DOI: 10.25728/avtprom.2024.09.13

Industrial Internet of Things: риски и защита в цифровую эпоху

А.А. Винявский («Лаборатория Касперского»)

В современных промышленных компаниях проблема киберинцидентов выходит за пределы кабинетов специалистов по информационной безопасности и становится вопросом, от которого напрямую зависит устойчивость и конкурентоспособность бизнеса. Существующие комплексные подходы с обеспечением эшелонированной защиты хороши, но они не в полной мере покрывают аспекты защиты важного класса систем на границе промышленного и ИТ-контуров – устройства Industrial Internet of Things.

В статье формулируются проблемы в области кибербезопасности, которые характерны для устройств Industrial Internet of Things. Рассматривается подход «Лаборатории Касперского» к созданию конструктивно безопасных систем – кибериммунитет. Описываются практические преимущества кибериммунитета для промышленных предприятий на примере шлюза промышленных данных Kaspersky IoT Secure Gateway (KISG).

Ключевые слова: Industrial Internet of Things, кибербезопасность, шлюз промышленных данных, кибериммунитет.

Введение

В современных промышленных компаниях проблема киберинцидентов выходит за пределы кабинетов специалистов по информационной безопасности и становится вопросом, от которого напрямую зависит устойчивость и конкурентоспособность бизнеса. Ведь как показал опыт компаний, которые сталкивались с киберинцидентами, последствия таких инцидентов измеряются прямыми финансовыми потерями для бизнеса, ударом по его репутации, жизнями и здоровьем сотрудников.

По мере происходящей сегодня активной цифровой трансформации предприятий неизбежно повышаются риски кибербезопасности.

Существующие комплексные подходы с обеспечением эшелонированной защиты хороши, но они не в полной мере покрывают аспекты защиты важного класса систем на границе промышленного и ИТ-контуров – устройства Industrial Internet of Things (IIoT). Рассмотрим причины, почему существующих способов защиты недостаточно, и как обеспечить повышенную безопасность промышленных IoT-устройств.

Переходный период для промышленных компаний

В рамках происходящей сегодня цифровой трансформации промышленных предприятий происходит глубокое взаимное проникновение (конвергенция) до настоящего времени отдельных миров информационных (ИТ) и операционных (ОТ) технологий. Четкой границы между ИТ и ОТ средами уже не существует, и она размывается все сильнее.

Современные предприятия стремятся к тому, чтобы проектировать в цифровой среде как само производство, так и производимые на нем изделия, обеспечивать сбор и аналитику данных с производства в режиме реального времени, оптимизировать конфигурации продукта и производства на основе имеющихся данных, обеспечивая петлю обратной связи для оптимизации производства и повышения качества продукции (рис. 1).

Если несколько лет назад только начинался шум вокруг темы метавселенной, то сегодня промышленные гиганты активно движутся в сторону «промышленной метавселенной» (Industrial Metaverse). Согласно

недавнему отчету[1] MIT Technology Review и Siemens, к 2030 г. рынок вокруг нее вырастет в 10 раз и достигнет 100 млрд долл. США.

Безопасность и промышленная метавселенная

Объединение информационных и операционных промышленных систем, конечно, позволяет оптимизировать технологические и бизнес-процессы компании и создает новые возможности для бизнеса, повышая его конкурентоспособность. Однако такая трансформация неизбежно повышает риски кибербезопасности.

Исторически миры ИТ и ОТ развивались параллельно и слабо пересекались. Их подходы к планированию, выработке требований, уровень регуляции, методы тестирования, ввода в эксплуатацию и, разумеется, подходы к обеспечению безопасности принципиально разные. Поэтому простое объединение систем приводит к тому, что поверхность атаки значительно увеличивается. Становится возможным атаковать ОТ-системы со стороны ИТ-части и наоборот. Например, промышленное оборудование можно атаковать со стороны ИТ-инфраструктуры, и нарушить технологический процесс. Такие случаи на практике происходили уже не раз.

Так, например, в 2022 г. кибератака привела[2] к пожару на сталелитейном заводе в Иране, в одном из цехов разлился расплавленный металл. Предположительно, хакерам удалось взломать АСУ ТП.

Эшелонированная защита

Комплексная безопасность промышленного предприятия сегодня обеспечивается в парадигме эшелонированной защиты (Defense-in-depth) – подхода, который направлен на создание нескольких слоев контроля безопасности на разных уровнях предприятия. Среди слоев такой защиты могут быть, например:

- обеспечение физической безопасности полевых устройств, центров управления и сетевой инфраструктуры;
- защита сети АСУ ТП и ее отдельных хостов (например, HMI);
- защита офисного сегмента, а также облачных сервисов.

Однако один лишь такой подход не в полной мере учитывает происходящие сегодня изменения, а именно проблему повсеместного использования устройств класса IIoT, которые сегодня все чаще применяются в различных отраслях промышленности для повышения производительности, улучшения качества продукции, оптимизации производственных процессов.

Пример такого устройства – IIoT-шлюз. Его задача – сбор промышленных данных непосредственно с оборудования и их передача в ИТ-системы (локальные или облачные) для последующей аналитики и принятия на их основе решений.

IIoT-устройства представляют собой относительно новый и слабо регулируемый с точки зрения информационной безопасности рынок. Большинство IIoT-устройств

Рис. 1. Концепция цифрового предприятия. Источник: Siemens

проектируются с недостаточным вниманием к вопросам информационной безопасности. Подобные устройства часто территориально распределены во время эксплуатации, что делает своевременное обновление и патчинг парка таких устройств затруднительным. Например, известно [1], что прошивка среднестатистического IoT-устройства устарела на 6 лет, а более половины устройств IoT подвержены атакам средней и высокой степени тяжести [2].

Более того, специфика IIoT-устройств часто не предполагает использования на них каких-то дополнительных (наложенных) средств защиты, например антивирусов. Причины этого понятны – компактность устройств, небольшие вычислительные ресурсы, сложность поддержки и обслуживания.

При этом, поскольку устройства промышленного IIoT имеют доступ к критическим системам, их взлом дает злоумышленникам возможность нарушить функционирование производственного оборудования, даже несмотря на использование продвинутых механизмов эшелонированной защиты.

Для решения описанных проблем у компаний сегодня существует два основных пути:

- принимать существующие риски кибербезопасности и внедрять решения на базе технологий IIoT, подвергая свои системы и бизнес опасности.
- приостанавливать инициативы по цифровизации, тем самым отставая в конкурентной гонке. Так, согласно отчету[3] Kaspersky Global Corporate IT Security Risks Survey, 53% компаний отказались от новых бизнес-проектов, связанных с внедрением решений класса IIoT, из-за неспособности устранить риски кибербезопасности, а 75% компаний не могли решить проблемы кибербезопасности, потому что не имели подходящего решения.

Оба пути пагубны для бизнеса в долгосрочной перспективе. Необходим иной подход – обеспечить повышенную защищенность критических узлов на границе контуров ОТ-ИТ, которыми являются IIoT-устройства.

[1] MIT Technology Review Insights – The emergent industrial metaverse. https://wp.technologyreview.com
[2] Predatory Sparrow: Who are the hackers who say they started a fire in Iran? BBC News. https://www.bbc.com
[3] Pushing the limits: How to address specific cybersecurity demands and protect IoT. Kaspersky report. https://www.kaspersky.com

Рис. 2. Шлюз Kaspersky IoT Secure Gateway

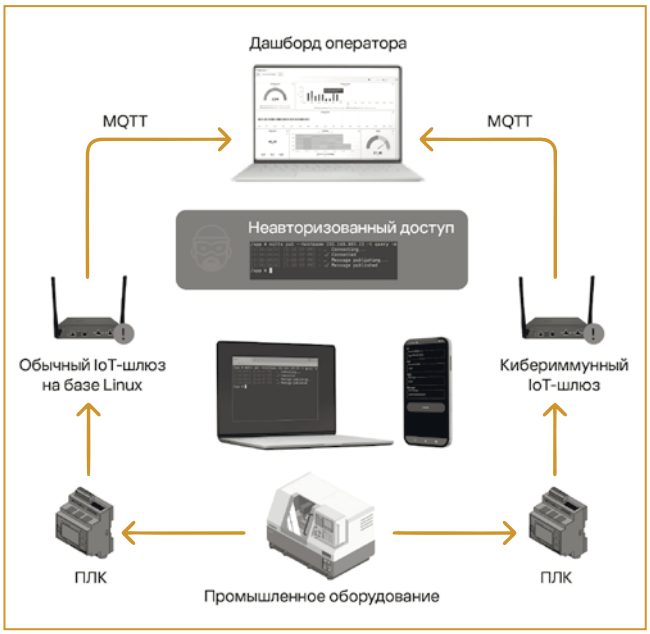

Рис. 3. Верхнеуровневая схема эксперимента со сравнением шлюзов

Кибериммунитет для обеспечения повышенной устойчивости устройств IIoT

«Лаборатория Касперского» называет повышенную защищенность кибериммунитетом. Кибериммунная система устойчива к внешним угрозам за счет того, что она обладает конструктивной безопасностью (Secure-by-Design). Кибериммунная система изначально проектируется так, чтобы ее ключевые ценности были устойчивы при любых обстоятельствах – даже в случае кибератаки. Защитные механизмы кибериммунной системы глубоко интегрированы в ее архитектуру и программный код, а не являются внешними (наложенными) средствами по отношению к изначально небезопасной системе.

Другими словами, кибериммунной системе не нужен антивирус – она защищена на уровне архитектуры. Причем благодаря архитектурным особенностям защита обеспечивается не только от известных, но и от неизвестных угроз.

Для обеспечения устойчивости системы к киберугрозам защита должна обеспечиваться не только на уровне прикладного кода, но и на глубоком системном уровне. В качестве операционной системы могут быть использованы различные ОС. В «Лаборатории Касперского» используется собственная микроядерная операционная система KasperskyOS, которая воплощает принципы кибериммунитета «из коробки».

Для этого и кибериммунная система, и операционная система, которая лежит в ее основе, построены на базе трех ключевых принципов:

• *разделение системы на изолированные домены безопасности.* В кибериммунной системе все компоненты изолированы друг от друга, а взаимодействия между ними производятся не напрямую, а через микроядро KasperskyOS.

• *контроль всех межпроцессных взаимодействий.* В кибериммунной системе каждое взаимодействие проверяется на соответствие политикам безопасности отдельным модулем – монитором безопасности Kaspersky Security Monitor. Любые взаимодействия, не разрешенные политиками, запрещены по умолчанию.

• *минимизация объема доверенной вычислительной базы.* Кода, критичного для безопасности системы, должно быть как можно меньше. На уровне операционной системы соблюдение этого принципа заключается в использовании компактного микроядра KasperskyOS (≈ 100 тыс. строк кода в противовес десяткам миллионов в ядре Linux).

Практические исследования специалистов по кибербезопасности «Лаборатории Касперского» показали, что KasperskyOS за счет своих архитектурных особенностей «из коробки» предотвращает подавляющее большинство широко распространенных угроз. При этом важный вклад в безопасность KasperskyOS вносит микроядерная архитектура. В независимом исследовании [3]] говорится, что 96% критичных эксплойтов Linux перестанут быть критичными в микроядерной архитектуре, 57% критичных эксплойтов Linux станут иметь низкий уровень критичности, большая часть которых будет устранена полностью в случае верифицированного микроядра, 29% всех эксплойтов Linux будут полностью устранены даже без верифицированного микроядра.

Все указанные принципы лежат в основе кибериммунного шлюза данных Kaspersky IoT Secure Gateway (KISG), обеспечивая его повышенную устойчивость к внешним киберугрозам (рис. 2). KISG может работать в двух режимах: как маршрутизатор с функциями межсетевого экрана, а также как однонаправленный шлюз с функцией преобразования прикладных протоколов. Шлюз данных разработан совместно с дочерним предприятием «Лаборатории Касперского» – НПО «Адаптивные промышленные технологии» («Апротех»).

Кибериммунитет – это основа целостного подхода «Лаборатории Касперского» к защите IIoT. Но помимо безопасной по умолчанию архитектуры кибериммунный шлюз также оснащен технологией безопасной загрузки и обновления (secure boot / secure update), что значительно его усиливает.

Часть этой функциональности реализована в KISG с помощью сторонних приложений, которые разрабатываются партнерами «Лаборатории Касперского». Доставка приложений на устройство, их безопасная установка и гарантия аутентичности осуществляется с помощью платформы Kaspersky Appicenter. Платформа также предоставляет все необходимые инструменты для разработки и управления жизненным циклом приложений.

Таким образом, конструктивная безопасность не противоречит подходу с использованием наложенных средств защиты – они могут дополнять друг друга.

Проверка практических преимуществ кибериммунного подхода

Для демонстрации практических преимуществ кибериммунного подхода была смоделирована атака на промышленную инфраструктуру.

Промышленный контроллер (ПЛК) был подключен к виртуальному промышленному оборудованию. Далее ПЛК был подключен в корпоративную сеть через два IoT-шлюза: один шлюз под управлением операционной системы с ядром Linux, второй — кибериммунный шлюз под управлением KasperskyOS. Оба шлюза имеют одинаковую уязвимость в стороннем компоненте, реализующем передачу данных в корпоративную сеть.

Смоделировав этот сценарий, проверялось, как сможет действовать злоумышленник, которому удалось внедриться в корпоративную сеть с помощью ноутбука, планшета или смартфона.

В случае шлюза на базе Linux у потенциального злоумышленника есть возможность проэксплуатировать уязвимость и повлиять на работу промышленного оборудования.

В случае кибериммунного шлюза, даже если злоумышленнику удастся проэксплуатировать уязвимость, он не сможет развить атаку за пределы конкретного компонента. Все дело в архитектуре шлюза и операционной системы, которая обеспечивает изоляцию компонентов устройства и контроль взаимодействий между ними (рис. 3).

Таким образом, использование кибериммунного шлюза позволяет внедрить цифровое решение и избежать сопутствующих рисков кибербезопасности.

Заключение

В условиях цифровой трансформации промышленных предприятий обеспечение комплексной кибербезопасности становится необходимым как никогда. При этом активное распространение устройств IIoT несет дополнительные риски, которые не снижаются даже такими передовыми подходами к защите инфраструктуры, как эшелонированная защита.

Надежно защитить устройства IIoT с помощью одних только традиционных средств безопасности — антивирусного ПО, экранов, средств мониторинга — также не видится возможным.

Единственный выход – встраивать безопасность глубоко в дизайн и архитектуру IIoT-устройств, следуя философии конструктивной безопасности (Secure by Design). Кибериммунитет предлагает конкретную методологию, как реализовать эту философию на практике.

Шлюз данных Kaspersky IoT Secure Gateway воплощает принципы кибериммунитета, позволяя минимизировать риски кибератак и безопасно интегрировать цифровые технологии в производственные процессы.

Список литературы

1. *Contos B.* The secret, insecure life of Security Cameras. Forbes. 2023. https://www.forbes.com
2. *O'Donnell L.* More Than Half of IoT Devices Vulnerable to Severe Attacks. Threat Post. 2020. https://threatpost.com
3. *Biggs S., Lee D., Heiser G.* The Jury Is In: Monolithic OS Design Is Flawed: Microkernel-based Designs Improve Security. August. 2018.

***Винявский Александр Анатольевич** – технологический евангелист «Лаборатории Касперского».*

СпецТек автоматизирует систему ТОиР «Архангельского ликеро-водочного завода»

НПП «СпецТек» выполняет проект автоматизации системы управления техническим обслуживанием и ремонтами (ТОиР) оборудования АО «Архангельский ликеро-водочный завод». Проект реализуется на основе возможностей программного комплекса TRIM.

Рынок алкогольной продукции в России характеризуется строгими правилами регулирования, высокой конкуренцией, сезонными колебаниями спроса. Поэтому производителям важно обеспечить высокую готовность и надлежащее техническое состояние оборудования, соблюдение технологического процесса и гибкость производства. В таких условиях необходимой составляющей успеха является управляемость процессов ТОиР, внедрение передовых видов организации ТОиР и практик управления надёжностью. Инструментом решения этих задач служат соответствующие средства автоматизации бизнес-процессов.

В этой связи руководство АО «Архангельский ликеро-водочный завод» (АЛВИЗ) приняло решение о внедрении современных программных решений и автоматизации системы управления ТОиР оборудования. Технологической основой проекта стал программный комплекс TRIM – отечественный продукт класса EAM/APM, внесенный в Единый реестр российских программ для ЭВМ и баз данных. Исполнитель проекта – компания НПП «СпецТек», разработчик TRIM, профессиональный консультант в области систем и методов управления производственными активами.

Весомым аргументом в пользу выбора программного продукта и исполнителя стало успешное выполнение аналогичного проекта на подмосковном предприятии «Завод Георгиевский. Традиции качества» (входит в Novabev Group, куда также входит АЛВИЗ), где TRIM используется в процессах ТОиР с ноября 2021 г.

Проект на АЛВИЗ начался с семинара, в рамках которого персонал заказчика, задействованный в процессах ТОиР и материально-технического обеспечения ТОиР, ознакомился с возможностями TRIM. К настоящему времени разработана также проектная документация. Исполнителю предстоит выполнить работы по созданию базы данных по оборудованию (совместно с заказчиком), обучить пользователей и администраторов системы, для чего разработать регламент работы в системе и инструкции. Выполнить миграцию данных из внешних систем, разработать и ввести в эксплуатацию конвертер, обеспечивающий взаимодействие с 1С: ERP.

Заказчику будет предоставлена лицензия на использование TRIM и поставлена десктопная версия программного продукта, а также приложение для мобильных устройств полевого персонала (операторы оборудования, ремонтники). Стационарная и мобильная части автоматизированной системы должны будут обеспечить информационную поддержку и автоматизацию операций при планировании и выполнении ТОиР, обеспечении ресурсами регламентных работ, при регистрации, обработке и устранении дефектов, регистрации эксплуатационного и технического состояния оборудования, складском учете запчастей и материалов, ведении документооборота в процессах ТОиР и материально-технического обеспечения ТОиР, анализе показателей надёжности и принятии решений по улучшениям.

Https://trim.ru