INNOSTAGE

ПОСТРОЕНИЕ И ЭКСПЛУАТАЦИЯ КИБЕРУСТОЙЧИВЫХ АСУ ТП В СОВРЕМЕННЫХ РЕАЛИЯХ

Айрат Мухаметшин

Заместитель руководителя отдела кибербезопасности АСУ ТП

ПРОБЛЕМАТИКА

Факторы влияния

1 РАЗВИТОСТЬ УПРАВЛЯЮШИХ ФУНКЦИЙ

АСУ ТП выполняют значительную часть операций
по управлению производственными объектами

2 КИБЕРЗАШИЩЕННОСТЬ

Устойчивость к кибератакам, способность
сохранения функционала

3 СОВМЕСТИМОСТЬ ПТК И СРЕДСТВ ЗАШИТЫ

Корректность выполнения функций по управлению
ТОУ во время кибератак

Влияние киберугроз на АСУ ТП

Условия управления ИБ объектов КИИ

Угрозы и нарушители

- Неуклонный рост количества инцидентов
- Сложность расследования

Ответственность

- Штрафы
- Санкции

Бюджетирование ИБ

- «ИБ денег не зарабатывает»
- Но «держаться надо»

Как быть?

Угрозы и нарушители

- Построение систем в защищенном исполнении
- Обеспечение совместимости ПТК АСУ ТП и средств защиты

Ответственность

Бюджетирование ИБ

- Обеспечение регулярности выполнения мер и «процессности» ИБ
- **Риск-ориентированный подход к обеспечению требований регуляторов**

АНАЛИЗ РИСКОВ ИБ В АСУ ТП:

ЧТО ТАКОЕ

ГДЕ НЕОБХОДИМ

Что такое «Анализ рисков ИБ в АСУ ТП»

Цель:

Выявление приоритетных направлений обеспечения ИБ

Задачи:

- Представление в денежном выражении последствий от инцидентов ИБ
- Обоснование затрат на реализацию мер обеспечения ИБ
- Целенаправленный выбор внедряемых средств защиты информации
- Присвоение приоритетов мероприятиям по защите информации

Позиционирование

ИБ

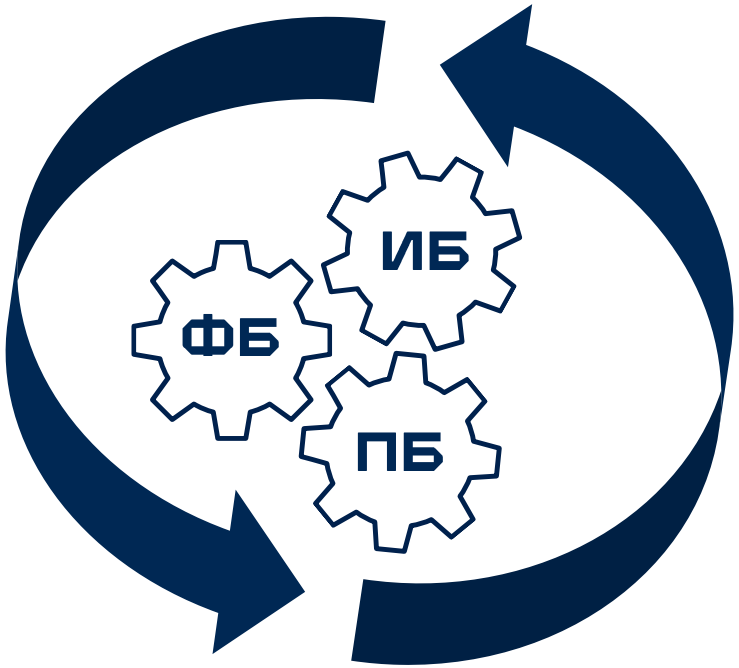
- Законодательство по ИБ ОКИИ
- Документы регуляторов
- Корпоративные стандарты ИБ

ФБ

- HAZOP-анализ
- Стандарты

ПБ

- Федеральный закон «О промышленной безопасности» № 116-ФЗ
- Федеральный закон «О безопасности объектов ТЭК» № 256-ФЗ



- Дополнение регуляторной составляющей и СТО
- Однозначная взаимосвязь инцидентов ИБ, ФБ, ПБ
- Основа комплексной риск-ориентированной системы мер по обеспечению ИБ объектов КИИ

Позиционирование

АУД

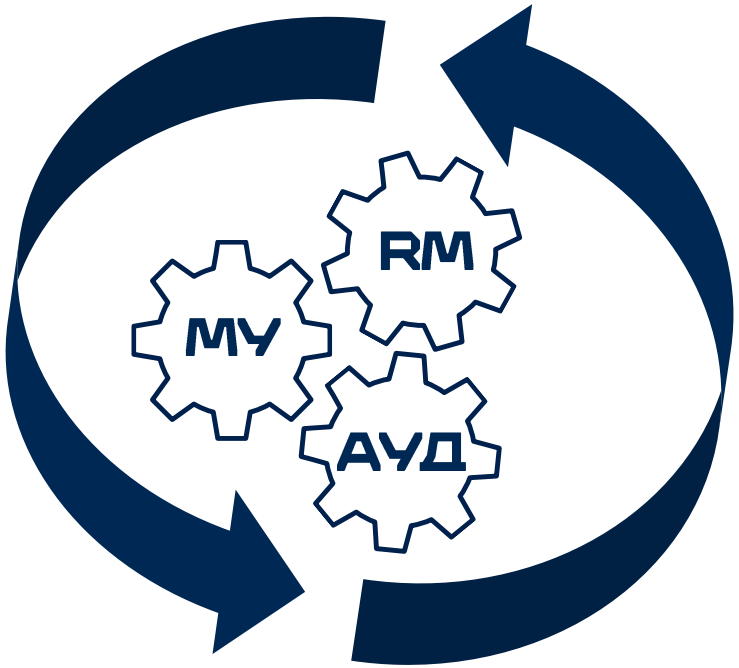
- Характеристики АСУТП
- Характеристики ТОУ и ТП

МУ

- Методика ФСТЭК России
- + MITRE
- + базы уязвимостей CVE

RM

- Методика оценки рисков
- Шкала оценки тяжести последствий



- Система выявления и ранжирования рисков
- Оценка потенциального ущерба
- Методы приоритезации направлений и обеспечительных мер

Схема реализации

1. Инвентаризация и определение ценности информационных активов
2. Идентификация последствий от реализации каждой из актуальных УБИ
3. Оценка потенциального ущерба от реализации каждой угрозы в отношении каждого информационного актива
4. Оценка эффективности внедренных защитных мер
5. Определение наихудших сценариев реализации негативных последствий
6. Оценка приемлемости риска с учетом шкалы оценки уровня приемлемости
7. Приоритезация мер защиты

Исходные данные

Информационная безопасность

- Результаты аудита ИБ
- Модель угроз
- Модель нарушителя ИБ
- **Статистика инцидентов ИБ**

Функциональная безопасность

- Структурные характеристики ПТК АСУ ТП
- Функциональные схемы АСУ ТП

Промышленная безопасность

- Декларация ПБ
- Паспорт безопасности ОПО
- Технологическая карта ТП

Описание работ

Сторона	Действия
Заказчик	Передача Исполнителю: • Перечня ОКИИ, для которых необходимо провести анализ рисков ИБ • Исходных данных по информационным активам в составе ОКИИ
Исполнитель	• Обследование ОКИИ, уточнение состава и структуры ИА • Уточнение модели угроз ИБ • Составление перечня последствий для ОКИИ от реализации УБИ
Заказчик и Исполнитель	• Формирование перечня последствий для технологического процесса • Оценка последствий инцидентов промышленной безопасности • Формирование шкалы оценки ущерба (установление границ приемлемости)
Исполнитель	• Составление деревьев событий при реализации актуальных УБИ • Проведение оценки рисков • Формирование реестра рисков

Отчетная документация

Отчет по анализу рисков ИБ АСУ ТП

- Методика оценки рисков
- Ценность информационных активов
- Последствия реализации угроз ИБ
- Шкала оценки ущерба от последствий реализации УБИ

Реестр рисков ИБ АСУ ТП

- Риски ИБ АСУ ТП (приемлемые и неприемлемые)
- Размер потенциального ущерба

АНАЛИЗ РИСКОВ:

КОГДА
ПРИМЕНЯТЬ

ДЛЯ ЧЕГО
НЕОБХОДИМ

Получаемые преимущества

Подразделения обеспечения ИБ

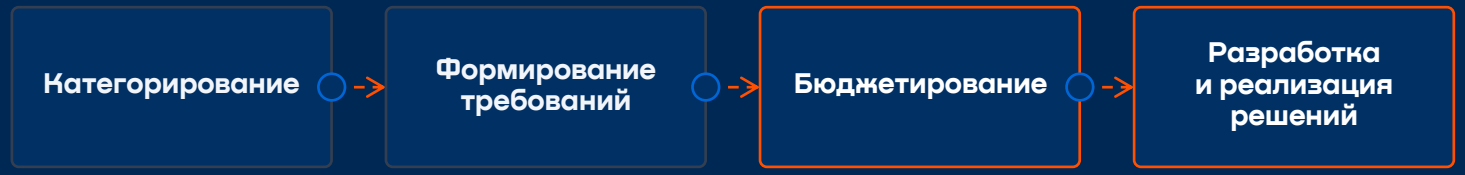
- Определение наиболее проблемных областей обеспечения ИБ
- Прогнозирование эффективности реализуемых мер ИБ
- Обоснование целесообразности внедрения решений по ИБ
- Упрощение согласования бюджета на обеспечение ИБ

Заказчик

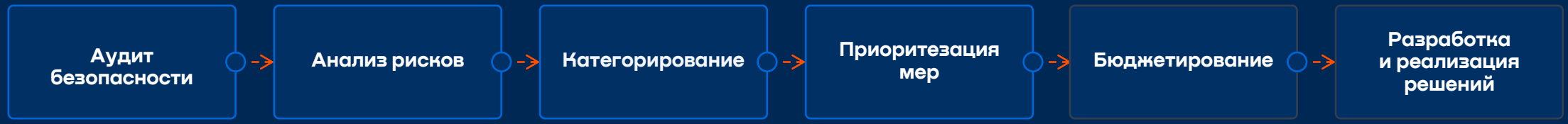
- Оценка потенциального экономического ущерба
- Эффективный бюджет на ИБ объектов КИИ

Когда применять?

«КЛАССИЧЕСКИЙ» ПУТЬ



«ИБ 2.0»



Конкурентные преимущества

Преемственность

- Использование результатов аудита, моделирования угроз ИБ, категорирования

Адаптивность

- Адаптация методики под отрасль и для Заказчика
- Встраиваемость в систему риск-менеджмента

Комплексность

- Промышленная + функциональная + информационная безопасность
- АСУ ТП + технологический процесс + бизнес-процесс

Завершенность

- Доведение оценки «до рубля»
- Разработка дорожной карты реализации мер

Сложности

Преемственность

- Отсутствие статистических данных по инцидентам
- Необходимость определять вероятность «экспертным путем»
- **Субъективность и непрозрачность оценки**

Адаптивность

- Получение перечня наихудших сценариев
- Определение ущерба
- Меры по нейтрализации наихудших сценариев
- **Оптимальное соотношение ущерб/ стоимость нейтрализации**

Практикум

	Бизнес-процесс	Критичность процесса
1	Производство упаковки	МС
2	Подготовка исходного сырья	МЕ
3	Контроль качества исходного сырья	МЕ
4	Контроль технологического процесса и действия персонала	МС
5	Сопровождение инфраструктуры предприятия	МС
6	Сетевое взаимодействие	МЕ
7	Управление технологическим процессом	МЕ
8	Удаленное поддержание работоспособности рабочих станций и контроль их состояния	МЕ

Бизнес-процессы и оценка их критичности

Практикум

1. **Воздействие на информацию**

   (утечка (перехват), модификация (подмена), уничтожение, блокирование (прерывание передачи)

2. **Ущерб для компонентов и подсистем объекта защиты**

3. **Ущерб бизнес-процессам, выполнение которых обеспечивается подсистемами и компонентами объекта защиты**

4. **Ущерб бизнесу, связанный с воздействием на бизнес-процессы**

5. **Ущерб, выходящий за рамки воздействия на бизнес — угроза жизни и здоровью людей, вред окружающей среде, ущерб инфраструктуре обеспечения жизнеспособности населения, ущерб государственным сервисам**

Практикум

	Сегмент ТОУ	Воздействие на исполнительный механизм	Технологический параметр, отклонение которого приведет к нарушению ТП	Следующее за отклонением технологического параметра нарушение ТП
1	Установка подготовки исходного сырья	Нерегламентированное обслуживание и некорректная эксплуатация, изменение алгоритма работы аппарата	Скорость подачи материалов для изготовления исходного сырья	Сырье некорректной консистенции и состава, что может провести к приготовлению готовой продукции в неправильных пропорциях, быстрому износу измельчителя или его заклиниванию, и как следствие к повреждению оборудования
2	Установка по производству готовой продукции	Нерегламентированное обслуживание и некорректная эксплуатация, изменение алгоритма работы аппарата	Расход основного ингредиента Расход сопутствующих ингредиентов	Приготовление исходного сырья в неправильных пропорциях

Воздействия на исполнительные механизмы, отклонения технологических параметров и вызванные ими нарушения технологического процесса

Промежуточные итоги и дальнейшие шаги

1. Формирование базовой методики
2. Формирование kill-chain цепочек
3. Доработка методики АР в соответствии с методиками аудита ISO 27005
4. Автоматизация разработки отчетной документации
5. Предоставление услуги оценки рисков как онлайн-сервиса ИБ

Контакты

Айрат Мухаметшин

Заместитель руководителя отдела кибербезопасности АСУ ТП

Innostage

моб. +7 (967) 368–79–65

Ayrat.Mukhametshin@innnostage-group.ru

СПАСИБО
ЗА ВНИМАНИЕ!