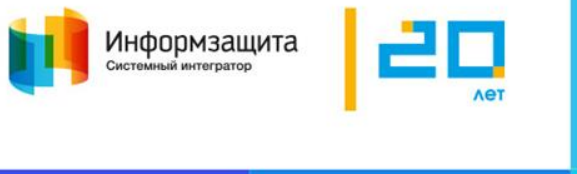

Модель угроз - технические аспекты и применяемые методики

Даренский Дмитрий

Начальник отдела промышленных систем

ЗАО НИП «ИНФОРМЗАЩИТА»

УГРОЗА БЕЗОПАСНОСТИ

- ВОЗМОЖНЫЕ ДЕЙСТВИЯ ИЛИ СОБЫТИЯ, КОТОРЫЕ МОГУТ ВЕСТИ К НАРУШЕНИЯМ СВОЙСТВ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
  - КОНФИДЕНЦИАЛЬНОСТИ
  - ДОСТУПНОСТИ
  - ЦЕЛОСТНОСТИ

МОДЕЛЬ УГРОЗ

- ОПИСАНИЕ СУЩЕСТВУЮЩИХ УГРОЗ ИБ, ИХ АКТУАЛЬНОСТИ, ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ И ПОСЛЕДСТВИЙ

ЗАЧЕМ НУЖНА МОДЕЛЬ?

- Определить от чего защищаться
- Определить что конкретно необходимо защищать
- Что и кто может создавать проблемы
- Насколько оно актуально, опасно, и может ли произойти

ТО ЕСТЬ

- Определить угрозы
- Определить объекты защиты и объекты воздействия
- Определить источники угроз
- Определить уровень риска реализации угроз
  - Уровень ущерба
  - Вероятность
  - Актуальность

Информзащита
Системный интегратор
20 лет

ЧТО ЗАЩИЩАТЬ

ОБЪЕКТЫ ЗАЩИТЫ

- ПРОЦЕСС
- ТИП СИСТЕМ
- ВИД СИСТЕМ
- ОТДЕЛЬНАЯ КОНКРЕТНАЯ СИСТЕМА

ОБЪЕКТЫ ВОЗДЕЙСТВИЯ

- АРМ
- СЕТЕВЫЕ УСТРОЙСТВА
- ТЕРМИНАЛЫ ЗАЩИТ
- КОНТРОЛЛЕРЫ
- УСТРОЙСТВА ВВОДА/ВЫВОДА
- HMI
- ПРИКЛАДНОЕ И СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
- БАЗЫ ДАННЫХ

Информзащита
Системный интегратор
20 лет

ОТ ЧЕГО ЗАЩИЩАТЬ

- УГРОЗЫ БЕЗОПАСНОСТИ
  - …
  - ОПРЕДЕЛЕНИЕ СЕТЕВОГО АДРЕСА (IP АДРЕСА)
  - ОПРЕДЕЛЕНИЕ ОТКРЫТЫХ ПОРТОВ УДАЛЕННОГО ХОСТА
  - ИДЕНТИФИКАЦИЯ ЗАПУЩЕННЫХ СЕТЕВЫХ СЛУЖБ
  - ОПРЕДЕЛЕНИЕ ТИПА ОС УДАЛЕННОГО ХОСТА
  - …
  - ПОДБОР ПАРОЛЯ И УЧЕТНОГО ИМЕНИ
  - …
  - ВНЕДРЕНИЕ ЛОЖНОГО ДОВЕРЕННОГО ОБЪЕКТА

ВСЕГО ОКОЛО 110 ВИДОВ

СОГЛАСНО СТАНДАРТУ ОАО «ФСК ЕЭС» СТО 56947007-29.240.01.150-2013 ПАО «ФСК ЕЭС»

(РАЗРАБОТАН НА ОСНОВЕ БАЗОВОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
В КЛЮЧЕВЫХ СИСТЕМАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ФСТЭК)

ИСТОЧНИКИ УГРОЗ

- Антропогенные
  - Обусловлены действиями людей
- Техногенные
  - Обусловлены техническими воздействиями без непосредственного участия человека

ОТНОШЕНИЕ К ОБЪЕКТУ ЗАЩИТЫ

- Внешние
  - Находятся за границами объекта защиты, не имеют прав доступа к нему
- Внутренние
  - Находятся внутри границ объекта защиты, имеют права доступа к нему

КАКАЯ МОЖЕТ БЫТЬ МОДЕЛЬ

БАЗОВАЯ МОДЕЛЬ УГРОЗ

- ПЕРЕЧЕНЬ БАЗОВЫХ УГРОЗ
- ОБОБЩЕННЫЙ ПЕРЕЧЕНЬ ОБЪЕКТОВ ВОЗДЕЙСТВИЯ ТИПОВ СИСТЕМ (РЗА, АСУ ТП, ПА, ПРОЧИЕ ПОДСИСТЕМЫ АСТУ)
- ОБОБЩЕННЫЙ ПЕРЕЧЕНЬ НАРУШИТЕЛЕЙ: ВНЕШНИЕ (РАЗРАБОТЧИКИ, СУБЪЕКТЫ НЕ ИМЕЮЩИЕ ПРАВ ДОСТУПА), ВНУТРЕННИЕ (АДМИНИСТРАТОРЫ ИТ, ОПЕРАТОРЫ, АДМИНИСТРАТОРЫ ИБ)

ЧАСТНАЯ МОДЕЛЬ УГРОЗ

- ОПРЕДЕЛЕНИЕ КРИТИЧНОСТИ ВЛИЯНИЯ СИСТЕМЫ НА УПРАВЛЯЕМЫЙ ПРОЦЕСС
- ПЕРЕЧЕНЬ БАЗОВЫХ УГРОЗ
- ПЕРЕЧЕНЬ ОБЪЕКТОВ ВОЗДЕЙСТВИЯ ОТДЕЛЬНЫХ ВИДОВ СИСТЕМ (РЗА ВЛ С ОДНОСТОРОННИМ ПИТАНИЕМ, РЗА БЛОКА ГЕНЕРАТОР-ТРАНСФОРМАТОР, АСУ ТП ПС, ССПИ)
- ПЕРЕЧЕНЬ НАРУШИТЕЛЕЙ: ВНЕШНИЕ (РАЗРАБОТЧИКИ, СУБЪЕКТЫ НЕ ИМЕЮЩИЕ ПРАВ ДОСТУПА), ВНУТРЕННИЕ (АДМИНИСТРАТОРЫ ИТ, ОПЕРАТОРЫ, АДМИНИСТРАТОРЫ ИБ)
- ОПРЕДЕЛЕНИЕ СТЕПЕНИ РИСКА РЕАЛИЗАЦИИ КАЖДОЙ КОНКРЕТНОЙ УГРОЗЫ
  - ОПРЕДЕЛЕНИЕ УРОВНЯ УЩЕРБА (ОПАСНОСТИ) УГРОЗЫ
  - ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗЫ
  - ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ УГРОЗЫ

В ЧЕМ ПОЛЬЗА

БАЗОВАЯ МОДЕЛЬ УГРОЗ

- ПОЗВОЛЯЕТ ОПРЕДЕЛИТЬ БАЗОВЫЙ НАБОР ТРЕБОВАНИЙ И РЕКОМЕНДАЦИЙ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОПРЕДЕЛЕННОГО ТИПА ОБЪЕКТОВ ЗАЩИТЫ
- ПОЗВОЛЯЕТ ОПРЕДЕЛИТЬ БАЗОВЫЙ НАБОР МЕР ЗАЩИТЫ

ЧАСТНАЯ МОДЕЛЬ УГРОЗ

- ПОЗВОЛЯЕТ ОПРЕДЕЛИТЬ НЕОБХОДИМОСТЬ ЗАЩИТЫ КОНКРЕТНОГО ВИДА ОБЪЕКТА ЗАЩИТЫ (СИСТЕМЫ)
- ПОЗВОЛЯЕТ ОПРЕДЕЛИТЬ КОНКРЕТНЫЙ ПЕРЕЧЕНЬ УГРОЗ, ТРЕБУЮЩИХ РЕАГИРОВАНИЯ
- ПОЗВОЛЯЕТ ОПРЕДЕЛИТЬ КОНКРЕТНЫЙ НАБОР МЕР ЗАЩИТЫ, ТРЕБУЮЩИХ РЕАЛИЗАЦИИ
- ЯВЛЯЕТСЯ ОСНОВОЙ ДЛЯ РАЗРАБОТКИ ТРЕБОВАНИЙ К СИСТЕМЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

РАЗРАБОТКА БАЗОВОЙ МОДЕЛИ

РАЗРАБОТКА КЛАССИФИКАТОРА ОБЪЕКТОВ ЗАЩИТЫ

- ОПРЕДЕЛЯЕМ ТИПЫ И ВИДЫ ОБЪЕКТОВ ЗАЩИТЫ
- ОПИСЫВАЕМ ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ ОБЪЕКТОВ ЗАЩИТЫ
- ОПРЕДЕЛЯЕМ ТИПЫ ТЕХНИЧЕСКОГО ИСПОЛНЕНИЯ ОБЪЕКТОВ ЗАЩИТЫ
  - ЭЛЕКТОМЕХАНИЧЕСКИЕ
  - МИКРОПРОЦЕССОРНЫЕ
  - МИКРОПРОЦЕССОРНЫЕ ПО СТАНДАРТУ МЭК 61850
- ОПИСЫВАЕМ МАКСИМАЛЬНО ВОЗМОЖНОЕ КОЛИЧЕСТВО ОБЪЕКТОВ ВОЗДЕЙСТВИЯ И ТИПОВЫЕ АРХИТЕКТУРЫ ОБЪЕКТОВ ЗАЩИТЫ С УЧЕТОМ ТИПОВ ИСПОЛНЕНИЯ

РАЗРАБОТКА БАЗОВОЙ МОДЕЛИ УГРОЗ

- ЭКСПЕРТНО ОПРЕДЕЛЯЕМ БАЗОВЫЙ НАБОР УГРОЗ ДЛЯ ОТДЕЛЬНОГО ТИПА ОБЪЕКТОВ ЗАЩИТЫ
- ЭКСПЕРТНО ОПРЕДЕЛЯЕМ (НА БАЗЕ ПЕРЕЧНЯ) ОБЪЕКТЫ ВОЗДЕЙСТВИЯ, В ОТНОШЕНИИ КОТОРЫХ КОНКРЕТНАЯ УГРОЗА АКТУАЛЬНА
- ЭКСПЕРТНО ОПРЕДЕЛЯЕМ (НА БАЗЕ ТИПОВОЙ АРХИТЕКТУРЫ) ИСТОЧНИКИ УГРОЗ

Информзащита
Системный интегратор

20 лет

СПАСИБО !
ВОПРОСЫ?

Даренский Дмитрий
Начальник отдела промышленных систем
ЗАО НИП «ИНФОРМЗАЩИТА»