Передовая практика. Кибериммунитет 2022

ARC White Paper
Июнь 2022 г.

«Лаборатория Касперского» выпустила KasperskyOS — операционную систему, разработанную в соответствии с принципом secure by design (исходной безопасности), на базе микроядерной архитектуры. Она оптимально подходит для сетевых устройств, промышленных систем управления и устройств интернета вещей.

Принцип кибериммунитета в основе KasperskyOS может стать платформой для безопасной цифровой трансформации промышленности.

Автор — Томас Менце, старший консультант

Содержание

Краткий обзор

Интернет вещей (IoT) предлагает существенные экономические преимущества для промышленности и развития сопутствующих сервисов. Эта технология позволяет сократить время простоя машин и объектов, получить важные данные об инфраструктуре, а также автоматизировать многие процессы.

Хотя сама по себе кибербезопасность связана с программным обеспечением и его применением, кибербезопасность в сфере IoT, где объединяются два мира — виртуальный и материальный, — это более сложное понятие.

Решения на базе IoT — от удаленного мониторинга, профилактического обслуживания, управления энергопотреблением и умных зданий до подключенных устройств и пользовательских технологий (например, мобильных приложений) — позволяют упростить эксплуатацию, сократить стоимость и время выхода на рынок.

По прогнозам аналитиков и экспертов в области технологий, в будущем количество IoT-устройств и приложений будет расти, что, в свою очередь, повлечет за собой их дальнейшее развитие, а также развитие IoT-сервисов. Все больше компаний хотят стать частью этого процесса. В то же время при реализации стратегий внедрения решений IoT многие предприятия действуют консервативно из-за опасений, связанных с безопасностью в этой сфере. Развертывание систем интернета вещей ставит перед предприятиями во всем мире новые уникальные задачи в области обеспечения безопасности, конфиденциальности и соответствия нормативным требованиям.

Если кибербезопасность — это программное обеспечение и его применение, то кибербезопасность в сфере IoT, где объединяются два мира — виртуальный и материальный, — это более сложное понятие. Во многих сценариях технического обслуживания и эксплуатации IoT-систем используются сквозные соединения, обеспечивающие доступ к данным для пользователей и приложений. Однако при использовании преимуществ IoT (например, профилактического обслуживания) компании должны хорошо знать необходимые стандарты безопасности (например, IEC 62443 или ISO 27000), поскольку эти операционные инструменты слишком важны и игнорировать угрозы вторжения, возникновения чрезвычайных ситуаций или других рисков нельзя.

Кибератаки на OT-инфраструктуру

Частота и сложность успешных кибератак на OT-системы должны стать предупреждением для владельцев активов, сетевых инженеров и команд по кибербезопасности. Это в равной степени относится и к сфере IT, и к сфере OT. Отсутствие скоординированной защиты сервисов и приложений как на границе сети (edge), так и в облаке (cloud) позволяет злоумышленникам атаковать производственное оборудование. Наличие множества компонентов автоматизации от разных производителей усложняет для инженеров контроль уровня кибербезопасности в сетях OT.

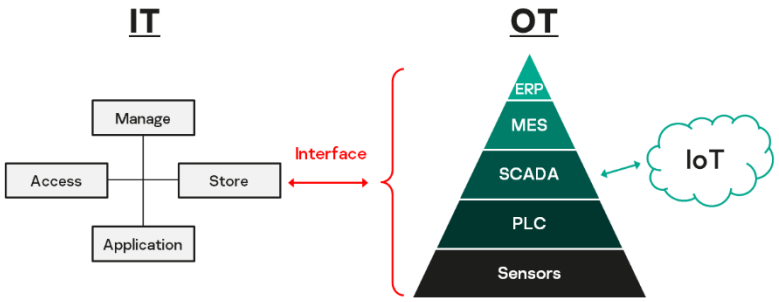
Чаще всего киберзащита направлена на обеспечение охраны труда, бесперебойной работы и предотвращение опасного воздействия на окружающую среду. Для этих целей инженеры всегда использовали методы защиты, которые возникли в традиционной IT-среде и были приспособлены для OT-систем. Однако быстрое развитие периферийных и облачных решений заставляет пользователей изменить подход к обеспечению безопасности. Чтобы защитить критически важные OT-системы, при планировании стратегий кибербезопасности на 2022 год и далее предприятиям следует выполнить, помимо прочего, следующие условия:

- разработать концепцию безопасности;
- определить необходимые уровни защиты для конкретных частей системы;
- поддерживать концепцию защиты на протяжении всего жизненного цикла объекта;
- обеспечить эффективность концепции безопасности.

В рамках эволюции на пути к Индустрии 4.0 первостепенную роль играет развитие автоматизации технологических процессов, сбор и обмен данных в режиме реального времени. Появляются новые типы атак на системы ПЛК, АСУ ТП, OT, IIoT и IoT, к которым теперь можно получить доступ через интернет. Из-за конвергенции IT и OT сетевые системы управления объединяются с корпоративными сетями, что приводит к дополнительным рискам безопасности из-за перекрестного трафика локальных сетей, интернета и сетей управления.

Проблема в том, что в большинстве OT-сетей возможности кибербезопасности ограничены. И типичные меры безопасности, такие как проверка на вирусы, защита рабочих мест или обнаружение аномалий, на практике неэффективны, поскольку большое количество компонентов и сетевых структур IIoT затрудняет установку исправлений уязвимостей и обновлений программного обеспечения, что снижает эффективность защиты.

Именно поэтому четкого разделения между IT- и OT-средой уже давно не существует. Это разделение исчезает во многих отраслях, и не только в контексте цифровой трансформации. Производители давно осуществляют техническое обслуживание оборудования удаленно. Это позволяет оперативно реагировать на проблемы и быстро устранять их при относительно невысоких затратах. Но под влиянием цифровой трансформации изменения в корпоративных сетях продолжают происходить. Сейчас необходимо повысить гибкость производства и устранить возможные ошибки в его процессах.



Источник: «Лаборатория Касперского»

На рисунке слева показано, как OT-инфраструктура должна все быть все больше подключена к сети, чтобы повысить цифровую эффективность. Все уровни пирамиды автоматизации OT связаны с IT во многих сценариях, и все большее количество IoT-сетей также интегрируется в систему автоматизации. Таким образом, область атаки пирамиды автоматизации продолжает увеличиваться.

Противодействие кибератакам в промышленности

Чтобы использовать возможности цифровых IIoT-систем и повысить эффективность работы, владельцы активов используют новую тактику. Одним из примеров может служить принцип NOA, разработанный ассоциацией NAMUR. В нем применяется односторонняя связь между IIoT-сетями и компонентами автоматизации технологических

процессов. Это означает, что повышение эффективности достигается за счет цифровых методов, но из-за использования второго канала связи данные цифровых датчиков изолированы от традиционной системы автоматизации. В документе NE 175 этот принцип описывается следующим образом:

> «Архитектура NAMUR Open Architecture (NOA) предназначена для легкого и безопасного использования производственных данных для мониторинга и оптимизации работы предприятий и активов.
>
> Из-за повсеместного использования IT-оборудования, интеллектуальных датчиков, полевых и мобильных устройств количество генерируемых данных постоянно растет. Зачастую к ним трудно получить доступ в рамках классической пирамиды автоматизации NAMUR. В архитектуре NOA передача данных происходит по второму каналу связи, не затрагивая традиционную структуру автоматизации и не влияя на систему автоматизации».

Источник: NAMUR

NAMUR — это крупная ассоциация, которая занимается вопросами автоматизации технологических процессов. Рабочие группы ассоциации NAMUR разрабатывают подобные концепции в сфере безопасности совместно с университетами. Не каждое производственное предприятие может определить или реализовать такую концепцию для собственных нужд. Создание собственной концепции защищенной связи требует переосмысления принципов безопасности, в основе которых лежат приоритеты OT: доступность, целостность и конфиденциальность данных, причем именно в таком порядке.

Безусловно, концепцию односторонней связи и защиты от воздействий для IIoT-систем следует использовать с самого начала. Это облегчает задачу по обеспечению безопасности для поставщиков технологий и дает пользователям свободу использования IIoT-систем для повышения эффективности предприятия.

Индустрия 4.0 требует трансформации кибербезопасности OT

Неудивительно, что облачные вычисления, приложения и инфраструктуры быстро становятся более сложными, и количество их поставщиков постоянно растет. Традиционных методов проверки и установки исправлений больше не хватает для эффективной защиты сложных облачных структур.

Кибербезопасность в автоматизации технологических процессов достигла критической точки. С одной стороны, системы должны работать максимально эффективно, чтобы обеспечить конкурентоспособность компаний. С другой стороны, использование IIoT-систем и облачной инфраструктуры представляет угрозу безопасности.

Кибербезопасность для OT-систем и облачных сетей нуждается в преобразовании. В сфере промышленности концепция «Индустрия 4.0» называется цифровой трансформацией. С точки зрения технологий автоматизации это правильное определение, но в контексте кибербезопасности такая трансформация еще не состоялась.

Какой может быть трансформация кибербезопасности? Возможно, это переход от кибербезопасности к кибериммунитету. Здесь понятие «кибериммунитет» определяется как технология защиты как от уже известных методов атак, так и от еще неизвестных атак, которые могут появиться в будущем.

Вернемся к вопросу о том, как использование интернета вещей влияет на кибербезопасность. В отчете ITSRS (https://www.kaspersky.com/blog/iot-report-2022/) рассматриваются некоторые особенности IoT.

- В 2021 году 53% организаций отказались от новых бизнес-проектов из-за неспособности устранить риски кибербезопасности, а 74% столкнулись с ситуацией, когда для обеспечения безопасности не было подходящего решения.

- 64% предприятий уже занимаются обслуживанием решений на базе IoT или используют их.

- Руководители 52% организаций обеспокоены сбором больших данных с IoT-устройств из-за риска кибердиверсий и шпионажа.
- Для 57% организаций, которые планируют внедрить IoT, риск нарушения кибербезопасности является наиболее серьезной проблемой.

Различные компании сталкиваются с совершенно разными рисками кибербезопасности. Эффективная защита должна адаптироваться к актуальным угрозам и требует совместных действий всех заинтересованных сторон. Киберзащита — это не продукт, который можно приобрести, установить и забыть, это непрерывный процесс.

Несмотря на все более широкое распространение технологий IoT, сотрудники более половины опрошенных компаний (57%) обеспокоены вопросами кибербезопасности и целостности данных при внедрении интернета вещей. Вторым препятствием к внедрению IoT (35%) называют нехватку ресурсов или ограниченный бюджет.

Наиболее значимые препятствия для внедрения IoT

Что касается различных отраслей, в промышленном секторе 53% компаний обеспокоены риском вторжения в контур безопасности и компрометации данных. Далее следует нехватка собственного опыта (35%). Аналогичные причины для беспокойства назвали представители сектора коммунальных услуг — 50% и 44% соответственно.

С развитием интернета вещей появляется множество новых угроз для устройств, платформ и операционных систем, для их коммуникаций и даже для систем, к которым они подключены (например, устройства интернета вещей могут использоваться в качестве точки атаки).

Для 52% опрошенных компаний сбор больших объемов данных с IoT-устройств является поводом для беспокойства из-за риска кибердиверсий, шпионажа и других продвинутых угроз.

Основные проблемы, связанные с большими данными в IoT-среде

Запрос на кибериммунность

Чтобы своевременно отвечать на вызовы, связанные с безопасностью IoT, а также поддерживать компании в использовании практических решений в области кибербезопасности, необходимо рассмотреть новые подходы.

Для усиления безопасности платформ IoT предпринимаются шаги по стандартизации методов их разработки. Эти инициативы курируют такие ассоциации, как Институт инженеров электротехники и электроники (IEEE), Европейский институт телекоммуникационных стандартов (ETSI).

Кроме того, существуют рекомендации для организаций по созданию безопасных IoT-систем или оценке состояния существующих решений, например «Модель зрелости безопасности IoT», разработанная консорциумом Industry IoT Consortium. С их помощью организации могут принять необходимые меры безопасности.

Среди общих рекомендаций по безопасности IoT упоминается использование шифрования и политики паролей, сегментации сети и брандмауэров, а также специальной защиты облачных инфраструктур, к которым подключаются IoT-устройства. Эти методы рекомендуются для всех технологических систем.

Существует также уникальный подход к безопасности IoT — кибериммунитет. Он фокусируется не на устранении потенциальных

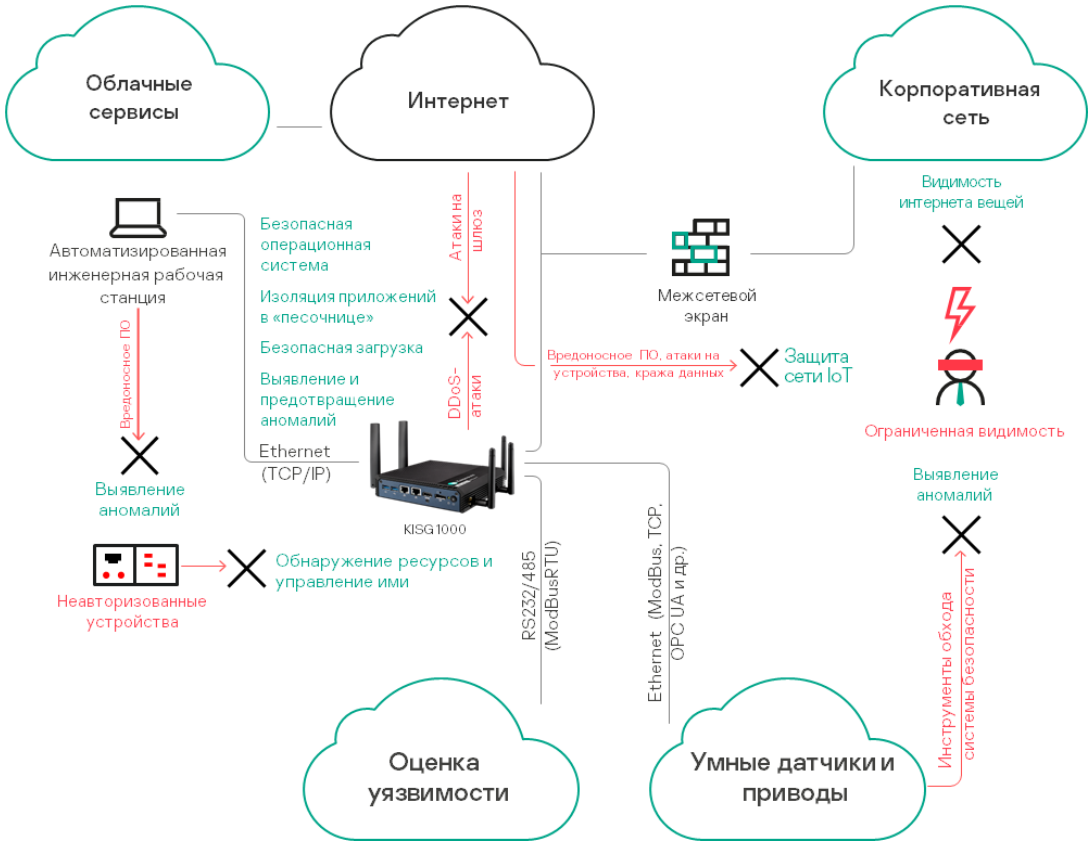
уязвимостей, а на создании условий, при которых эксплуатировать эти уязвимости и повлиять на работу системы будет невозможно. Так что даже если одна из систем подвергнется атаке, это не повлияет на надежную работу всей платформы.

Этот принцип можно реализовать с помощью специализированной операционной системы и особой методологии разработки. В такой операционной системе используется микроядерная архитектура, содержащая всего несколько тысяч строк кода, что позволяет устранить уязвимости и уменьшить поверхность атаки. «Лаборатория Касперского» разработала такое программное обеспечение — операционную систему KasperskyOS с минимальным количеством доверенных компонентов.

KasperskyOS создана с применением передовых практик в области безопасного программного обеспечения, включая архитектуру множественных независимых уровней безопасности MILS (Multiple Independent Levels of Security). Это гарантирует, что атаки не могут повлиять на работоспособность системы.

Как именно KasperskyOS помогает обеспечить кибербезопасность IoT? Она может стать основой для создания шлюзов с кибериммунитетом. Это связующие элементы на границе между средами OT (сенсоры/актуаторы) и IT (корпоративная сеть или интернет), через них проходят все данные. Следовательно, инфраструктуру и ее данные можно защитить на уровне шлюзов, обладающих «врожденной» киберзащитой.

Типичная IoT-инфраструктура с применением кибериммунных шлюзов на базе операционной системы KasperskyOS может выглядеть следующим образом (на примере шлюза Kaspersky IoT Secure Gateway 1000):



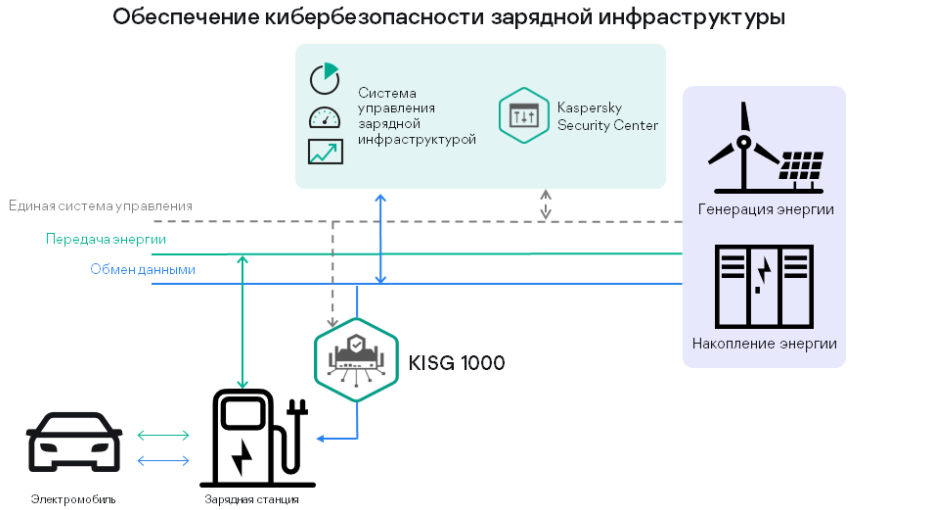
Источник: «Лаборатория Касперского»

Передовая практика: зарядная станция для электромобилей

Поставщики средств автоматизации в какой-то момент исправили уязвимости в системе безопасности зарядных станций для электромобилей, которые могли привести к атакам типа «отказ в обслуживании» (DoS).

Всего поставщики исправили 13 недостатков, в том числе три критические уязвимости. Точки зарядки устанавливаются на частной территории, на общественных парковках и на улице. Затронуты три

линейки продуктов для зарядных станций: City, Parking и Smart Wallbox.



Источник: «Лаборатория Касперского»

Эксплуатация уязвимостей и ее последствия

Владельцев зарядных станций предупредили, что без обновления прошивки «существует риск несанкционированного доступа к веб-серверу зарядной станции и, следовательно, настройкам и учетным записям зарядной станции».

Подобные манипуляции могут привести, например, к атакам типа «отказ в обслуживании», несанкционированному использованию зарядной станции, перебоям в работе, невозможности передачи данных о зарядке в систему мониторинга.

Уязвимости можно использовать удаленно, если станции напрямую подключены к интернету. Коммерческая инфраструктура зарядных станций обычно насчитывает сотни зарядных устройств, поэтому, если злоумышленнику удастся получить доступ к одному из них, он сможет захватить их все. Для усиления безопасности зарядной станции было рекомендовано заменить ее внутренний коммуникационный порт. Для этого требовалось разобрать корпус устройства или, при наличии сетевого подключения, подключиться к системе контроля зарядной станции.

Поскольку количество зарядных устройств для электромобилей продолжает расти, вполне вероятно, что появятся новые серьезные уязвимости. К примеру, злоумышленники могут выполнять манипуляции с записями или настройками зарядного устройства, чтобы изменять предельные значения заряда, красть и использовать учетные данные других пользователей для зарядки. В худшем случае злоумышленники могут даже найти способ нарушить работу электросети.

Это пример того, как важно использовать системы для защиты IoT-компонентов от кибератак известных и неизвестных типов. Такие механизмы защиты требуются для работы в сети и резервного копирования в системах критически важной инфраструктуры. В этом случае операционная система KasperskyOS может обеспечить эффективную защиту от эксплуатации уязвимостей.

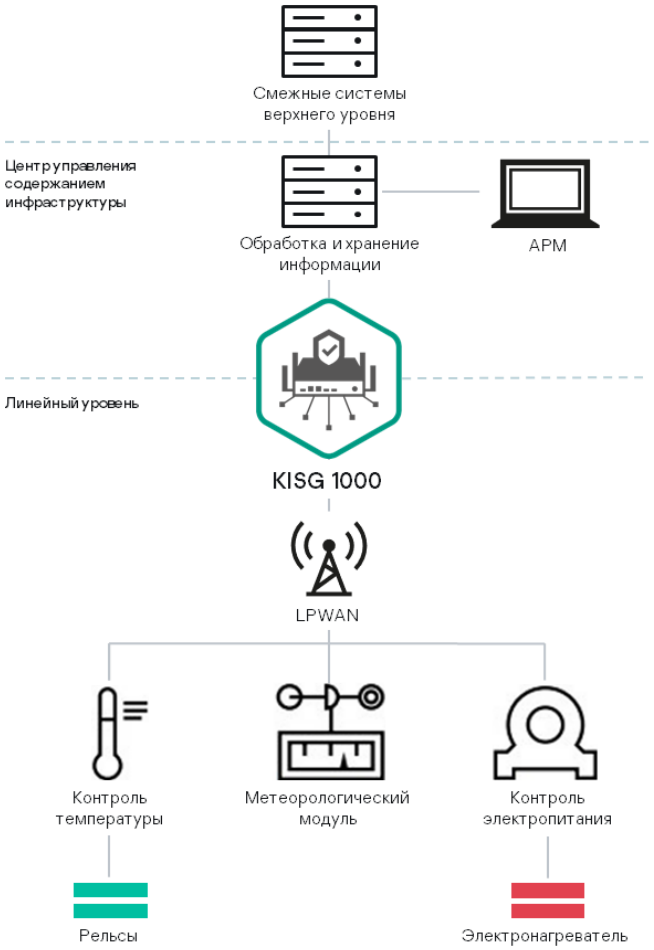
Передовая практика: обогрев стрелок железнодорожных путей

Как крайне важный вид передвижения, железные дороги нуждаются в экономически эффективных методах контроля за использованием своих ресурсов. Чтобы существенно снизить количество потребляемой энергии, была введена интеллектуальная IoT-система для обогрева железнодорожных стрелок. Обогрев включается только тогда, когда система, учитывая данные о различных параметрах окружающей среды, полученные от интеллектуальных датчиков, считает возможным замерзание стрелок.

Проект такой сложности невозможно реализовать без обеспечения кибербезопасности, ведь система обогрева подключена к интернету и поэтому особенно уязвима. Железнодорожный транспорт является частью критически важной инфраструктуры, и последствия успешной кибератаки на него могут быть катастрофическими. Например, если интеллектуальная система обогрева не сможет определить погодные условия из-за того, что злоумышленник изменил ее конфигурацию, рельсы могут обледенеть, что поставит под угрозу все движение на железной дороге.

На границе уровней OT и IT был установлен шлюз Kaspersky IoT Secure Gateway 1000 на базе KasperskyOS. Благодаря реализации принципа кибериммунитета, шлюз обеспечил целостность обработки сигналов, не требуя большого объема обслуживания или настройки. Кибератаки на KISG 1000 будут безуспешными. То же самое произойдет, если злоумышленники попытаются изменить данные, поступающие с метеопередатчиков.

Благодаря Kaspersky IoT Secure Gateway 1000 система остается надежной, правильно определяет погодные условия и обеспечивает автоматический обогрев железнодорожных стрелок даже в агрессивной среде.



Источник: «Лаборатория Касперского»

Заключение

Цифровизация объединяет информационные технологии (IT), традиционные операционные технологии (OT) и интеллектуальную собственность для повышения конкурентоспособности промышленности.

Именно это мы наблюдаем в промышленности — слияние OT-, IT-систем и интеллектуальной собственности. Чтобы полностью реализовать эту инфраструктуру, большинству компаний требуется время. Мы можем наблюдать, как целая отрасль медленно движется к Индустрии 4.0, заменяя оборудование по частям. К сожалению, эта трансформация несет с собой ряд новых угроз и рисков.

По мере внедрения подключенных производственных систем вместе с цифровой трансформацией появляется новый профиль киберугроз. Несмотря на то, что Индустрия 4.0 представляет собой идеальную картину производства, которая помогает компаниям значительно повысить свою конкурентоспособность и эффективность, необходимые меры для безопасности IT-систем остаются неясными.

В целом, кибербезопасность должна стать неотъемлемой частью любого проекта. Но вместо того, чтобы развиваться параллельно с ним, она должна закладываться с самого начала. Срок службы АСУ ТП составляет более 30 лет. Здесь необходимо применение новых концепций кибербезопасности, таких как кибериммунитет. Использование системы, в архитектуре которой заложена защита от существующих и потенциальных киберугроз, безусловно, является очень практичным методом. Принцип кибериммунитета может сделать цифровую трансформацию более безопасной.

Поэтому многие OEM-производители и другие лидеры рынка объединяются с поставщиками технологий в области кибербезопасности, чтобы разрабатывать безопасные в своей основе продукты и делать это ключевым преимуществом своих решений. Например, для защиты промышленных и других IoT-сред «Лаборатория Касперского» совместно с НПО «Адаптивные промышленные технологии» (Апротех) разработала кибериммунные шлюзы на базе операционной системы KasperskyOS. Шлюзы Kaspersky IoT Secure Gateway можно интегрировать с

Siemens MindSphere, IBM Bluemix, Yandex IoT Core и другими облачными платформами. Эти устройства станут надежными инструментами цифровой трансформации, обладая «врожденной» киберзащитой и обеспечивая защиту IoT-систем и данных.

О «Лаборатории Касперского»

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности и цифровой приватности с 1997 года. Глубокие экспертные знания и многолетний опыт лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами. Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 240 тысяч корпоративных клиентов во всем мире.

Подробнее на www.kaspersky.ru

О кибериммунитете и операционной системе KasperskyOS

Кибериммунитет — это «врожденная» защищенность IT-системы, ее способность 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 в сценариях работы, предусмотренных на этапе проектирования.

«Лаборатория Касперского» разработала кибериммунный подход к созданию IT-решений, а также собственную микроядерную операционную систему KasperskyOS — платформу для разработки кибериммунных продуктов. Кибериммунности можно достичь с помощью KasperskyOS, следуя особой методологии разработки продуктов на ее базе.

«Лаборатория Касперского» развивает KasperskyOS и методологию разработки, а также создает кибериммунные продукты в сотрудничестве со своими технологическими партнерами. Портфолио включает линейку IoT-гейтвеев для промышленности, умного города и

других отраслей, решение для построения управляемой и функциональной инфраструктуры тонких клиентов, специализированный SDK для создания безопасных и надежных приложений для электронных блоков управления (ECU) в автомобилестроении, а также другие проекты.

Подробнее на os.kaspersky.ru
Узнать больше: KasperskyOS_Info@kaspersky.com

Об НПО «Адаптивные промышленные технологии»

НПО «Адаптивные промышленные технологии» (Апротех) — дочерняя компания «Лаборатории Касперского», помогающая предприятиям эффективно и безопасно пройти цифровую трансформацию 4.0. Этому способствуют передовые кибериммунные IoT-шлюзы компании, которые организуют транспорт данных в сквозных цифровых сервисах, разрабатываемых совместно с партнерами для решения бизнес-задач заказчиков. Услуги Апротех, в числе которых консалтинг и аудит, исследовательские работы и обучение, упрощают кибербезопасный переход к новым технологиям.

Подробнее на www.aprotech.ru

Аналитик: Томас Менце (Thomas Menze)

Аббревиатуры:

ERP	Планирование ресурсов предприятия (Enterprise Resource Planning)
IoT	Интернет вещей (Internet of Things)
IT	Информационные технологии
KISG	Kaspersky IoT Secure Gateway
MES	Автоматизированная система управления производственными процессами (Manufacturing Execution System)
NOA	Namur Open Architecture
OT	Операционные технологии
ПЛК	Программируемый логический контроллер
АСУ ТП	Автоматизированные системы управления технологическими процессами