KASPERSKY lab

KASPERSKY INDUSTRIAL CYBERSECURITY: ОБЗОР КОМПОНЕНТОВ РЕШЕНИЯ

www.kaspersky.ru/ics

РОСТ ЧИСЛА АТАК НА ПРОМЫШЛЕННЫЕ СИСТЕМЫ

Число кибератак на промышленные системы растет. Если недавно эта проблема носила умозрительный характер, сейчас она приобрела реальные очертания[1].67% процентов офицеров безопасности определяют уровень угроз для АСУ ТП как критический или высокий — таким образом, по сравнению с предыдущим годом, этот показатель увеличился на 43%[2].

За 2015 фискальный год специалисты ICS-CERT отреагировали на 295 киберинцидентов, связанных с атаками на критическую инфраструктуру в США. Этот показатель также оказался выше, чем годом ранее, — на 20%[3].

В последние три года риск прерывания цепочек поставок и нарушения производства стал первостепенной проблемой для деловых кругов всего мира. Сегодня на передний план выходит риск кибератак[4]. Особенно велика их опасность для организаций, эксплуатирующих промышленные системы или объекты критически важной инфраструктуры.

Нарушение промышленной безопасности чревато последствиями, выходящими далеко за рамки финансового ущерба и потери деловой репутации. Во многих случаях защита промышленных систем от киберугроз имеет критическое значение с экологической, социальной и макроэкономической точки зрения.

Операционные технологии и информационные технологии: в чем разница

Автоматизированные системы управления технологическими процессами (АСУ ТП) — собирательный термин, описывающий автоматизированные системы, которые контролируют производственный процесс. Термин АСУ ТП относится к широкому спектру компьютеров, специфических устройств управления и сетевых архитектур, используемых для контроля промышленных процессов в самых разных отраслях промышленности. АСУ ТП обычно включает в себя SCADA (Supervisory Control And Data Acquisition — диспетчерское управление и сбор данных), РСУ (распределенные системы управления) и ПЛК (программируемые логические контроллеры).

В терминах организационной системы все это можно разбить на две категории:

- Информационные технологии (IT) — системы, необходимые для достижения бизнес-целей.
- Операционные технологии (OT) — системы, необходимые для целей промышленной автоматизации.

Многие стратегии обеспечения IT-безопасности прежде всего ориентированы на защиту данных и базируются на модели **Конфиденциальность-Целостность-Доступность**. В операционных технологиях самое важное — непрерывность, поэтому защищаются не данные, а сам процесс производства. Другими словами, в промышленных сетях порядок приоритетов безопасности обратный: **Доступность-Целостность-Конфиденциальность**. Это определяет специфические потребности в области кибербезопасности — высочайший уровень безопасности для промышленных предприятий бесполезен, если он подвергает риску непрерывность (или целостность) процессов.

1 PwC: Global State of Information Security («Глобальное состояние информационной безопасности»), 2015 г.
2 SANS 2016 State of ICS Security Survey («Исследование о состоянии безопасности АСУ ТП»)
3 ICS-CERT Monitor, ноябрь-декабрь 2015 г.
4 Allianz Risk Barometer, 2015 г.

УГРОЗЫ И РИСКИ

Несмотря на то, что угрозы для АСУ ТП стали широко известными, многие модели обеспечения IT-безопасности основаны на устаревших предположениях, что для защиты промышленного предприятия достаточно физической изоляции систем (через так называемые «воздушные зазоры») и концепции security by obscurity (безопасность через неясность). Это далеко не так — в эпоху четвертой промышленной революции большинство промышленных сетей так или иначе доступны через интернет[5].

Масштабное исследование «Лаборатории Касперского», которое опиралось на данные облачной сети Kaspersky Security Network, показало, что большинство промышленных рабочих станций подвержены тем же угрозам, что и бизнес-системы (IT), включая троянцы, компьютерные черви, потенциально нежелательные и опасные программы и эксплойты, которые используют уязвимости ОС Windows.

Червь Kido (известный также как Conficker) не предназначался специально для атак на промышленные сети, однако его неоднократно там обнаруживали. Червь Kido может полностью перегрузить сети, вызывав остановку критически важных процессов Привычные методы обеспечения промышленной кибербезопасности не могут должным образом защитить от таких угроз: стратегии «воздушного зазора» или «безопасности через неясность» уже не отвечают реальности, ведь из-за облачных SCADA и веб-приложений «промышленные системы управления становятся все более похожими на пользовательские компьютеры»[6].

Растет число угроз для АСУ ТП со стороны программ-вымогателей. С 2015 по 2016 год эта категория угроз стала гораздо масштабнее и разнообразнее. Особенно опасны программы-вымогатели для промышленных сред — заражение этих систем может иметь сильный эффект и вызвать широкомасштабный ущерб. Это делает АСУ ТП привлекательной мишенью для злоумышленников. При этом программы-вымогатели, атакующие АСУ ТП, имеют свою специфику: вредоносное ПО нацелено не на шифрование файлов, а на прерывание технологического процесса или блокирование доступа к важнейшим активам.

Помимо угроз общего характера, промышленный сектор сталкивается с целенаправленными атаками и специализированным вредоносным ПО. Stuxnet, Citadel, Energetic Bear/Havex, Miancha, BlackEnergy, Irongate, PLC Blaster — этот список постоянно пополняется. И, как показали атаки Stuxnet и Black Energy, одного зараженного USB-накопителя или фишингового письма достаточно, чтобы злоумышленники преодолели «воздушный зазор» и проникли в изолированную сеть.

Многие специализированные атаки разворачиваются и на уровне корпоративной сети, и на уровне АСУ ТП. Примером может служить атака BlackEnergy на украинские электростанции, которая в декабре 2015 году привела к многочасовому отключению электричества. Для реализации этой атаки злоумышленники использовали несколько векторов. Сначала они получили доступ к учетным данным системы SCADA с помощью таргетированной фишинговой рассылки. Обладая этими данными доступа, они начали выключать электрораспределительную сеть. После этого они внедрили вредоносный модуль KillDisk, который уничтожил или перезаписал важные системные файлы в промышленной сети. Параллельно с этим, колл-центр поставщика электричества подвергся DDoS-атаке, и это помешало потребителям электроэнергии вовремя сообщить об отключениях.

5 ICS and their online availability (АСУ ТП и их доступность через интернет), «Лаборатория Касперского», 2016 г.

6 Can we learn from SCADA security incidents? (Чему могут научить инциденты кибербезопасности SCADA?), Европейское агентство по сетевой и информационной безопасности, 2016 г.

Помимо вредоносного ПО и целевых атак, промышленные организации сталкиваются с целым рядом угроз и рисков, направленных на людей, процессы и технологии. Как явствует из сказанного выше, недооценка этих опасностей может иметь серьезные последствия. «Лаборатория Касперского» разработала комплексный набор технологий, решений и сервисов, чтобы помочь своим клиентам предотвратить риски, включая следующие:

- ошибки операторов или подрядчиков (третьих сторон), работающих с системами SCADA;
- действия сотрудников (намеренные и случайные);
- несоблюдение требований регулирующих органов;
- неосведомленность о том, как расследовать инциденты и собирать о них достоверные данные;
- отсутствие отчетности по инцидентам.

Необходимость в специализированных решениях промышленной кибербезопасности

Только те поставщики защитных решений безопасности, которые понимают различия между промышленными системами и стандартными сетями коммерческих предприятий, могут предложить продукты, отвечающие уникальным потребностям систем ICS и операторов производственных инфраструктур. По мнению Forrester, промышленные предприятия, выбирающие поставщика решений безопасности, должны «ориентироваться на опыт специализированной работы в сфере промышленности»[7]. Аналитическая компания говорит о «Лаборатории Касперского» как об одном из немногих производителей, предлагающих специализированные решения в сфере промышленной безопасности, которые основаны на реальном опыте работы.

7 «Профессионалы в области кибербезопасности больше не могут не замечать угрозы для критической инфраструктуры» (S&R Pros Can No Longer Ignore Threats to Critical Infrastructure), исследование Forrester, 2014

«ЛАБОРАТОРИЯ КАСПЕРСКОГО» — НАДЕЖНЫЙ ПОСТАВЩИК РЕШЕНИЙ ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ

«Лаборатория Касперского» — признанный лидер в обеспечении кибербезопасности и защите промышленных систем[8]. Компания постоянно разрабатывает решения, которые успешно противостоят постоянно развивающимся угрозам для критически важных инфраструктур. Компания также помогает промышленных предприятиям, регулирующим органам и государственным учреждениям прогнозировать изменения в структуре угроз и противостоять атакам.

«Лаборатория Касперского» приобрела статус доверенного партнера и поставщика решений безопасности для ведущих промышленных предприятий, которые много лет пользуются ее защитой от вредоносного ПО. Кроме того, компания сотрудничает с крупнейшими поставщиками решений для промышленной автоматизации (Emerson, Rockwell Automation, Siemens и др.), чтобы обеспечить взаимную совместимость, а также создать специализированные процедуры и платформы сотрудничества, которые позволят защитить промышленные среды от существующих и возникающих киберугроз (в том числе комплексных целенаправленных атак).

«Лаборатория Касперского» развивает свой набор специализированных решений, удовлетворяющих специфические потребности промышленного сектора экономики. Эти решения обеспечивают защиту от киберугроз на всех уровнях промышленных систем (в том числе серверов SCADA, человеко-машинного интерфейса, рабочих станций, ПЛК и сетевых соединений), не влияя на непрерывность работы и стабильность технологического процесса.

Решение для защиты критической инфраструктуры Kaspersky Industrial CyberSecurity соответствует стратегии многоуровневой защиты, созданной «Лабораторией Касперского», и использует сочетание разных методов защиты. Помимо технологий и сервисов, защищающих систему на всех этапах, Kaspersky Industrial CyberSecurity обеспечивает безопасность за счет целого ряда средств, включая контроль целостности, предотвращение вторжений, а также оценку уязвимостей и защищенности от вредоносного ПО (см. схему ниже).

8 Справочное руководство по решениям в области безопасности операционных технологий, Gartner, 2016

KASPERSKY INDUSTRIAL CYBERSECURITY: СЕРВИСЫ

Набор экспертных сервисов, предлагаемый «Лабораторией Касперского», составляет важную часть решения Kaspersky Industrial CyberSecurity. В него входят обучение сотрудников, анализ защищенности промышленных сетей, интеграция решения, подготовка предложений по улучшению системы безопасности и расследование инцидентов безопасности.

Знания (обучение и аналитика)

Тренинги по кибербезопасности. Курсы для специалистов по IT-безопасности, операторов и инженеров АСУ ТП. В процессе тренинга участники получают понимание актуальных угроз и эффективных методов защиты от них.

Аналитические отчеты. Актуальные аналитические отчеты о состоянии защиты, подготовленные ведущими экспертами в области кибербезопасности и отвечающие потребностям клиента (например, о ПО и инфраструктуре).

Повышение осведомленности. Игровые тренинги для офицеров безопасности и инженеров. Тренинги повышают осведомленность об угрозах, специфических для промышленных сред, и повышают навыки противодействия таким угрозам. В частности, игра Kaspersky Industrial Protection Simulation моделирует реальные атаки на автоматизированные промышленные системы и показывает, на что необходимо обратить особенное внимание при защите критической инфраструктуры. Доступны версии для разных отраслей: очистка сточных вод, производство электроэнергии и др.

Экспертные услуги

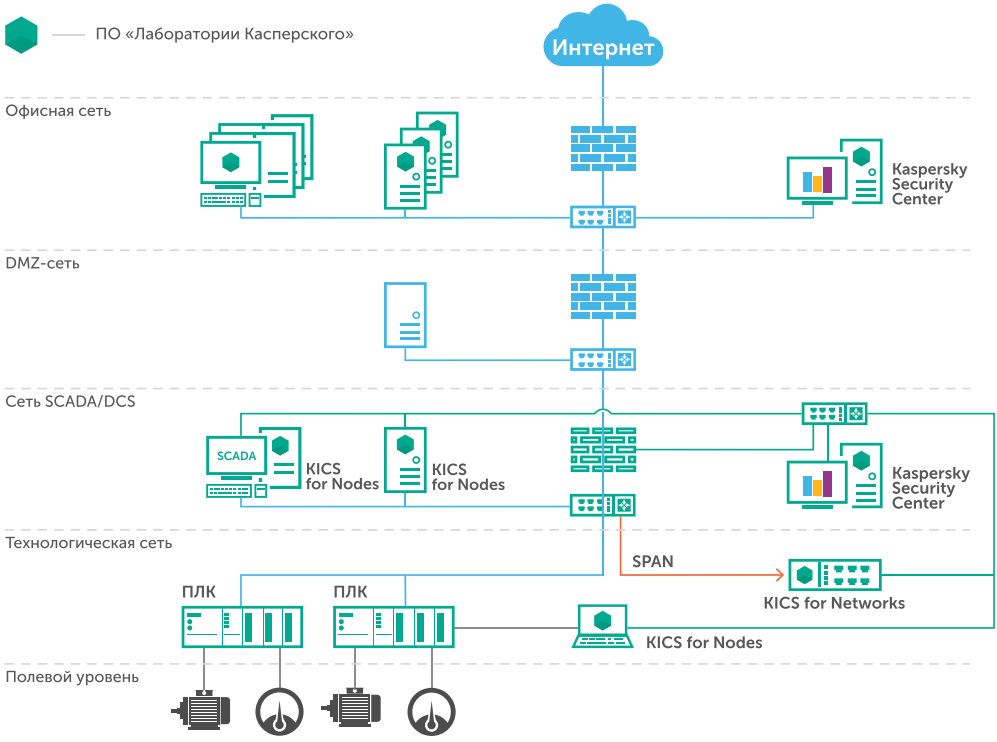
Оценка защищенности от киберугроз. Предварительная оценка защищенности инфраструктуры, которая проводится до установки решения и практически не влияет на производственные процессы. Это первый шаг к пониманию уровня защищенности от актуальных угроз и необходимых мер по защите инфраструктуры в контексте потребностей заказчика.

Интеграция решения. Помощь экспертов «Лаборатории Касперского» в интеграции решения в архитектуру с уникальными или специализированными компонентами (аппаратными и программными), в том числе для специфических алгоритмов, протоколов, ПО и оборудования. Специалисты «Лаборатории Касперского» могут адаптировать средства защиты к работе с существующими системами.

Расследование инцидентов. Услуги по анализу вредоносного ПО и устранению последствий инцидентов. В случае возникновения инцидента в области кибербезопасности эксперты «Лаборатории Касперского» помогут собрать и проанализировать данные, реконструировать инцидент на временной шкале, определить источник и характер угроз и разработать план восстановления системы. Кроме того, «Лаборатория Касперского» предлагает сервис анализа вредоносного ПО — в соответствии с собственными методиками эксперты проанализируют образец вредоносного ПО, его функции и поведение, а также дадут пошаговые рекомендации по удалению его из системы и откату вредоносных действий.

KASPERSKY INDUSTRIAL CYBERSECURITY: ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Чтобы обеспечить высочайший уровень защиты производственной инфраструктуры от атак любой направленности, нужно обезопасить и узлы, и сеть. Управление решением Kaspersky Industrial CyberSecurity — как и всеми защитными продуктами «Лаборатории Касперского» — осуществляется из единой консоли управления Kaspersky Security Center: это позволяет добиться оптимального контроля, простоты администрирования и прозрачности. Централизованное управление упрощает контроль безопасности не только различных уровней производственной инфраструктуры, но и прилежащих сетей корпоративной системы (см. рис. ниже).



KASPERSKY INDUSTRIAL CYBERSECURITY FOR NODES

Решение Kaspersky Industrial CyberSecurity для узлов создано специально для защиты от угроз, возникающих при использовании систем ICS/SCADA. Оно обеспечивает безопасность на уровне сервера ICS/SCADA, человеко-машинного интерфейса и инженерных систем, максимально предотвращая риск человеческого фактора, целенаправленных атак и диверсий. Решение совместимо с программными и аппаратными компонентами промышленных систем автоматизации, таких как SCADA, системы управления технологическими процессами (PCS) и распределенные системы управления (DCS).

Риски и угрозы	Защитные технологии «Лаборатории Касперского»
Запуск нежелательного ПО	Контроль программ (белые и черные списки); политики разрешения и запрета по умолчанию
Вредоносное ПО, в том числе атаки нулевого дня	Расширенные средства обнаружения вредоносного ПО и защиты от него; автоматическая защита от эксплойтов
Атаки на промышленные сети	Сетевой экран, системы обнаружения и предотвращения вторжений (IPS/IDS) и защита от сетевых атак (на уровне хоста)
Подключение нежелательных устройств	Контроль доступа к устройствам
Уязвимости в ПО промышленных систем	Оценка уязвимостей
Ложные срабатывания специального (промышленного) ПО	Сертификация ведущими поставщиками ICS-систем; система доверенных обновлений

Контроль целостности аппаратного и программного обеспечения

Благодаря тому, что конфигурация конечных точек в ICS-системах относительно статична, меры контроля целостности в таких системах оказываются гораздо более эффективными, чем в динамических корпоративных сетях. Решение Kaspersky Industrial CyberSecurity for Nodes содержит следующие технологии контроля целостности.

Контроль запуска программ и Контроль активности программ
Помимо прочего, механизмы контроля программ позволяют:

- контролировать установку и запуск приложений согласно белым и черным спискам;
- контролировать доступ приложений к ресурсам операционной системы: файлам, папкам, системному реестру и т. д.;
- контролировать все типы исполняемых файлов, используемые в среде Windows, включая файлы с расширением exe, dll, ocx, драйверы, элементы ActiveX, сценарии, интерпретаторы командных строк и драйверы режима ядра;
- обновлять данные о репутации приложений;
- использовать стандартные и заданные клиентом категории приложений для управления списками контролируемых приложений;

- выполнять тонкую настройку контроля приложений для различных пользователей;
- предотвращать работу в режимах, допускающих только обнаружение: блокировать любые приложения, не включенные в белые списки, или (в режиме «наблюдения») разрешать исполнение приложений, не включенных в белые списки, с обязательной регистрацией этой активности в Kaspersky Security Center, где может быть выполнена ее оценка.

Контроль доступа к устройствам
Управление доступом к съемным и периферийным устройствам и системным шинам на основе категорий и семейств устройств, а также идентификаторов конкретных устройств:

- поддержка политик белых и черных списков;
- точное назначение политик каждому отдельному пользователю или компьютеру либо группе пользователей или компьютеров;
- режим только предотвращения или только обнаружения.

Сетевой экран и защита от сетевых атак (на уровне хоста)

Настройка и исполнение политики доступа к сети для защищенных узлов, в том числе серверов, диспетчерских пультов и рабочих станций. Компонент обладает следующими основными возможностями:

- контроль доступа к портам и сетям с ограничениями;
- обнаружение и блокирование сетевых атак, запускаемых из внутренних источников (таких как ноутбуки подрядчиков), которые могут распространять вредоносное ПО, находящее и заражающее хост при его подключении к промышленной сети.

Автоматическая защита от эксплойтов

Компонент создает изолирующий слой, позволяющий защитить процессы SCADA от инъекции вредоносного кода в память и от изменений, таких как настройка передачи содержимого эксплойтами.

Проверка целостности ПЛК

Возможность дополнительно контролировать конфигурацию ПЛК при помощи периодической сверки со специально выбранным сервером или рабочими станциями, защищенными «Лабораторией Касперского». Результирующие контрольные суммы сравниваются с сохраненными значениями (Etalon); формируется отчет об отклонениях.

Расширенная защита от вредоносного ПО

Надежные технологии «Лаборатории Касперского» для обнаружения вредоносного ПО и защиты от него, адаптированные и оптимизированные для использования в средах, где потребляется значительное количество ресурсов и важна постоянная доступность системы. Компонент рассчитан на статичные или редко обновляемые инфраструктуры.

Для защиты от вредоносного ПО «Лаборатория Касперского» использует полный спектр технологий:

- обнаружение вредоносного ПО при помощи сигнатурного, эвристического и поведенческого анализа;
- обнаружение по запросу и во время обращения;
- обнаружение вредоносного кода в памяти (резидентного вредоносного ПО);

- обнаружение руткитов;
- максимальные возможности обнаружения вредоносного ПО (настраиваемое и направленное обнаружение) при помощи облачных сетей безопасности Kaspersky Security Network (KSN) и Kaspersky Private Security Network (KPSN).

Доверенные обновления

Проверки совместимости, выполняемые до выпуска баз данных или компонентов и до обновления ПО или конфигурации систем управления производственными процессами, с целью предотвратить воздействие обновлений защиты от вредоносного ПО на доступность защищаемой системы.

Потенциальные проблемы чрезмерного потребления ресурсов решаются при помощи одной или нескольких из следующих мер:

- «Лаборатория Касперского» испытывает обновление базы данных на совместимость с ПО поставщика SCADA на собственном тестовом оборудовании;
- поставщик системы SCADA выполняет испытание на совместимость;
- «Лаборатория Касперского» проверяет обновления антивирусной базы для клиента, интегрировав образы SCADA, рабочих станций, серверов и человеко-машинного интерфейса в собственное тестовое оборудование;
- обновления «Лаборатории Касперского» для защиты от вредоносного ПО испытываются на площадке клиента, и их развертывание автоматизируется при помощи Kaspersky Security Center.

Оценка уязвимостей

Средство пассивной оценки уязвимостей: выявление уязвимостей ПО и сообщение о них без нарушения технологических процессов.

Централизация развертывания, управления и контроля

Развертывание решения Kaspersky Industrial CyberSecurity for Nodes и управление им выполняется через центральную консоль, что позволяет:

- централизованно управлять политиками безопасности, а также назначать индивидуальные настройки защиты для различных узлов и групп;
- выполнять тестирование обновлений перед их развертыванием в сети, обеспечивая абсолютную целостность процессов;
- обеспечивать доступ на основе ролей с учетом политик безопасности и срочных мер.

KASPERSKY INDUSTRIAL CYBERSECURITY FOR NETWORKS

Решение «Лаборатории Касперского», созданное специально для защиты систем АСУ ТП от киберугроз, выполняет свои задачи на абстрактном уровне управления процессами. Оно анализирует и проверяет источники трафика, а также обеспечивает контроль целостности — как промышленной сети, так и процессов управления производством. В то же время множество встроенных дополнительных технологий обеспечивают эффективное обнаружение аномалий.

Решение Kaspersky Industrial CyberSecurity for Networks борется с многочисленными угрозами и рисками, характерными для промышленных систем.

Риски и угрозы	Защитные технологии «Лаборатории Касперского»
Отсутствие информации для специалистов по кибербезопасности о состоянии производственной сети и процессов	Обнаружение подозрительных событий в системах контроля процессов
Подключение несанкционированных сетевых устройств к промышленной сети	Проверка целостности сети, позволяющая выявлять среди подключенных устройств новые и неизвестные
Установление несанкционированных сетевых соединений в промышленной сети	Проверка целостности сети, позволяющая выявлять новые (несанкционированные и подозрительные) соединения между известными узлами сети
Причиняющие вред команды, отправляемые на ПЛК следующими источниками: • оператором, инженером или третьей стороной (подрядчиком, поставщиком) по ошибке • вредоносным ПО или злоумышленником (целевая атака)	Отслеживание обращений к ПЛК и от ПЛК; контроль команд и значений параметров технологического процесса
Отсутствие данных для расследования киберинцидентов и проведения криминалистического анализа	Отслеживание событий в технологической сети и их безопасная регистрация в журнале
Отсутствие информации для операторов SCADA об угрозах кибербезопасности	Оповещение операторов (через интеграцию с человеко-машинным интерфейсом) о подозрительных изменениях в параметрах технологического процесса
Отсутствие информации о действиях третьих сторон (подрядчиков, поставщиков) с активами системы ICS	Оповещение операторов (через интеграцию с человеко-машинным интерфейсом) о попытках конфигурирования ПЛК и опасных командах по управлению процессами

Пассивное инспектирование трафика в производственной сети

Решение Kaspersky Industrial CyberSecurity for Networks выполняет пассивный анализ аномалий сетевого трафика, оставаясь невидимым для злоумышленников. Для установки достаточно активировать или настроить зеркальное отражение порта; интеграция в существующую производственную инфраструктуру очень проста и выполняется через SPAN-порт уже используемого коммутатора или ответвителя сетевого трафика.

Архитектура, основанная на иерархии, и единая точка контроля

Сетевые датчики, пассивно соединенные с сегментом управляемой сети через SPAN-порт или ответвитель сетевого трафика, администрируются через единое устройство управления, обеспечивающее следующие возможности:

- сбор и сохранение информации о событиях от всех датчиков (информацию можно использовать для реагирования на инциденты, а также для проведения расследований и криминалистического анализа);
- сообщение обо всех выявленных событиях и аномалиях сторонним системам, включая SIEM, почтовые системы, серверы системного журнала, системы управления сетями (по протоколу SNMP);
- отслеживание общего здоровья системы;
- возможность управления через Kaspersky Security Center.

Целостность сети и мониторинг сети

Решение Kaspersky Industrial CyberSecurity for Networks позволяет идентифицировать все активы, соединенные по Ethernet в общей сети — в том числе серверы SCADA, человеко-машинный интерфейс, ПЛК и RTU. Все новые и неизвестные устройства, а также все коммуникации между ними определяются автоматически. Это позволяет службам IT-безопасности развивать и поддерживать собственную надежную базу сетевых активов, что безопаснее, чем использование уязвимых инструментов управления, которые часто становятся мишенью атак.

Достоверный мониторинг АСУ ТП

Решение «Лаборатории Касперского» предлагает надежную платформу для отслеживания передаваемых команд по управлению процессами, а также телеметрических данных. Среди прочего доступны следующие возможности:

- выявление любых команд, конфигурирующих ПЛК или изменяющих состояние ПЛК, включая команды остановки, паузы, изменения программы ПЛК, изменения прошивки ПЛК;
- контроль параметров и алгоритмов технологических процессов;
- защита от внешних угроз, а также снижение риска вмешательства сотрудников, обладающих специальными знаниями, таких как инженеры, операторы SCADA и другие внутренние участники с прямым доступом к системам.

Возможность криминалистического анализа

Решение «Лаборатории Касперского» обеспечивает заказчиков системой безопасного ведения журналов, содержащей средства для анализа данных и проведения криминалистического анализа. Дополнительное преимущество этой системы — способность предотвращать изменения системных событий.

Прозрачность активов промышленной сети

Решение Kaspersky Industrial CyberSecurity for Networks позволяет выявлять все активы, подключенные к сети Ethernet, в том числе серверы SCADA, HMI, инженерные рабочие станции, ПЛК и RTU.

Благодаря этому отделы IT-безопасности могут создавать собственные надежные и безопасные инвентарные перечни, не попадая в зависимость от потенциально уязвимых средств управления активами информационной и производственной систем, которые часто служат целью атак.

ДОПОЛНИТЕЛЬНЫЕ СЕРВИСЫ

Kaspersky Security Network (KSN)

Kaspersky Security Network — это облачная сеть со сложной распределенной структурой, выполняющая сбор и анализ данных об угрозах безопасности, поступающих с миллионов узлов по всему миру. KSN не только выявляет и блокирует новейшие угрозы и атаки «нулевого дня», но и помогает определять и заносить в черные списки источники интернет-атак, собирая данные о репутации веб-сайтов и приложений.

Подключать к сети KSN можно все корпоративные решения «Лаборатории Касперского», в том числе и промышленные. Основные возможности сети KSN:

- высокий уровень обнаружения;
- оперативное реагирование (традиционные решения на основе сигнатур реагируют на угрозы через несколько часов, с использованием KSN — через 40 секунд);
- более низкий уровень ложных срабатываний;
- сокращение потребления ресурсов решениями безопасности на локальном уровне.

Kaspersky Private Security Network (KPSN)

Для организаций с особыми требованиями к конфиденциальности данных «Лаборатория Касперского» создала сеть Kaspersky Private Security Network. Она обладает всеми преимуществами KSN, но без передачи информации за пределы корпоративной сети.

Сеть KPSN можно развернуть в собственном центре обработки данных любой организации, что позволяет внутренним IT-специалистам сохранять над ней полный контроль. Использование Kaspersky Private Security Network позволяет соблюдать требования, принятые в разных странах, и конкретные отраслевые нормативы.

Основные возможности сети KPSN

- Репутационный анализ файлов и URL-адресов: MD5-хэши файлов, регулярные выражения для проверки URL-адресов и модели поведения вредоносного ПО собираются в центральном хранилище, распределяются по категориям и оперативно передаются клиенту.
- Система управления записями (RMS): защитное ПО может ошибочно определять файлы и URL-адреса как доверенные или недоверенные. Система RMS помогает снизить количество ложных срабатываний, исправляя ошибки и выполняя постоянный анализ для повышения качества.
- Сбор и анализ данных при помощи облачных технологий.

Решения для защиты крупного бизнеса:
kaspersky.ru/enterprise