ПРОМЫШЛЕННАЯ КИБЕР-БЕЗОПАСНОСТЬ: ЗАЩИТА САМОГО УЯЗВИМОГО ЗВЕНА

С помощью уникальной экспертизы и специализированных технологий мирового уровня «Лаборатория Касперского» защищает предприятия от инцидентов промышленной кибербезопасности.

В последние годы заметно возросло количество кибератак на промышленные системы, в том числе на автоматизированные системы управления технологическими процессами (АСУ ТП) и системы диспетчерского контроля и сбора данных (SCADA).

Нашумевшие атаки Stuxnet и BlackEnergy продемонстрировали, что зараженного USB-накопителя или фишингового письма достаточно, чтобы злоумышленники преодолели физическую изоляцию сети (так называемый «воздушный зазор»). Традиционных мер безопасности уже недостаточно для защиты промышленных сред от киберугроз.

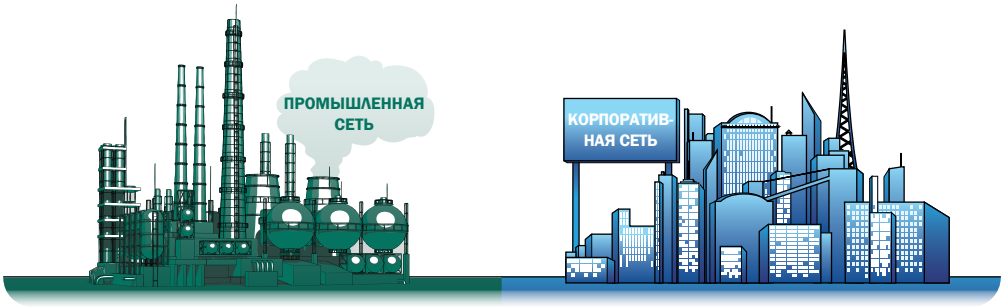
В течение последних четырех лет риск прерывания цепочки поставок и нарушения производства признается во всем мире главной проблемой промышленных корпораций. Поэтому неудивительно, что кибербезопасность приобретает особую значимость[1].

Особенно велика опасность для организаций, эксплуатирующих промышленные системы или объекты критически важной инфраструктуры.

Промышленная кибербезопасность требует особого подхода

Несмотря на существование общих угроз, требования к кибербезопасности для сред АСУ ТП и обычных коммерческих организаций очень сильно различаются.

В корпоративных средах важна в первую очередь защита конфиденциальных данных, а в промышленных системах, где каждая минута простоя и каждая ошибка могут вызвать непоправимые последствия, главный приоритет — обеспечение бесперебойной работы. Поэтому компаниям, управляющим промышленными средами, нужно особенно ответственно подходить к выбору поставщика защитных решений.



В промышленной кибербезопасности приоритеты стоят в обратном порядке по сравнению с обычными корпоративными системами, а именно: доступность, целостность, конфиденциальность.

1 Прогноз рисков Allianz Risk Barometer, 2016 г.

РЕШЕНИЯ ДЛЯ ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ ДОЛЖНЫ ВКЛЮЧАТЬ ТРИ КЛЮЧЕВЫХ КОМПОНЕНТА:

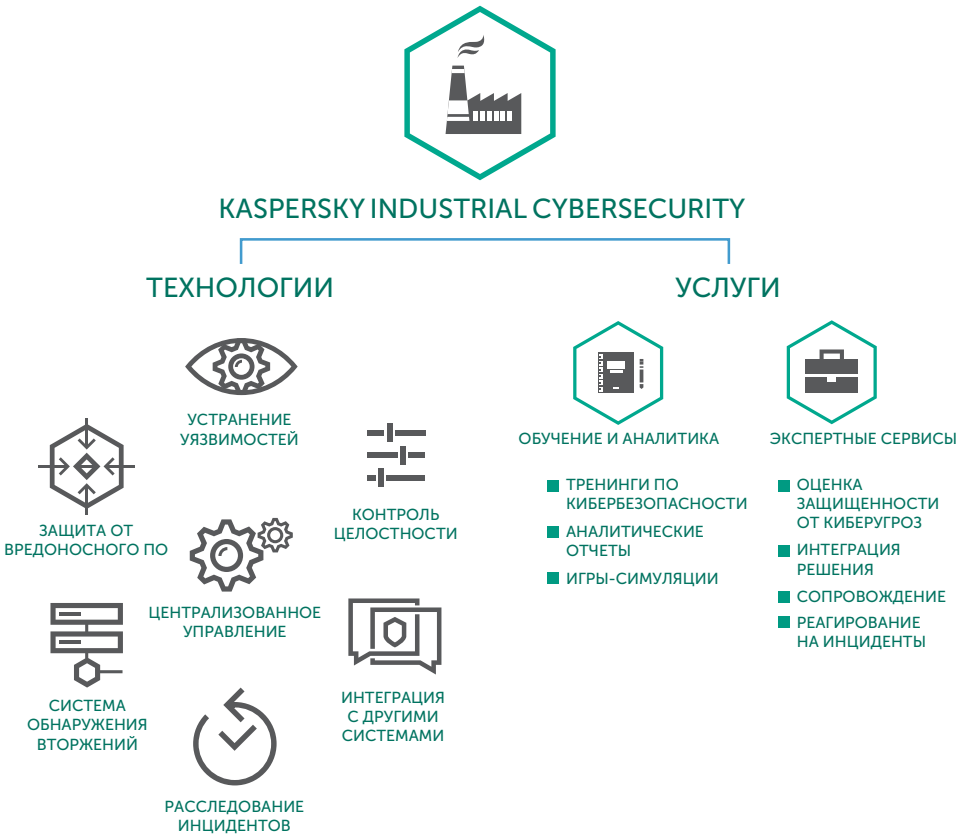
- Процессно-ориентированный подход к обеспечению кибербезопасности
- Программа повышения осведомленности сотрудников
- Специализированные решения для промышленных сред

«ЛАБОРАТОРИЯ КАСПЕРСКОГО» ПРИДЕРЖИВАЕТСЯ ЦЕЛОСТНОГО ПОДХОДА К ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ:

- **Процессы.** Для обеспечения промышленной кибербезопасности не может быть готового универсального решения «из коробки». Обеспечение безопасности – это процесс, который начинается с аудита среды и подготовки персонала к изменениям. После этого защитные решения постепенно развертываются — так, чтобы не затрагивать работу ключевых систем.
- **Люди.** Для кибербезопасности важную роль играет каждый сотрудник – от директора до инженера. Поэтому необходимо заниматься обучением персонала и организовывать тренинги, такие как игра-симуляция Kaspersky Industrial Protection Simulation (KIPS).
- **Технологии.** «Лаборатория Касперского» предлагает решения, основанные на уникальных технологиях и созданные специально для задач промышленной кибербезопасности. Они отказоустойчивы, не препятствуют технологическим процессам и могут работать даже в условиях физической изоляции.

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity – это решение, состоящее из технологий и сервисов, призванное защитить промышленные системы на каждом уровне (включая серверы АСУ ТП/SCADA, человеко-машинные интерфейсы, инженерные рабочие станции, ПЛК, сетевые соединения и прочее), не нарушая непрерывности работы и не снижая стабильности технологического процесса.



Число угроз, нацеленных на критически важную инфраструктуру, растет, и правильный выбор консультанта и технологического партнера для защиты систем сегодня важен как никогда. Обратитесь к нашим экспертам и подробно узнайте о будущем промышленной кибербезопасности.

Подробнее о решении: kaspersky.ru/ics