Кибериммунитет промышленных систем

Дмитрий СОКОЛОВ,
главный архитектор, Kaspersky

Юрий КОЛЕНКИН,
главный эксперт, компания «Синимекс»

В современных условиях промышленные системы все чаще становятся целью злоумышленников, которые стараются вмешаться в работу систем АСУ ТП и полевых устройств для вывода из строя промышленного оборудования или, наоборот, проникновения через подключение к промышленной сети внутрь закрытых контуров предприятия. Для компаний, которые эксплуатируют объекты критической информационной инфраструктуры (КИИ), все эти вызовы и риски являются неприемлемыми с точки зрения и законодательства, и сохранения бизнеса. В качестве решения проблем по защите промышленных систем от внешних вредоносных воздействий была придумана концепция кибериммунных систем, которые имеют устойчивость к атакам извне и встроенные средства обеспечения их безопасного функционирования.

Принципы кибериммунности

Кибериммунитет – подход к построению и разработке исходно безопасных (secure-by-design) ИТ-систем, которые обладают встроенной защитой от кибератак. 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. «Лаборатория Касперского» разработала кибериммунный подход к созданию IT-решений, а также собственную операционную систему KasperskyOS – платформу для разработки кибериммунных продуктов. Такие специализированные операционные системы не чувствительны к внешним воздействиям, поскольку содержат встроенные механизмы контроля и защиты внутренних процессов, а также всех коммуникаций, используемых ресурсов. Функционал системы, построенной на базе кибериммунной ОС, ограничен набором только тех функций, которые были определены при ее разработке.

В информационной системе предприятия можно выделить три места, где кибериммунные системы наиболее эффективны.

Сегментирование. Задача выделения промышленных информационных систем в корпоративной сети в самостоятельные защищенные сегменты является наиболее важной и распространенной при применении кибериммунных решений. Сегментирование позволяет локализовать вредоносные воздействия в отдельных сегментах и не допустить распространения вредоносного ПО по всей корпоративной сети предприятия. Причем защищенные сегменты промышленной сети могут работать по своим протоколам, отличным от IP, – это усложняет задачу воздействия на них вредоносных кодов, поскольку при преобразовании протоколов с большой долей вероятности вредоносные фрагменты кода будут проигнорированы кибериммунным устройством.

Само устройство. Наиболее эффективной защитой является использование кибериммунной операционной системы со встроенными механизмами защиты на борту самого́ интеллектуального устройства: станка, автомобиля, инфомата или удаленного АРМ. Сейчас российскими производителями ведется работа по созданию и внедрению подобных решений, однако в большинстве случаев это требует замены уже установленного устройства кибериммунным. В процессе импортозамещения оборудования и при строительстве нового производства лучше отдавать предпочтение подобным системам со встроенной защитой, однако далеко не всегда такое замещение возможно по функциональным причинам.

Защита сети. Манипулирование стандартными сетевыми протоколами часто является основным способом перемещения злоумышленников по информационным системам предприятия, поэтому использование сетевых устройств со встроенными средствами защиты, иммунными к большинству известных атак, также является важной задачей при построении защищенных промышленных информационных систем. Кибериммунные маршрутизаторы позволяют блокировать распространение вредоносного воздействия на другие устройства информационной системы. Использование в ядре корпоративной сети кибериммунных маршрутизаторов и коммутаторов также может значительно усилить защищенность сети промышленного предприятия.

Следует отметить, что пока нет стандартов, которые определяют принципы построения кибериммунных систем, хотя работа в этом направлении ведется. Так, существует предварительный стандарт для оборудования, которое должно быть защищено от любого вида воздействий. В частности, предварительный стандарт ПНСТ 819-2023 «Информационные технологии. Интернет вещей. Системы с разделением доменов. Термины и определения» содержит основные определения для построения защищенных систем Интернета вещей, а ПНСТ 818-2023 «Базовые компоненты» описывает набор основных компонентов для кибериммунных систем. В целом эти два стандарта определяют принципы организации промышленного Интернета вещей. К основным принципам кибериммунности относятся изоляция, сегментация доменов, разделение процессов и др. При соблюдении этих принципов можно быть уверенным, что построенная система будет устойчива к различным непредсказуемым атакам.

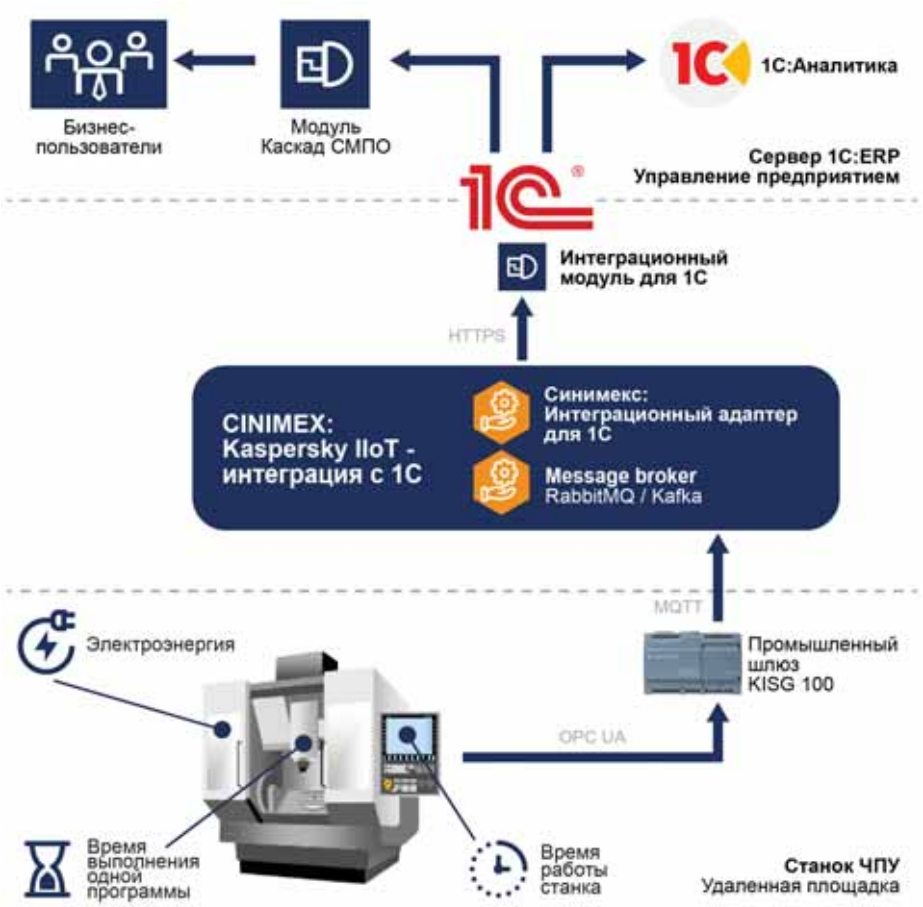

Рисунок. *Пример информационной системы, защищенной с помощью кибериммунного устройства*

Пример кибериммунитета

Для иллюстрации принципов построения кибериммунных систем можно рассмотреть пример решения, предложенного нашими компаниями при организации защищенного взаимодействия с промышленным оборудованием (см. рисунок). В этой конфигурации кибериммунный шлюз взаимодействует с промышленным оборудованием по протоколу OPC UA. Далее шлюз преобразовывает сообщения от оборудования в стандартный формат IP и передает их во внешний мир по промышленному протоколу MQTT, который гарантирует доставку сообщений в корпоративные системы. Для работы такого шлюза необходимо развернуть в целевой схеме подключения MQTT Broker, который и обеспечивает администрирование и доставку сообщений в виде «бизнес-событий». Последние загружаются в учетные системы заказчика и в дальнейшем используются в работе систем управления производством. В этом случае кибериммунное устройство за счет преобразования протоколов обеспечивает разделение сегментов промышленной и офисной сетей.

Мы разработали специальный продукт «Синимекс: Kaspersky IIoT-интеграция с 1С» – легковесный ETL-движок – для подключения кибериммунной платформы на базе KasperskyOS производства «Апротех» к решениям на базе «1С:ERP». Ядро решения входит в реестр российского ПО и сертифицировано «1С».

Особенность внедрения первых проектов заключалась в том, что одним из компонентов целевой схемы был программно-аппаратный комплекс (ПАК), т. е. физическое устройство, выполняющее функции шлюза между промышленным и офисным сегментами сети. Необходимо было обеспечить условия для его работы: организовать подключение к аппаратным стендам в промышленной сети, обеспечить настройку ПО на кибериммунной платформе.

Поскольку задача интеграции в подобных проектах связана с подключением промышленных станков и прочего оборудования, находящегося в закрытом контуре предприятия, то нужно быть готовым работать на территории заказчика в полном соответствии с требованиями ИБ, а для проведения тестирования необходимо настроить эмуляторы оборудования (для этого тоже нужны соответствующие компетенции).

Особенности кибериммунных решений

В целом при проектировании своих решений мы руководствуемся принципами и методологиями, наработанными за многие годы внутри компании. Чтобы решение на базе KasperskyOS было кибериммунным, при его создании необходимо следовать специальной методологии:

- четко определить цели безопасности (например, конфиденциальность данных), а также условия, в которых будет эксплуатироваться система;
- разделить решения на изолированные домены безопасности, учитывая функциональность и степень доверия к каждому из них;
- обеспечить контроль информационных потоков между этими доменами, разрешая только заданные виды взаимодействий.

Для интегратора, который занимается построением промышленных систем, использование кибериммунного устройства в общей схеме подключения снимает значительную часть вопросов обеспечения ИБ – они решаются на уровне программно-аппаратного комплекса, незначительно замедляя работу основных систем.

Если говорить про конкретное устройство, которое мы использовали в своих проектах, то существенным преимуществом оказались встроенные возможности ПАК транслировать поток данных из протокола OPC UA в события MQTT. Это позволяет на аппаратном уровне сразу «из коробки» упростить реализацию целевой интеграционной схемы для определенного класса задач – автоматизировать передачу большого потока информации от промышленного устройства в систему мониторинга, гарантировать ее целостность, конфиденциальность и доставку, а также обеспечить минимальную задержку. Устройство выступает в роли диода данных, однако его функционал может быть несколько шире. Наложенные средства защиты целостности и конфиденциальности не смогли бы работать на скоростях, необходимых для технологических процессов.

В рамках внедрения кибериммунных систем мы выполняем комплекс работ, связанных как с безопасностью, так с анализом и хранением данных производственного процесса, получаемых с промышленного оборудования. Например, проект может включать в себя бесшовную интеграцию оборудования с их цифровыми двойниками и системами класса ERP, а также визуализацию и анализ данных производства на Dashboard, выявление значимых событий на уровне оборудования для своевременного реагирования.

Заключение

Кибериммунные решения интересуют в первую очередь российские предприятия с высокими требованиями к ИБ, например оборонные заводы, а также коммерческие предприятия, которые находятся на активном этапе цифровизации и стремятся обрабатывать события с использованием цифровых сервисов и ИТ-решений (в том числе от внешних разработчиков). Прозрачность производственных процессов, возможность анализа промышленных данных – типовые преимущества внедрения цифровизации производственных процессов, но это предъявляет дополнительные требования к обеспечению кибербезопасности.

Интерес промышленности к решениям данного класса со временем только возрастает.

Для компаний, которые планируют внедрять кибериммунную платформу или только работают над принятием такого решения, важно заранее провести анализ корпоративной инфраструктуры, в рамках которого эксперты интегратора проводят:

- оценку кибербезопасности текущей архитектуры;
- анализ соответствия требованиям регуляторов в области кибербезопасности;
- аудит существующих интеграционных решений.

По результатам обследования формируются архитектура целевой системы с использованием кибериммунных решений, включающая новые интеграционные механизмы и поэтапный план внедрения, который важен для безостановочной работы предприятия. Лучший вариант – проведение предварительного исследования теми инженерами, которые в дальнейшем будут его внедрять. В этом случае можно говорить о внедрении кибериммунного решения под ключ без необходимости привлекать дополнительные ресурсы третьих сторон. ■