Анализ защищенности систем безопасности АСУ ТП

Kaspersky ICS Security Assessment

kaspersky активируй будущее

Современные вызовы безопасности АСУ ТП

- Устаревшие и проприетарные промышленные решения с уязвимостями, низкое качество обнаружения угроз и отсутствие продуктов для защиты от них
- Финансовые потери от атак: нарушение промышленных процессов или утрата контроля над ними, затраты на восстановление после инцидента и штрафы со стороны регулятора
- Сложности в интеграции IT- и OT-систем, включая ошибки конфигурации, конфликты ПО и угрозы безопасности
- Дефицит специалистов, необходимость поддержания актуальности их знаний и навыков в сфере безопасности

Повышение устойчивости промышленных сред к киберугрозам

Долгое время стандартом защищенности АСУ ТП считалась их функциональная безопасность, то есть предотвращение аварий на производстве, человеческих жертв и загрязнения окружающей среды. Информационная безопасность ограничивалась же изоляцией сети и ее защитой от физического воздействия. Однако интеграция систем поддержки, телеметрии и других решений с OT- и IT-сетями расширила поверхность атаки, повысив риски для уязвимых решений АСУ ТП. При этом специалистам SOC не хватает инструментов для полноценного контроля над всей инфраструктурой. В этих условиях предприятиям следует пересмотреть свои подходы к защите производственных систем. Так или иначе, информационная безопасность АСУ ТП тесно связана с функциональной: успешная хакерская атака может привести к аварии на производстве.

~40% компьютеров АСУ ТП по всему миру подверглись атакам вредоносного ПО с начала 2024 года[1]

Сервис анализа защищенности промышленных систем помогает выявить и оценить потенциальные риски в OT-инфраструктуре, определить уровень защиты промышленных сетей, а также возможные угрозы для критически важных систем.

Десятилетний опыт в сфере анализа защищенности АСУ ТП, подтвержденный сертификатами от профильных организаций, гарантирует высокий профессионализм экспертов «Лаборатории Касперского» и актуальность их знаний.

Подход «Лаборатории Касперского» к анализу защищенности промышленных систем

Наш подход основан на эталонной модели Пердью и предусматривает использование следующих методов:

1

Анализ защищенности АСУ ТП

Инвентаризация активов в контексте безопасности, анализ уязвимостей и подготовка рекомендаций по защите промышленной сети и средств автоматизации

2

Внутреннее тестирование на проникновение[2]

Выявление возможных путей проникновения в промышленную сеть через корпоративную

3

Внешнее тестирование на проникновение[2]

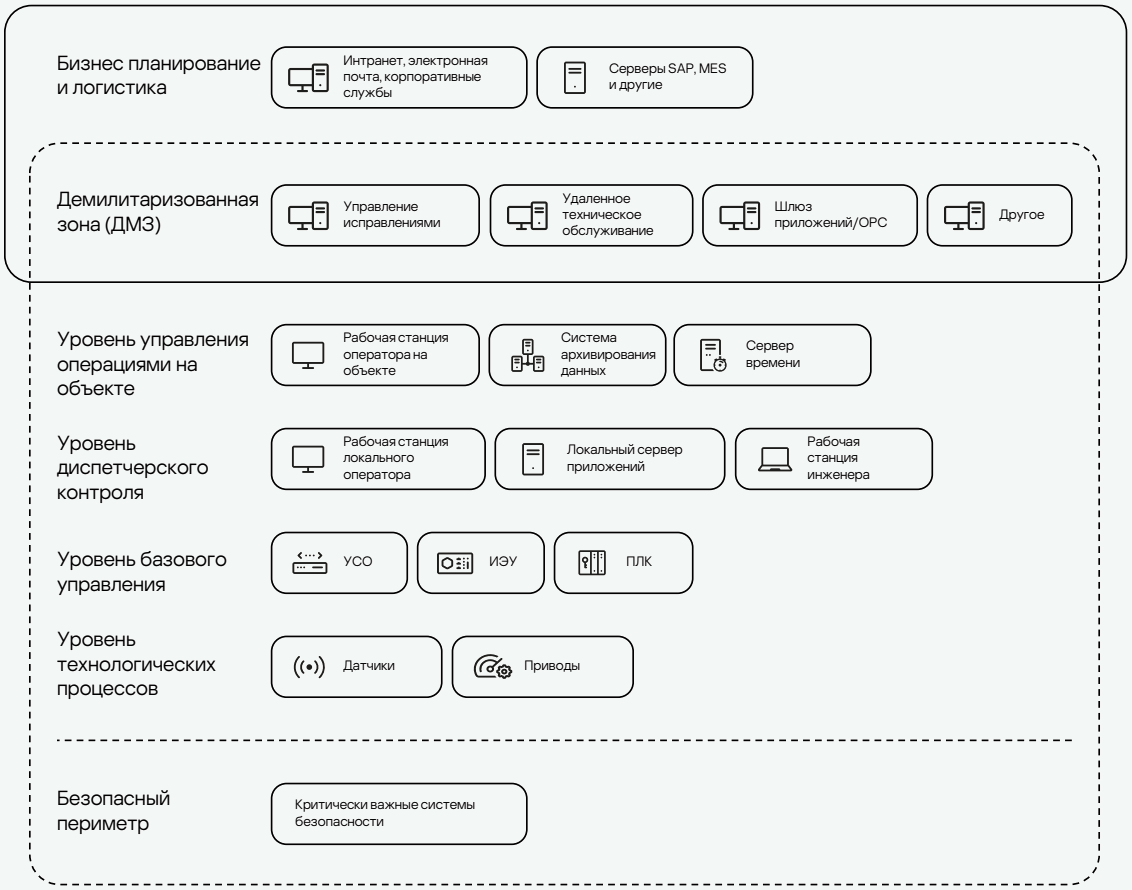
Поиск возможностей проникновения в корпоративную сеть через интернет

Мы используем методы черного, серого и белого ящиков, чтобы провести максимально полный анализ защищенности.

[1] Статистика Kaspersky ICS CERT. Ознакомиться с цифрами можно по ссылке

[2] Сервис тестирования на проникновения можно приобрести отдельно. Узнайте больше о Kaspersky Penetration Testing по ссылке

Модель Purdue



Тестирование на проникновение на корпоративном сегменте инфраструктуры (IT)

Анализ защищенности промышленных систем на производственном участке инфраструктуры (OT)

Как мы это делаем

1

Подготовка

Определение объема работ, целей и ограничений проекта

2

Удаленный анализ

Анализ файлов конфигурации и интервью с ключевыми участниками проекта

3

Работа на объекте

Анализ инфраструктуры

4

Подготовка отчетности

Оформление и представление результатов

5

Подведение итогов

Встреча для обсуждения результатов анализа

Результаты анализа защищенности АСУ ТП

Общий отчет

Аналитический отчет

Подробный технический отчет

- Моделирование угроз и приоритезация уязвимостей
- Моделирование атак на основе известных угроз
- Безопасная стандартная конфигурация для сокращения поверхности атаки
- Взаимодействие с поставщиком/производителем для повышения безопасности
- Использование экспертных знаний и машиночитаемых данных для эффективного мониторинга и реагирования
- Оценка возможных последствий атак для технологических процессов
- Интеграция защитных технологий в промышленные решения
- Подготовка инструкций по безопасной настройке промышленных систем
- Совместная работа с производителем над устранением уязвимостей
- Проверка безопасной конфигурации производителем
- Определение поверхности и возможных последствий атаки

Благодаря Kaspersky ICS Security Assessment вы можете:

Усилить защиту локальных систем

Повышение уровня защиты операторов, инженеров и другого персонала

Предотвратить сбои оборудования

Выявление уязвимостей, которые могут использовать злоумышленники для нарушения работы сборочных линий, производственного оборудования или роботизированных систем

Защитить интеллектуальную собственность

Пресечение кражи технологических схем, проектов и программ

Обеспечить качество и безопасность продукции

Предотвращение нарушений производственных процессов, которые могут повлиять на качество продукции

Важные преимущества, которые следует учесть при выборе сервиса анализа защищенности систем безопасности АСУ ТП

Экспертиза в разных отраслях

Наши сертифицированные эксперты обладают глубокими знаниями и практическими навыками, которые позволяют им эффективно работать с промышленным оборудованием и инфраструктурами в различных отраслях, включая железнодорожную и нефтегазовую промышленность, энергетику, промышленное производство и другие.

Проверенная методология тестирования

Наша методология основана на опыте сотен реализованных проектов. Тестирование может включать подготовительный этап в лабораторных, учебных или других симулированных условиях, чтобы минимизировать риски для работающего производства.

Практические рекомендации

В результате анализа вы получите подробный анализ выявленных рисков и уязвимостей с конкретными шагами по их устранению.
Мы объясним их влияние на производственные процессы, чтобы вы могли внедрить эффективные меры защиты.

Соответствие мировым стандартам

Мы руководствуемся международными стандартами и принятыми в отрасли методиками, включая NIST, CIP, ISA и другие.

Kaspersky ICS Security Assessment

Подробнее

Разработано экспертами

Security Services

www.kaspersky.ru

#kaspersky
#активируйбудущее