Сколько безопасности требуется от **встраиваемой** в промышленное устройство **ОС**?

Парьев Сергей
Руководитель группы R&D
Лаборатория Касперского

OS Day 2024

- Промышленные устройства
- Откуда возникает потребность в защите промышленных устройств?
- Анализ/моделирование угроз
- Как защищать?
- ОС как центральный элемент защиты
- Встроенные в ОС механизмы защиты
- KasperskyOS RT (real-time)

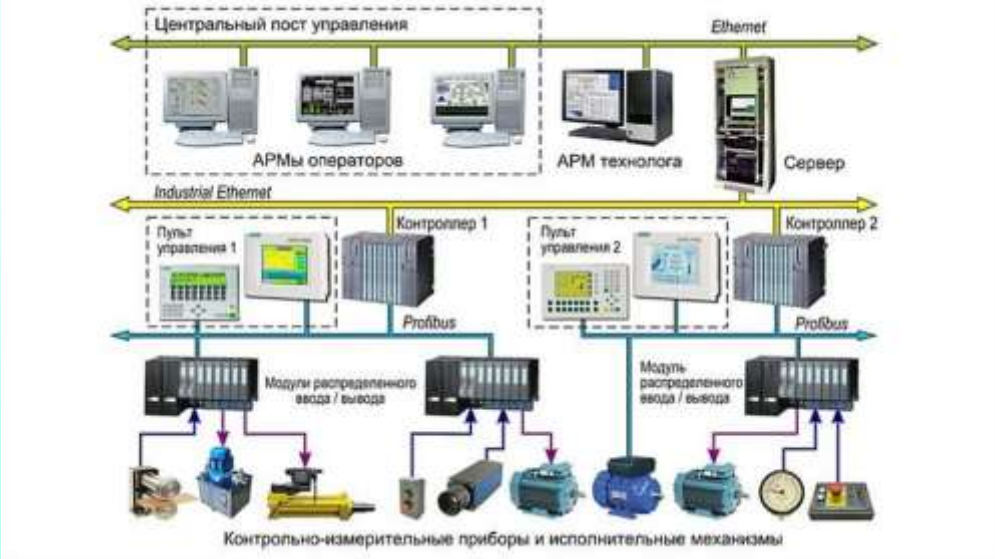
Промышленные устройства и системы управления (примеры)

Примеры промышленных устройств:

- ПЛК (программируемые логические контроллеры)
- Терминалы РЗА (релейной защиты и автоматики)
- УСПД (устройства сбора и передачи данных)

Примеры систем управления:

- АСУ ТП (автоматизированная система управления технологическим процессом)
- АСТУ (автоматизированная система технологического управления)
- АСКУЭ (автоматизированная система коммерческого учета электроэнергии)



https://technogroupp.com/articles/kompleks-tehnicheskih-sredstv-asu-tp/

Откуда возникает потребность в защите промышленных устройств

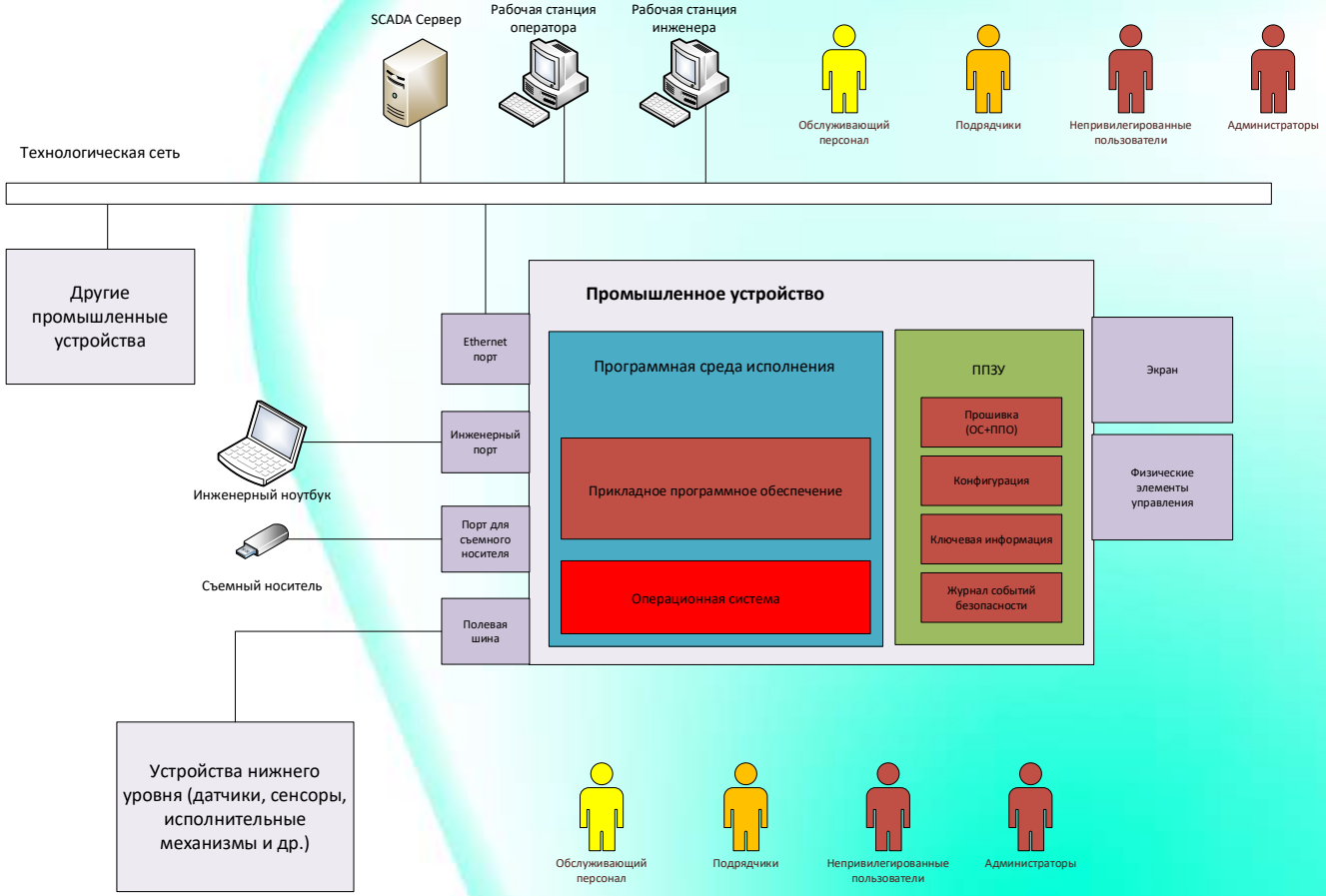
Нормативные требования:

- О безопасности критической информационной инфраструктуры (ФЗ-187 и подзаконные акты)
  - Особенно интересен приказ №239 ФСТЭК России “Об утверждении требований по обеспечению безопасности значимых объектов критической инфраструктуры Российской Федерации”
- Отраслевые:
  - Распоряжение №62р ПАО “Россети” от 28.02.2022 “Об утверждении требований по обеспечению безопасности информации микропроцессорных устройств релейной защиты и автоматики”
  - Требования отраслевой аттестации/сертификации
  - Внутренние требования больших компаний (СТО)
- Международные стандарты:
  - ИСО/МЭК 62443 (в частности части 4-1 и 4-2) “Сети коммуникационные производственные. Безопасность сети и систем”
  - МСО/МЭК 62351 "Управление энергосистемами и связанный с ним обмен информацией. Безопасность данных и коммуникаций”

Реальная опасность атак:

- Увеличивающаяся статистика атак на промышленные системы по всему миру
- Кратный рост атак и их изощренности в РФ после 2022 года

Схема работы промышленного устройства



Типы нарушителей:

- Внешние
  - Отдельные хакеры
  - Хакерские группировки
- Внутренние
  - Пользователи
  - Администраторы
  - Подрядчики
  - Обслуживающий персонал

Возможности нарушителя:

- Базовые
- Базовые повышенные
- Средние

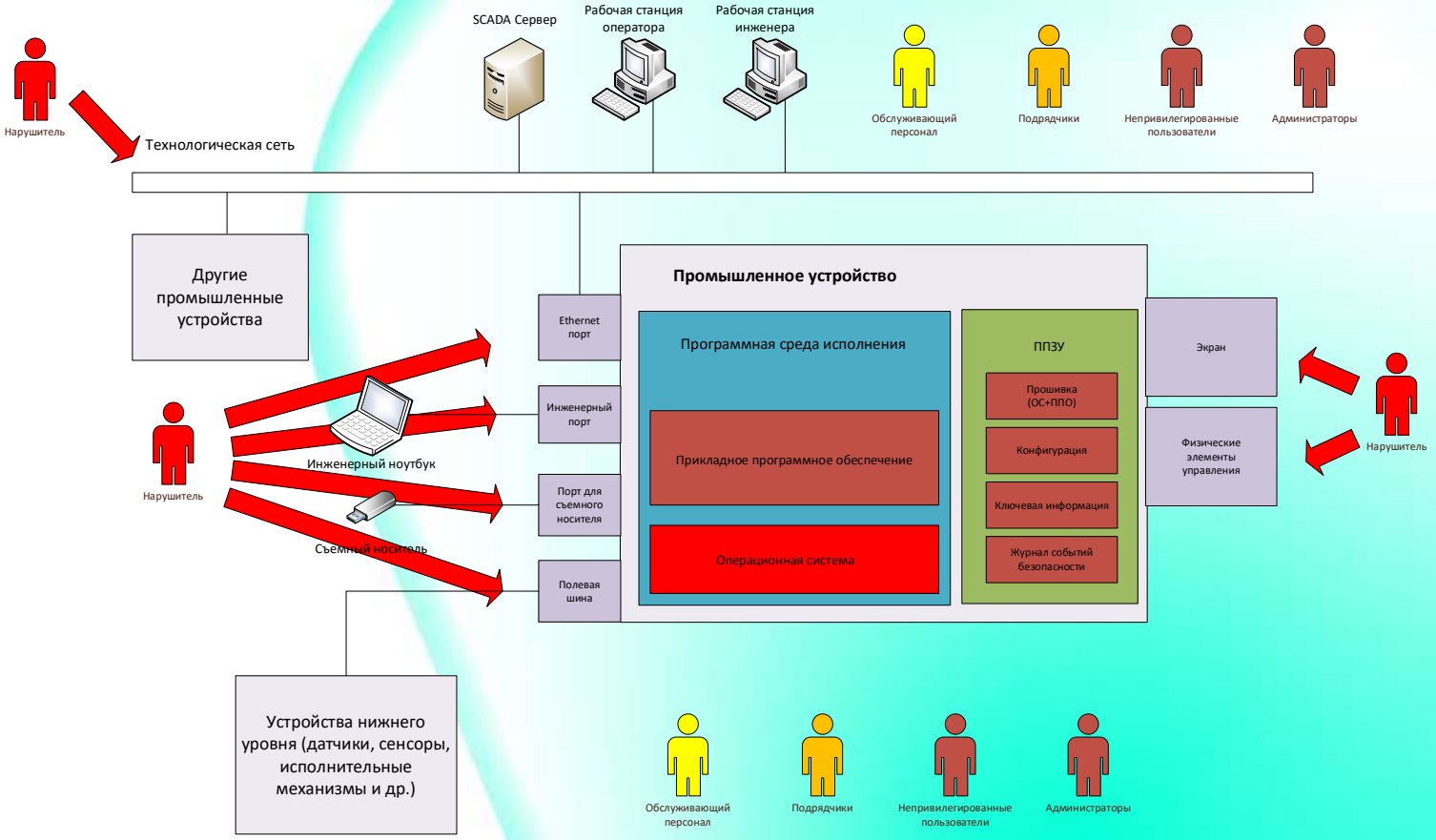
Защищаемые активы и их свойства:

- Прошивка (ОС + прикладное ПО) – целостность
- Конфигурация – целостность
- Ключевая информация – целостность, конфиденциальность
- Журнал событий безопасности – целостность (конфиденциальность)
- Командно-информационный обмен с верхним уровнем – целостность (конфиденциальность)
- Командно-информационный обмен с инженерной станцией – целостность (конфиденциальность)
- Командно-информационный обмен с другими устройствами – целостность (конфиденциальность)
- Командно-информационный обмен с нижним уровнем – целостность (но обычно не защищается)
- Программная среда исполнения – целостность, доступность
- Промышленное устройство (его работоспособность) – доступность

Актуальные типы угроз безопасности информации:

- УБИ.1 Угроза утечки информации
- УБИ.2 Угроза несанкционированного доступа
- УБИ.3 Угроза несанкционированной модификации (искажения) информации
- УБИ.4 Угроза несанкционированной подмены информации
- УБИ.5 Угроза удаления информационных ресурсов
- УБИ.6 Угроза отказа в обслуживании
- УБИ.8 Угроза нарушения функционирования (работоспособности)

Вектора атак (1)



Вектора (способы) атак:

- Локальная работа с физическими элементами управления и экраном
- Локальное подключение к Ethernet порту и эксплуатация уязвимостей
- Локальное подключение к инженерному порту и эксплуатация уязвимостей
- Локальное подключение съемного носителя
  - С модифицированными данными и проведение штатной процедуры обновления
  - Несанкционированная выгрузка данных с устройства
- ~~Локальное подключение к полевой шине~~
- ~~Удаленное (относительно) подключение к полевой шине~~
- Удаленные сетевые атаки
  - Прослушивание трафика
  - Встраивание между верхним уровнем/другими устройствами и подмена/модификация/блокирование трафика
  - Атака устройства “мусорным” трафиком
  - Сетевое подключение к устройству и эксплуатация уязвимостей
- Подмена прошивки на одном из этом её передачи от производителя

Построение защиты:

- Комплексная подсистема безопасности промышленной системы
  - Для значимых объектов КИИ в соответствии с Приказом ФСТЭК России №239
  - Международные стандарты (ИСО/МЭК 62443, ИСО/МЭК 62351)
- Встроенные механизмы и наложенные СЗИ
- Приоритет встроенных механизмов
- Предпочтительно, чтобы встроенные механизмы находились в ОС
  - ОС должна защищать и себя и прикладное ПО, насколько это возможно
  - Прикладные разработчики не должны заниматься разработкой механизмов защиты
  - Для разработки механизмов защиты необходимы специальные знания, люди, инструментарий и т.д.
  - Подтверждение соответствия (испытания, сертификация)

Все угрозы

Аудит (журнал событий безопасности):

- Журнал содержит перенумерованные записи с метками времени
- Журналируются все значимые срабатывания механизмов защиты, а также важные изменения состояния устройства
- Возможность интеграции с системами централизованного сбора событий безопасности (например, SIEM)
- Для обеспечения неотказуемости пользователей от своих действий можно дополнительно подписывать соответствующие записи журнала
- Журнал событий безопасности не сбрасывается при сбросе устройства к заводским настройкам
- Контроль доступа к журналу событий безопасности

https://www.kp.ru/guide/initsiativnyi-audit.html

Угроза несанкционированного доступа (все вектора)

Контроль доступа к устройству:

- Учетные записи пользователей
- Ролевая (персонализированная) модель доступа
  - Роль определяет доступы к функциям устройства
- Аутентификация по логину/паролю
- Аутентификация по сертификату
- Контроль доступа по физическим интерфейсам
- Возможность централизованного управления пользователями
- “Корень” доверия (Root of Trust) в устройстве
- Контроль активности пользовательских сеансов

https://trudovik.pro/catalog/oformlenie_stroyki/stroitelnye_znaki/2125/?oid=2126

Сетевые вектора атаки (ряд угроз)

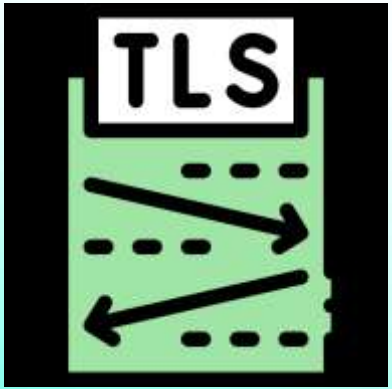


image: Flaticon.com

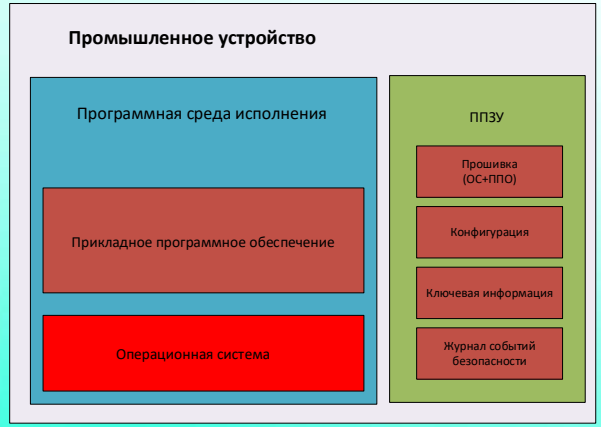
Контроль сетевых потоков:

- Защищенные каналы связи с устройством (TLS)
- Поддержка VLAN
- Поддержка SNMPv3
- Фильтрация соединений по MAC, IP, TCP/IP портам
- Разрешение/запрет использования сетевых интерфейсов
- Защита от базовых сетевых атак и ошибок (сетевой флуд, пакеты неправильной длины, неправильные заголовки и т.д.)

Вектор атаки – эксплуатация уязвимостей (ряд угроз)

Контроль целостности программной среды исполнения:

- Доверенная загрузка и контроль целостности прошивки
- Доверенные обновления
- Контроль целостности конфигурации
- Контроль целостности и конфиденциальности ключевой информации
- Изоляция процессов
- Разграничение доступа к ресурсам ОС
- Периодический контроль целостности исполняемых процессов
- Базовый анализ аномального поведения процессов
- Дополнительные механизмы, усложняющие эксплуатацию уязвимостей (рандомизация адресного пространства, санитайзеры, защита кодовых страниц от записи, защита страниц данных от исполнения и др.)



Вектор атаки – подключение съемного носителя

Контроль использования съемных носителей:

- Запрещение/разрешение использования физического интерфейса (в целом, для пользователя)
- Запрещение/разрешение использования съемных носителей (в целом, для пользователя)
- Контроль использования съемных носителей по идентификаторам
- Запрещение/разрешение чтения/записи с/на съемный носитель

Все угрозы

Дополнительные механизмы:

- Бэкапирование и восстановление
- Стартовая и периодическая проверка основных функций и механизмов защиты
- Сторожевой таймер, срабатывающий при зависании устройства
- Централизованное управление настройками безопасности

Преимущества KasperskyOS RT (real-time):

- Полностью российская ОС
- Микроядерная архитектура
- Изоляция процессов, строгий контроль использования межпроцессного взаимодействия в соответствии с заранее разработанной политикой безопасности
- RT планировщик, защита от инверсии приоритетов, RT таймера и др. RT функциональность
- Поддержка POSIX
- Планы сертификации во ФСТЭК России
- Готовые к использованию встроенные механизмы защиты
- Кибериммунная методология РБПО для разработчиков
- Российская техническая поддержка

Спасибо за внимание

Вопросы?

Парьев Сергей
Руководитель группы R&D
Лаборатория Касперского