DOI: 10.25728/avtprom.2021.07.03

Кибериммунный подход к защите промышленного IoT

М.Р. Нуриев («Лаборатория Касперского»)

Сформулированы проблемы в области кибербезопасности, характерные для устройств промышленного Internet вещей. Рассмотрены аппаратно-программные решения, разработанные «Лабораторией Касперского» для обеспечения информационной безопасности технологии промышленного Internet вещей.

Ключевые слова: кибербезопасность, промышленный Internet вещей, кибериммунный шлюз, кибериммунитет.

Ключевой элемент Industry 4.0 — это технология промышленного Internet вещей (Industrial Internet of Things, IIoT) [1,2]. Масштабное внедрение этой технологии создает новые возможности для развития производства и решает ряд важнейших задач: рост производительности оборудования, снижение материальных и энергетических затрат, повышение качества, рентабельности производства и конкурентоспособности. Согласно отчету MarketResearch, к 2028 г. мировой рынок промышленного IoT достигнет 1119,4 млрд долл. США со среднегодовым темпом роста в 17% на промежутке 2021-2028 гг.

Удешевление датчиков, распространение беспроводных технологий и рост вычислительных мощностей способствует массовому внедрению Internet вещей в производство. Это позволяет собирать больше данных о производственных процессах и активах и производить их непрерывный мониторинг для использования в системах класса ERP и MES. Большие данные могут использоваться для создания цифровых двойников и прогностической аналитики. Эти технологии позволяют эффективнее управлять запасами, уточнять сроки плановых ремонтов и замены оборудования, анализировать рыночные цены на сырье и комплектующие.

Сенсоры в составе технологии Industrial Internet of Things не могут напрямую подключаться к IT-инфраструктуре. Часто они ограничены небольшими размерами, удаленным расположением или требованиями энергоэффективности. Эту проблему решают шлюзы. Они выполняют сразу несколько задач: сбор данных с датчиков, конвертация данных для их передачи по сотовым сетям и Ethernet, передача управляющих команд, обнаружение и классификация подключенных устройств, а также обеспечение кибербезопасности.

Проблемы безопасности IoT

Одна из главных проблем Internet вещей — уязвимость к кибератакам. Это среда, в которой работают самые разные устройства, и уровень информационной безопасности у них тоже разный. Вот самые распространенные проблемы, ведущие к слабой защищенности IIoT:

- при разработке устройств не учитываются требования кибербезопасности;
- устаревшее ПО и недостаточное внимание к программным обновлениям;
- передача данных без шифрования;
- стандартные настройки безопасности;
- незащищенные интерфейсы;

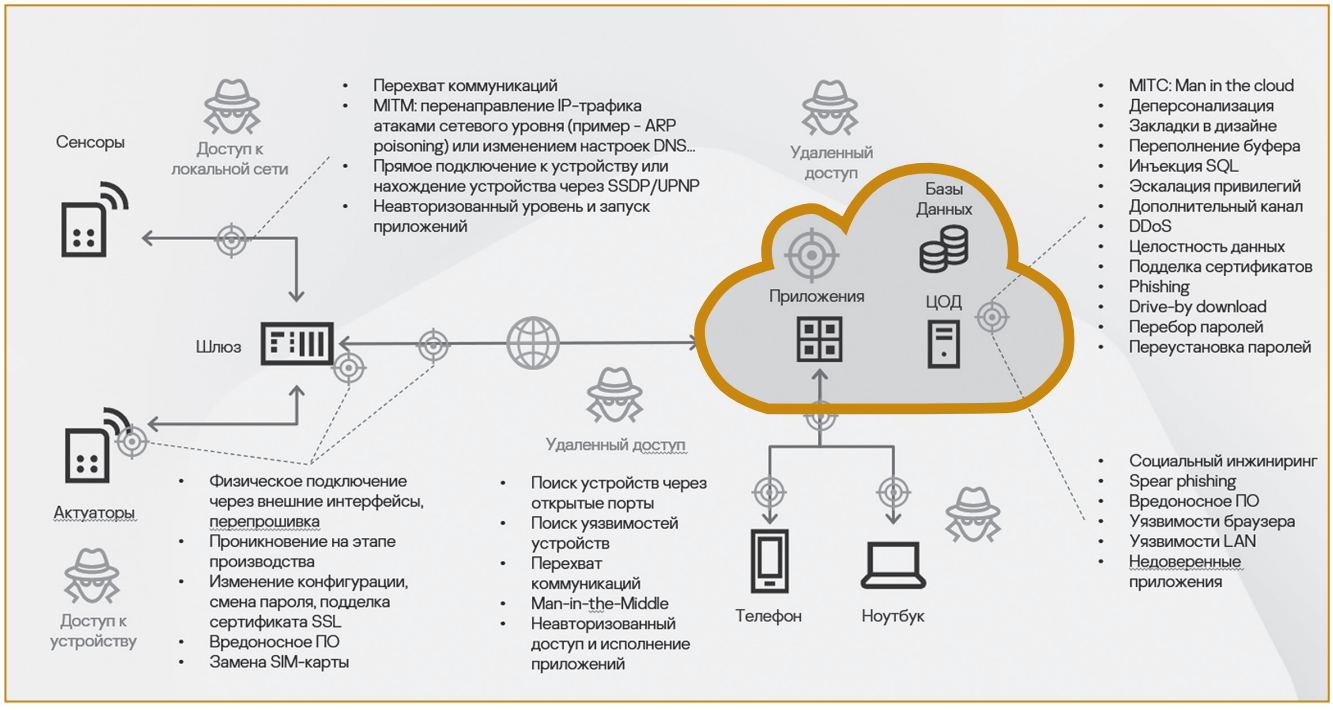

Рис. 1. Потенциальные направления атак на инфраструктуру IoT

• недостаточная защита облачной инфраструктуры;
• уязвимости в ОС общего назначения;
• невозможность оснастить многие IoT-устройства наложенными средствами безопасности.

Часто уязвимости в IIoT-инфраструктуре позволяют хакерам проникнуть в информационную сеть предприятия. Это может привести к утечке чувствительных данных и финансовым потерям. Последствия атак на Internet вещей могут быть гораздо шире, поскольку информационные системы становятся киберфизическими, то есть имеющими выход в реальный мир. Злоумышленник может получить контроль над системами, управляющими реальными объектами — насосами, реле, двигателями и т.д. В лучшем случае последствием станет снижение производительности, а в худшем — авария на производстве.

Специалисты «Лаборатории Касперского» проанализировали основные векторы атак на инфраструктуру Internet вещей (рис. 1). Для защиты уровней облака и управления IoT уже существуют традиционные решения. Это такие продукты, как Kaspersky Security для виртуальных и облачных сред, Kaspersky Security Center, Kaspersky DDoS Prevention и подобные решения от других производителей. Уровнем ниже находятся шлюзы, каналы передачи данных и само IIoT-оборудование. Для обеспечения защиты от перехвата трафика на этом уровне техниками типа MITM[1], атак на устройства, к которым организован доступ снаружи, и от несанкционированных новых подключений требуются специализированные решения.

Рис. 2. KISG 100 — первый кибериммунный IoT-шлюз

Рис. 3. Шлюз KISG 1000

Платформа кибербезопасности для Industrial Internet of Things

Для решения проблем безопасности IoT в «Лаборатории Касперского» создано решение Kaspersky IoT Infrastructure Security. В него входят исходно безопасные шлюзы Kaspersky IoT Secure Gateway 100 (KISG 100) и Kaspersky IoT Secure Gateway 1000 (KISG 1000), а также Kaspersky Security Center, программная платформа для централизованного мониторинга и администрирования KISG 1000. Оба шлюза работают под управлением специа-лизированной операционной системы KasperskyOS. Расскажем подробнее о составляющих решения и о том, что обеспечивает их безопасность.

KISG 100 — это первый кибериммунный[2] шлюз, вышедший на рынок и предназначенный для Industrial Internet of Things (рис. 2). Он разработан совместно с дочерним предприятием «Лаборатории Касперского» — Апротех. Шлюз собирает большой объем ранее недоступной информации, генерируемой IIoT-устройствами, что позволяет использовать ее для машинного обучения, предиктивного анализа и создания цифровых двойников. KISG 100 не позволяет получить доступ к оборудованию извне, поскольку выступает в роли дата-диода, пропуская данные только в одном направлении. Сам шлюз защищен от кибератак по умолчанию благодаря технологиям KasperskyOS. Устройство построено на аппаратной платформе Siemens SIMATIC IOT2040. За счет использования распространенного протокола OPC UA шлюз подходит для развертывания в инфраструктуре с самым разнообразным оборудованием от различных производителей. Для обработки и анализа информация передается в облачную IIoT-платформу Siemens MindSphere.

В конце 2020 г. Kaspersky IoT Secure Gateway 100 стал лауреатом премии World Leading Internet Scientific and Technological Achievements 2020. Об этом объявили на одном из самых масштабных мероприятий в мировой IT-индустрии — 7-й Всемирной

[1] Атака посредника или атака «человек посередине» (Man in the middle (MITM)) — вид атаки в криптографии и компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом. Является методом компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.

[2] Кибериммунитет — новый подход к разработке безопасных IT-решений на базе KasperskyOS. Такие решения защищены от подавляющего числа кибератак (как существующих, так и еще неизвестных) и будут выполнять свои критические функции даже в условиях агрессивной среды.

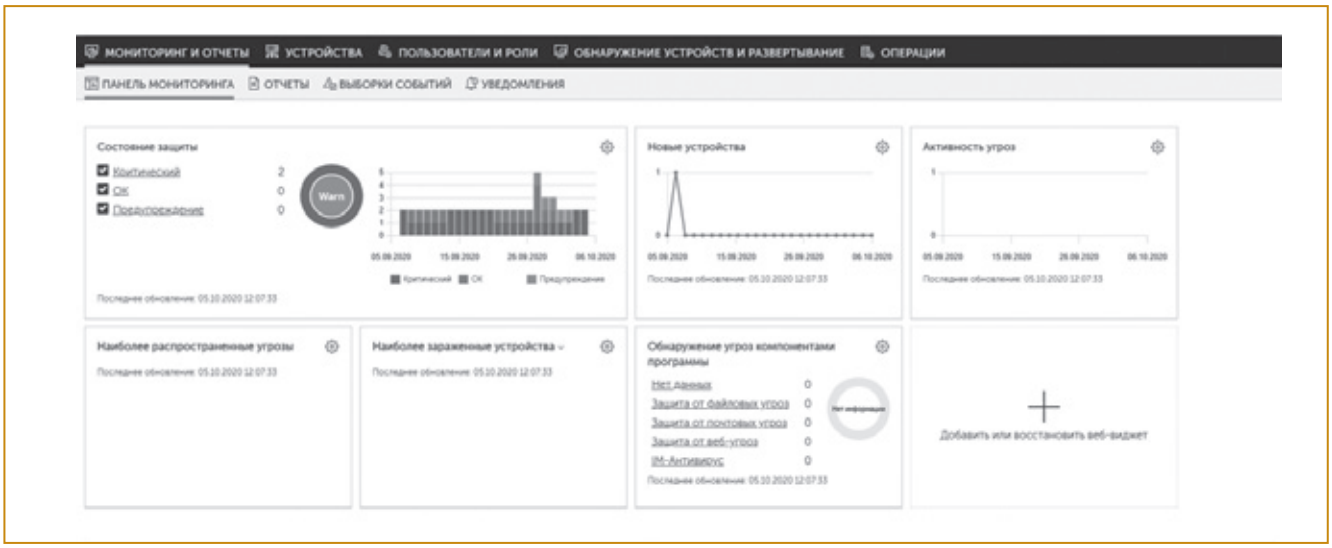

Рис. 4. Для централизованного мониторинга и управления всеми событиями шлюза KISG 1000 используется платформа Kaspersky Security Center

конференции по вопросам Internet в г. Учжэне (Китай). Шлюз был включен в число 15 лучших инновационных разработок 2020 г. в области Internet наравне с продуктами Microsoft, Huawei и Alibaba.

KISG 1000 — шлюз на основе KasperskyOS, обладающий исходной безопасностью и встроенными средствами защиты всей IoT-инфраструктуры (рис. 3). Устройство агрегирует данные, конвертирует их и обеспечивает безопасную передачу данных в частные или публичные облака. KISG 1000 не только собирает, проверяет и распределяет телеметрию, но также передает на устройства управляющие команды, полученные по MQTT[3]. В будущем планируется добавить поддержку других протоколов (Zigbee, LoRa, Modbus, CanBus, PROFINET, CoAP, AMQP, XMPP). Шлюз имеет встроенные функции безопасности: обнаружение и классификация устройств в сети, регистрация событий безопасности в IoT-системах и защита от сетевых атак (IDS/IPS). Централизованное управление и мониторинг всех событий шлюза ведется через платформу Kaspersky Security Center (рис.4).

Шлюз работает на аппаратной платформе Advantech UTX-3117. Благодаря возможности работы с несколькими облачными платформами по протоколу MQTT он может применяться как в промышленности, так и в других отраслях. Сейчас KISG 1000 проходит стадию пилотирования. В частности, он тестируется в проекте общегородской цифровой платформы диспетчеризации коммунальной инфраструктуры в г. Оренбурге.

Шлюзы KISG 100 и KISG 1000 могут работать в составе одной инфраструктуры, дополняя друг друга. Если промышленное оборудование работает на протоколе OPC UA и его надо подключить к облаку, данные собираются с помощью KISG 100. Если есть отдельное требование мониторинга событий безопасности — используется KISG 1000 (рис.5).

Основа защиты — специализированная ОС

Одной из главных проблем безопасности Internet вещей являются уязвимости в системах общего назначения. Согласно исследованиям «Лаборатории Касперского», в 2020 г. девять из десяти взломанных компьютеров, управлявших устройствами Internet вещей, работали под управлением считающейся многими безопасной ОС Linux. В традиционных ОС огромная кодовая база не позволяет вовремя отслеживать уязвимости и затрудняет проектирование защищенных решений. Вторым недостатком является то, что в системах общего назначения все программы работают в едином адресном пространстве и могут влиять друг на друга. Использовав уязвимость в одном приложении, злоумышленник может получить контроль над всей системой. Проектировать максимально защищенные решения на базе таких систем становится очень затратно, а то и просто невозможно.

Ключевой элемент решений для защиты Industrial Internet of Things — специализированная операционная система KasperskyOS. Она была разработана с нуля «Лабораторией Касперского», чтобы обеспечить защиту от любых атак — как существующих, так и еще неизвестных. При создании ОС применялись проверенные и хорошо описанные архитектурные подходы MILS[4] и FLASK[5], а также собственные технологии.

KasperskyOS имеет микроядерную архитектуру. Объем кода ядра составляет несколько десятков тысяч строк (для сравнения — в минимальной сборке Linux порядка 10 млн строк). Компактное ядро не только обеспе-

[3] MQTT (message queuing telemetry transport) — упрощенный сетевой протокол, работающий поверх TCP/IP, ориентированный на обмен сообщениями между устройствами по принципу издатель-подписчик. Протокол получин широкое распространение благодаря взрывному росту IoT.

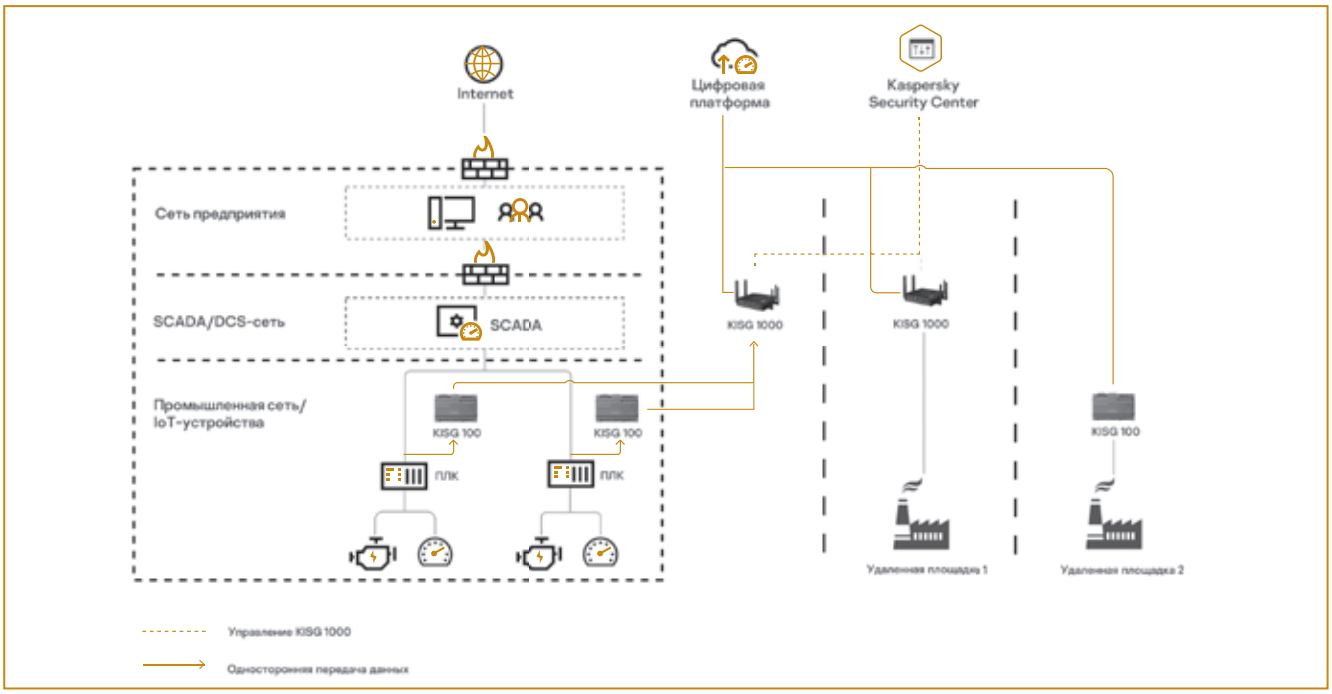

Рис. 5. Схема применения двух шлюзов Kaspersky IoT Secure Gateway в IIoT-инфраструктуре

чивает небольшую поверхность атак, но и позволяет провести максимально полную верификацию кода.

В соответствии с подходом MILS программные компоненты в решениях на базе KasperskyOS находятся в изолированных доменах. Даже если они содержат уязвимости или вредоносный код, система в любом случае остается безопасной.

Система безопасности состоит из двух частей (архитектура FLASK): точка принятия решений по политикам и точка применения политик. Такая схема упрощает анализ системы и влечет за собой непротиворечивость политик безопасности.

Все взаимодействия между изолированными компонентами контролирует подсистема Kaspersky Security System (KSS). Это единственная точка принятия решений безопасности. В отличие от большинства аналогов KSS позволяет гибко использовать одновременно несколько хорошо исследованных моделей безопасности: на базе мандатных ссылок, на базе конечных автоматов, модель ролевого доступа, модели с темпоральной логикой и др. Это позволяет описать практически любое поведение системы.

Немаловажно, что при создании кибериммунных продуктов на базе KasperskyOS необходимо использовать особую методологию разработки. К стандартным шагам проектирования программного продукта добавляется необходимость тщательно определять цели безопасности, верифицировать их достижение, моделировать угрозы и разрабатывать политики безопасности.

Вывод

Один из главных драйверов качественных изменений в промышленности — это Internet вещей. Однако массовому внедрению IoT-технологий препятствуют, в числе прочего, вопросы кибербезопасности. Помочь индустриальной цифровой трансформации могут специализированные решения. Для снижения затрат и максимального уровня защищенности безопасность оптимальнее закладывать в основу таких решений. Сделать это можно с помощью кибериммунной операционной системы и специальной методологии разработки.

Список литературы

1. The Industrial Internet Of Things (IIoT): An analysis framework (англ.) // Computers in Industry. — 2018-10-01. Vol. 101. P. 1–12. ISSN 0166-3615. doi:10.1016/j.compind.2018.04.015.
2. *Скляр В.* Информационная безопасность интернета вещей: кто вещь, а кто хозяин? Хабр. 2018. Ноябрь

Нуриев Марат Радисович —менеджер по развитию бизнеса IoT-решений на базе KasperskyOS.
Https://os.kaspersky.ru

[4] MILS (Multiple Independent Levelsof Security) – архитектура множественных независимых уровней защиты, использующая множество приложений с множественными доступами. Система разбивается на блоки таким образом, что сбой или повреждение одного блока никак не сказывался на других блоках.

[5] Flux Advanced Security Kernel (FLASK) — архитектура безопасности операционной системы, которая обеспечивает гибкую поддержку политик безопасности.