INNOSTAGE

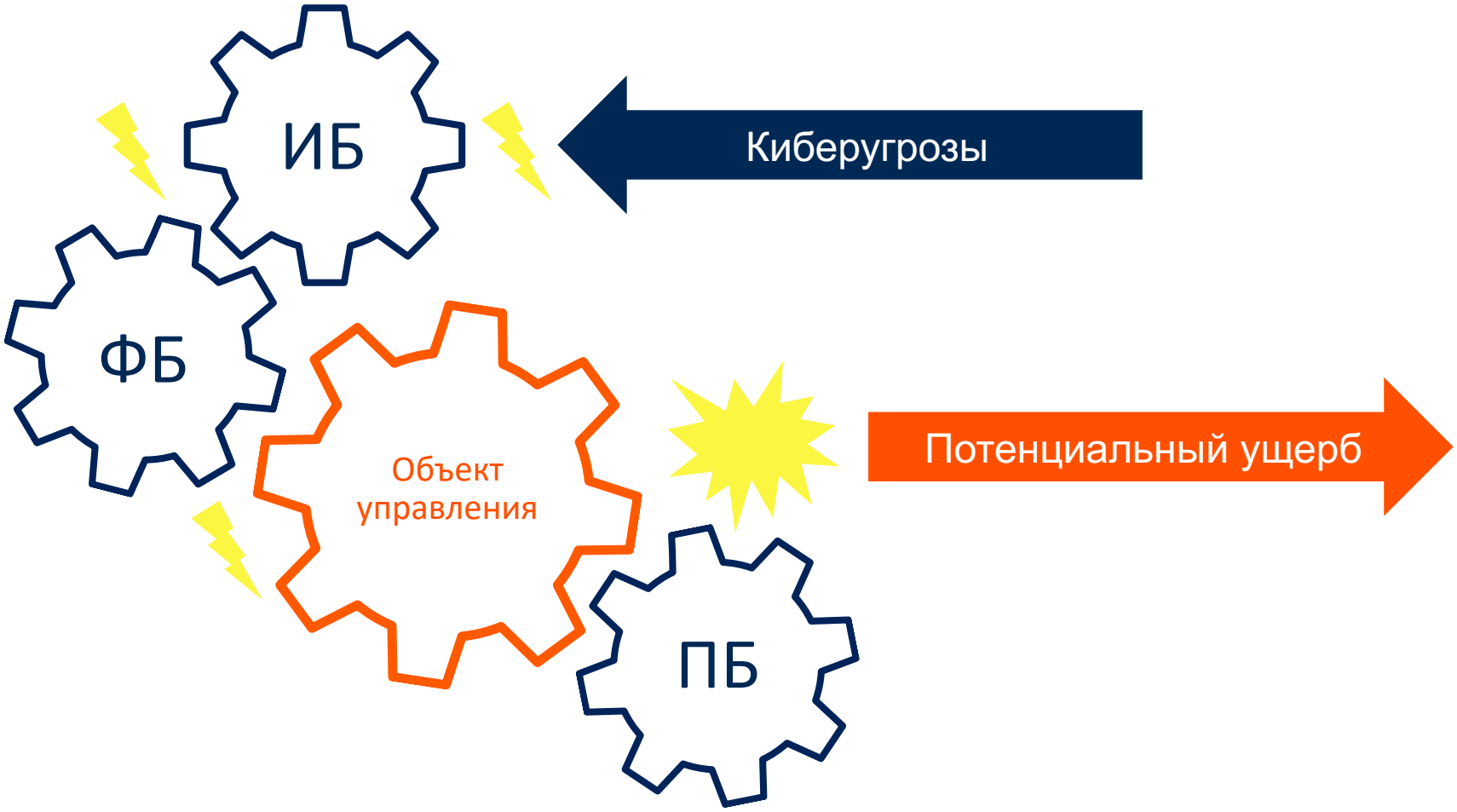
Анализ рисков информационной безопасности в АСУ ТП: что, где, когда и для чего

Авраменко Дмитрий

Руководитель отдела Кибербезопасности АСУ ТП

Проблематика

Влияние киберугроз на ОКИИ



Условия управления ИБ на объектах КИИ

Угрозы и нарушители

- Неуклонный рост количества инцидентов
- Сложность расследования

Ответственность

- Штрафы
- Санкции

Бюджетирование ИБ

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

Нормативная база

- Методическая неопределенность: «делать надо, но непонятно как»

В чем проблема?

Решения принимаются на основе:

- Интуиции и исходя из собственного опыта
- «Выжидающем» подходе – до серьезных инцидентов
- Исключительно на результатах моделирования угроз ИБ

При этом:

- «Директивный» характер НТД
- Отсутствие понимания, с чего начинать
- Необходимость «отстоять» бюджет ИБ

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

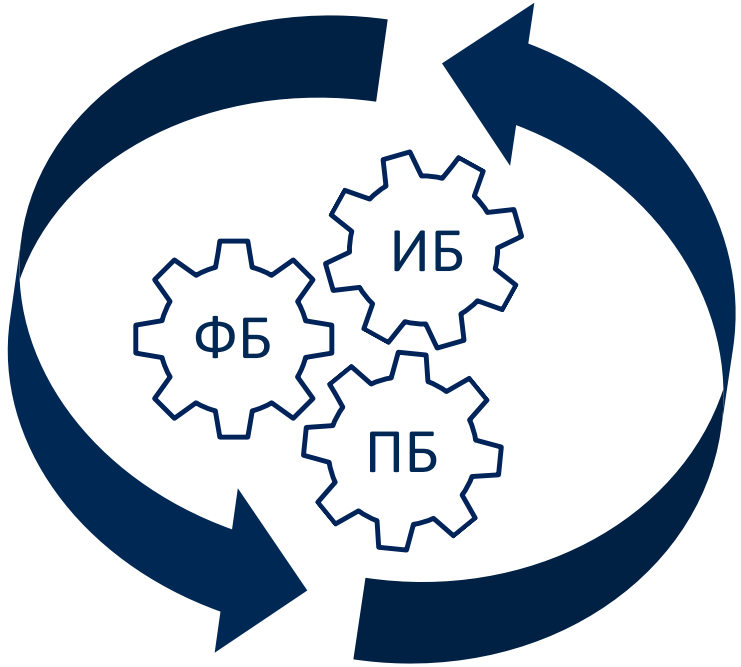
- Законодательство по ИБ ОКИИ
- Документы Регуляторов
- Корпоративные стандарты ИБ

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

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

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

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
- Обоснование целесообразности внедрения решений по ИБ
- Прогнозирование эффективности реализуемых мер ИБ
- «Упрощение» согласования бюджета на обеспечение ИБ

Предприятие в целом

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

Когда применять?

Преимущества

Преемственность

- Использование результатов аудита, моделирования угроз ИБ, категорирования

Адаптивность

- Адаптация методики под отрасль и для Заказчика
- Совместная проработка в части оценки ущерба

Комплексность

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

Завершенность

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

Сложности

Вероятностный подход

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

Подход «от сценария»

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

Дальнейшие шаги

1. Наработка статистики инцидентов
2. Алгоритмизация и автоматизация расчетов
3. Автоматизация разработки отчетной документации
4. Предоставление услуги оценки рисков как «продукта»

Контакты

Авраменко Дмитрий

Руководитель отдела Кибербезопасности АСУ ТП, Innostage

Dmitry.Avramenko@innostage-group.ru

Спасибо за внимание!