

IT Security Conference 2016

МОДЕЛИРОВАНИЕ СИСТЕМ
ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ
КОРПОРАТИВНЫХ ОБЛАЧНЫХ
ХРАНИЛИЩ

Галибус Т.В., Краснопрошин В.В.



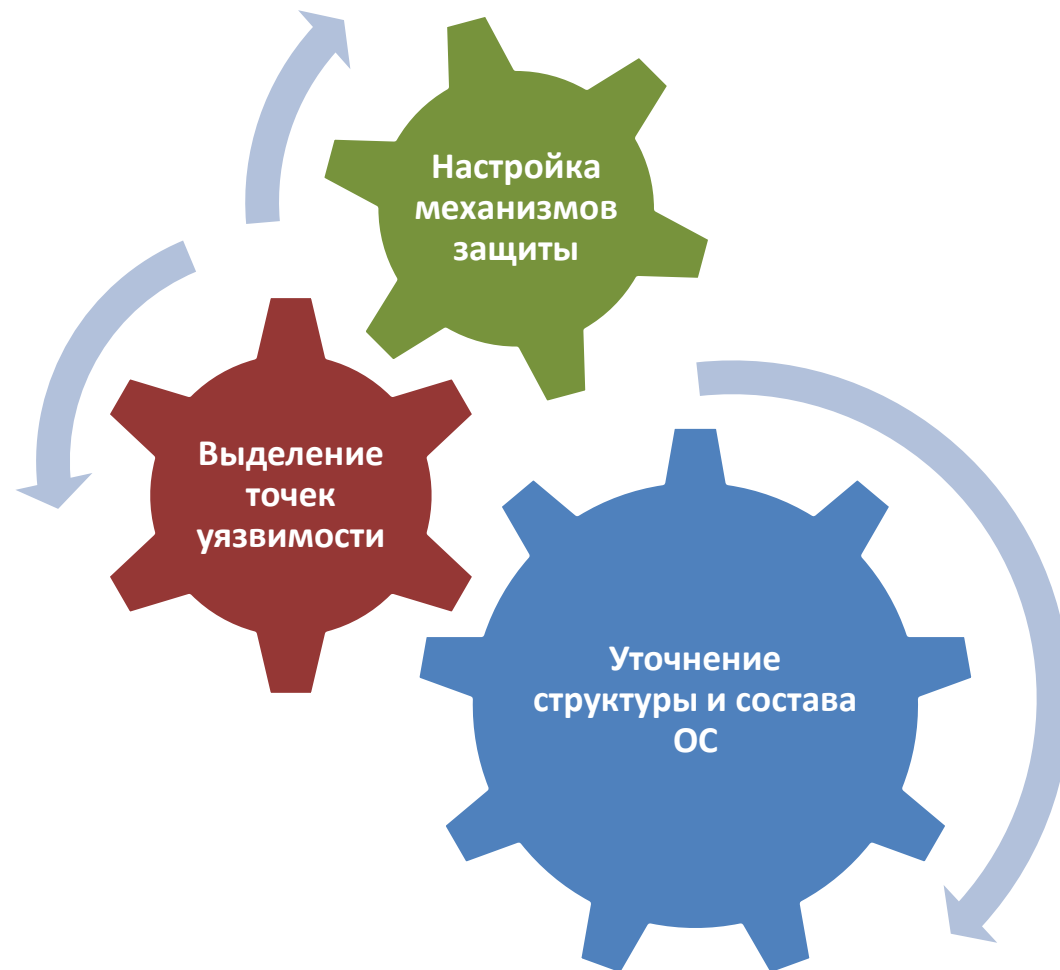
Преимущества и уязвимости облачных сервисов

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

Построение комплексной СЗИ ОС



Итерационный процесс моделирования СЗИОС

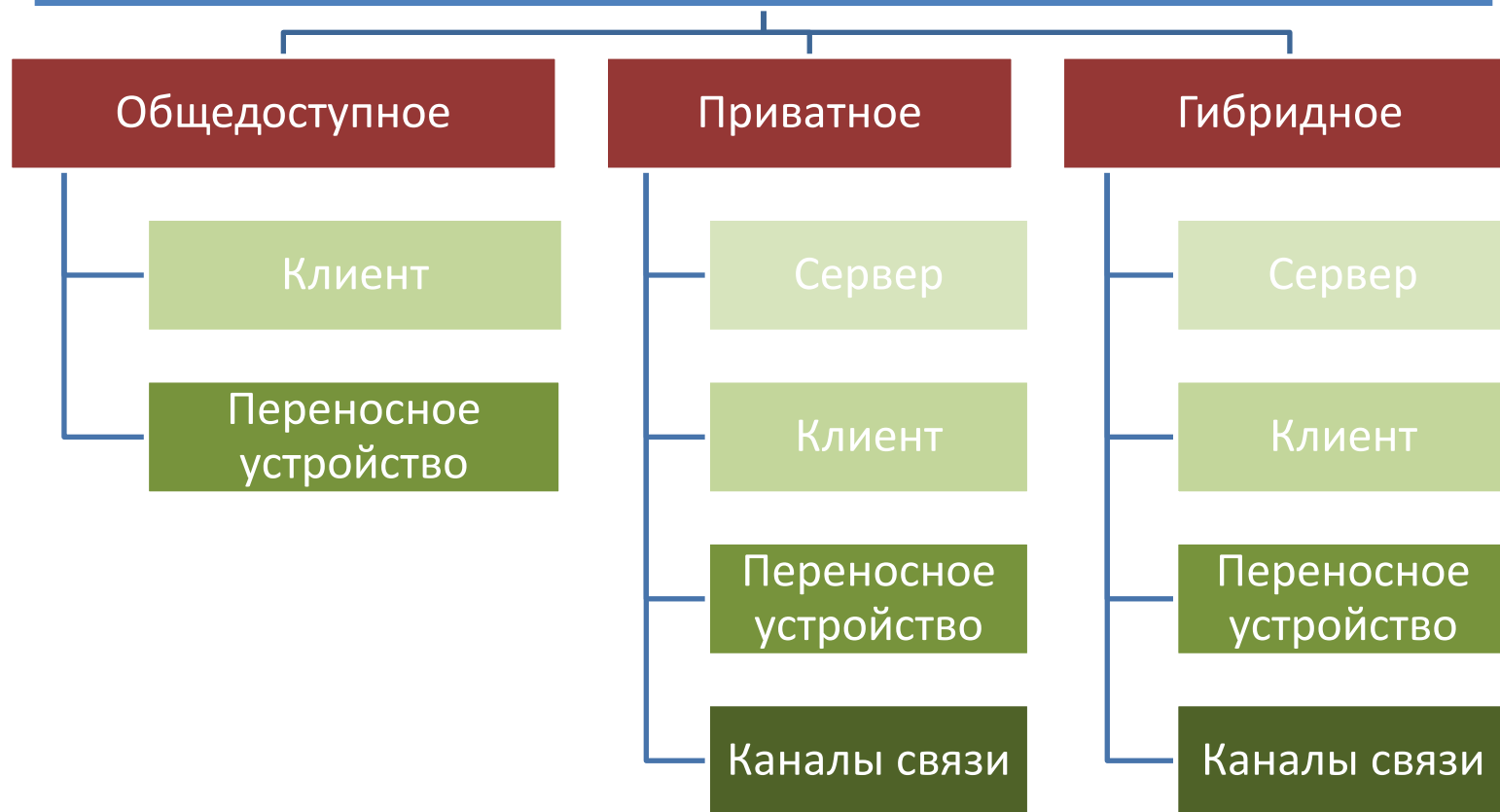


Этапы моделирования СЗИОС

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

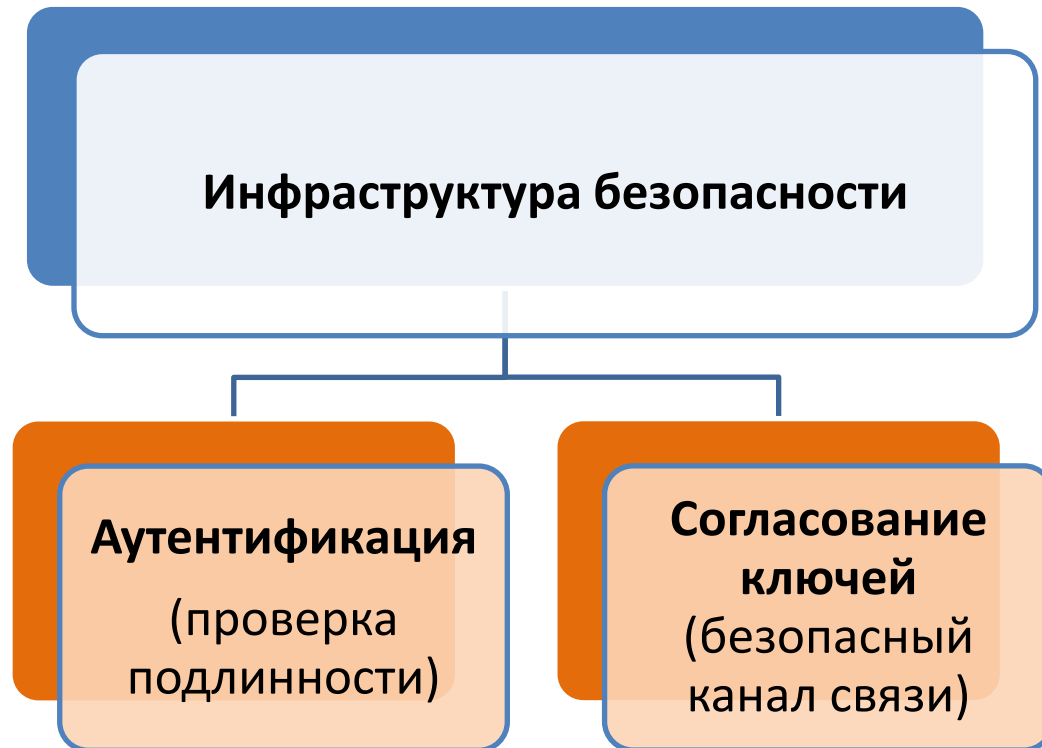
Структура и состав облачной системы

Облачные сервисы: обработка, хранение, перемещение данных



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

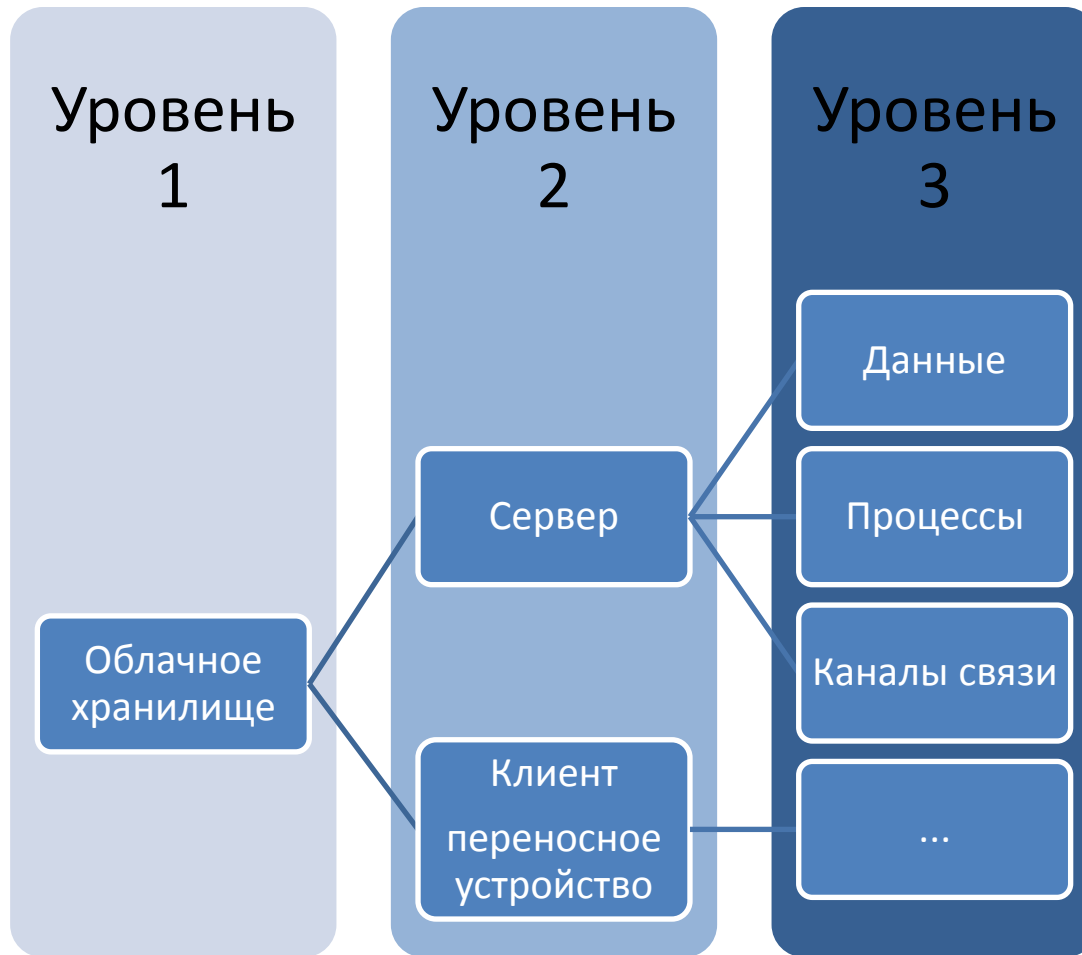
Механизмы согласования ключа

- 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)

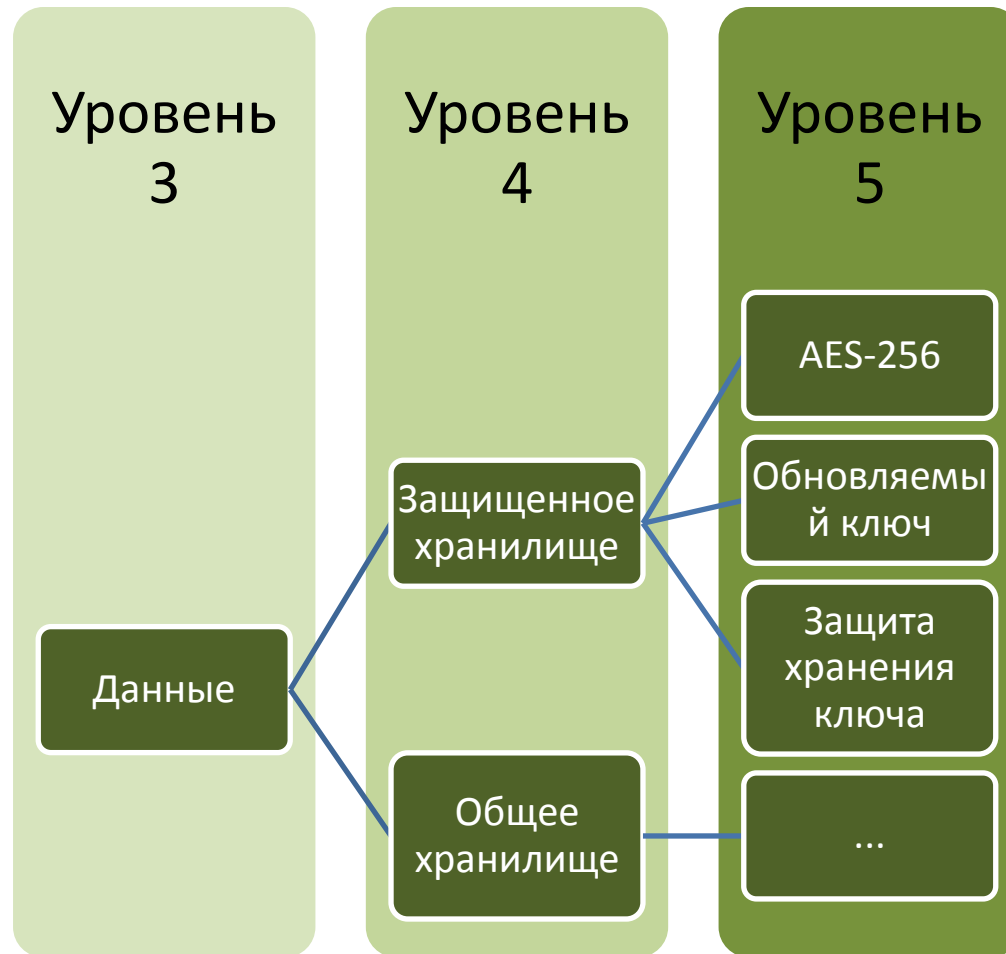
Анализ первого этапа

- 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**

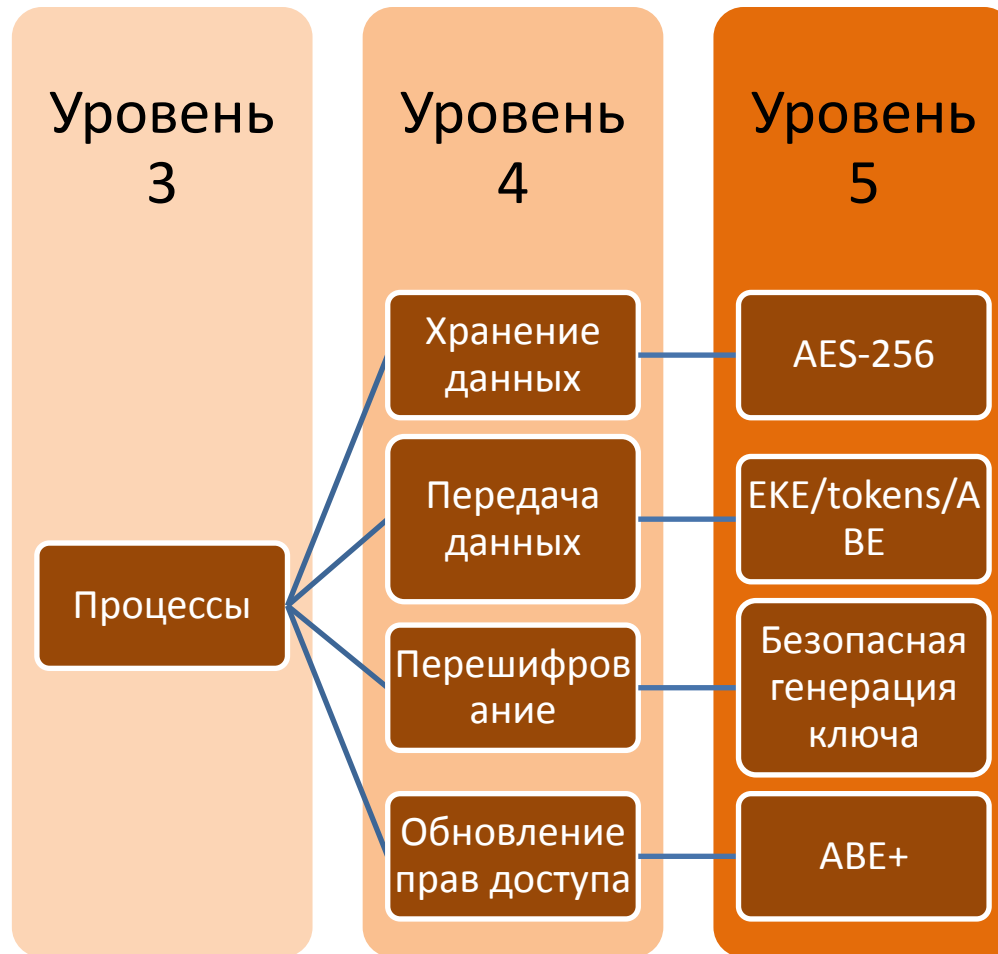
Этап 2 - детализация



Этап 2 - детализация



Этап 2 - детализация



Оптимизационная модель СЗИ ОС

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

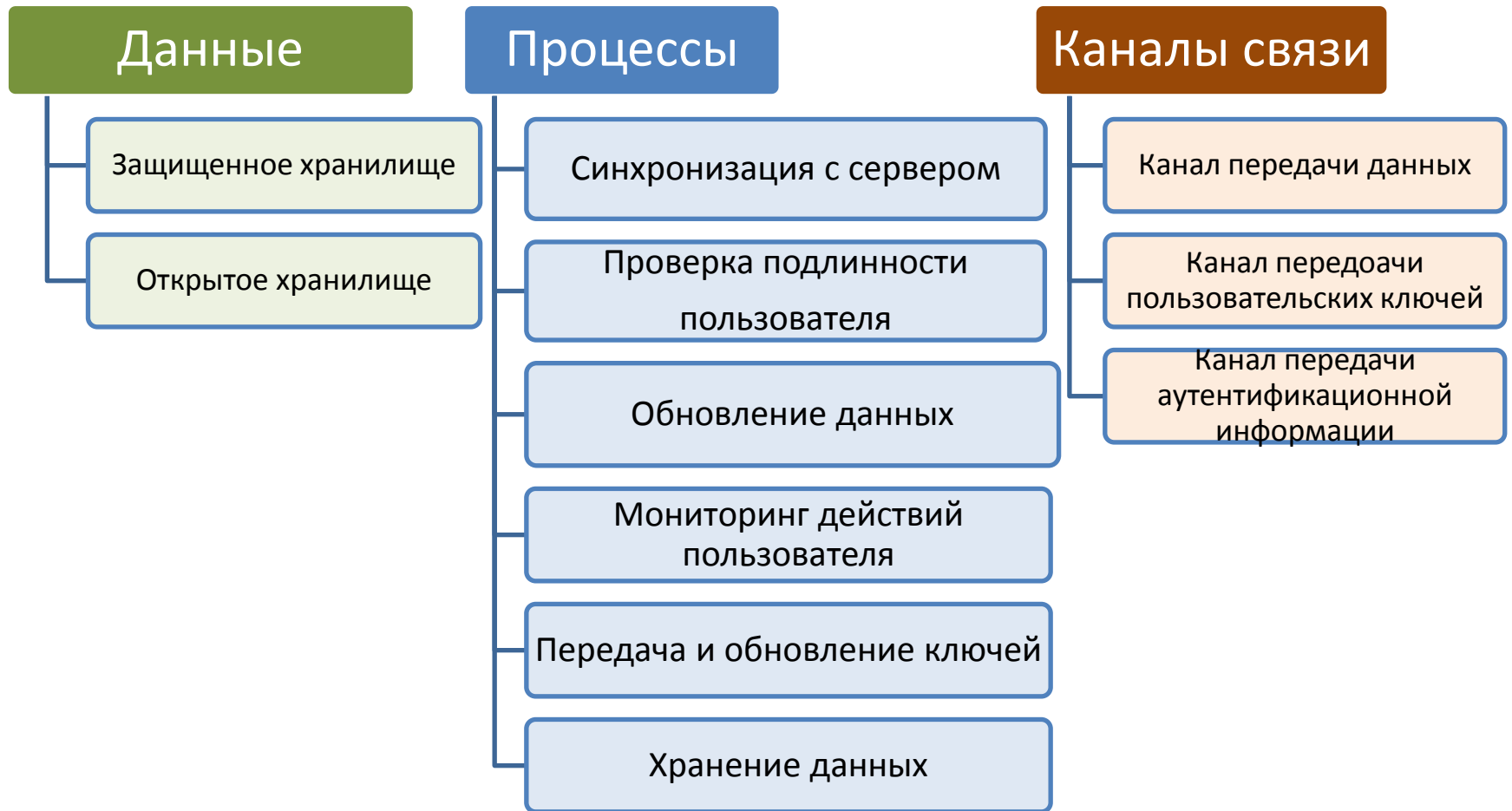
- где D- определяет матрицу меток безопасности данных узлов сети,
- Ch – матрицу меток безопасности каналов сети,
- а Pr – совокупность пар подматриц матрицы D.
- Требуемый уровень (профиль) безопасности определяется новым защищенным состоянием системы

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

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

$$SDS \rightarrow SDS_{pr}$$

Пример: СЗИ для мобильного устройства



Утилита администратора

The screenshot displays the StorGRID administrator interface. At the top, the logo and name 'STORGRID' are visible on the left, and a user greeting 'Welcome Anton Zalesky' with login details is on the right. Below the header is a navigation bar with icons for Views, Folders, Up, and various file operations. The address bar shows 'http://localhost:18080/webdav/EncryptionTest/'. A table lists folders: Folder1 and Folder2, both owned by 'Owner'. A 'Sharing properties' dialog box is open in the foreground, containing the following fields and controls:

- Share name:** Project Documentation
- Share duration:** Calendar icons with 'until' in between.
- Invite internal:** Input field with 'D' and an 'Add' button.
- Invite external:** Input field and an 'Add' button.
- External password:** Input field with a lock icon and a 'One time access' checkbox.
- Shared with:** A table listing participants and their rights.

Name	Rights	
Developers group	Download	Remove
janedoe	Download	Edit Remove
johndoe	Download/Upload	Edit Remove

Below the table is a 'Show participants from higher level' button. The 'Invitation email message' field contains the text: 'This folder include all documentation about the new project'. At the bottom, 'Domain manager settings' include a 'Share quota' of 1 GB and a checked 'Force encryption' option. An 'OK' button is located at the top right of the dialog box.

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.