УЦСБ ИНТЕГРАТОР СИЛЬНЫХ РЕШЕНИЙ

Гибкий подход к обеспечению информационной безопасности АСУ ТП

Алексей Комаров
Менеджер по развитию решений
Уральский Центр Систем Безопасности

Екатеринбург
29 ноября 2016 года

http://ZLONOV.ru komarov.alexey @zlonov

www.USSC.ru

Почему УЦСБ?

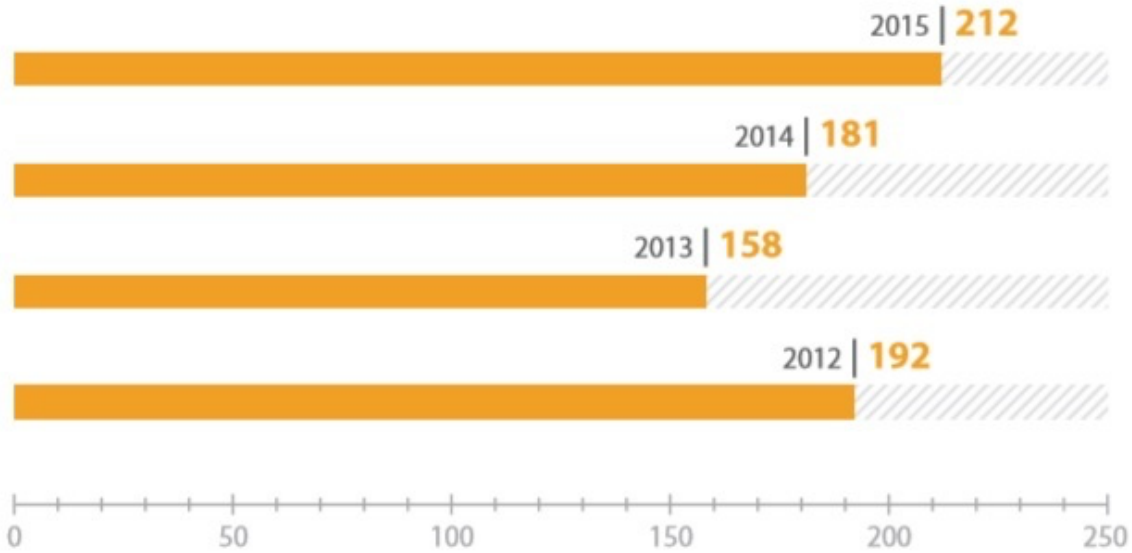
- Разработка корпоративных стандартов
- Аудиты действующих АСУ ТП
- Проектирование СОИБ АСУ ТП
- Ввод в эксплуатацию и поддержка систем обеспечения ИБ АСУ ТП
- Разработка собственного решения - **DATAPK**
- а также: вебинары, семинары, курсы…

Актуальность темы ИБ АСУ ТП

- Уязвимость компонентов АСУ ТП
- Инциденты ИБ в АСУ ТП
- Оценка текущего уровня защищённости
- Требования законодательства
- Анализ АСУ ТП как объекта

Уязвимость компонентов АСУ ТП

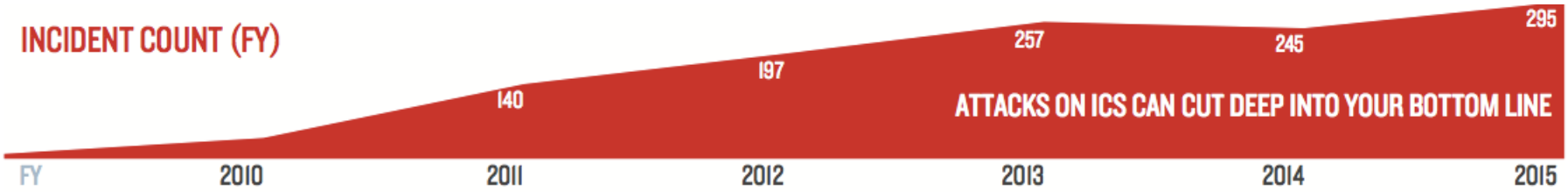
Результаты исследования программного обеспечения 752 различных устройств, поддерживающих низкоуровневый протокол HART, источник: Digital Security



Общее количество уязвимостей, обнаруженных в компонентах АСУ ТП, источник: Positive Technologies

Число инцидентов по годам

- В 2015 инцидентов ИБ АСУ ТП зафиксировано на 15% больше, чем в любом из прошлых лет. Рост год к году составил 20%.



Из 314 опрошенных компаний-владельцев АСУ ТП в 2015 году

- 34% подтвердили, что сталкивались с инцидентами более двух раз за последний год,
- из них 44% не смогли определить источник атаки.

источники: ICS-CERT, SANS

Инциденты… реальны

Дата	Страна	Инцидент
дек 2014	Германия	Федеральное управление по информационной безопасности признало факт компьютерной атаки на сталелитейный завод.
июнь 2015	Польша	Более десятка рейсов крупнейшей польской авиакомпании LOT отменены из-за хакерской атаки на IT-систему аэропорта Варшавы.
март 2015	**Россия**	**Специалисты уральских оборонных предприятий обнаружили необъяснимый сбой в иностранном оборудовании.**
июль 2015	Германия	Хакеры взломали компьютеры зенитных ракет бундесвера
сент 2015	США	За последние 4 года на Минэнерго США было совершено 159 успешных кибератак
дек 2015	США	Иранские хакеры атаковали дамбу в Нью-Йорке
дек 2015	Украина	Замминистра энергетики США обвинила Россию в организации блэкаута на Украине
март 2016	Япония	Хакеры случайно получили доступ к SCADA-системе водоочистной станции и изменили её настройки
апр 2016	Германия	На компьютерах германской АЭС обнаружено вредоносное ПО
июль 2016	**Россия**	**ФСБ обнаружила масштабную кибератаку на предприятия оборонно-промышленного комплекса и иные объекты критически важной инфраструктуры**

Мифы о безопасности в АСУ ТП

- «Нет подключения к внешним сетям»
  - WiFi, модемы и пр.
- «Достаточно межсетевого экрана на периметре»
  - Проблемы настройки, уязвимости, «закладки»
- «Специфика не позволит хакерам разобраться»
  - Для атаки не нужно быть экспертом в АСУ ТП
- «Мы никому не интересны»
  - Халатность, размер ущерба
- «Систем промышленной безопасности достаточно»
  - Простой технологического процесса тоже ведёт к потерям

Основные сложности обеспечения ИБ

- Атака стоит существенно меньше потерь от её реализации
- Скрытность и длительность атак (от 3 до 9 лет)
- АСУ ТП работают по 5-10 лет без обновления
- При разработке АСУ ТП про ИБ не думали
- Атакующим хорошо известны уязвимости
- Самое слабое звено защиты - сотрудники
- Офисные средства слабоприменимы

Что может случиться на практике?

- **Халатность**
  - Подключение внешних устройств (носители информации, модемы и пр.)
  - Подключение сторонних СВТ (свой ноутбук для игр)
- **Направленные атаки**
  - Шпионаж
  - Саботаж
- **Хищение**
  - Сырья, готовой продукции
  - Ресурса производственной линии (изготовление неучтенной продукции)

Направленная атака на АСУ ТП

Объект атаки:
- АРМ, серверы, АСО
- Общее ПО

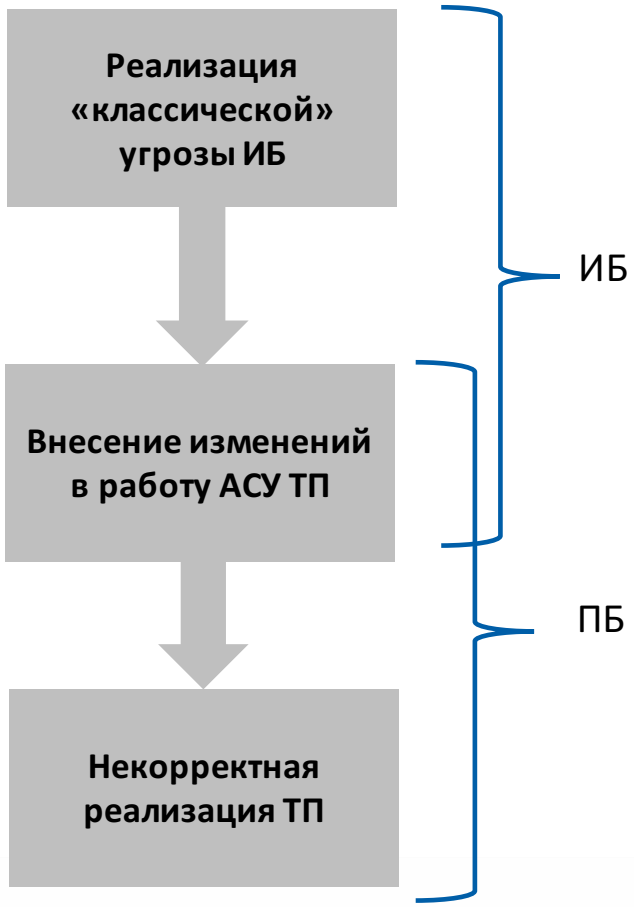
Цель атаки:
- Закрепиться в защищаемом периметре

Объект атаки:
- ПЛК
- Специальное ПО

Цель атаки:
- Получение возможности манипуляции ТП

Объект атаки:
- ТОУ

Цель атаки:
- Нарушение реализации ТП
- Порча оборудования



Пример (почти) из практики

- Команда УЦСБ в Industrial CTF: задача по взлому умной электрической сети, построенной на основе архитектуры microgrid:
- 4 инженерных объекта, которые нам и предстояло атаковать:
  - солнечная электростанция; гидроэлектростанция; подстанция высокого напряжения; распределительная подстанция;
- 3 источника электричества:
  - солнечные батареи;
    гидроэлектростанция;
    основная энергосистема страны;
- 2 потребителя электричества:
  - город; завод.

Отзыв участника команды

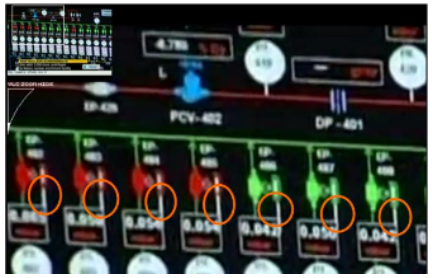
- «**Взломав сеть,** мы начали сбор информации. Сканирование сети, поиск сетевых папок, определение железок и другие разведывательные мероприятия. Данная стадия заняла почти весь день. Параллельно со сбором информации мы **получали доступ к различным компонентам системы**».
- «**Под конец дня у нас была полная картина сети**, информация о всех элементах, протоколах управления. Была часть паролей от оборудования. Мы **получили полное управление над тремя из четырех инженерных объектов**».

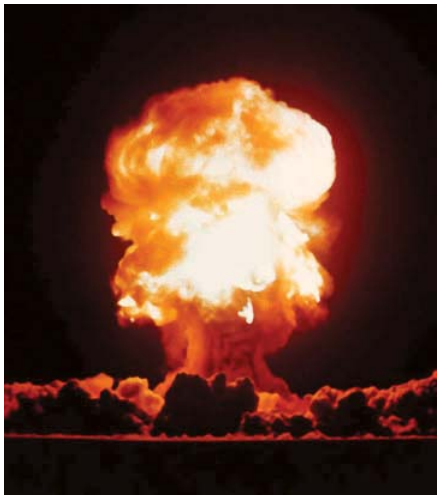
Отзыв участника команды

- «В первый день мы **обесточили завод и вывели из строя оборудование**: в обход блокировки напрямую соединили работающий генератор с землёй, чем вызвали короткое замыкание».
- «Во второй день мы успешно осуществили **полное погашение энергосистемы** (синхронно отключили все три источника электричества) и **организовали перегрузку в сети**».

Временной вектор атаки

Подготовка	Реализация	Нанесение ущерба





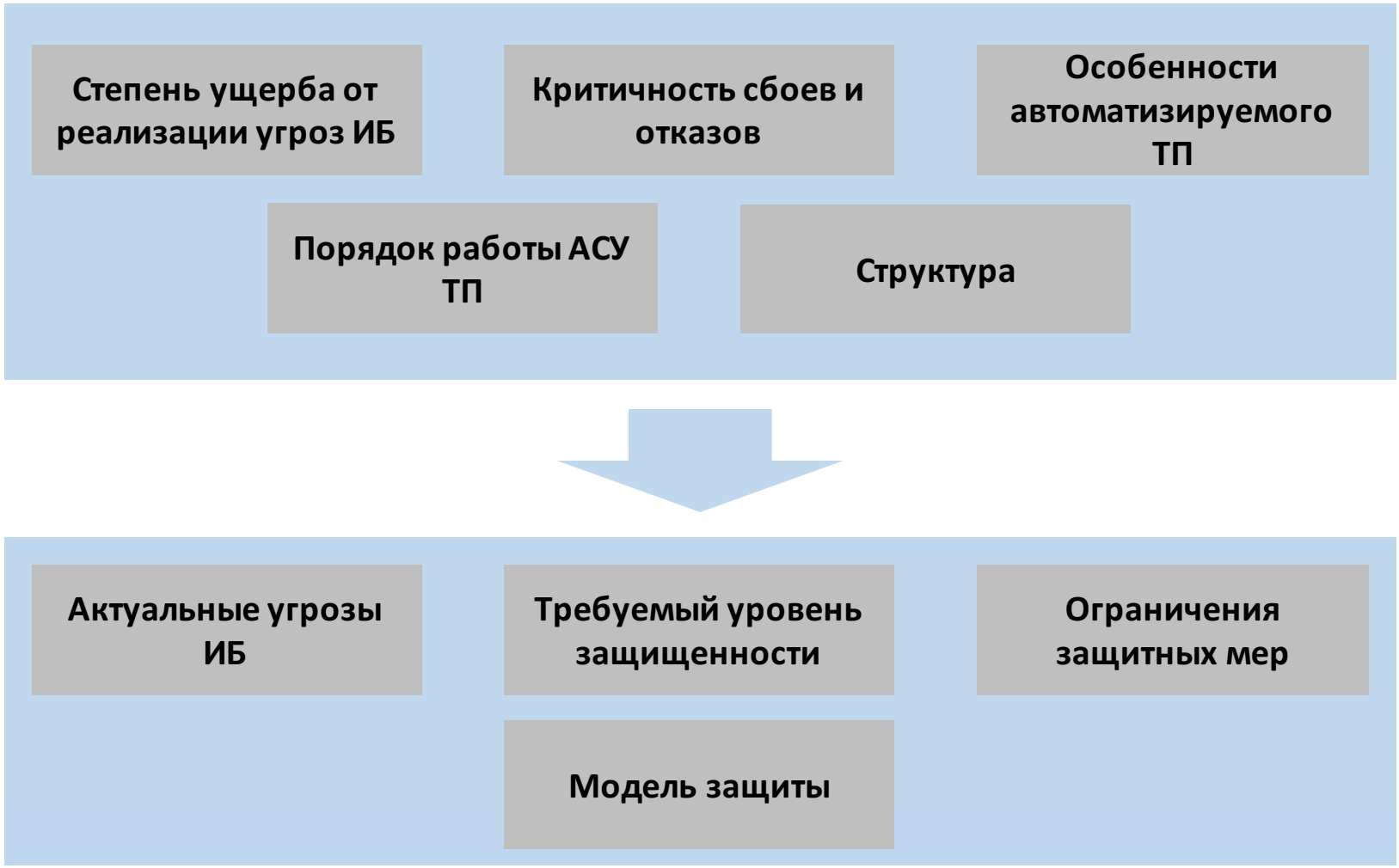
В традиционных системах все 3 стадии могут проходить за считанные **секунды**, в АСУ ТП – могут длиться **годы**

Проактивная защита	Активная защита	Реактивная защита

Выбор стратегии защиты

Проактивная защита	Активная защита	Реактивная защита
Цель стратегии: • Не дать произойти инциденту **Способ достижения:** • *Блокировка* нежелательных изменений состояния системы 	**Цель стратегии:** • Выявить атаку в ходе реализации **Способ достижения:** • *Анализ* состояний системы с целью выявления подозрительных изменений 	**Цель стратегии:** • Минимизировать ущерб от реализации инцидента **Способ достижения:** • *Возврат* системы в целевое состояние 

Выбор защитных мер по итогам анализа



С чего начать?

Технические меры защиты

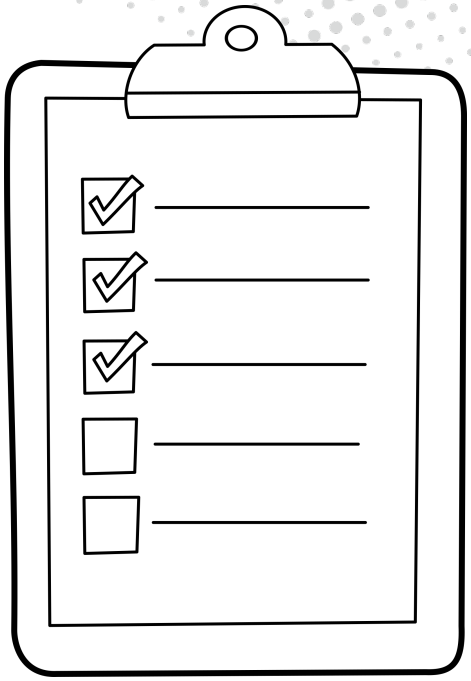
Организационные мероприятия

Физическая безопасность

Аудит - самый важный первый шаг

- Качественный аудит ИБ АСУ ТП позволит:
  - получить **объективную и независимую оценку текущего уровня обеспечения ИБ АСУ ТП**, с учетом корпоративных и отраслевых документов, требований законодательства РФ и опыта лучших мировых практик;
  - **запланировать реализацию комплекса мер**, направленных на повышение уровня защищённости АСУ ТП;
  - **выделить и обосновать** актуальные технические требования к системе защиты информации в АСУ ТП.

Что входит в задачи аудита?



- **обследование организационных и технических мер** обеспечения ИБ АСУ ТП;
- **анализ защищённости АСУ ТП** в виде тестирования эффективности принятых защитных мер;
- **оценка соответствия** положениям корпоративных и отраслевых документов, требованиям законодательства РФ и международных стандартов в области ИБ АСУ ТП;
- **анализ угроз** ИБ и уязвимостей, разработка **модели угроз** ИБ АСУ ТП;
- **разработка организационно-технических рекомендаций** (плана) по повышению уровня ИБ АСУ ТП;
- разработка **задания на проектирование** и технических требований к системе защиты АСУ ТП.

Какие меры эффективнее?

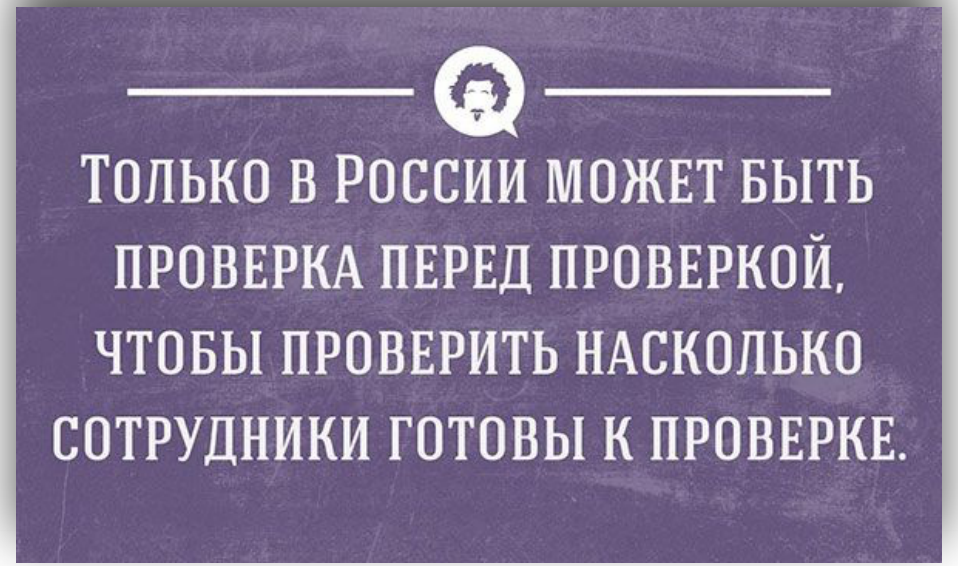
Технические меры защиты

Организационные мероприятия

Физическая безопасность

Типичные проблемы - организационные

- Ответственность работников за несоблюдение требований по ИБ АСУ ТП не установлены
- Обучение и повышение осведомлённости производится эпизодически (системы нет)
- Нет регламента предоставления и пересмотра прав доступа



Типичные проблемы - технические

- Унаследованное ПО не имеет возможности централизованного управления парольными политиками и правами доступа
  - Отзыв доступа при увольнении не производится из-за использования общих учётных записей

Типичные проблемы - технические

- Не реализовано ограничение программной среды
  - так как нет соответствующего регламента и перечня разрешённого ПО

Ключевая проблема (одна из…)

- Не осуществляется регистрация событий безопасности, не говоря уже об управлении инцидентами и проведении расследований.

Не только технические средства защиты

- Существенно повысить уровень защищённости можно и без приобретения дорогостоящих средств защиты.
- Грамотно выполненный квалифицированными специалистами аудит информационной безопасности АСУ ТП позволяет определить правильные компенсирующие меры, эффективные как с точки зрения обеспечиваемого уровня защищённости, так и с точки зрения экономической обоснованности.
- Применение же технических средств защиты должно обязательно учитывать особенности объекта защиты – нужно принимать во внимание различные режимы работы АСУ ТП (штатный/нештатный, автоматизированный/автоматический и т.д.), а также максимально исключить влияние средства защиты непосредственно на сам технологический процесс.

Журнал "Information Security/ Информационная безопасность" #4, 2015

Реализация технических мер защиты

- Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности. В качестве средств защиты информации в первую очередь подлежат рассмотрению механизмы защиты (параметры настройки) штатного программного обеспечения автоматизированной системы управления при их наличии

Приказ ФСТЭК России от 14.03.2014 №31

Актуальные направления защиты

<table>
<tr><th colspan="3">Классы мер по обеспечению ИБ</th></tr>
<tr><th>Превентивные</th><th>Детектирующие</th><th>Компенсирующие</th></tr>
<tr><td colspan="2">Обеспечение сетевой безопасности</td><td rowspan="4">Применение средств резервного копирования и восстановления</td></tr>
<tr><td>Безопасная настройка компонентов</td><td>Управление конфигурациями и изменениями</td></tr>
<tr><td>Управление доступом</td><td>Регистрация и сбор событий безопасности</td></tr>
<tr><td>Защита от вредоносного ПО</td><td>Контроль защищённости</td></tr>
<tr><td colspan="2">Физическая безопасность и ИТСО</td><td></td></tr>
<tr><td colspan="3">Организационные меры (Политика ИБ, обучение персонала, расследования)</td></tr>
</table>

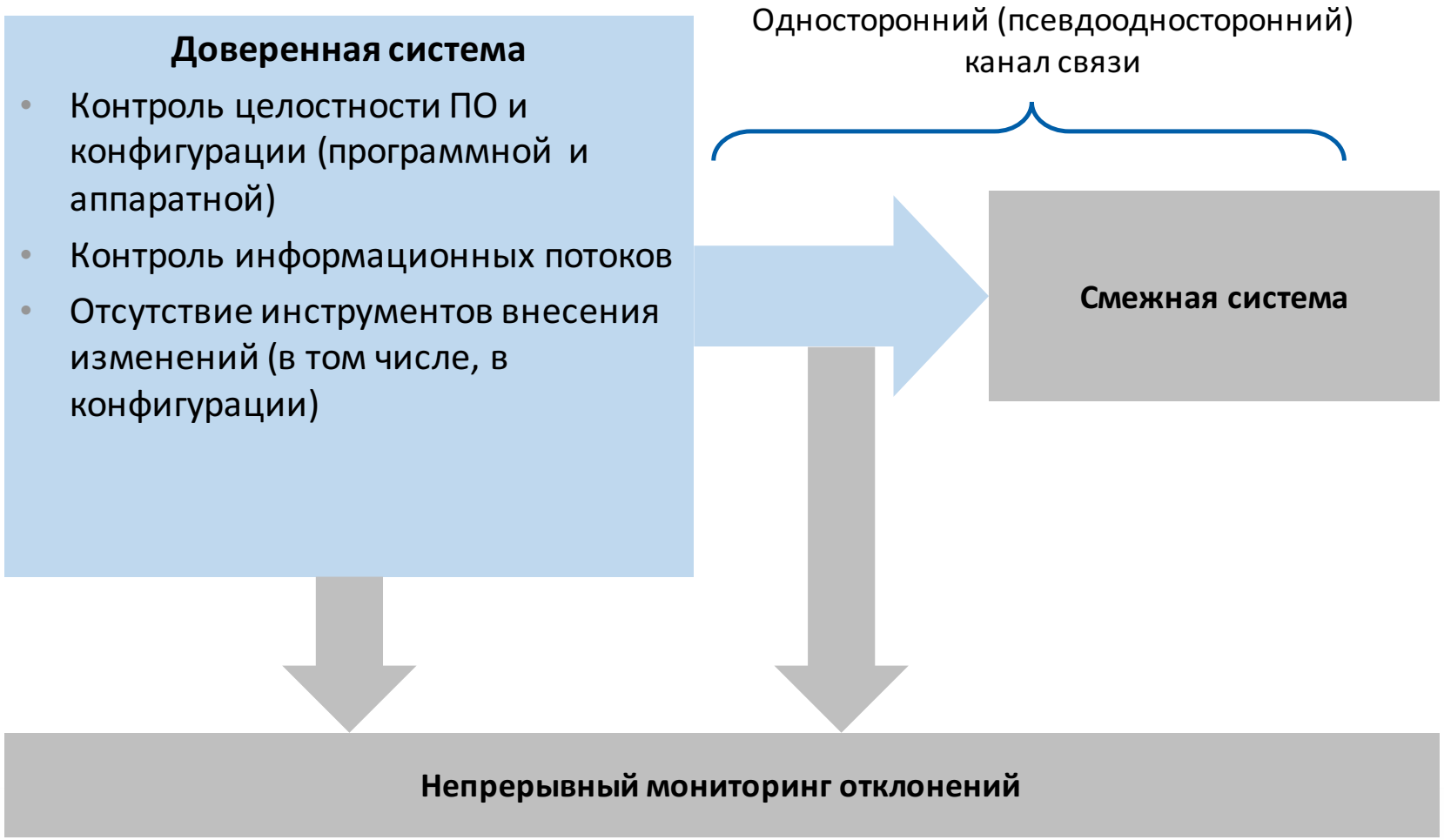
Актуальные направления защиты

Классы мер по обеспечению ИБ		
Превентивные	Детектирующие	Компенсирующие
Большая разнообразность и зависимость от конечной системы	**Допускает унифицированную реализацию** **САМСИБ** - система анализа и мониторинга состояния ИБ	**Целесообразно реализовывать как элемент АСУ ТП**

Факторы и мероприятия ИБ

Факторы	Мероприятия ИБ
Изменение компонентов АСУ ТП и/или их конфигураций	Инвентаризация компонентов АСУ ТП Контроль конфигураций компонентов АСУ ТП Централизованный сбор, корреляция, систематизация и анализ значимости событий ИБ в АСУ ТП
Возникновение новых уязвимостей	Контроль защищённости компонентов АСУ ТП Обнаружение компьютерных атак
Изменение требований по обеспечению ИБ	Контроль соответствия требованиям по обеспечению ИБ

Модель защиты АСУ ТП



Модель защиты

Изолированная среда

- Контроль неизменности программной и аппаратной среды
- Исключение взаимодействия с системами меньшей степени доверия (или только гарантированно однонаправленное взаимодействие), включая **систему обеспечения ИБ**
- Пассивный мониторинг сетевого сегмента защищаемой системы

Контролируемая среда

- Контроль за изменениями программной и аппаратной среды
- Контроль за действиями пользователей и процессов
- Пассивный мониторинг сетевого сегмента защищаемой системы
- Контроль взаимодействия со смежными системами

Интегрированная среда

- Контроль за изменениями программной и аппаратной среды
- Контроль за действиями пользователей и процессов
- Контроль взаимодействия со смежными системами
- Пассивный мониторинг сетевого сегмента защищаемой системы
- организация безопасного обмена недоверенными системами (корпоративные системы, внешние системы)

ПАК DATAPK - основные функции

- Ведение каталога компонентов АСУ ТП, выявление изменений в их составе
- Централизованный сбор, корреляция, систематизация и анализ значимости событий ИБ в АСУ ТП
- Контроль и управление конфигурациями компонентов АСУ ТП
- Выявление уязвимостей, контроль защищённости компонентов АСУ ТП
- Анализ сетевых потоков и обнаружение компьютерных атак и аномалий трафика
- Контроль соответствия требованиям по обеспечению ИБ

DAT APK

Полуфиналист Skolkovo Startup Village 2016

Sk Сколково STARTUP VILLAGE

Инновационный центр Сколково, Москва

Что в основе DATAPK?

- Проекты по защите «больших», действующих АСУ ТП
- Работа с разработчиками АСУ ТП
- Анализ рынка средств ИБ для АСУ ТП
- Для действующих АСУ ТП нужна Система анализа и мониторинга состояния ИБ (САМСИБ)
- DATAPK позволяет построить САМСИБ

Режимы функционирования ПАК DATAPK

Функции Подсистемы мониторинга состояния ИБ	Пассивный мониторинг	Активный мониторинг	Сканирование защищённости
Определение текущего состава компонентов АСУ ТП	Нет	Нет	Да
Выявление изменений в составе компонентов АСУ ТП	Да	Да	Да
Сбор конфигураций компонентов АСУ ТП	Нет	Да	Да
Проверка компонентов АСУ ТП на наличие уязвимостей	Нет	Нет	Да
Обнаружение компьютерных атак	Да	Да	Да
Выявление сетевых аномалий	Да	Да	Да
Сбор событий информационной безопасности с компонентов АСУ ТП	Да / Нет	Да	Да

Реализация замкнутой программной среды

Безопасная конфигурация:
- Управление доступом
- Регистрация событий ИБ
- Идентификация и аутентификация

Пассивный мониторинг:
- Выявление изменений состава ОЗ
- Выявление сетевых аномалий
- Сбор событий ИБ

Активный мониторинг:
- Управление конфигурацией

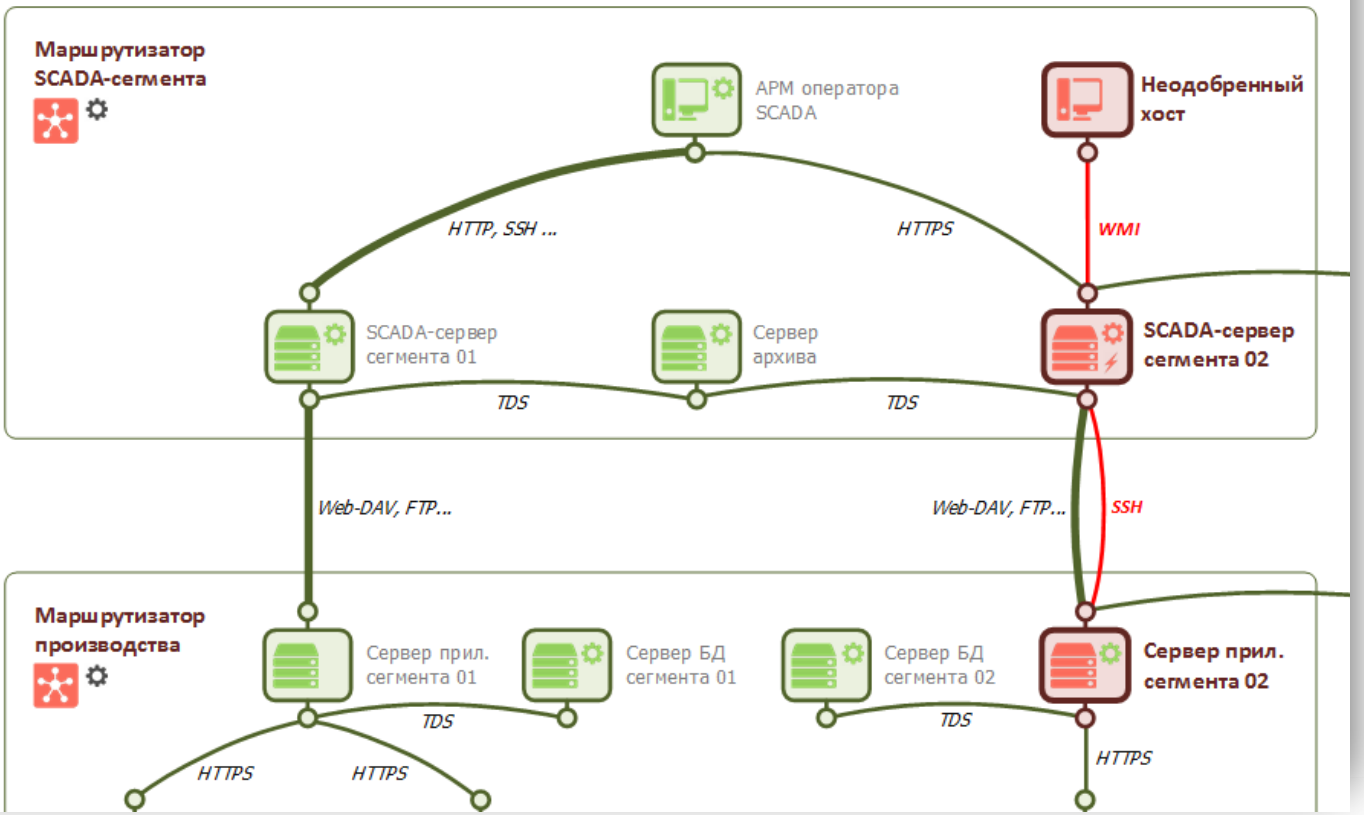
Сканирование защищенности:
- Контроль соответствия требованиям ИБ
- Поиск уязвимостей

datapk

- Панель мониторинга
- Объекты защиты
- Потоки данных
- Оценка соответствия
- Список задач
- Управление политиками
- Настройки

DATAPK

* Станция переработки СПДТ 31-02



Выявлено событие информационной безопасности!

Необходимо немедленно оповестить ответственного сотрудника по телефону:

+7(343)286-24-39

Сообщите ему нижеследующую информацию:

Код события: ИБ #15.23-1

Тип события: Нарушение целостности

Описание события: Обнаружен новый поток данных между "Сервер архивов" и "АРМ инженера АСУ ТП"

Возможное последствие: Нарушение замкнутости функционирования оборудования, ПО ИСиС или систем защиты

Дополнительная служебная информация:

Источник: 192.168.243.112
Получатель: 195.64.213.460
Протокол: ICMP
Дата и время выявления: 03 марта 2016 17:22
Крайнее время оповещения: 17:52
Осталось: 29 минут 43 секунды

Введите код подтверждения сотрудника:

Принять

Спасибо за внимание!

Компания УЦСБ
Тел.: +7 (343) 379-98-34
E-mail: info@ussc.ru
www.USSC.ru

Алексей Комаров
http://ZLONOV.ru
@zlonov
komarov.alexey