-wit.ru

Стоимость редакционной подписки (для жителей РФ)

Издание, периодичность		Стоимость подписки, руб.	
		экземпляр	на год
Connect. Мир информационных технологий 8 номеров в год	Российский авторитетный бизнес-журнал. Мониторинг и экспертиза возможностей информационных технологий и телекоммуникаций для оптимизации бизнеса. Информатизация и связь в отраслях, ведомствах и регионах России и СНГ.	**250***	**2000***

* Не включает доставку.
Читателям, живущим за пределами РФ, необходимо отправить в редакцию заявку в простой письменной форме на e-mail: secretar@connect.ru
(в этом случае к стоимости журнала будет добавлена сумма почтовых расходов).

Подписка в альтернативных агентствах

ООО «УП Урал-Пресс», г. Москва (499)700-05-07 (доб. 3028)

Выбрать наиболее удобное для вас агентство можно также на сайте **www.connect-wit.ru** (раздел подписки) или по телефону: (495) 925-1118

Рекламодатели номера

ГП КС ..... 2-я обл.
Информзащита ..... 1-я обл., 4—8
Ростелеком-Солар ..... 11—12
ЭЛВИС-ПЛЮС ..... 13—16

Редакция журнала «Connect. Мир информационных технологий»

Редакционный отдел
editor@connect-wit.ru
(495) 925-1118

Выпускающий редактор
Валерия Назарова
vnazarova@connect-wit.ru

Журналисты-обозреватели
Валерий Коржов
korzhov@connect-wit.ru
Дмитрий Шульгин
shulgin@connect-wit.ru

Литературный редактор
Елена Шевелева

ИЗДАТЕЛЬ ООО «ИД КОННЕКТ»

Генеральный директор
Евгений Самохвалов
evs@connect-wit.ru
(495) 925-1118

Заместитель генерального директора
Дмитрий Корешков
dima_k@connect-wit.ru

Директор по региональным проектам
Инга Орлова
regions@connect-wit.ru
(903) 742-54-71

Отдел рекламы
(495) 925-1118

Макетирование и верстка
Алексей Григорьев

Цветокоррекция
Александра Шанина

Фото на обложке
Алексей Шанин

Тел.: (495) 925-1118 (многоканальный),
факс: (495) 925-1118
E-mail: editor@connect-wit.ru
http://www.connect-wit.ru

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), регистрационнай номер ПИ № ФС77-54349

Учредитель: ООО «Коннект-ИКТ»

Адрес редакции: 129626, Москва, 3-я Мытищинская ул., д. 3, стр.1

Тел.: (495) 925-1118 (многоканальный)
Факс: (495) 925-1118

E-mail: editor@connect-wit.ru
http://www.connect-wit.ru

Отпечатано ООО «Полиграфический комплекс «Союзпечать»
Тираж 15 000
Цена свободная

При использовании материалов ссылка на журнал обязательна.
Ответственность за рекламные материалы несет рекламодатель.

Мнения авторов и компаний могут не совпадать с мнением редакции.

© «Connect. Мир информационных технологий»

Читайте в мартовском номере

Тема номера

Ломать или строить?
О стратегии цифровой трансформации в отраслях

Цифровая трансформация как требование времени или как новые риски для компании?

Готовность отечественных предприятий к трансформации. Что трансформируем, или уровень зрелости компании

Цели и задачи трансформации в ГОСах. Что хочет государство. Что может государство

Трансформация в крупнейших корпорациях России. Общие черты в постановке целей и задач