IT Security Conference 2016

МОДЕЛИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ КОРПОРАТИВНЫХ ОБЛАЧНЫХ ХРАНИЛИЩ

Галибус Т.В., Краснопрошин В.В.

Преимущества и уязвимости облачных сервисов

- виртуальное распределение ресурсов
- прозрачность обслуживания
- отсутствие централизованного контроля над содержимым облака

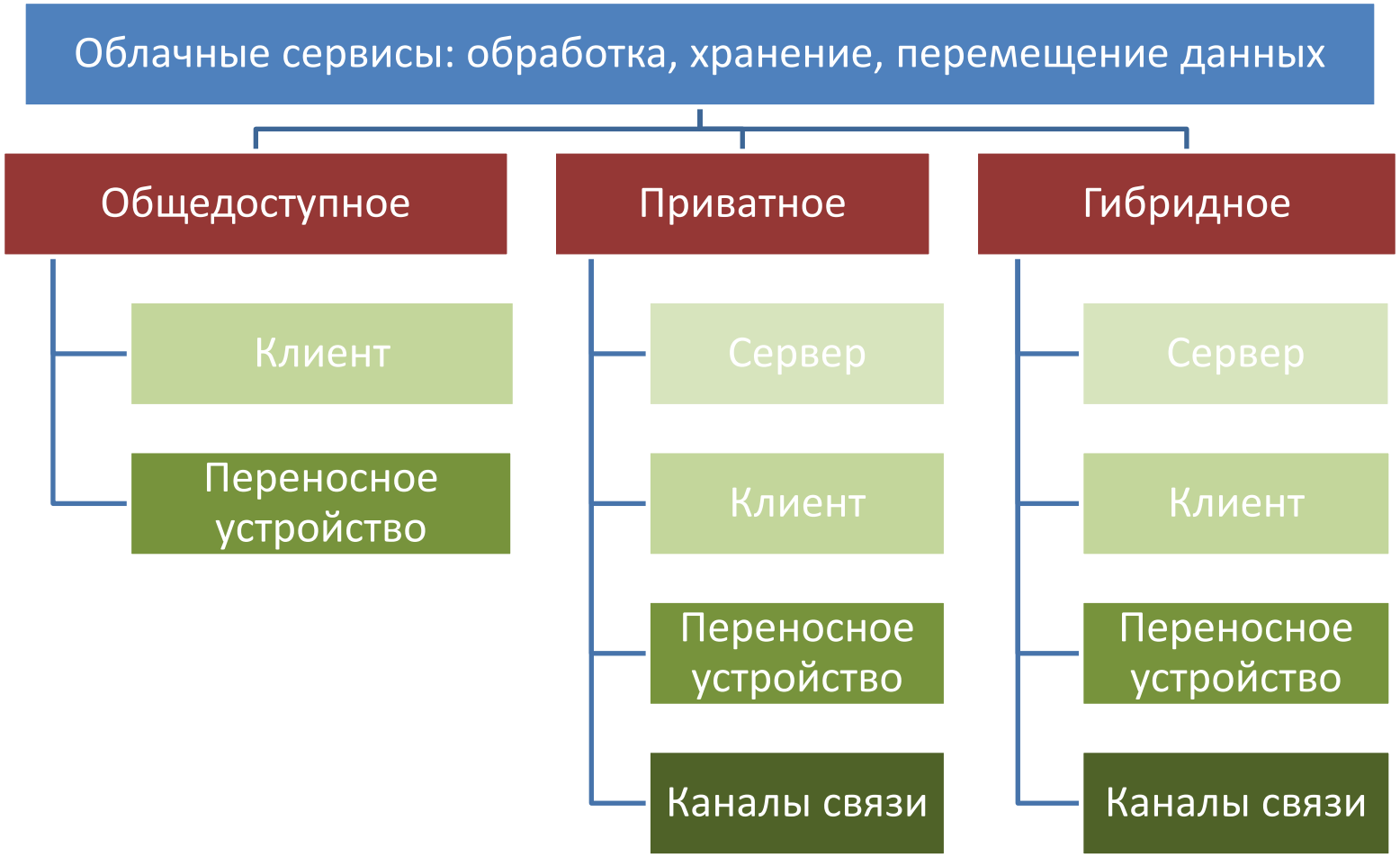
Построение комплексной СЗИ ОС

Итерационный процесс моделирования СЗИОС

Этапы моделирования СЗИОС

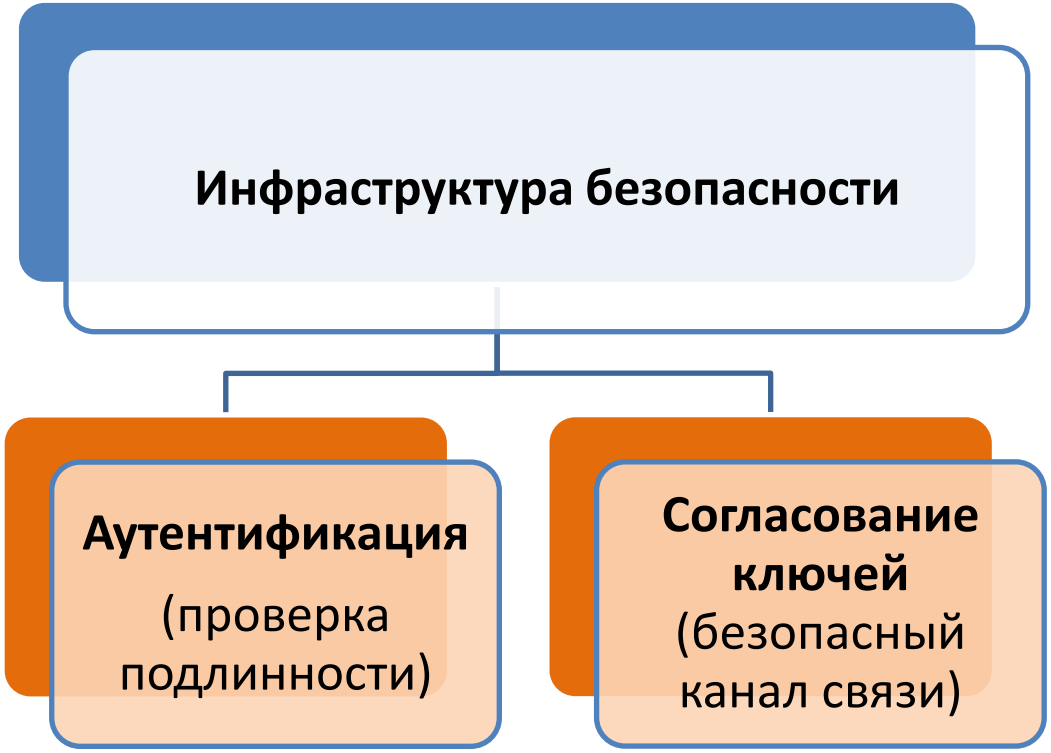
- Первый этап (*уровень инфраструктуры*):
  - Аутентификация
  - Согласование ключа
- Второй этап (*компонентный уровень*)
  - Авторизация
  - Аудит и мониторинг
  - Иные дополнительные механизмы

Структура и состав облачной системы



Первый этап

- Организация базовых механизмов – аутентификации и согласования ключей.



Методы аутентификации

- Парольная аутентификация
- Аутентификация на основе пароля и PIN
- Аутентификация с применением токенов (OAuth)
- Двухфакторная аутентификация
- Мультифакторная аутентификация

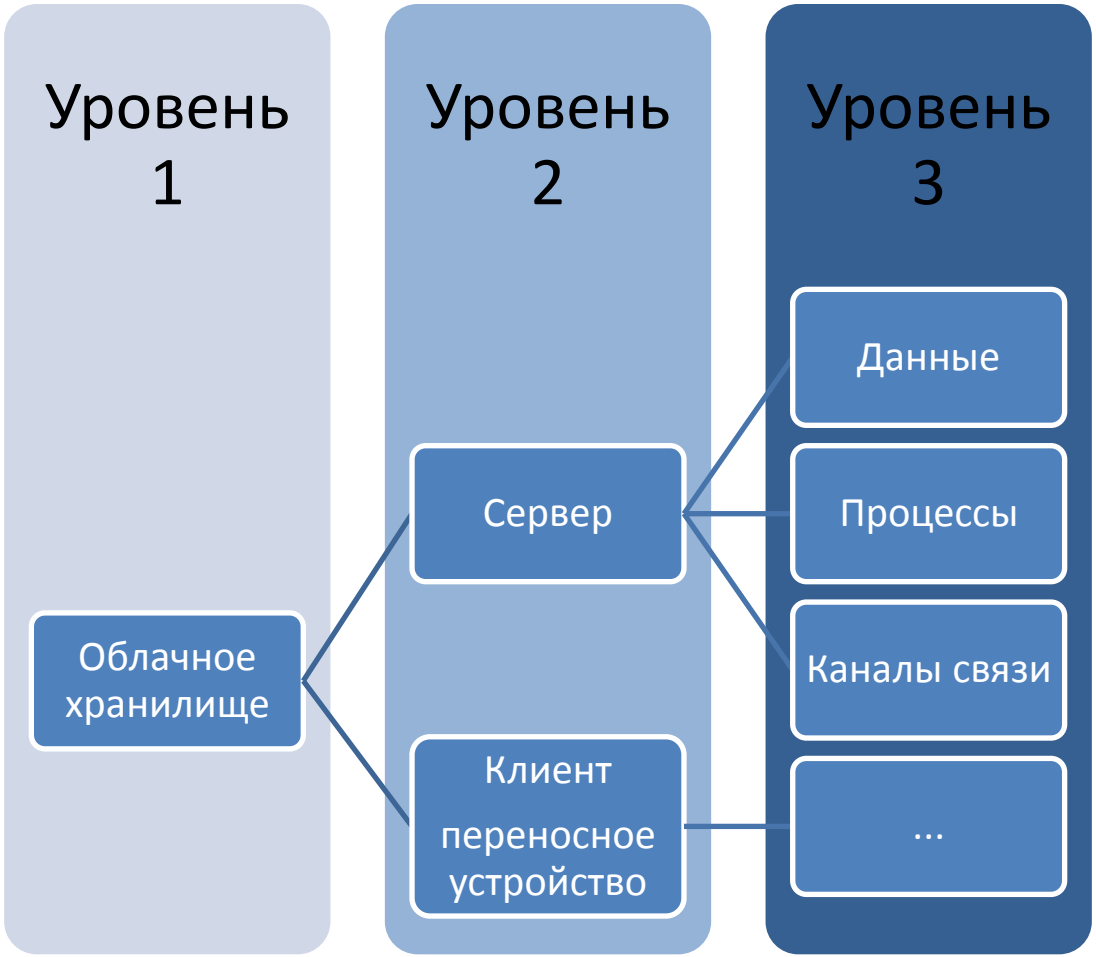
Механизмы согласования ключа

- На основе протокола Kerberos (симметричное шифрование)
- На основе инфраструктуры ОК (шифрование с открытым ключом)
- На основе инфраструктуры ША (шифрование с атрибутами)
- На основе гибридной инфраструктуры (несколько видов шифрования)

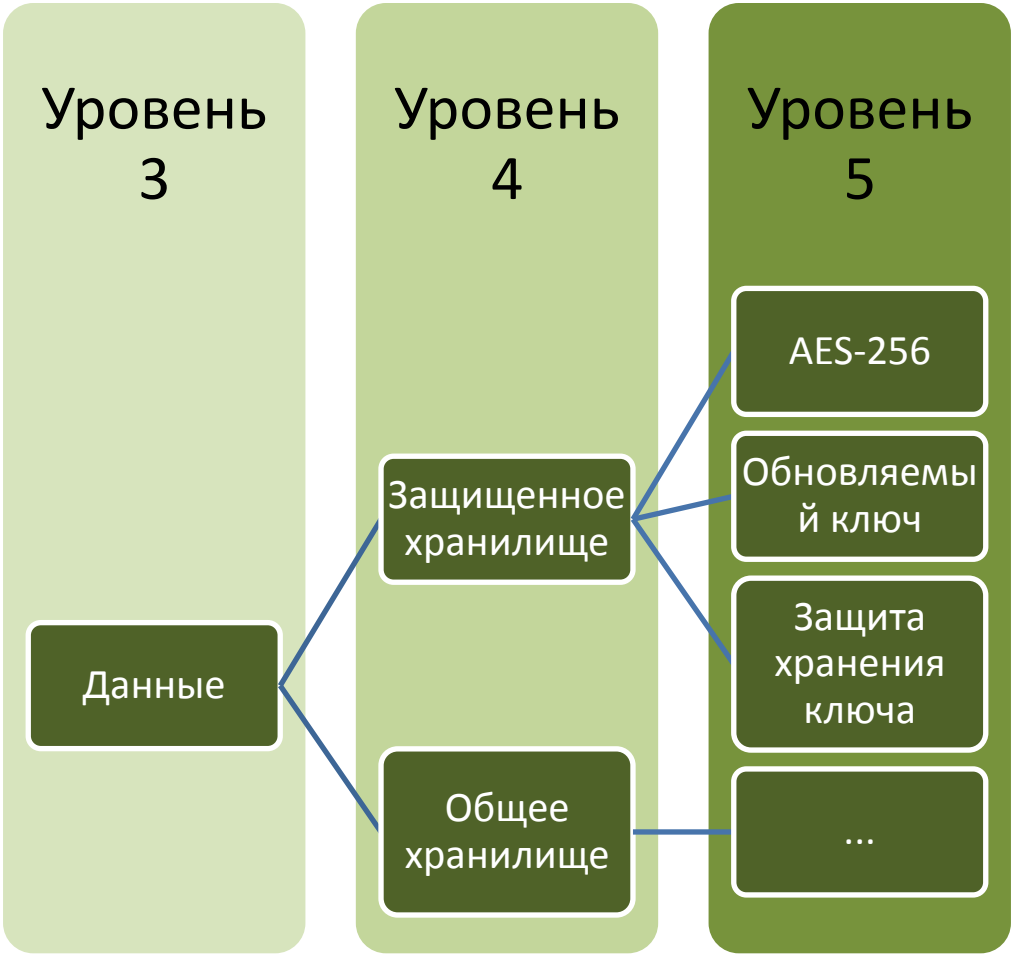
Анализ первого этапа

- наиболее подходящей ИБ для системы защиты корпоративного облака является **гибридная инфраструктура на основе ИША**
- позволяет обеспечить достаточно высокую степень защиты пользовательской аутентификации и передачи ключей, при условии выбора **надежных криптографических протоколов**
- не решает проблему настройки таких важных механизмов, как **аудит** и **авторизация**

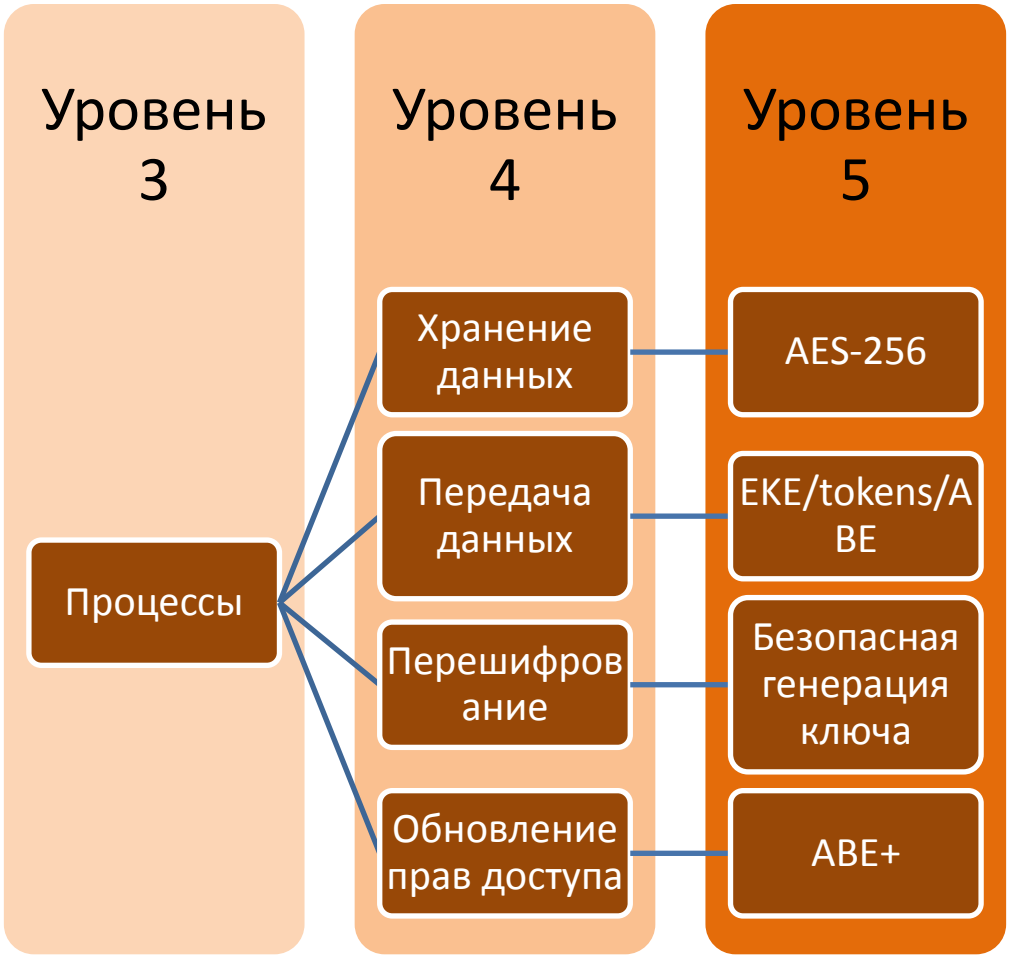
Этап 2 - детализация



Этап 2 - детализация



Этап 2 - детализация



Оптимизационная модель СЗИ ОС

$$SDS = (D, Ch, Pr),$$

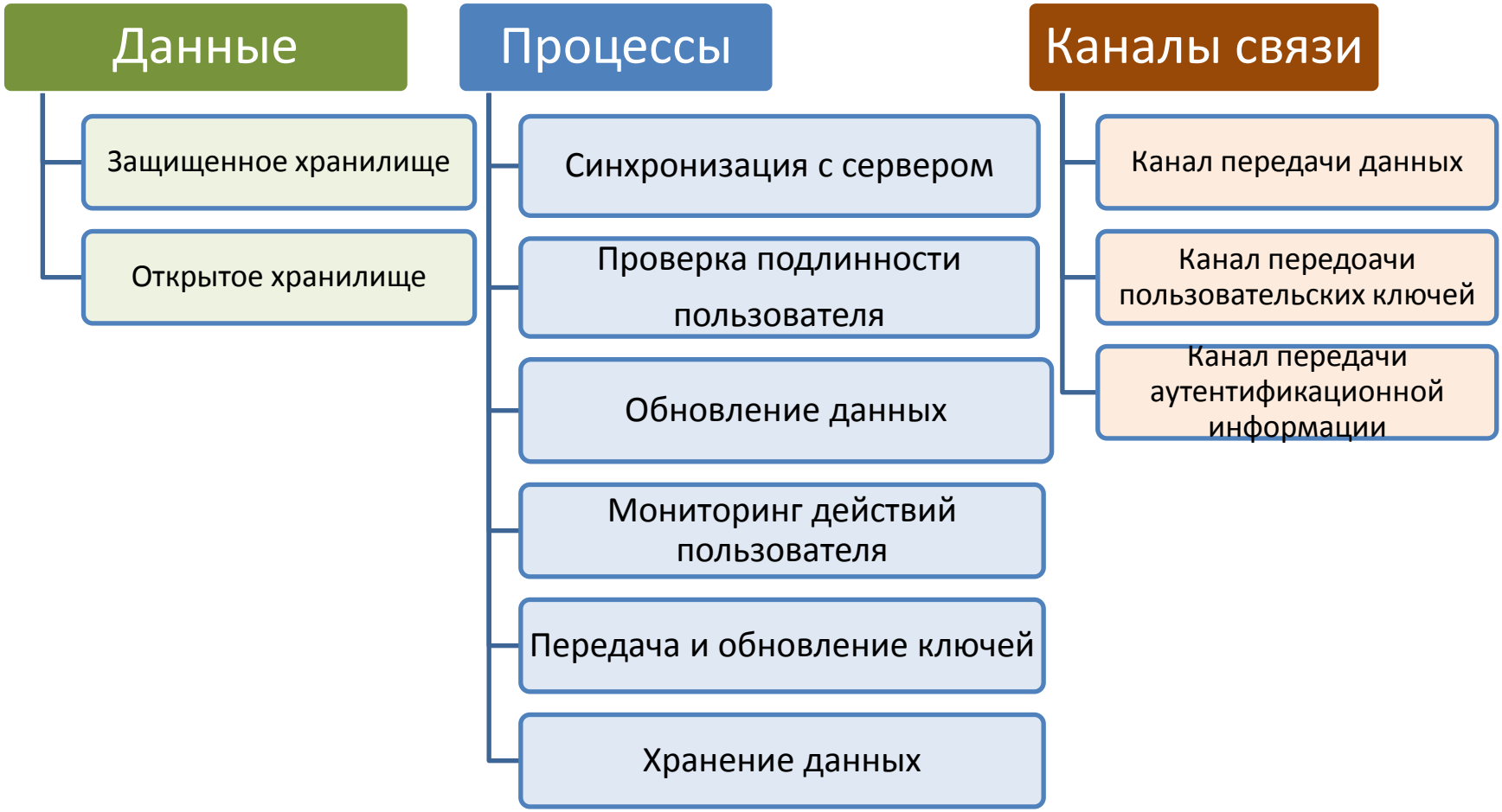
- где D- определяет матрицу меток безопасности данных узлов сети,
- Ch – матрицу меток безопасности каналов сети,
- а Pr – совокупность пар подматриц матрицы D.
- Требуемый уровень (профиль) безопасности определяется новым защищенным состоянием системы

$$SDS_{pr} = (D_{pr}, Ch_{pr}, Pr_{pr}),$$

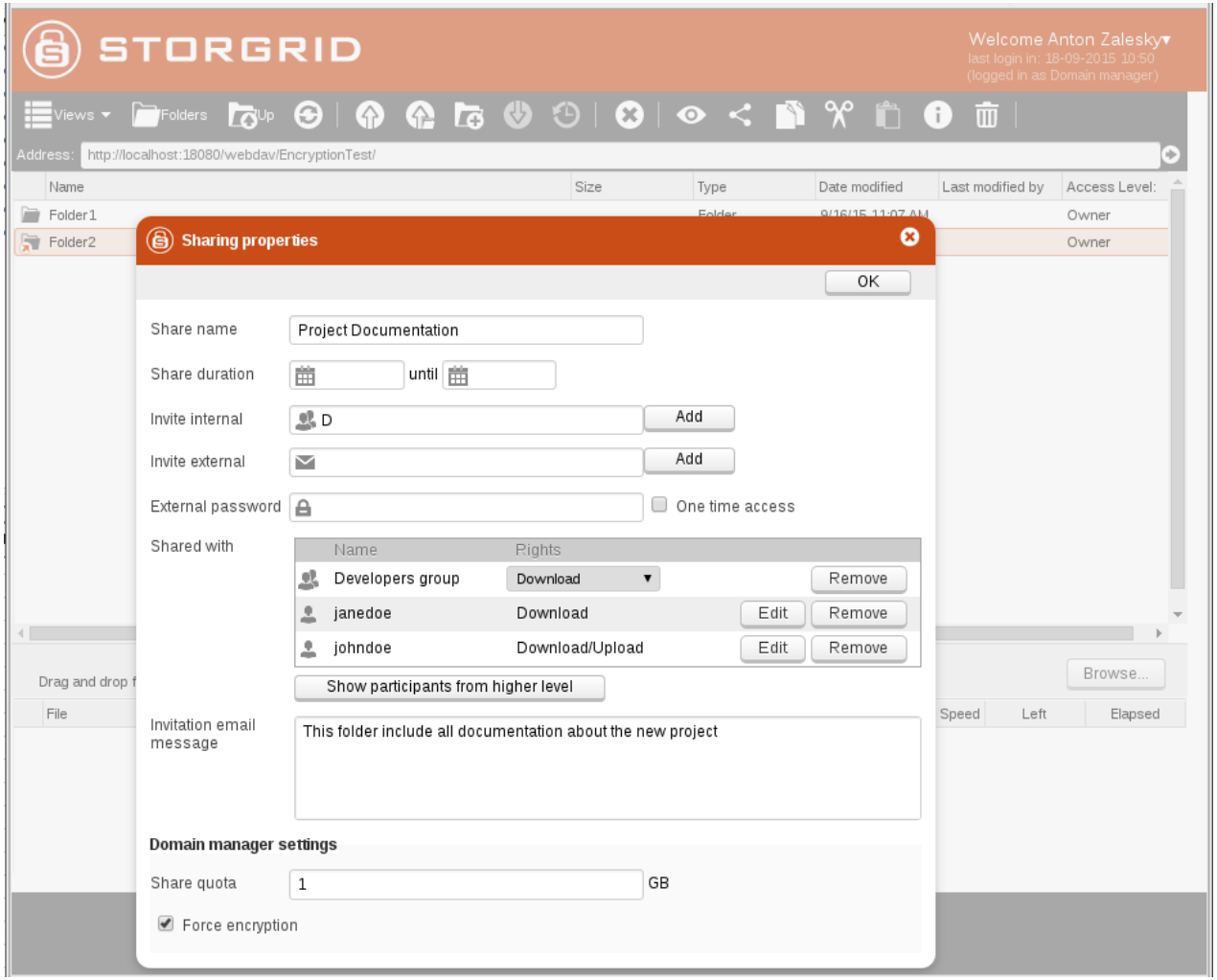
- Таким образом конфигурация СЗИ – это решение многокритериальной оптимизационной задачи:

$$SDS \rightarrow SDS_{pr}$$

Пример: СЗИ для мобильного устройства



Утилита администратора



Заключение

- Предлагается поэтапная методология построения СЗИОС
- Возможность автоматической организации механизмов безопасности в облаке
- Методика оследовательной настройки и выбора наиболее подходящих методов для минимизации наиболее распространенных угроз.