УЦСБ ИНТЕГРАТОР СИЛЬНЫХ РЕШЕНИЙ

Практика построения систем защиты АСУ ТП по итогам аудитов информационной безопасности

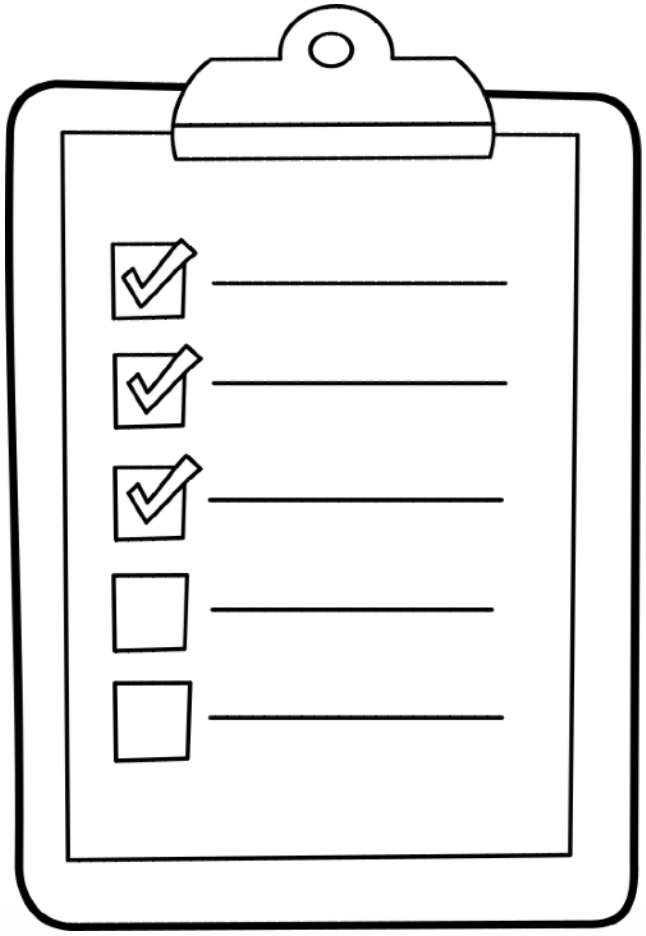
Секция 3. Кибербезопасность: Как справиться с новыми вызовами?

Алексей Комаров
Менеджер по развитию решений
Уральский Центр Систем Безопасности
akomarov@USSC.ru
https://ZLONOV.ru/

Челябинск, 05 декабря 2018 года
16:35-16:55

Содержание

- УЦСБ и ИБ АСУ ТП
- Предпосылки проведения аудитов
- Нюансы проведения аудитов
- Формирование решения по защите - выбор подхода
- Система анализа и мониторинга состояния информационной безопасности АСУ ТП - **DATAPK®**



УЦСБ и ИБ АСУ ТП

- Разработка корпоративных стандартов
- **Аудиты**, анализ и моделирование угроз
- Проектирование, ввод в эксплуатацию и поддержка **систем обеспечения ИБ**
- Собственный продукт: **DATAPK®**
- **Вебинары**, семинары, курсы

Основные предпосылки для проведения аудита

- Уязвимость компонентов АСУ ТП
- Угрозы ИБ в АСУ ТП
- Инциденты ИБ в АСУ ТП
- Анализ АСУ ТП как объекта
- Требования законодательства

Основные предпосылки для проведения аудита

- Уязвимость компонентов АСУ ТП
- Угрозы ИБ в АСУ ТП
- Инциденты ИБ в АСУ ТП
- Анализ АСУ ТП как объекта
- **Требования законодательства**

Федеральное законодательство

193-ФЗ

Федеральный закон №193-ФЗ от 26.07.2017 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

187-ФЗ

Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности КИИ РФ»

194-ФЗ

Федеральный закон №194-ФЗ от 26.07.2017 «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

Неправомерное воздействие на КИИ РФ

194-ФЗ

- 1. Создание, **распространение** и (или) **использование** ПО или иной компьютерной информации для неправомерного воздействия на КИИ:
  - принудительные работы до 5 лет / лишение свободы до 5 лет / штраф до 1 млн руб
- 2. **Неправомерный доступ** к информации КИИ, если он повлёк вред:
  - принудительные работы до 5 лет / лишение свободы до 6 лет / штраф до 1 млн руб
- 3. **Нарушение правил эксплуатации средств** хранения, обработки или передачи охраняемой законом информации КИИ либо правил доступа, если оно повлекло причинение вреда для КИИ:
  - принудительные работы до 5 лет / лишение свободы до 6 лет / запрет занимать должности до 3 лет

УК РФ Статья 274.1

Усиление ответственности

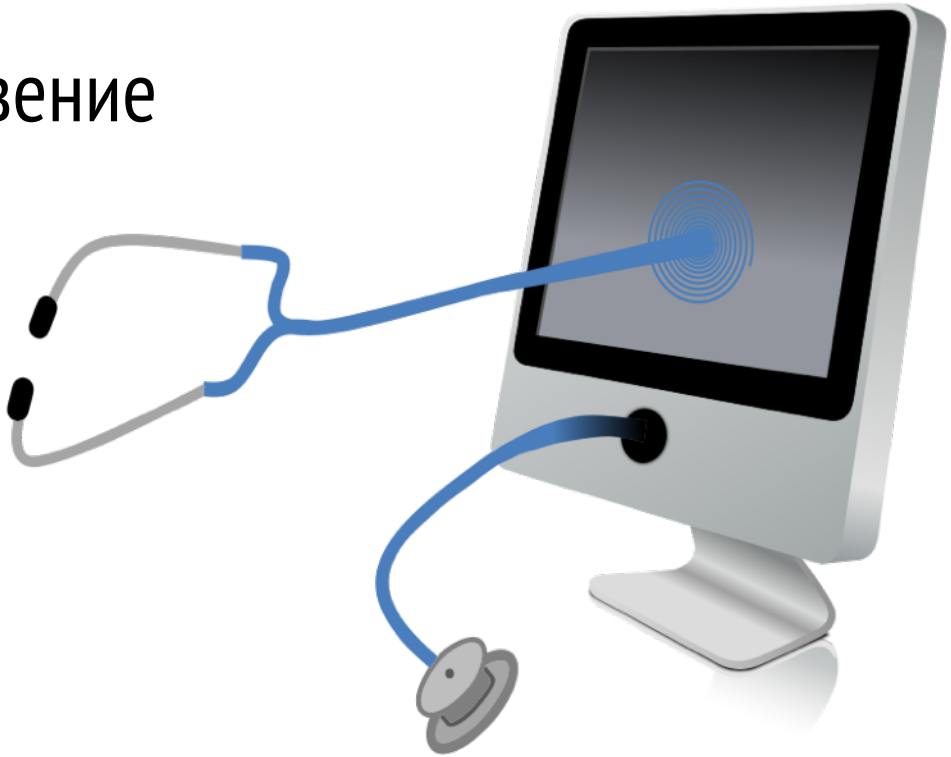
194-ФЗ

- 4. Группой лиц или
  с использованием служебного положения:
  - лишение свободы до 8 лет / запрет занимать должности до 3 лет
- 5. Если повлекло тяжкие последствия:
  - лишение свободы до 10 лет / запрет занимать должности до 5 лет

УК РФ Статья 274.1

Некоторые нюансы проведения аудита ИБ АСУ ТП

- Трудности со сбором данных
- Тестирование на проникновение
- Моделирование угроз
- Оценка ущерба
- Представление результатов



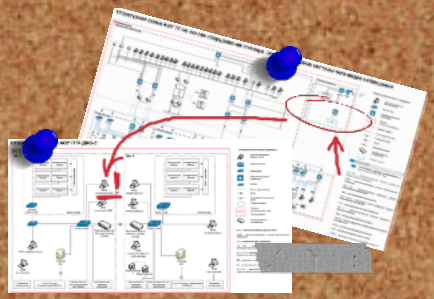
Сбор данных

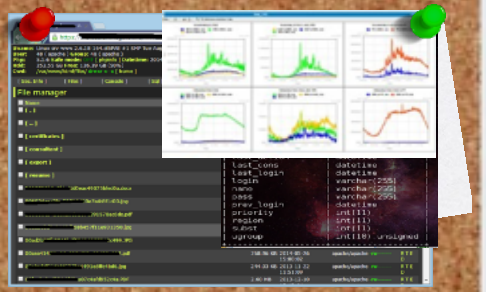

задачи
Интервьюирование
Анализ документации
Инструментальное обследование
Программа обследования
журнал ТО
Проект
ЭД
кого опрашивать?
Имя: Иван Ив
Год рождения
Образование: среднее
Оператор
Имя: Петр Иванов
Год рождения: 198
Образование: высшее
Инженер КИПиА
Имя: Степан Широк
Год рождения: 198
Образование: высшее
Разработчик
проекта нет или утерян
• Технологический регламент
• Инструкции персонала
• Осмотр и документирование
нельзя использовать стороннее ПО
• Встроенные средства системного и прикладного ПО

Тестирование на проникновение

задачи

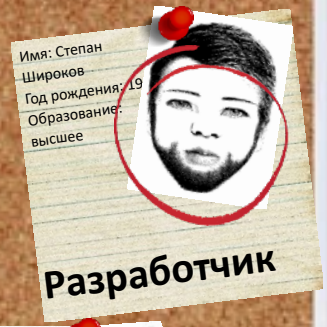
1. **Разработка Программы и выбор инструментов**





2. **Проникновение в защищаемый сегмент**

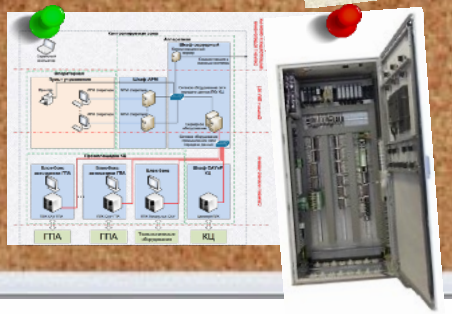
→ только **до границы** сегмента АСУ ТП



Разработчик

3. **Демонстрация атак**

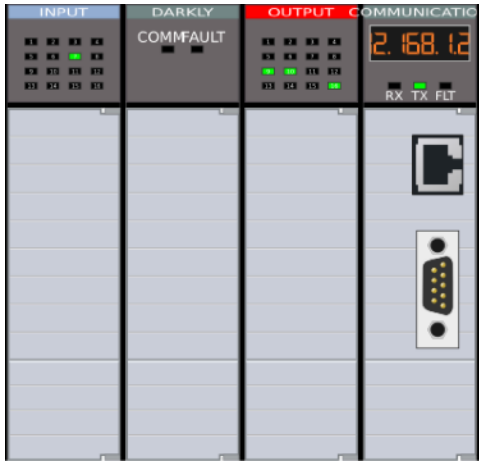
→ **на стенде** разработчика



Моделирование угроз

- 1. Моделирование в соответствии с методикой КСИИ
  - Базовая модель угроз безопасности информации в КСИИ от 18.05.2007 г.
  - Методика определения актуальных угроз безопасности информации в КСИИ от 18.05.2007 г.
- 2. Моделирование в соответствии с Проектом методики для ГИС
  - https://fstec.ru/component/attachments/download/812
- 3. Моделирование в соответствии с 239 приказом
  - ст. 11.1 Приказа ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»

Оценка ущерба



Информационная Безопасность

Промышленная Безопасность

Направленная атака на АСУ ТП

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

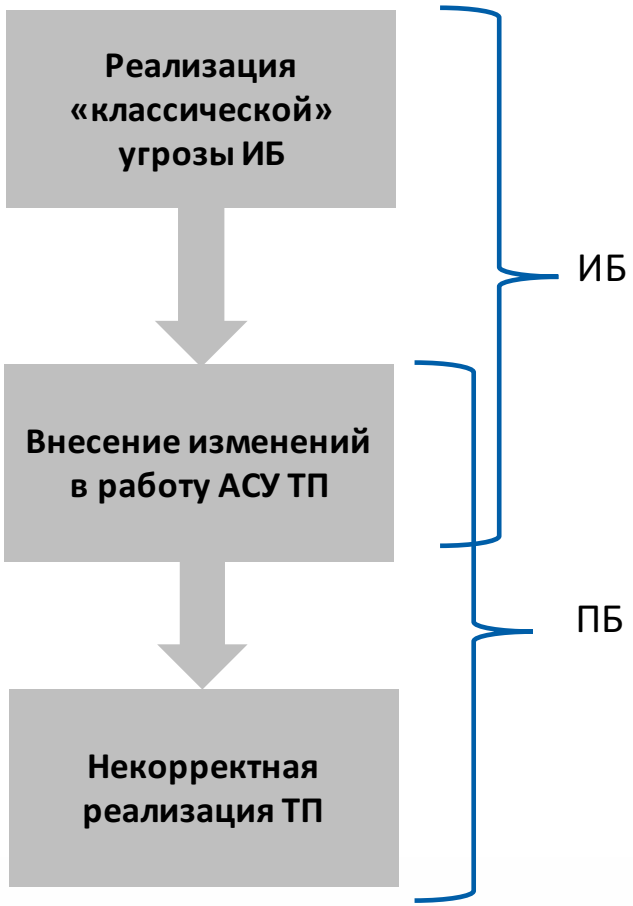
Цель атаки:
- Закрепиться в защищаемом периметре

Объект атаки:
- ПЛК
- Специальное ПО

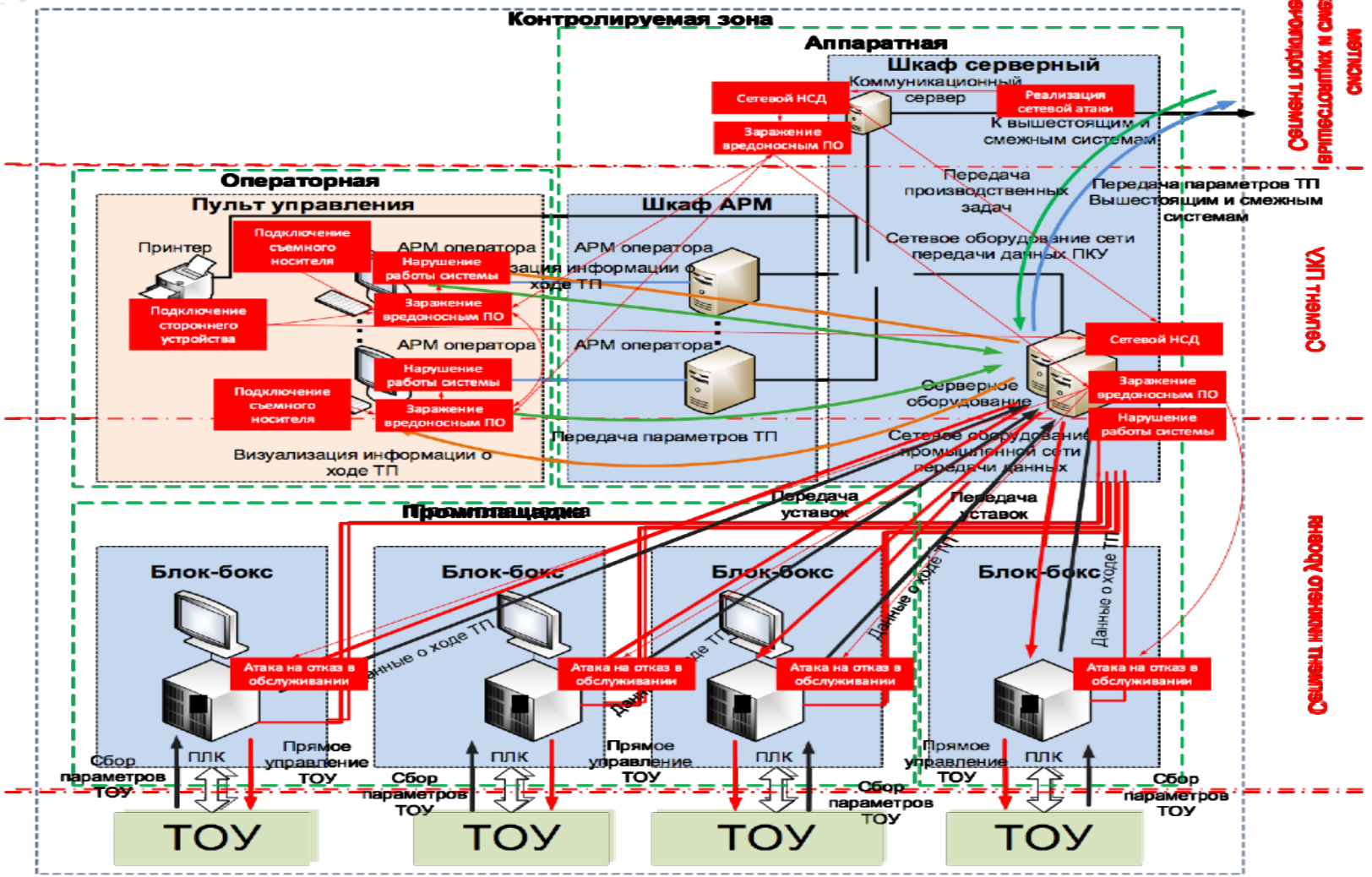
Цель атаки:
- Получение возможности манипуляции ТП

Объект атаки:
- ТОУ

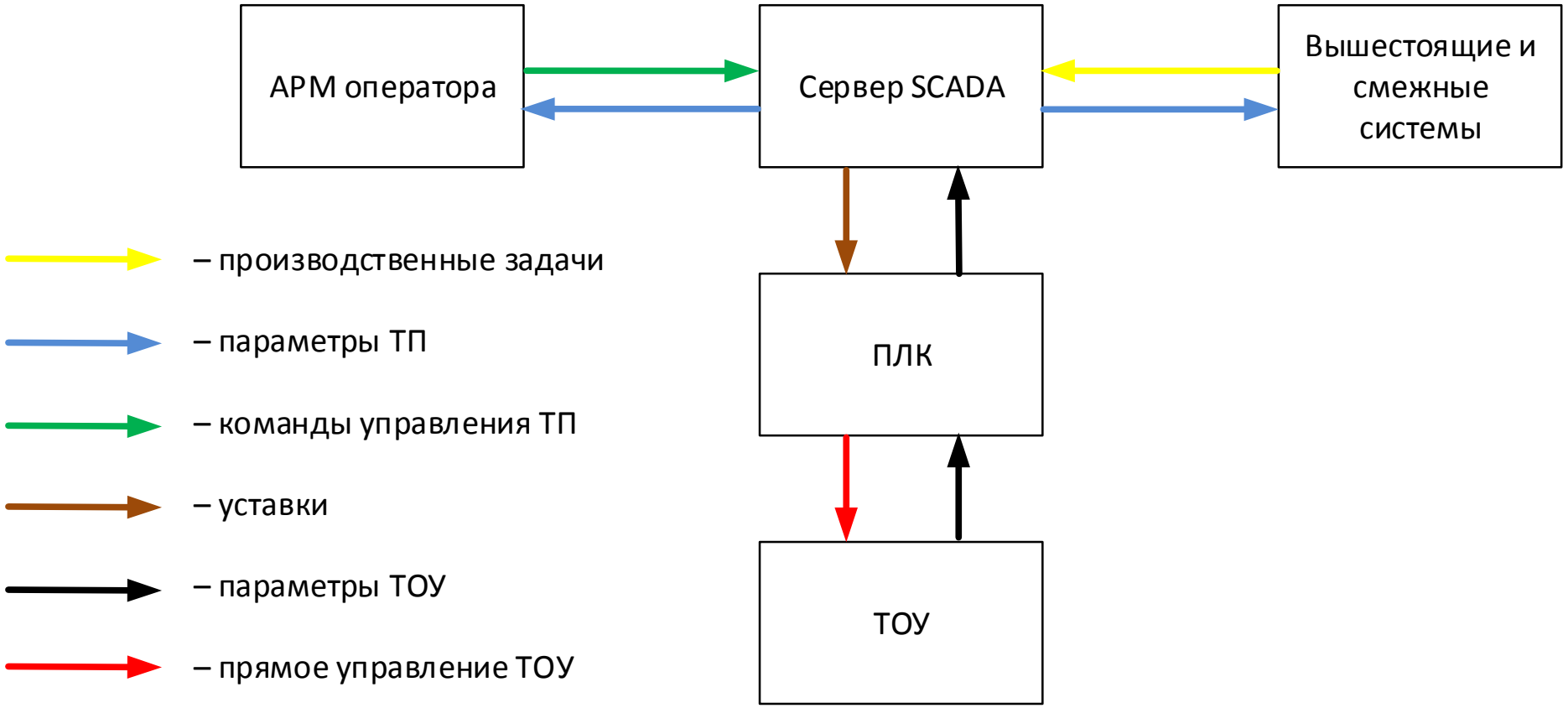
Цель атаки:
- Нарушение реализации ТП
- Порча оборудования



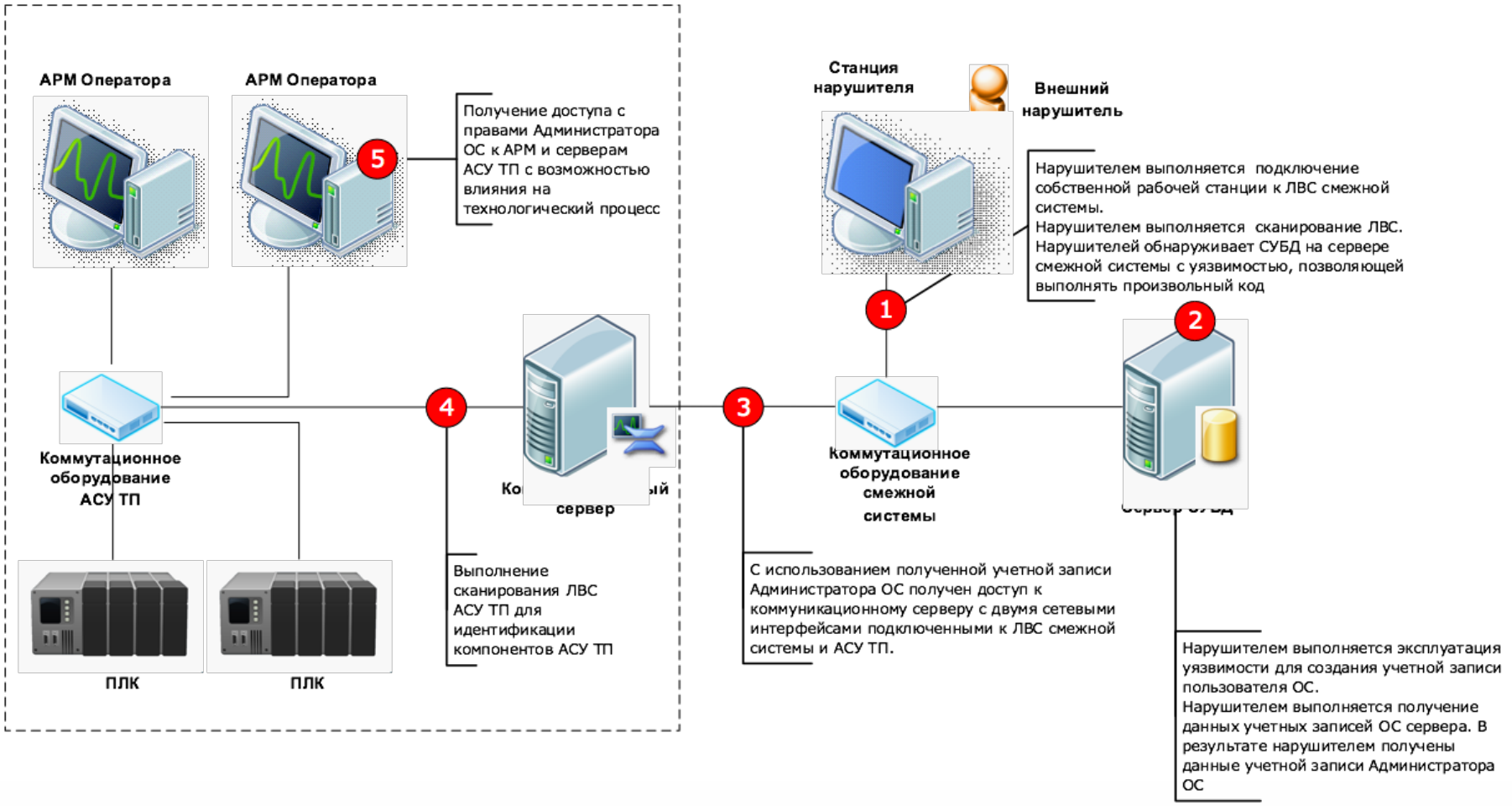
Представление результатов



Представление результатов



Визуализация сценариев



Выбор подхода к построению системы защиты

- Немного статистики
- Организационные и технические меры
- Встроенные и навесные средства защиты
- Выбор стратегии защиты

Статистика

- Результаты аудитов ИБ АСУ ТП:
  - В предприятиях металлургической отрасли и ТЭК
  - Более 30 производственных объектах
  - Включали более 150 АСУ ТП

Технические меры защиты

✓	**Сетевая безопасность**	• Обеспечивается для **88%** объектов • Для **17%** АСУ ТП есть удаленный доступ из корп. сети
–	**Встроенные механизмы защиты**	• HMI – аутентификация, режим киоска, ограничения доступа к меню • Системное ПО – по умолчанию • ПЛК – отключены
–	**Антивирусная защита**	• Применяется в **25%** АСУ ТП • Обновляется в **11%** АСУ ТП
–	**Обновления**	• Своевременные для **8%** АСУ ТП

Организационные мероприятия

Организационно-распорядительная документация	• Присутствует у **100%** предприятий
Специалисты ИБ на производственных объектах	• Присутствуют на **15%** объектов
Контроль выполнения требований ИБ подрядчиками	• Не осуществляется

Не только технические средства защиты

- ...в качестве первоочередных мер далеко не всегда требуется внедрение технических средств
- Существенно повысить уровень защищён-ности часто можно и без приобретения дорогостоящих средств защиты

Комментарий эксперта

Алексей Комаров
Региональный представитель, компания УЦСБ

Опыт выполнения проектов по проведению аудитов информационной безопасности промышленных систем автоматизации и управления на предприятиях ТЭК, в металлургической отрасли и др. показывает, что в качестве первоочередных мер далеко не всегда требуется внедрение технических средств. Так, например, из технических мер защиты на большинстве (88%) обследованных объектов уже были реализованы меры сетевой безопасности (той или иной степени полноты и достаточности), но при этом в 17% случаев для АСУ ТП присутствовал удаленный доступ и/или доступ из корпоративной сети. Встроенные механизмы защиты применяются в основном для ограничения несанкционированного взаимодействия на уровне человек-машина (режим киоска и пр.), на нижнем же уровне (ПЛК) такие механизмы чаще всего либо не настроены, либо отключены. Антивирусная защита иногда применяется (в 25% случаев), но базы почти не обновляются (обновления осуществляются только в 11%), да и сами своевременные обновления системного и прикладного ПО встречались у 8% АСУ ТП. Таким образом, существенно повысить уровень защищенности часто 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 защищенности, 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.

- ...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

Техническая реализация защитных мер

- **«Встроенные» защитные меры**
  - Ниже влияние на стабильность работы системы
  - Менее развитые механизмы защиты
  - Необходимо закладывать соответствующие решения при создании системы
- **«Навесные» защитные меры**
  - Выше вероятность сбоя или ошибки второго рода
  - Развитые механизмы защиты
  - Требуют дополнительных вычислительных ресурсов и ресурсов сетей передачи данных

Временной вектор атаки

Подготовка	Реализация	Нанесение ущерба

Прокативная защита	Активная защита	Реактивная защита

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

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
		

Актуальные направления защиты

Классы мер по обеспечению ИБ		
Превентивные	**Детектирующие**	**Компенсирующие**
Обеспечение сетевой безопасности		Применение средств резервного копирования и восстановления
Безопасная настройка компонентов	Управление конфигурациями и изменениями	
Управление доступом	Регистрация и сбор событий безопасности	
Защита от вредоносного ПО	Контроль защищённости	
Физическая безопасность и ИТСО		
Организационные меры (Политика ИБ, обучение персонала, расследования)		

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**

Функции DATAPK®

- Инвентаризация компонентов АСУ ТП
- Контроль конфигураций компонентов АСУ ТП
- Централизованный сбор, корреляция, систематизация и анализ значимости событий ИБ в АСУ ТП
- Контроль защищённости компонентов АСУ ТП
- Обнаружение компьютерных атак
- Контроль соответствия требованиям по обеспечению ИБ (включая 187-ФЗ и его подзаконные акты)

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

DATAPK

Полуфиналист Skolkovo Startup Village 2016

STARTUP VILLAGE
Инновационный центр Сколково, Москва

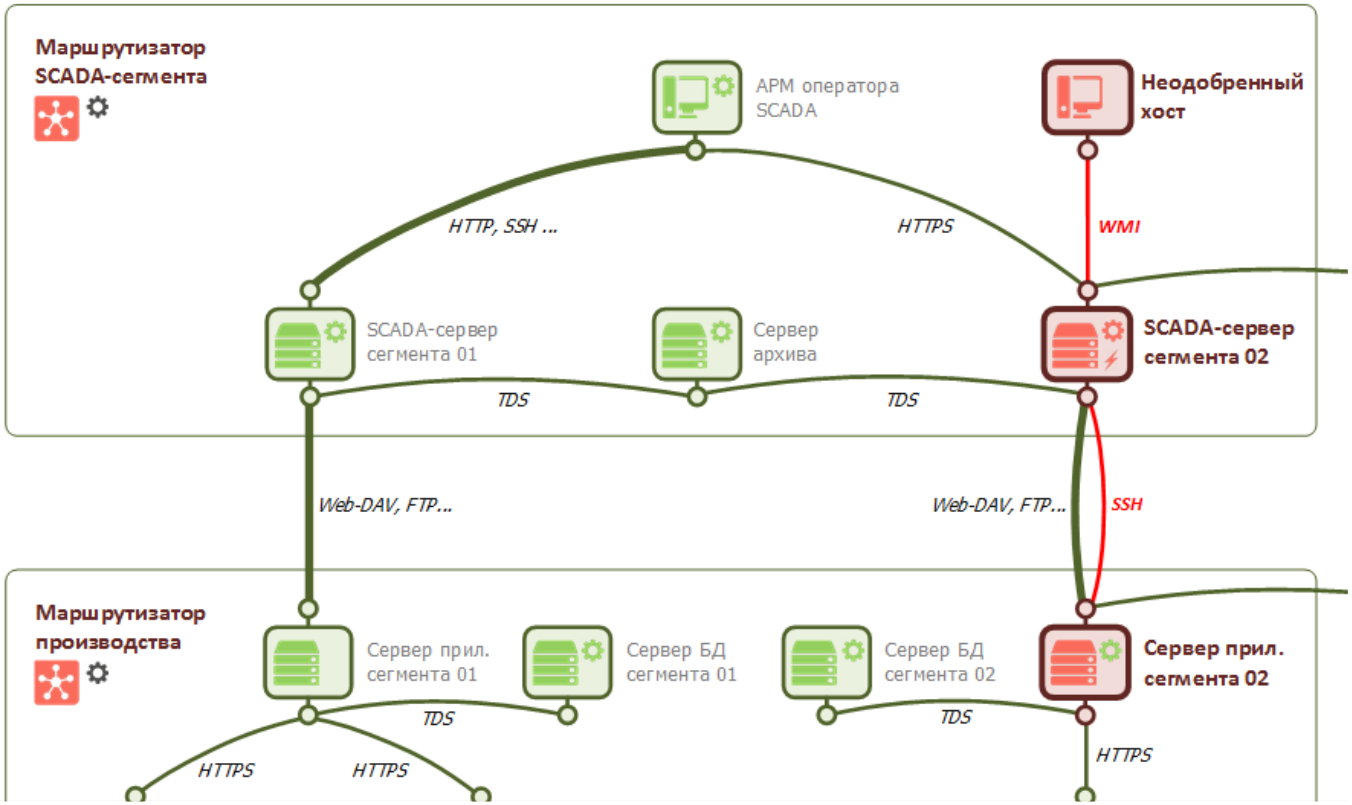
Схема реализации функций DATAPK®

datapk

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

DATAPK

* Станция переработки СПДТ 31-02



DATAPK® – компромисс между встроенными и навесными средствами

Модуль	Функции модуля
Модуль мониторинга	Сбор событий ИБ Обнаружение атак Выявление сетевых аномалий Сбор конфигураций Определение текущего состава активов Выявление изменений в составе активов Проверка активов на наличие уязвимостей
Модуль корреляции	Корреляция событий ИБ Выявление изменений конфигураций
Модуль анализа	Выявление инцидентов ИБ Оценка выполнения требований безопасной конфигурации Формирование отчетов Интеграция со смежными системами

Режимы функционирования DATAPK®

Пассивный мониторинг	однонаправленное получение информации, мониторинг на основе анализа сетевого трафика, без воздействия на компоненты системы
Активный мониторинг	взаимодействие с компонентами системы (запрос-ответ), сбор конфигураций и событий
Сканирование защищенности	выявление уязвимостей компонентов АСУ ТП

Таблицы по закрытию мер из 239 и 31 приказов ФСТЭК

Приложение
к Требованиям по обеспечению
безопасности значимых объектов
критической информационной
инфраструктуры Российской Федерации,
утвержденным приказом ФСТЭК России от
«25» декабря 2017 г. №239

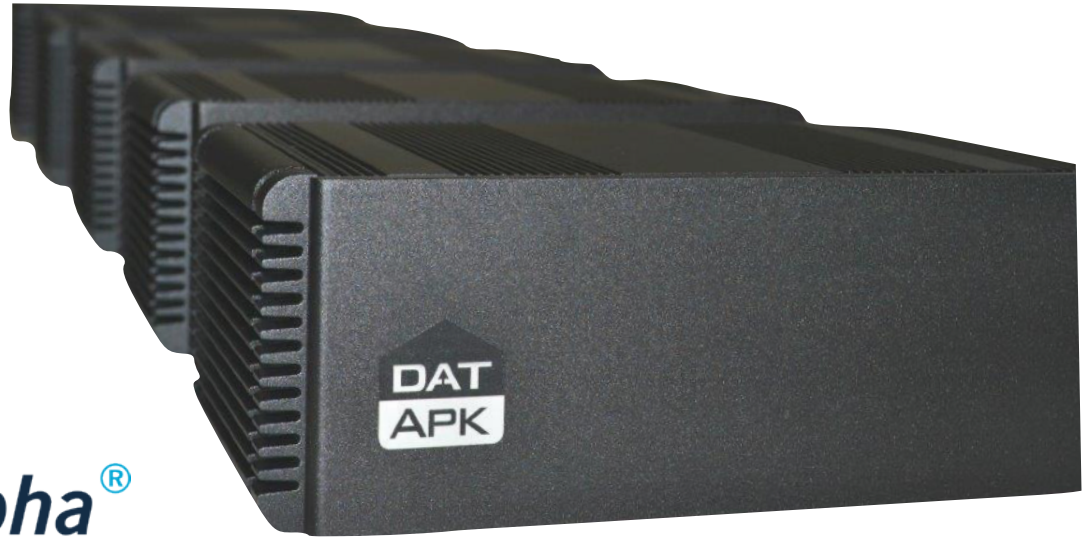
Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1

Можно запросить - akomarov@ussc.ru

DATAPK® - российская разработка

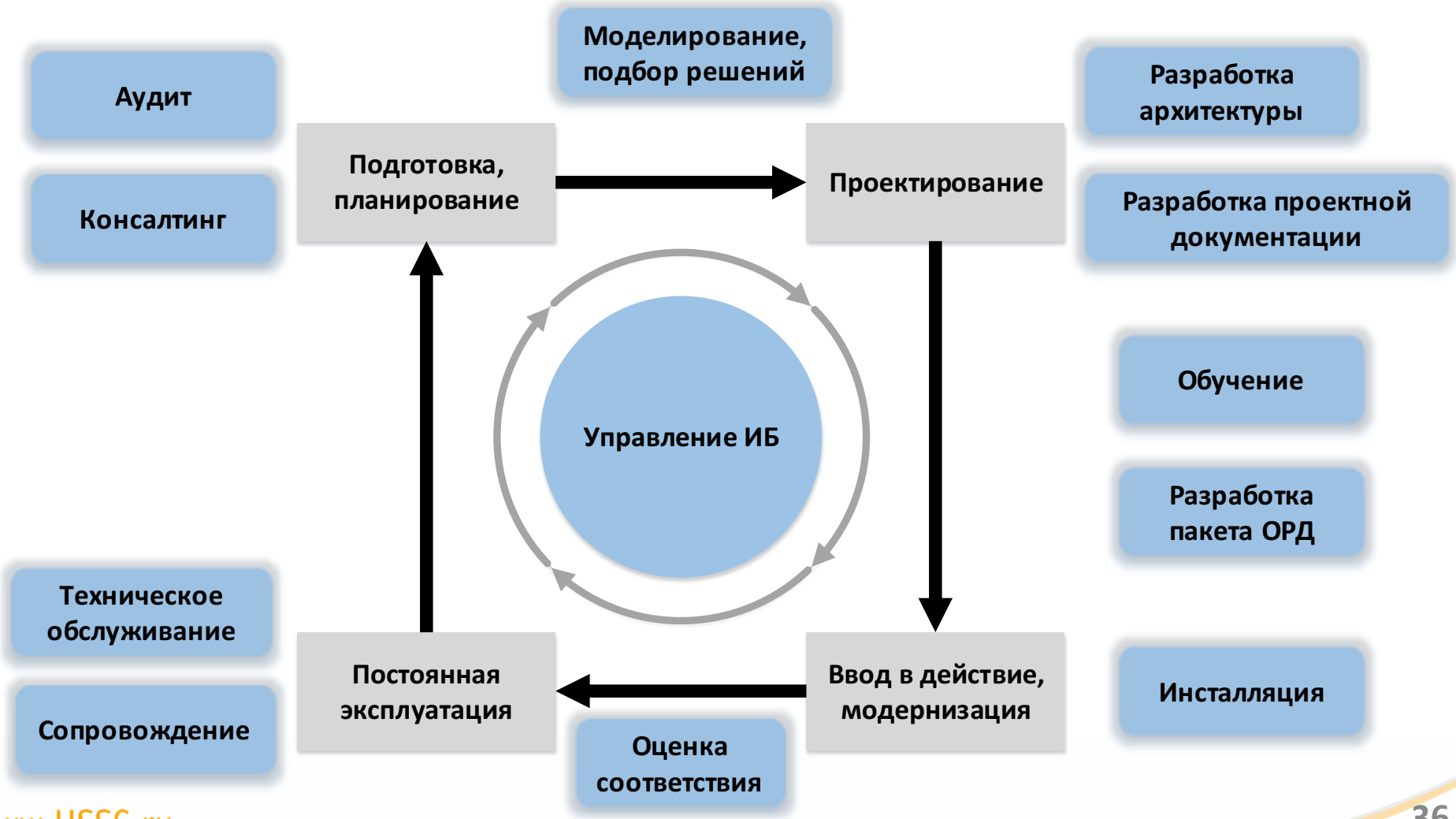
- Сертификат ФСТЭК России №3731
- Включен в Единый реестр российских программ для электронных вычислительных машин и баз данных
- Использует уникальные модули платформы CyberLympha (резидент Сколково)



Sk Участник

CyberLympha®

Безопасность – процесс, а не продукт



Серии вебинаров УЦСБ

- «ИБ АСУ ТП NON-STOP» (2 сезона)
- «Кибербезопасность АСУ ТП»
- «Безопасность КИИ и требования 187-ФЗ»

https://www.ussc.ru/events

https://youtube.com/usscpublic

Сообщества и группы

- Безопасность **КИИ 187-ФЗ**
  - Telegram-чат КИИ 187-ФЗ https://t.me/kii187fz
  - группа Facebook https://facebook.com/groups/kii187fz
  - группа ВКонтакте https://vk.com/kii187fz
  - Twitter https://twitter.com/kii187fz
- Сообщество **ruCyberSecurity**
  - Форум: https://ruCyberSecurity.ru
  - Slack: http://bit.ly/ruCyberSecurity

Спасибо! Вопросы?

Алексей Комаров
Менеджер по развитию решений
Уральский Центр Систем Безопасности

akomarov@USSC.ru
https://ZLONOV.ru