Kaspersky Industrial CyberSecurity: обзор компонентов решения

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity: обзор компонентов решения

Введение

Исторически сложилось так, что промышленные компании по всему миру по-разному подходят к защите своих информационных и операционных технологий (IT и OT). Большинство давно используют проверенные системы обнаружения нарушений безопасности и реагирования на инциденты в корпоративной инфраструктуре. Но в промышленной инфраструктуре они придерживаются традиционного подхода на основе «воздушного зазора». Между тем промышленные предприятия становятся все более «цифровыми»: активно инвестируют в интеллектуальные технологии и новые системы автоматизации и реализуют концепцию четвертой промышленной революции. Это приводит к исчезновению зазора между IT- и OT-средами, не позволяющего киберугрозам добраться до систем управления производственными процессами. Согласно исследованию Kaspersky ICS CERT, в 2019 году. доля промышленных компьютеров, на которых были обнаружены вредоносные объекты, достигла 46,4%[1].

О каких угрозах идет речь?

В первую очередь, всегда есть риск случайного заражения обычным вредоносным ПО. Необязательно быть главной целью киберпреступников, чтобы стать их жертвой. Банковский троянец или программа-вымогатель, случайно попавшие в автоматизированные системы управления технологическим процессом (АСУ ТП) с помощью зараженного флеш-накопителя или фишингового письма, могут серьезно навредить бизнесу. И хотя случайные заражения происходят не так часто, очевидно, что задавшийся целью киберпреступник также может проникнуть в промышленную сеть и нанести ощутимый ущерб производственным процессам, дорогостоящему оборудованию или украсть ценную информацию.

Как комплексно защитить АСУ ТП?

1. Защита промышленных рабочих мест для предотвращения случайного заражения и целенаправленных вторжений.
2. Мониторинг промышленных сетей и обнаружение аномалий для выявления вредоносных действий на уровне программируемых логических контроллеров (ПЛК).
3. Тренинги для сотрудников, позволяющие минимизировать число инцидентов и влияние человеческого фактора.
4. Специальные сервисы для исследования инфраструктуры, проведения экспертного анализа и минимизации ущерба от инцидентов.

1 Ландшафт угроз для систем промышленной автоматизации. Статистика за второе полугодие 2019., Kaspesky ICS CERT https://ics-cert.kaspersky.ru/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-overall-global-statistics-h2-2019/

Что предлагает «Лаборатория Касперского»?

Kaspersky Industrial CyberSecurity «Лаборатории Касперского» – это набор специализированных продуктов и сервисов, призванных обеспечить кибербезопасность промышленных организаций. Решение помогает реализовать комплексный подход к кибербезопасности на всех уровнях, начиная с анализа защищенности и тренингов для сотрудников и заканчивая передовыми технологиями защиты АСУ ТП и реагированием на инциденты.

Компоненты Kaspersky Industrial CyberSecurity

В 2020 г. «Лаборатория Касперского» была отмечена в четырех категориях отчета Gartner по промышленной безопасности«Competitive Landscape: Operational Technology Security»[2], в частности:

- защита конечных узлов АСУ ТП;
- мониторинг промышленных сетей;
- обнаружение аномалий, реагирование на инциденты, отчетность;
- сервисы промышленной кибербезопасности[2]

ARC Advisory Group отмечает, что «Лаборатория Касперского» предлагает уникальную комбинацию машинного обучения, аналитических данных и экспертизы специалистов, которая помогает обеспечить адаптивную защиту против любого вида киберугроз[3].

Исследование Forrester[4] показало, что окупаемость инвестиций в Kaspersky Industrial CyberSecurity для компании составляет 368% без учета дополнительных выгод, таких как поддержка экспертов и уверенность в безопасности организации.

2 Gartner: Competitive Landscape: Operational Technology Security, март 2020 г. https://ics.kaspersky.com/KICS-cited-in-Gartnercompetitive-landscape-OTsecurity

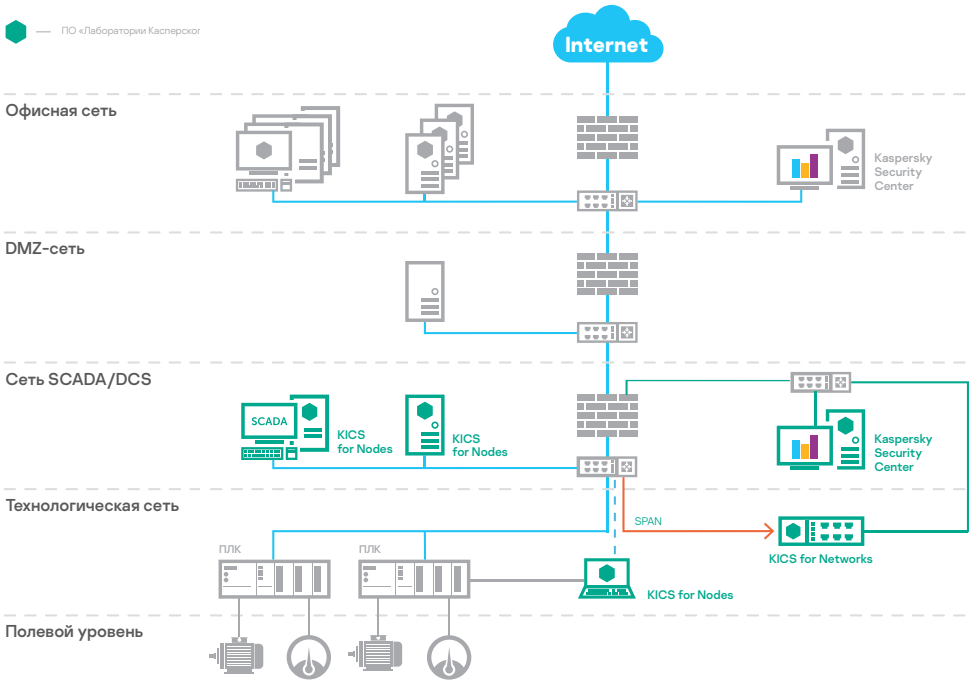
3 Arc Advisory: Kaspersky Moves Forward with Improved Cybersecurity Solutions, 2018 г.

4 Forrester Research: The Total Economic Impact™ of Kaspersky Industrial CyberSecurity, апрель 2019 г. https://www.kaspersky.com/ forrester-tei-for-kics

Продукты

Продукты в составе Kaspersky Industrial CyberSecurity (KICS) предназначены для комплексной защиты промышленной инфраструктуры вашей организации. KICS for Nodes защищает промышленные рабочие места, в то время как KICS for Networks следит за безопасностью промышленных сетей.

Развертывание компонентов Kaspersky Industrial CyberSecurity



KICS for Networks

KICS for Networks – решение для мониторинга промышленных сетей, подключаемое пассивно к сети АСУ ТП в виде программного обеспечения или виртуального устройства.

Преимущества

- ✓ **Обнаружение устройств:** пассивная идентификация и учет устройств в промышленной сети
- ✓ **Deep Packet inspection (DPI):** анализ телеметрии технологических процессов практически в режиме реального времени
- ✓ **Контроль целостности сети:** обнаружение несанкционированных хостов и потоков в сети
- ✓ **Система обнаружения вторжений:** оповещения о вредоносной активности в сети
- ✓ **Контроль команд:** проверка команд, передаваемых по промышленным протоколам
- ✓ **Поддержка внешних систем:** обнаружение угроз внешними системами благодаря интеграции через API
- ✓ **Использование машинного обучения для обнаружения аномалий (MLAD):** позволяет выявлять аномалии в цифровых и физических процессах с помощью телеметрии в режиме реального времени и обработки исторических данных (рекуррентная нейронная сеть)

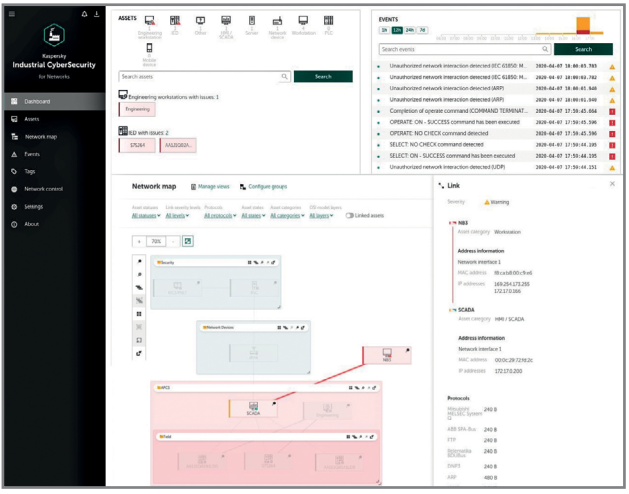
KICS for Networks выявляет аномалии и вторжения в АСУ ТП на ранних этапах и обеспечивает необходимые контрмеры для предотвращения ущерба технологическим процессам.

Возможности продукта не зависят от используемого промышленного модуля, поэтому клиенты не ограничены в выборе поставщиков для своей инфраструктуры.

Интерфейс KICS for Networks включает панель управления, данные которой обновляются в режиме реального времени, и карту сети, что позволяет удобно работать с устройствами предприятия и событиями безопасности.

Пример модуля KICS for Networks

Интерфейс KICS for Networks



KICS for Nodes

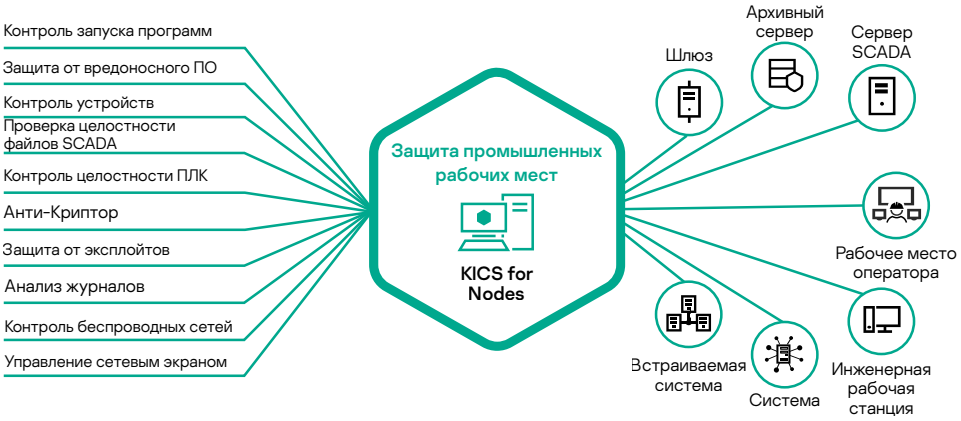
Kaspersky Industrial CyberSecurity for Nodes – продукт для защиты конечных узлов промышленной среды, предлагаемый в виде ПО для компьютеров на базе Windows и Linux.

Преимущества

- ✓ **Незначительное влияние на защищаемые устройства**
- ✓ **Высокая совместимость**
- ✓ **Расширенная защита от вредоносного ПО**
- ✓ **Контроль среды**

Kaspersky Industrial CyberSecurity for Nodes позволяет минимизировать потребление ресурсов. Благодаря модульной архитектуре этого продукта можно устанавливать только необходимые защитные компоненты. При этом они могут быть сконфигурированы как для режима предотвращения угроз, так и только для обнаружения. Это отличный подход для низкопроизводительных систем, которым требуется вся доступная вычислительная мощность.

Возможности Kaspersky Industrial CyberSecurity for Nodes и поддерживаемые конечные узлы



«Мы выбрали своим партнером “Лабораторию Касперского”, поскольку оказалось, что Kaspersky Industrial CyberSecurity можно развернуть без прерывания наших операций, и к тому же это решение совместимо с нашими системами управления».

Ян Хоубен, директор завода AGC Glass Germany GmbH

KICS for Nodes защищает промышленные узлы от различных типов киберугроз, которые могут быть вызваны человеческим фактором, вредоносным ПО, целевыми атаками и диверсиями. Продукт совместим с программными и аппаратными компонентами промышленных систем автоматизации, таких как SCADA, ПЛК и РСУ.

Kaspersky Security Center

Kaspersky Security Center – это решение для централизованного управления безопасностью. Оно обеспечивает простоту контроля и прозрачность не только для промышленных уровней инфраструктуры на множестве объектов, но и для окружающих корпоративных сетей.

Преимущества

✓ **Управление системами**
- Централизованный сбор системных данных
- Централизованное развертывание ПО
- Мониторинг уязвимостей и управление исправлениями
- Расширенные клиентские средства управления

✓ **Управление политиками**
- Централизованное управление политиками безопасности
- Удаленное планирование и выполнение задач

✓ **Отчетность и уведомления**
- Журнал событий
- Информативная панель управления и отчеты
- Уведомления по электронной почте и SMS

✓ **Интеграция с SIEM-системами**
- Arcsight, Splunk, Qradar
- Syslog-сервер

✓ **Интеграция с человеко-машинным интерфейсом**

✓ **Интеграция с панелью управления MES**
- Отправка информации о состоянии безопасности на хост, совместимый со стандартом IEC 104/ OPC 2.0

Сервисы

Набор экспертных сервисов, предлагаемый «Лабораторией Касперского», составляет важную часть решения Kaspersky Industrial CyberSecurity. В него входят обучение сотрудников, анализ защищенности промышленных сетей, расследование инцидентов безопасности и другие сервисы.

Экспертные сервисы

- **Оценка защищенности от киберугроз.** «Лаборатория Касперского» проводит оценку промышленной кибербезопасности, куда входят внешнее и внутреннее тестирование на проникновение, оценка защищенности промышленной инфраструктуры, и все это – при минимальном влиянии на производственные процессы. Эксперты «Лаборатории Касперского» предоставляют важную информацию об инфраструктуре компании с точки зрения кибербезопасности и рекомендации по укреплению защиты АСУ ТП.
- **Анализ угроз (Threat Intelligence).** Актуальные аналитические данные, собранные экспертами «Лаборатории Касперского», помогают клиенту укрепить защиту от промышленных целевых кибератак. Они предоставляются в виде потоков данных или персонализированных отчетов и полностью удовлетворяют потребности конкретных клиентов в соответствии с региональной и отраслевой спецификой, а также параметрами программного обеспечения АСУ ТП.

«Мы высоко ценим опыт „Лаборатории Касперского" в области обеспечения кибербезопасности промышленных систем, высокий профессионализм и комплексность их решения по сравнению с другими поставщиками. Все это позволило создать благоприятные условия для развития целостной стратегии безопасности в нашей компании».

Ондрей Сикора, менеджер C&A в Plzeňský Prazdroj

«Прохождение тренинга „Лаборатории Касперского“ стало очень важным и своевременным шагом, с учетом текущей ситуации с защитой критической инфраструктуры в Казахстане».

Нурлан Кулышев, специалист по ИТ «КазМунайТениз».

«Решение Kaspersky Industrial CyberSecurity учитывает реальные потребности нашего предприятия и отвечает основным требованиям по обеспечению кибербезопасности технологических процессов».

Сергей Слаута, директор дирекции по автоматизации технологических процессов НЛМК

- **Реагирование на инциденты.** В случае возникновения киберинцидента 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.

Тренинги для сотрудников разных уровней

- **Тренинги по промышленной кибербезопасности.** Интерактивные модули очного и онлайн-обучения, а также игровые тренинги для сотрудников, взаимодействующими с промышленными компьютерными системами, и их руководителей. Участники знакомятся с актуальным ландшафтом угроз и векторами атак, характерными для промышленных сред, изучают практические сценарии и приобретают навыки кибербезопасной работы. Очный курс может быть адаптирован в зависимости от потребностей заказчика и проведен за один либо два дня.

- **Программы для обучения специалистов.** Обучающие модули, посвященные тестированию на проникновение и цифровой криминалистике в АСУ ТП, создавались специально для профессионалов в сфере кибербезопасности. Участники приобретают экспертные навыки, требуемые для проведения комплексного тестирования на проникновение или криминалистического анализа в промышленных средах. По итогам прохождения тренинга выдаются сертификаты.

Всё о кибербезопасности ICS:
https://ics-cert.kaspersky.ru
https://ics.kaspersky.ru/

#Kaspersky
#BringontheFuture

www.kaspersky.ru

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* World Leading Internet Scientific and Technological Achievement Award at the 3rd World Internet Conference

** China International Industry Fair (CIIF) 2016 special prize