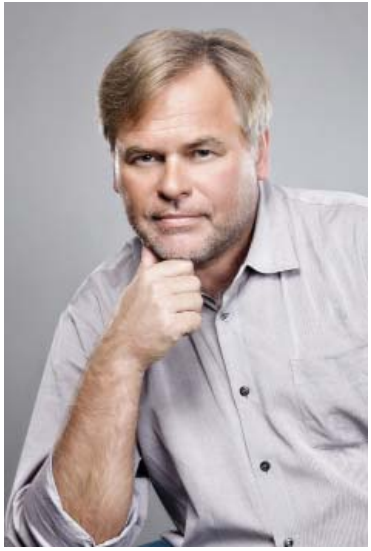
KASPERSKY lab

Стратегический подход к защите критических инфраструктур

KASPERSKY INDUSTRIAL CYBERSECURITY

2015



Нуждаются ли промышленные информационные сети в защите от кибератак? Еще недавно этот вопрос вряд ли обсуждался на советах директоров многих промышленных предприятий. Сначала непрерывность и доступность производственного процесса, а уже потом безопасность. Однако за последние несколько лет все изменилось. Ряд кибератак на промышленные объекты по всему миру показал, насколько уязвимы промышленные системы перед современным кибероружием и насколько важен вопрос информационной безопасности критической инфраструктуры. Стало очевидно, что простой физической изоляции уже недостаточно и пришла пора принимать более серьезные меры.

Мы давно работаем над созданием комплекса решений, способного обеспечить информационную безопасность на всех уровнях технологической сети. Мы понимаем, что защищать такие системы может быть не просто, но делать это надо обязательно, и делать надо максимально качественно. Это без преувеличения может быть вопросом жизни и смерти. Именно поэтому безопасность критической инфраструктуры – ключевой приоритет для нашей компании.

Евгений Касперский

Актуальные аспекты защиты критических инфраструктур

Число вредоносных атак на промышленные системы, в том числе на автоматизированные системы управления технологическими процессами (АСУ ТП) в последнее время значительно возросло. И если раньше физической изоляции между производственными системами и внешними сетями вполне хватало для обеспечения хорошего уровня защиты, то теперь это не так. Одного зараженного USB-накопителя может быть достаточно, чтобы вредоносное ПО преодолело защитный барьер и попало в изолированную сеть.

АСУ ТП требуют совершенно иного подхода к обеспечению информационной безопасности по сравнению с классической офисной IT-инфраструктурой. В корпоративных средах основное внимание уделяется сохранности конфиденциальных данных, а бесперебойная работа не настолько важна, как для АСУ ТП, где цена минуты простоя, как и любой другой ошибки, очень велика. Поэтому в обеспечении безопасности производственных процессов действует противоположный подход, при котором основной задачей является поддержание их непрерывности и оперативное устранение любых сбоев.

Кроме того, такие защитные решения должны отвечать требованиям государственных и отраслевых регуляторов, проектных организаций и интеграторов.

Подход «Лаборатории Касперского»

В основе подхода «Лаборатории Касперского» к защите промышленных объектов лежат многолетняя экспертиза в области кибербезопасности, глубокое понимание природы уязвимостей информационных систем, тесное сотрудничество с международными и отечественными регуляторами в области формирования требований к защите промышленных систем. Практической реализацией данного подхода является комплексное решение, повышающее доступность технологических процессов за счет обнаружения и предотвращения умышленных и неумышленных действий, которые могут привести к нарушению или остановке работы предприятий.

Для обеспечения информационной безопасности промышленных систем «Лаборатория Касперского» предлагает решение Kaspersky Industrial CyberSecurity, которое защищает индустриальную инфраструктуру промышленного объекта от киберугроз. Решение Kaspersky Industrial CyberSecurity разрабатывалось с учетом ключевых особенностей промышленных объектов; особое внимание при этом уделялось обеспечению непрерывности производственных процессов. Решение предназначено для защиты индустриальных сетей, построенных на базе технологии Ethernet. Широкие возможности настройки Kaspersky Industrial CyberSecurity позволяют сконфигурировать решение в точном соответствии с требованиями конкретного промышленного объекта.

KASPERSKY INDUSTRIAL CYBERSECURITY:

- Защищает производственные предприятия от киберугроз
- Обеспечивает безопасность индустриальных сетей и непрерывность производственных процессов
- Минимизирует время простоев и задержки технологических процессов
- Включает набор сервисов для максимально эффективной защиты предприятия

Kaspersky Industrial CyberSecurity: состав решения

Kaspersky Industrial CyberSecurity представляет собой комплексное решение, включающее набор функциональных компонентов и защитных технологий, а также ряд экспертных сервисов. Подбор оптимальной конфигурации защитных технологий и набора сервисов осуществляется после полного обследования системы кибербезопасности промышленного объекта экспертами «Лаборатории Касперского».

Гибкость выбора и настройки защитных компонентов решения позволяет реализовать защиту для различных составных частей АСУ ТП, таких как ПЛК, SCADA-серверы, HMI-панели, рабочие станции инженеров и операторов. Это обеспечивает получение первых результатов уже на первых этапах внедрения проекта.

Уникальный опыт экспертов «Лаборатории Касперского», применяемый в рамках сервисного предложения, обеспечивает качественный анализ состояния системы кибербезопасности индустриального объекта, эффективное внедрение и компетентную поддержку решения Kaspersky Industrial CyberSecurity на всех этапах жизненного цикла АСУ ТП, а также консультирование специалистов компании-клиента в любых вопросах противодействия киберугрозам. Это предложение оценят по достоинству:

- компании, которым требуется содействие в анализе текущего состояния системы кибербезопасности и определении областей, которые требуют модернизации;
- предприятия, уже реализующие стратегию защиты промышленного объекта от киберугроз и рассматривающие решения ведущих производителей;
- организации, столкнувшиеся с попытками нештатного воздействия на технологические процессы и нуждающиеся в экстренном анализе причин и расследовании инцидентов.

KASPERSKY INDUSTRIAL CYBERSECURITY

ФУНКЦИОНАЛЬНЫЕ КОМПОНЕНТЫ

МОНИТОРИНГ УЯЗВИМОСТЕЙ

ЗАЩИТА
ОТ ВРЕДОНОСНОГО ПО

КОНТРОЛЬ ЦЕЛОСТНОСТИ

ЦЕНТРАЛИЗОВАННОЕ
УПРАВЛЕНИЕ

СИСТЕМА ПРЕДОТВРАЩЕНИЯ
ВТОРЖЕНИЙ

ИНТЕГРАЦИЯ С ДРУГИМИ
РЕШЕНИЯМИ

СИСТЕМА РАССЛЕДОВАНИЯ
ИНЦИДЕНТОВ

СЕРВИСЫ

ОБУЧЕНИЕ

- ТРЕНИНГИ ПО ИБ
- АНАЛИТИЧЕСКИЕ ОТЧЕТЫ
- СИМУЛЯЦИЯ

ЭКСПЕРТНЫЕ СЕРВИСЫ

- ОЦЕНКА БЕЗОПАСНОСТИ
- РАЗРАБОТКА РЕШЕНИЯ
- СОПРОВОЖДЕНИЕ
- РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

Kaspersky Industrial CyberSecurity: функциональные компоненты

Все решения «Лаборатории Касперского» разрабатываются на единой технологической базе, что позволяет достичь максимальной эффективности защитных инструментов благодаря их тесной интеграции. Функциональные компоненты Kaspersky Industrial CyberSecurity построены на базе уникальных и зарекомендовавших себя в отрасли технологий, многие из которых имеют патенты по всему миру.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Все операции по управлению системой защиты предприятия осуществляются из единой консоли, которая обеспечивает централизованное выполнение следующих задач:

- развертывание систем и приложений;
- управление политиками безопасности;
- обновление антивирусных баз;
- разграничение прав доступа администраторов безопасности;
- настройка и формирование детальных отчетов о работе компонентов.

ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Эффективное сочетание сигнатурных методов, эвристического анализа и проактивной защиты обеспечивает многоуровневую защиту рабочих станций Windows® от вредоносного ПО. Использование локальной репутационной базы «Лаборатории Касперского», а также инструменты отмены (отката) вредоносных действий позволяют еще больше усилить систему безопасности, тем самым обеспечивая защиту от известных, неизвестных и сложных угроз.

МОНИТОРИНГ УЯЗВИМОСТЕЙ

Технологии «Лаборатории Касперского» производят анализ используемых на узлах индустриальной сети приложений или операционных систем на наличие уязвимостей и неустановленных обновлений и исправлений. Порядок устранения обнаруженных уязвимостей может быть приоритизирован вручную или автоматически.

КОНТРОЛЬ ЦЕЛОСТНОСТИ

Контроль целостности промышленной сети достигается за счет интегрированного взаимодействия следующих компонентов и технологий.

Пассивный анализ трафика

Трафик в промышленной сети обрабатывается в пассивном режиме, не оказывая никакого воздействия на технологическую сеть. Это позволяет легко интегрировать решение в индустриальную сеть через SPAN-порт или TAP-устройство без необходимости дополнительной переконфигурации, а также делает присутствие Kaspersky Industrial CyberSecurity незаметным для злоумышленников.

Контроль целостности сети

Компонент обеспечивает мониторинг целостности индустриальной сети, включая обнаружение новых устройств в сети и коммуникаций между устройствами.

Контроль целостности индустриального процесса

Компонент обнаруживает передачу программируемым логическим контроллерам (ПЛК) несанкционированных команд, а также попытки установки недопустимых значений параметров технологического процесса.

Контроль запуска приложений

Контроль программ с поддержкой динамических белых списков в режиме «Запрет по умолчанию» блокирует выполнение программ и загрузку модулей, не входящих в указанный список. Для удобства настройки и отладки поддерживается тестовый режим, позволяющий настроить политику и убедиться в ее работоспособности перед применением или обновлением режима «Запрет по умолчанию» в реальной среде.

Контроль подключения внешних устройств

Компонент определяет устройства, которым разрешены подключение и доступ к узлам технологической сети. Администраторы могут применять маски, создавая правила Контроля устройств, чтобы вносить в белый список несколько устройств.

Контроль целостности проектов ПЛК

Благодаря постоянному мониторингу состояния системы компонент обеспечивает обнаружение изменений проектов ПЛК (программируемого логического контроллера) и позволяет информировать о них специалиста по информационной безопасности.

Kaspersky Industrial CyberSecurity: функциональные компоненты

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Защита от сетевых атак и межсетевой экран

Компоненты мониторинга сетевой активности в технологической сети ограничивают сетевые подключения к ее узлам и блокируют подозрительную активность.

Защита от эксплойтов

Технология автоматической защиты от эксплойтов противодействует вредоносному ПО, использующему уязвимости в программном обеспечении для получения контроля над компьютером. Она позволяет выявлять характерные для них закономерности и блокировать их выполнение. Для этого производится контроль запуска исполняемых файлов уязвимых программ, а также мониторинг их активности.

СИСТЕМА РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ

Система протоколирования и хранения событий и система анализа данных, входящие в состав Kaspersky Industrial CyberSecurity – эффективный инструмент для оценки системы безопасности, который позволяет производить расследование инцидентов.

ИНТЕГРАЦИЯ С ДРУГИМИ РЕШЕНИЯМИ

Технологии и компоненты Kaspersky Industrial CyberSecurity позволяют осуществлять передачу событий в SIEM-системы, SCADA-системы, системы управления сетями, на сервер Syslog по специальным интерфейсам, а также предоставляют возможность отправки информации о событии по электронной почте. Это позволяет эффективно встроить решение Kaspersky Industrial CyberSecurity в существующие рабочие процессы организации.

Kaspersky Industrial CyberSecurity: сервисы

Важной составляющей Kaspersky Industrial CyberSecurity является набор экспертных сервисов, в рамках которых предоставляются услуги по обучению сотрудников компании-клиента, обследованию технологической сети, проектированию системы кибер-безопасности, формированию предложения по установке и настройке решения, а также по расследованию инцидентов безопасности.

ОБУЧЕНИЕ

Тренинги по ИБ

Обеспечение кибербезопасности индустриальных объектов требует не только внедрения автоматизированных программных инструментов защиты, но и обучения сотрудников компании-клиента, поскольку недостаточная осведомленность сотрудников в области кибербезопасности является одной из основных причин случайных заражений. «Лаборатория Касперского» проводит тренинги как для специалистов по информационной безопасности, так и для операторов и инженеров АСУ ТП. Слушатели тренингов получают информацию об актуальных киберугрозах, тенденциях их развития, а также эффективных средствах противодействия им.

Аналитические отчеты

Число угроз и их качественный состав меняются с каждым днем. Для повышения уровня защиты, эффективного реагирования на инциденты и противодействия кибератакам необходимо обладать актуальной информацией о существующих угрозах. «Лаборатория Касперского» предлагает услугу предоставления регулярных аналитических отчетов ведущих экспертов в области информационной безопасности. Отчеты адаптируются в соответствии с потребностями клиента, с учетом отрасли, программного и аппаратного обеспечения и пр.

Симуляция

«Лаборатория Касперского» предлагает обучающую игру, рассчитанную на руководителей и технических специалистов. Цель игры – повысить осведомленность об актуальных проблемах кибербезопасности АСУ ТП и способах их решения. В рамках игрового процесса симулируются кибератаки на системы промышленной автоматизации и демонстрируются основные проблемы обеспечения безопасности АСУ ТП. Игроку предлагается использовать широкий набор средств и мер. Реализованная в игре экономическая модель обучает процессу выбора оптимальной стратегии защиты, минимизирующей потери предприятия в результате кибератак. Предусмотрено несколько вариантов игры для различных сфер промышленной деятельности, в том числе отраслей водоочистки, генерации и передачи электроэнергии и пр.

Kaspersky Industrial CyberSecurity: сервисы

ЭКСПЕРТНЫЕ СЕРВИСЫ: ОЦЕНКА БЕЗОПАСНОСТИ

Оценка безопасности системы

Чтобы построить эффективную систему защиты индустриального объекта необходимо, в первую очередь, правильно идентифицировать возможные киберугрозы и провести анализ рисков, связанных с кибератаками. Чтобы помочь в этом, «Лаборатория Касперского» предлагает сервис по оценке защищенности индустриальных объектов. В рамках данного сервиса специалисты «Лаборатории Касперского» при содействии специалистов компаний-партнеров проводят анализ документации, регламентирующей требования к информационной безопасности, осуществляют обследование промышленной сети предприятия и интервьюирование сотрудников. На основе полученной информации разрабатывается актуальная модель угроз индустриального объекта, дается оценка рисков вероятных кибератак, а также будут предоставляться рекомендации по принятию мер для снижения выявленных рисков.

Тест на проникновение

«Лаборатория Касперского» предлагает сервис по проведению тестирования на проникновение. В рамках сервиса сертифицированные эксперты компании осуществляют тестирование промышленной системы на проникновение с учетом требований к доступности, целостности и конфиденциальности АСУ ТП в соответствии с международными стандартами, такими как PTES, NIST 800-115, OSSTMM и др. На основе полученной в рамках тестирования информации клиенту предоставляется отчет, содержащий список обнаруженных в оборудовании уязвимостей нулевого дня, оценку проведенных тестовых атак, а также рекомендации по устранению найденных уязвимостей.

Анализ архитектуры

При разработке систем промышленной автоматизации и их компонентов ключевые требования к системе кибербезопасности учитываются уже на этапе проектирования системы. «Лаборатория Касперского» предлагает сервис, в рамках которого эксперты в области кибербезопасности проводят анализ архитектуры промышленной системы клиента на этапе проектирования и разработки, формируют требования кибербезопасности, проводят моделирование киберугроз, оценивают риски эксплуатации обнаруженных уязвимостей, а также предлагают рекомендации по доработке архитектуры и реализации системы.

ЭКСПЕРТНЫЕ СЕРВИСЫ: РАЗРАБОТКА РЕШЕНИЯ

Разработка политик и процедур

«Лаборатория Касперского» совместно с компаниями-партнерами предлагает сервис по разработке политик и процедур кибербезопасности систем промышленной автоматизации клиента. Результатом выполнения данной услуги является пакет документов, которые регламентируют процесс внедрения и работы системы кибербезопасности с учетом особенностей технологических и бизнес-процессов, существующих в компании-клиенте.

Адаптация решения

Для систем автоматизации технологического процесса, имеющих уникальную в своем роде архитектуру или построенных на базе узкоспециализированных и малораспространенных в отрасли программно-аппаратных компонентов, «Лаборатория Касперского» предлагает услуги по адаптации рекомендуемых инструментов по обеспечению кибербезопасности с учетом особенностей таких систем. Например, в рамках сервиса осуществляется поддержка работы со специфическими программными и программно-аппаратными комплексами (в том числе SCADA, ПЛК) с учетом характерных для них уязвимостей, а также промышленных сетевых коммуникационных протоколов. Кроме того, осуществляется поддержка специфичных для компании-клиента алгоритмов контроля ключевых параметров управления технологическим процессом.

Kaspersky Industrial CyberSecurity: сервисы

ЭКСПЕРТНЫЕ СЕРВИСЫ: СОПРОВОЖДЕНИЕ

Техническая поддержка

В рамках сервиса технической поддержки специалисты «Лаборатории Касперского» помогают оперативно устранять любые технические проблемы, связанные с функционированием системы обеспечения кибербезопасности технологического процесса.

Тестирование обновлений

Предлагаемый «Лабораторией Касперского» сервис по тестированию обновлений компонентов системы кибербезопасности предназначен для проверки совместимости компонентов системы кибербезопасности со специфическими программно-аппаратными комплексами, используемыми на стороне клиента, до их внедрения в работающую систему. Это позволяет сохранить высокую скорость реакции на новые угрозы кибербезопасности без риска нарушения непрерывности технологического процесса.

Регулярная поддержка

Некоторые изменения в информационных системах промышленного объекта, например связанные с расширением производства, модернизацией существующих или введением новых систем автоматизации, могут потребовать дополнительной настройки и адаптации системы кибербезопасности. В рамках сервиса регулярной поддержки «Лаборатория Касперского» обеспечивает техническое обслуживание своих систем защиты на регулярной основе. Это подразумевает регулярный анализ системы защиты на соответствие требованиям инфраструктуры индустриального объекта и, если это необходимо, переконфигурирование или обновление функциональных компонентов Kaspersky Industrial CyberSecurity.

ЭКСПЕРТНЫЕ СЕРВИСЫ: РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

Анализ вредоносного ПО

«Лаборатория Касперского» предлагает сервис по анализу вредоносного ПО. Сервис рассчитан на организации, специалисты которых в состоянии самостоятельно обнаружить вредоносное ПО, попавшее в технологическую сеть. В рамках сервиса эксперты «Лаборатории Касперского» производят классификацию полученного у компании-клиента образца вредоносного ПО, анализируют его функции и поведение, а также разрабатывают рекомендации и план по устранению вредоносных действий. Вся собранная во время анализа информация предоставляется компании-клиенту в форме подробного отчета.

Реагирование на инцидент

В рамках расследования инцидента информационной безопасности специалисты «Лаборатории Касперского» осуществляют сбор и анализ данных, восстанавливают хронологию событий, определяют возможные источники и причины возникновения инцидента, а также формируют набор рекомендаций и мер по устранению последствий инцидента.

О «Лаборатории Касперского»

«Лаборатория Касперского» – крупнейшая в мире частная компания, работающая в сфере информационной безопасности, и один из наиболее быстро развивающихся вендоров защитных решений. Компания входит в четверку ведущих мировых производителей решений для обеспечения IT-безопасности пользователей конечных устройств (IDC, 2014). С 1997 года «Лаборатория Касперского» создает инновационные и эффективные защитные решения и сервисы для крупных корпораций, предприятий среднего и малого бизнеса и домашних пользователей. «Лаборатория Касперского» – международная компания, работающая почти в 200 странах и территориях мира; ее технологии защищают более 400 миллионов пользователей по всему миру. Более подробная информация доступна на сайте www.kaspersky.ru.

АО «Лаборатория Касперского»
www.kaspersky.ru

Решения для бизнеса:
www.kaspersky.ru/corporate

+7 (495) 737-34-12
sales@kaspersky.com