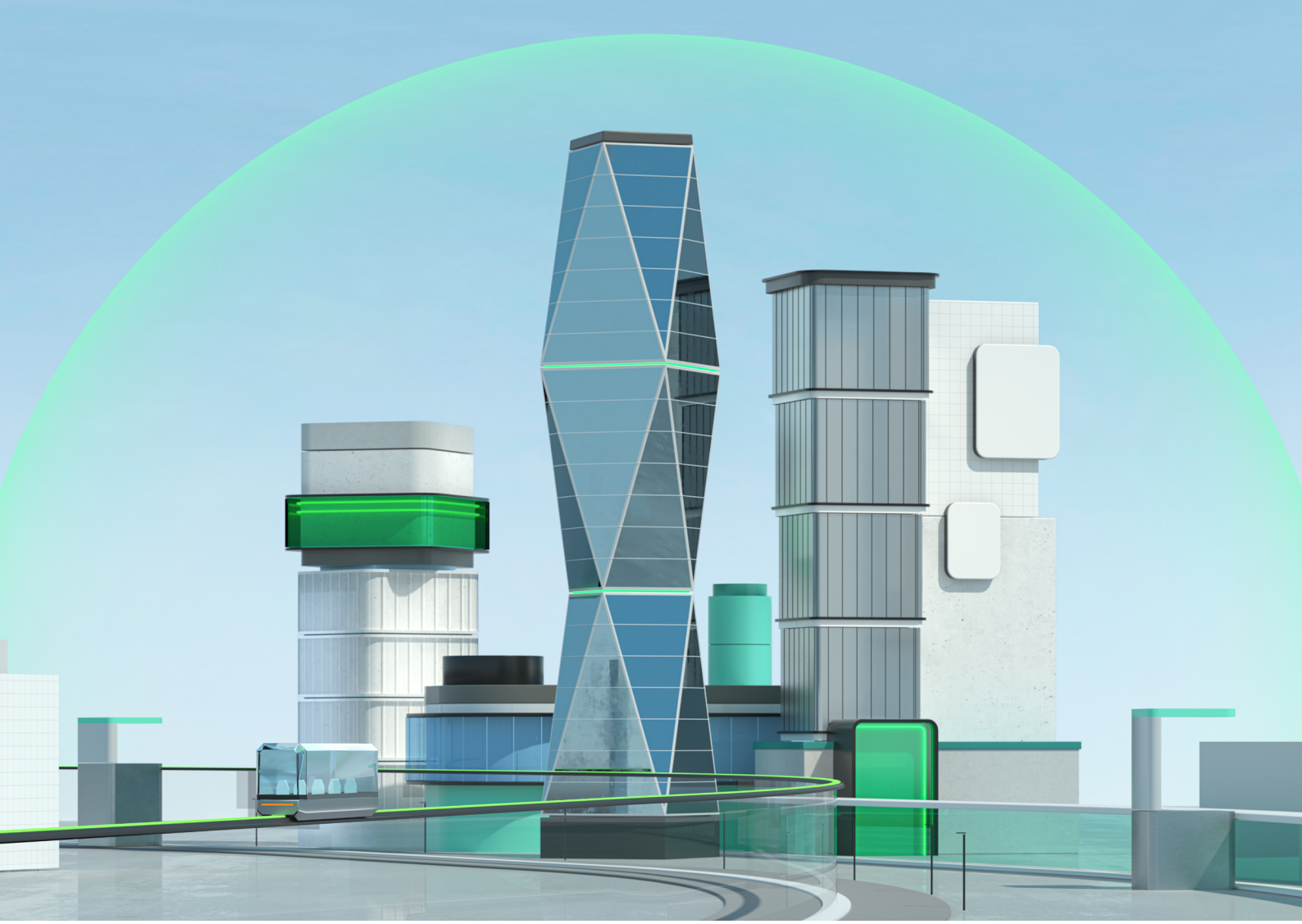


Контроллеры интернета вещей на базе KasperskyOS для систем диспетчеризации и автоматизации в инфраструктуре умного города и в промышленности

Кибериммунные контроллеры для IoT

INSPARK ISS KasperskyOS

Использование интеллектуальных систем для автоматизации в умном городе и в промышленности позволяет оптимизировать процессы и, таким образом, получать экономические выгоды.

Важную роль в объединении систем интернета вещей играют контроллеры — промежуточные устройства, которые собирают данные с инженерных систем и прочего оборудования, отправляют их в облачные платформы и приложения для последующей аналитики и передают обратно управляющие воздействия, полученные от этих платформ и приложений.

Подобные контроллеры сегодня становятся границей физического и цифрового миров. Они открывают новые возможности благодаря повышению связности и общей «интеллектуализации» интернета вещей, будь то системы умного города или промышленное производство. В то же время использование таких устройств несет угрозы новых киберрисков.

Риски для интеллектуальных систем на базе IoT

Повсеместная цифровизация и автоматизация увеличивает число возможных целей для злоумышленников, а атаки становятся все сложней. В 2021 году одна таргетированная кибератака обходилась крупному российскому бизнесу порядка 50 млн рублей, а малому и среднему бизнесу порядка 2,2 млн рублей. Согласно отчету «Лаборатории Касперского», почти 25% кибератак в 2022 году в России и странах СНГ пришлись на промышленные предприятия. Все больше киберугроз возникает на стыке IT- и OT-сред предприятий. Именно там, где применяются контроллеры интернета вещей.

Ключевые уязвимости интеллектуальных систем, в которых применяются контроллеры, следующие:

Подмена данных, собираемых прикладными системами на полевом уровне

Несанкционированное изменение структуры защищаемой системы

Недостаточный контроль целостности системы

В условиях отсутствия на рынке зарубежных и отечественных контроллеров с требуемой киберзащищенностью, требуется разрабатывать устройства с новым подходом к безопасности.

Кибериммунитет

Подход «Лаборатории Касперского» к разработке исходно безопасных (Secure by Design) IT-систем.

Кибериммунная система способна противостоять кибератакам без использования дополнительных (наложенных) средств безопасности. Подавляющее большинство типов атак на кибериммунную систему неэффективно и не может повлиять на выполнение ею критических функций.

Решение проблемы: кибериммунные контроллеры для IoT

Кибериммунные контроллеры для IoT позволяют устранить киберриски, связанные с атаками на системы диспетчеризации и автоматизации в инфраструктуре умного города и в промышленности.

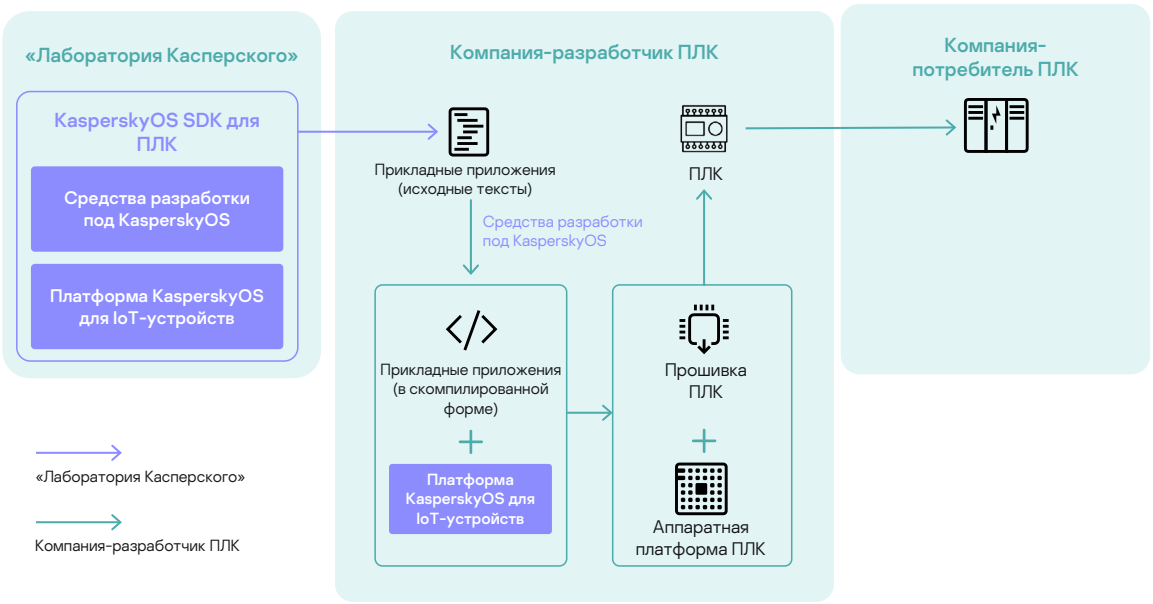
Это становится возможным благодаря встраиванию безопасности непосредственно в архитектуру решения - как на уровне прикладного кода, так на уровне операционной системы.

Для реализации всех требований кибериммунитета необходима системная платформа. В качестве такой платформы идеально подходит микроядерная операционная система KasperskyOS, которая создавалась специально в соответствии с этими требованиями.

Заложенные в ее архитектуру возможности гарантируют целостность и аутентичность передаваемых данных инженерных систем, образов прошивки контроллера, сертификатов и политики безопасности.

KasperskyOS может быть портирована на различные аппаратные платформы. В SDK уже имеется набор базовых компонент, таких как сетевая и файловая подсистемы). Кроме того, благодаря поддержке большинства POSIX-вызовов могут быть легко портированы программные компоненты из других операционных систем.

«Лаборатория Касперского» поставляет производителям платформу, включающую в себя ядро операционной системы, монитор безопасности, драйверы, готовые политики безопасности и популярные сторонние библиотеки. Также, производители получают все необходимые средства разработки.



Использование KasperskyOS SDK для контроллеров интернета вещей

Технологии KasperskyOS

Безопасность, заложенная в архитектуру операционной системы.

В основе операционной системы лежат проверенные и хорошо описанные подходы MILS и FLASK, а также собственные технологии «Лаборатории Касперского».

Уникальное микроядро и система безопасности по умолчанию блокируют все неавторизованные действия

Изолированные компоненты не могут неавторизованно влиять на работу друг друга.

Все межпроцессные взаимодействия имеют типизированные интерфейсы и строго задекларированы.

Функции безопасности в KasperskyOS отделены от функциональной логики системы.

Политики безопасности конструируются в терминах конкретных задач с помощью специально разработанного языка PSL.

Разработчик решения на базе KasperskyOS может комбинировать множество разных моделей, чтобы построить политику, которая наиболее точно соответствует поставленным целям безопасности.

Используя специальную методологию, на базе KasperskyOS можно создавать решения, обладающие кибериммунитетом.

Реализованный проект

Компания «Информационные системы и стратегии» (ООО «ИСС») реализовала версию контроллера интернета вещей СЭМ.ПРО.К.02.01 на базе KasperskyOS. Контроллер спроектирован на базе процессора с архитектурой ARM9. Взаимодействие контроллера с верхним уровнем облачных платформ и приложений происходит по Ethernet, а с полевыми устройствами — по Ethernet, I2C, RS-485 и GPIO.

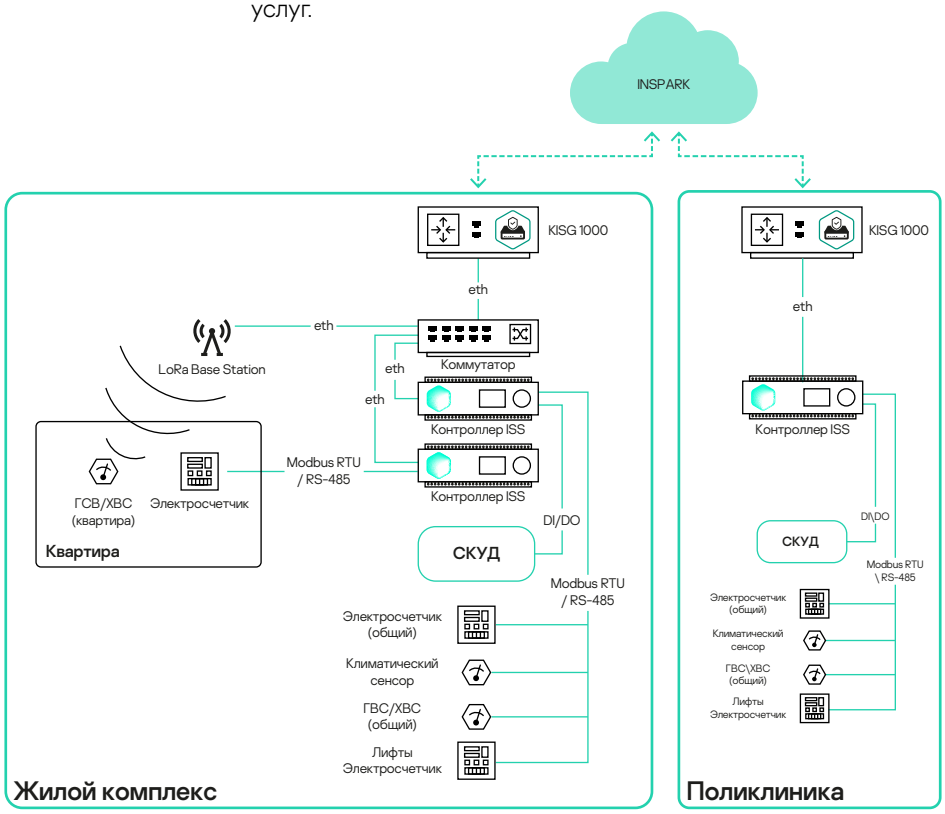
СЭМ.ПРО.К.02.01 обеспечивает сбор достоверных телеметрических данных от устройств для использования их в системах диспетчеризации и автоматизации.

Особенности продукта

- Безопасность на уровне операционной системы.
- Централизованное удаленное управление устройствами с помощью инструментов облачной платформы.
- Набор из 10 модулей расширения коммуникационных портов.
- Непрерывность мониторинга и управления за счет автономного управления устройствами при обрыве связи контроллера с облачной платформой.
- Встроенная поддержка двухуровневой архитектуры, с использованием на нижнем уровне контроллеров сбора данных, существенно удешевляющая внедрение комплексных систем.
- Интеграция с платформой промышленного интернета вещей Inspark IoT-platform компании Inspark.

Типовой сценарий применения

Кибериммунные контроллеры могут использоваться в системах энерго-менеджмента, для централизованного сбора показателей ЖКХ и их комплексного мониторинга на базе облачной платформы. Это позволяет следить за фактическим потреблением ресурсов в режиме онлайн и повысить прозрачность коммунальных услуг.



Защита систем ЖКХ в умном городе с помощью технологий «Лаборатории Касперского»

os.kaspersky.ru
www.kaspersky.ru

INSPARK ISS KasperskyOS