КОНЦЕПЦИЯ ПЛАТФОРМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ПИБ)

Александр Реут
Заместитель генерального директора
по информационным технологиями
НПО им. С. А. Лавочкина
19 апреля 2017 г.

СОДЕРЖАНИЕ

- Введение и проблематика
- Ключевые принципы построения
- «Вероятный противник»
- **S U S E**
- Компоненты системы
- Open Enterprise Server Инфраструктурные службы
- **eDirectory** - управление пользователями
- **SSO** - Служба единого доступа
- Работа службы **DSfW**
- Почта и коллективная работа **GroupWise**
- Портал коллективной работы **Vibe**
- Управление печатью **iPrint**
- **PrinterGuard**
- Управление Интернетом **SQUID + SAMS**
- Контроль доступа **SQUID**
- Идентификация
- Виртуальная архитектура **ИТ-систем**

Введение и проблематика

- Высокий уровень амортизации существующей ИТ-инфраструктуры
- Низкий уровень управляемости инфраструктурой
- Низкий уровень взаимной интеграции решений
- Неконтролируемый канал утечки данных на распечатанных на бумаге документах
- Отсутствие контроля использования рабочих мест пользователей
- Неконтролируемое использование внешних носителей в организации

Виртуальная архитектура ИТ-систем

SWOT АНАЛИЗ ДЛЯ ПРИНЯТИЯ РЕШЕНИЯ

СИЛА

СЛАБОСТЬ

ВОЗМОЖНОСТИ

УГРОЗЫ

Ключевые принципы построения

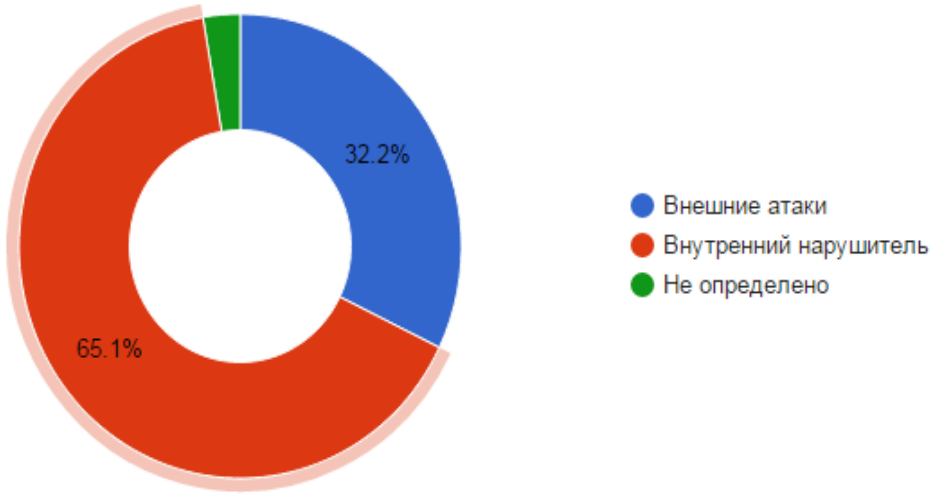
• Снижение итоговой стоимости за счет моновендорности или пакетных решений
• Максимальный уровень интеграции и взаимосвязанности решений (пользовательский каталог + почта + рабочие станции + печать + файловые хранилища)
• Технологическая совместимость со всеми бизнес-системами (NX,1С+база данных)
• Централизованное управление рабочими местами пользователей и доступом к ним в соответствии с принятыми политиками информационной безопасности
• Создание единого информационного пространства для коллективной работы пользователей
• Максимально прозрачная работа для конечных пользователей
• Управление печатью и контроль за работой пользователей с бумажными носителями информации

«Вероятный противник»

«Враг внешний»
Лица или организации, которые ***осознанно и целенаправленно*** пытаются получить доступ к конфиденциальной информации или нарушить работу ИТ-инфраструктуры.

«Враг внутренний»
Пользователи, которые ***целенаправленно или по халатности*** нарушают принятые в организации политики, инструкции или регламенты информационной безопасности

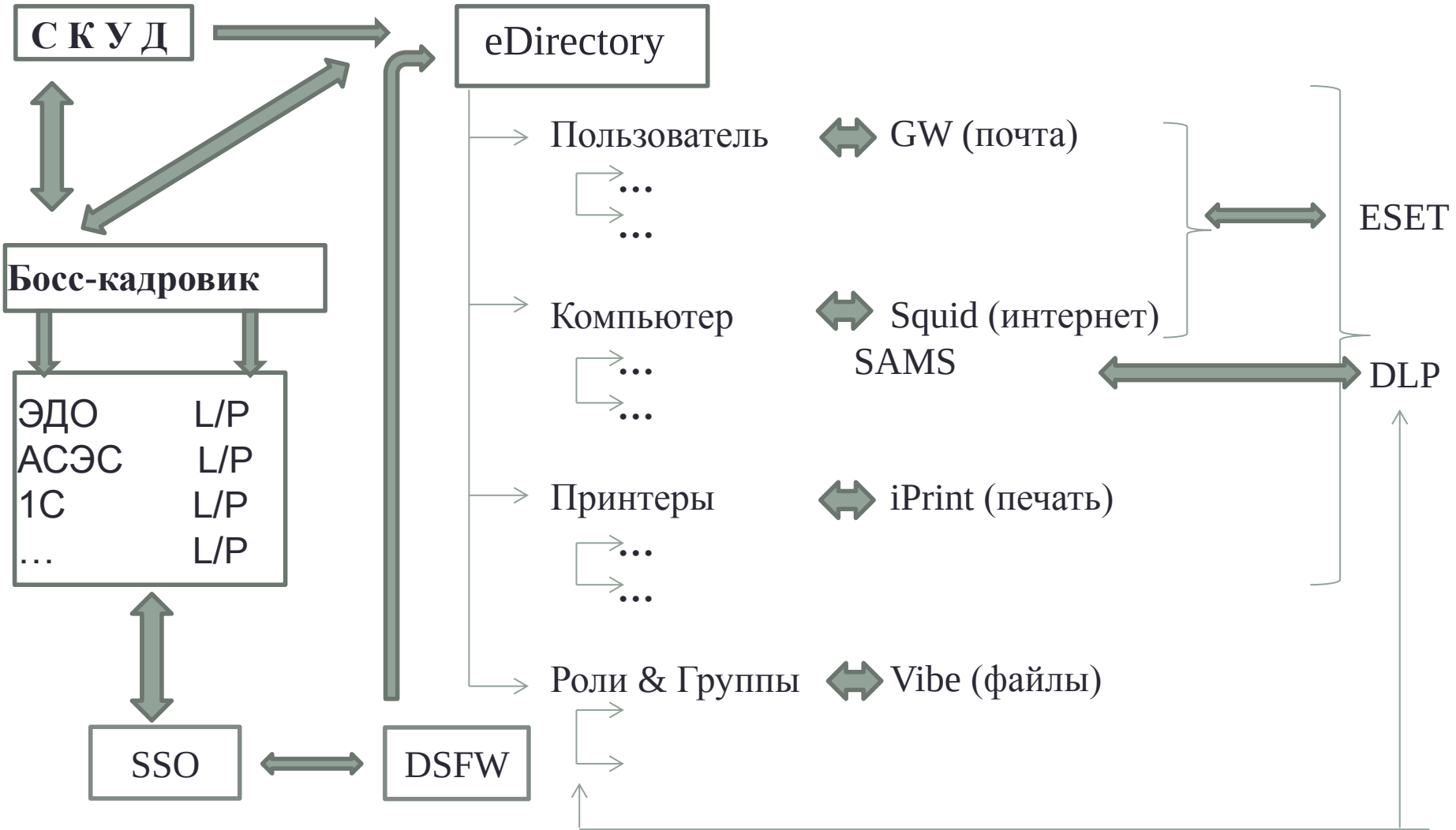
«Неизбежные случайности»
Угрозы и риски, связанные со сбоями и отказами элементов ИТ-инфраструктуры в результате ***обстоятельств непреодолимой силы.***



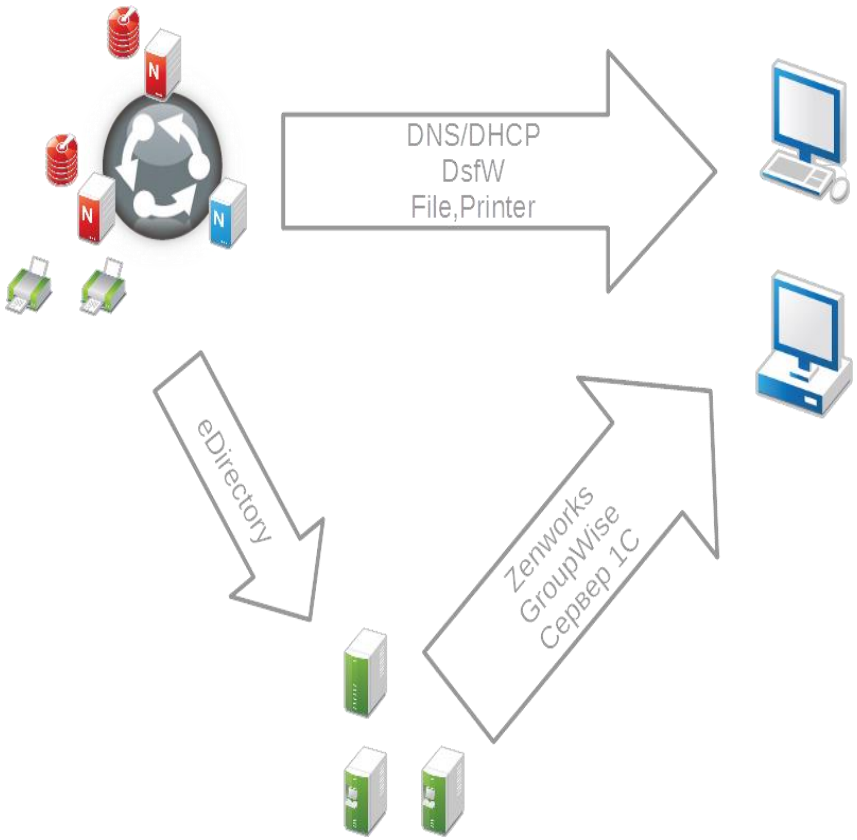
SUSE

АО «НПО Лавочкина»

LINUX



Компоненты системы



Open Enterprise Server:

- Инфраструктурные службы
- каталог пользователей
- ролевой доступ и права пользователей

GroupWise:

- Корпоративная почта
- Групповая работа
- Календари
- Обмен мгновенными сообщениями

SQUID:

- Контроль доступа корпоративного уровня
- Доступ с мобильных устройств
- Аудит использования Интернет

ZenWorks:

- Управление и контроль над рабочими
- станциями

SecureLogin

- Служба единого доступа к информационным ресурсам организации

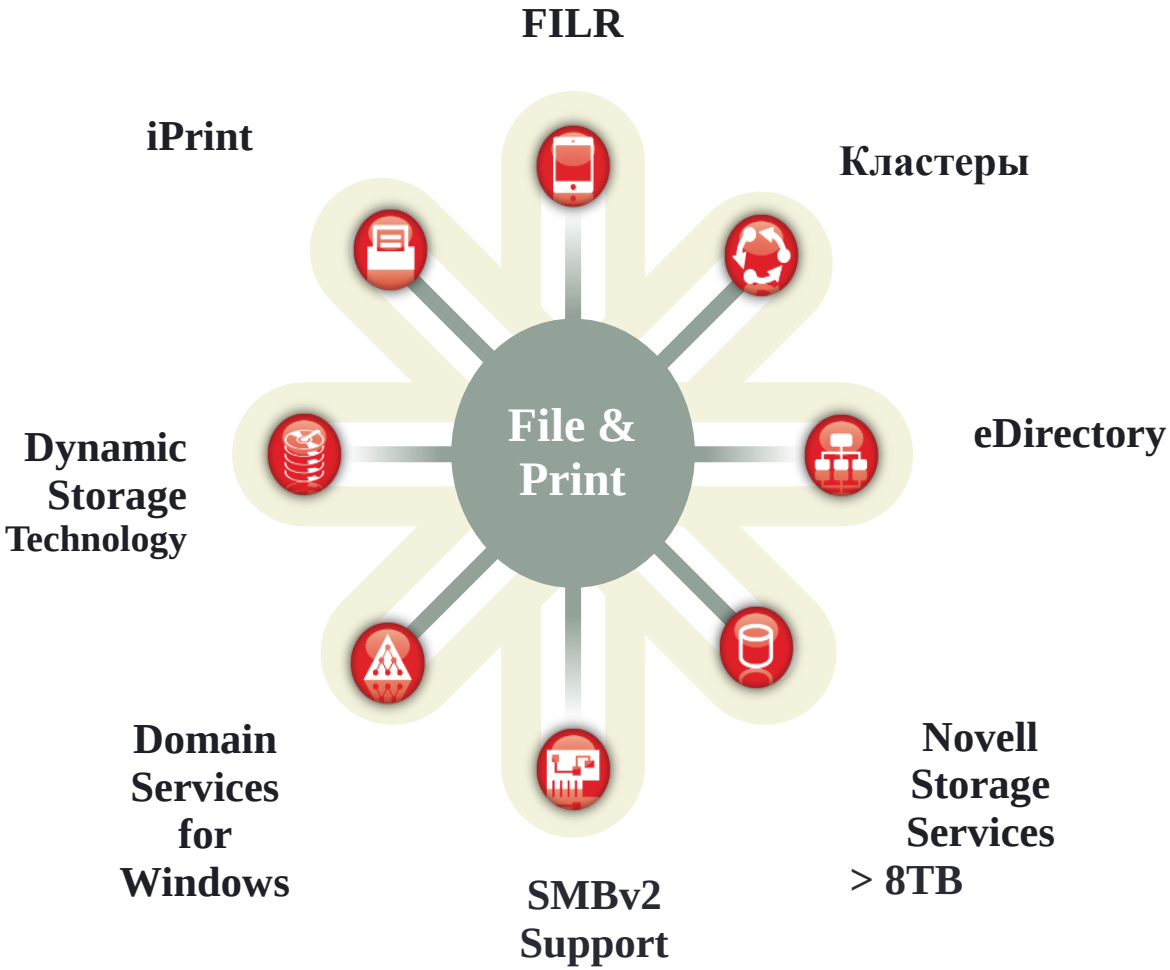
Vibe

- Портал коллективной работы
- Squid + SAMS
- - Контроль использования Интернет

iPrint + PrinterGuard:

- - централизованная печать
- - Расширенное управление печатью и контроль печати на локальных принтерах

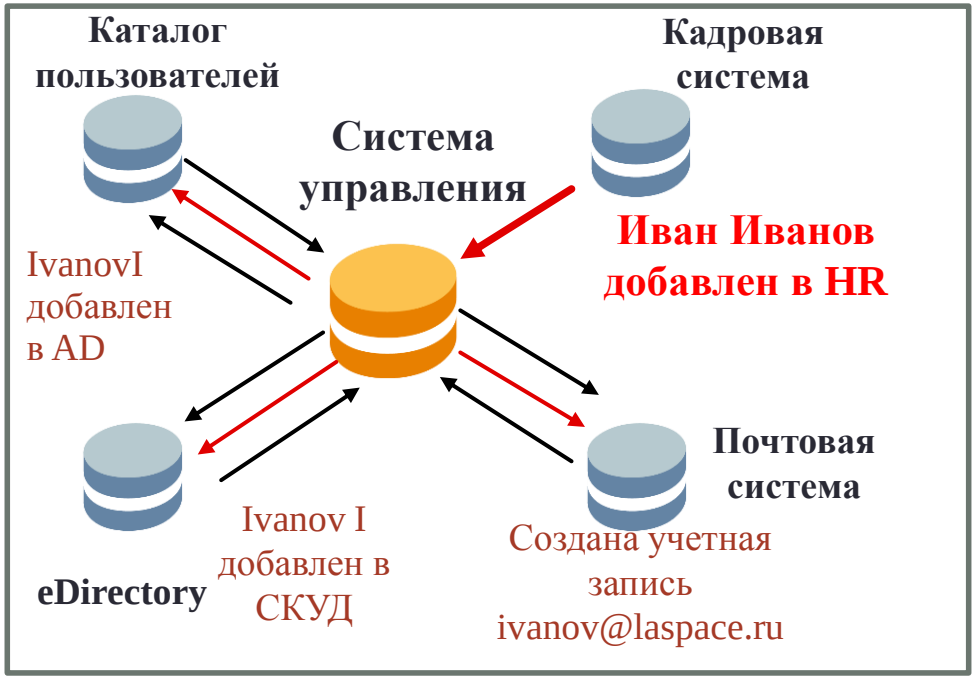
Open Enterprise Server
Инфраструктурные службы

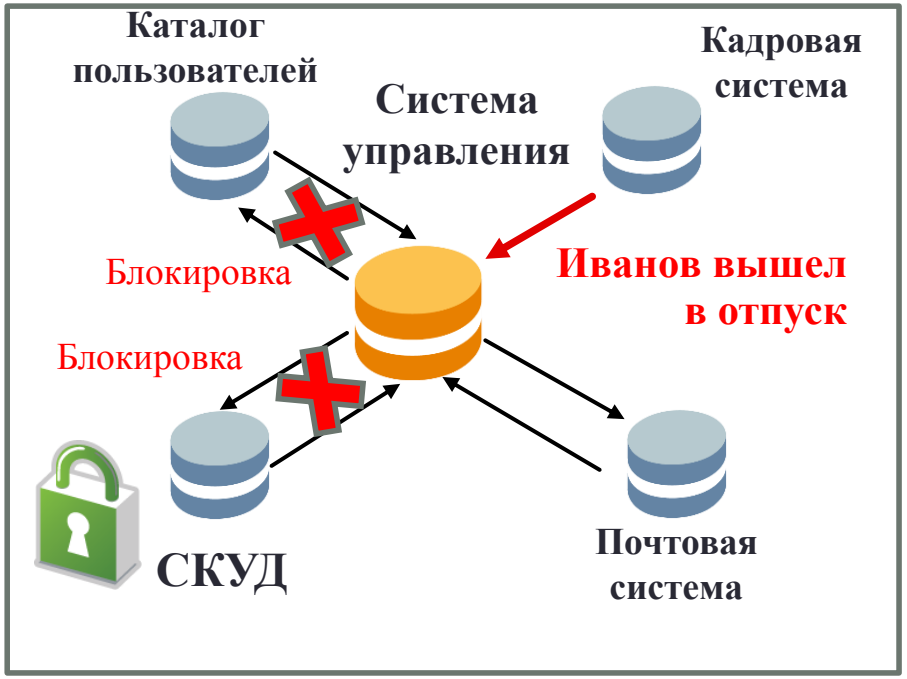


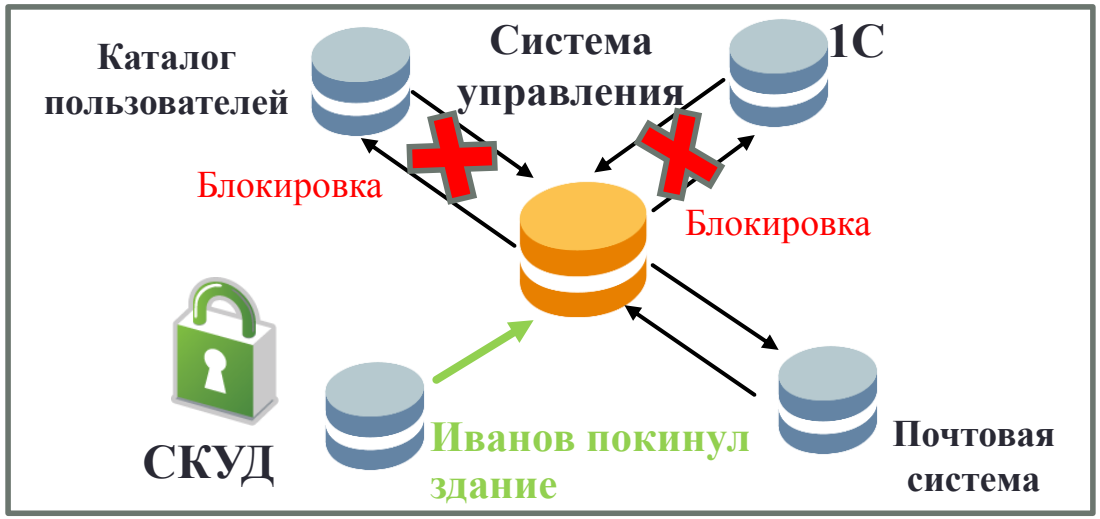
Open Enterprise Server:

- Инфраструктурные службы
- Возможность гибкого выбора для заказчика клиентских станций и работы с дисковыми накопителями
- Простая IT инфраструктура с использованием единого хранилища учетных данных

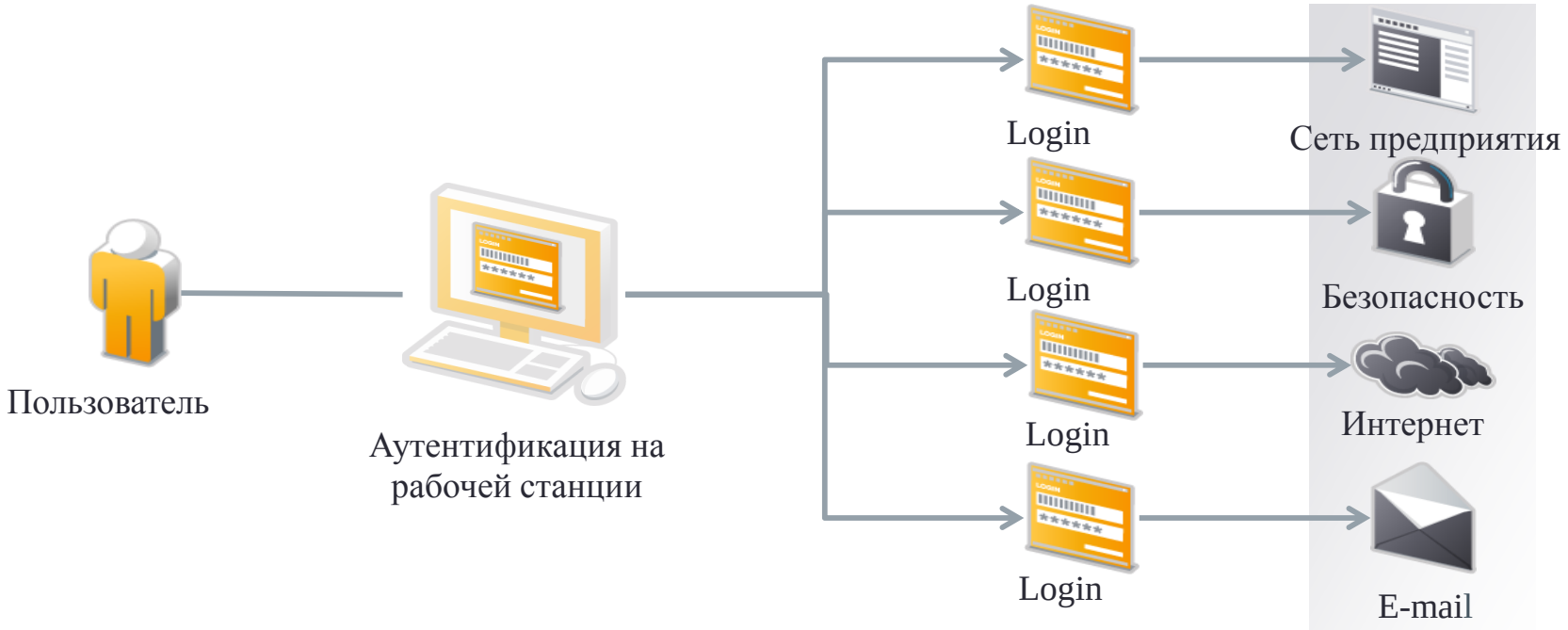
eDirectory - управление пользователями







SSO - Служба единого доступа



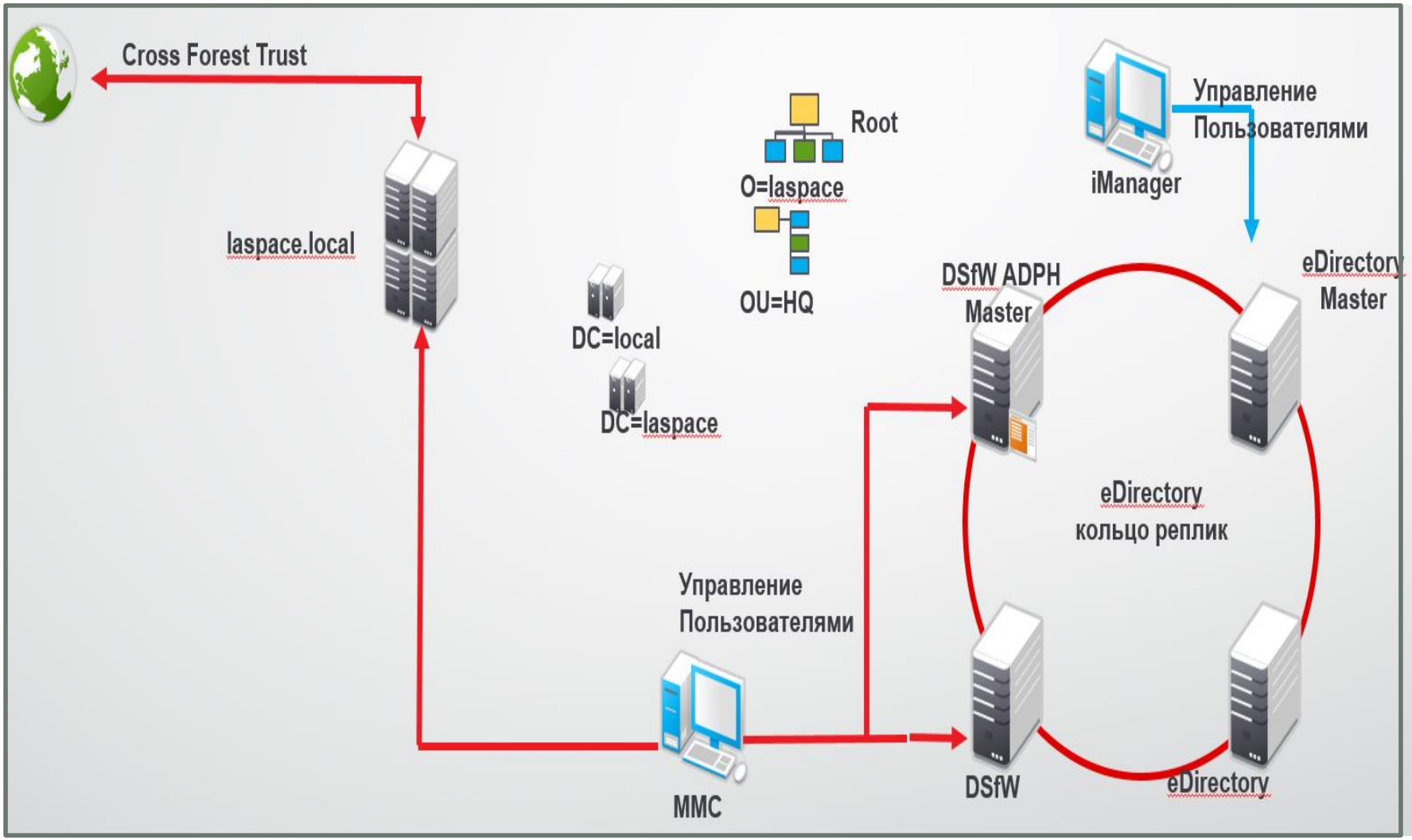
Требования

- LDAP-каталог для хранения аутентификационных данных (AD, eDirectory, SunOne, etc.)
- Устанавливаемый на рабочее место агент (для мониторинга запуска приложений)

Преимущества

- Организация как правило уже имеет корпоративный каталог
- Пользователи уже имеют настроенные рабочие места
- Не требуется дополнительное оборудование

Работа службы DSfW



Почта и коллективная работа GroupWise

Портал коллективной работы Vibe

Управление печатью iPrint

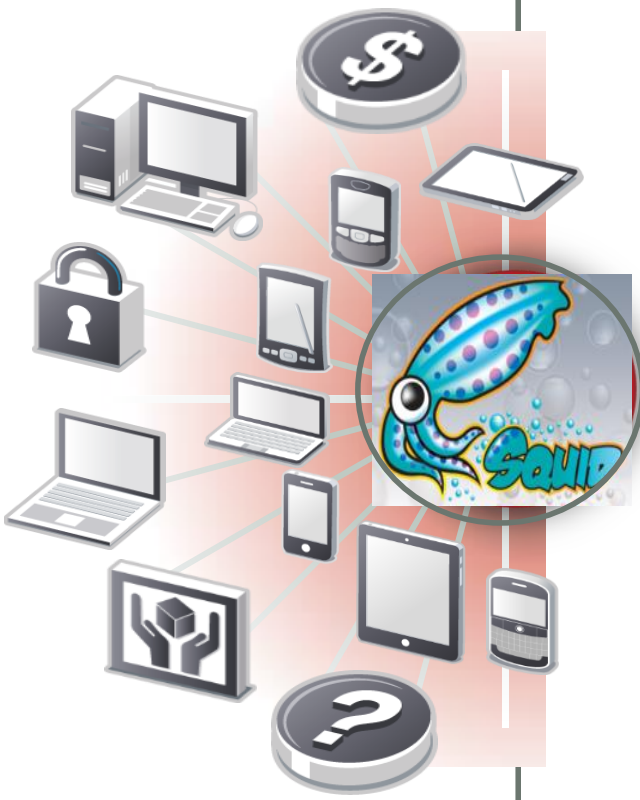
- Служба печати корпоративного уровня
- Сервис самообслуживания
- Кросс-платформенный клиент
  - **Windows, Mac, Linux**
- Печать с мобильных устройств
  - **iOS, Android, BB10, Windows Mobile**
- Печать в филиалах
  - **Централизованное управление**
  - **Локальная печать**
- Поддержка всех производителей принтеров
- Аудит использования принтеров
- Автоматическая установка драйверов
- Разграничение доступа
- Геолокация (использование карты для нахождения принтера)

PrinterGuard

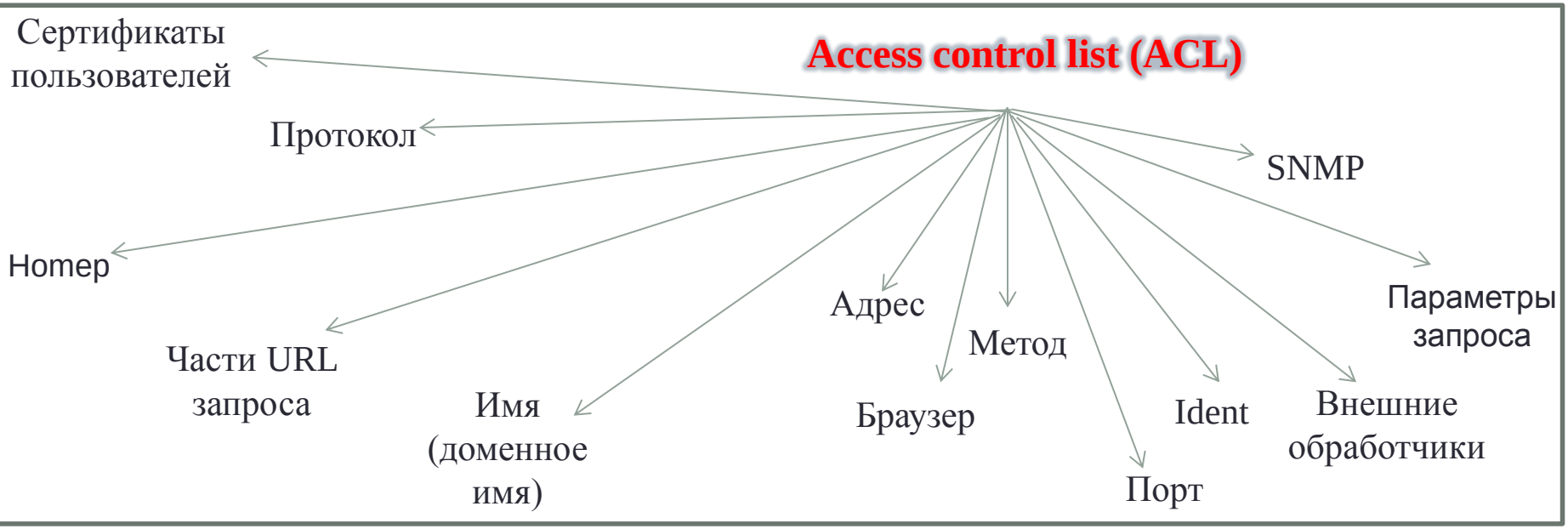
- Интеграция с системой печати **iPrint**
- Управление политиками и заданиями печати для локальных принтеров
- Блокирование печати по слову в документе
- Блокирование печати в нерабочее время
- Блокирование печати по квоте (количество листов на отдел, количество листов на сотрудника в день/неделю/месяц)
- Создание истории печати с сохранением документа
- Возможность интеграции со СКУД для реализации двухфакторного доступа к печатаемому документу по пропуск-карте
- Работа на ОС SUSE

Управление доступом в Интернет Squid + SAMS

- Контроль доступа корпоративного уровня
- Сервис самообслуживания
- Кросс-платформенный доступ с
  - **Windows, Mac, Linux**
- Доступ с мобильных устройств
  - **iOS, Android, Windows Mobile**
- Контроль в филиалах
  - **Централизованное управление**
  - **Локальная настройка**
- Поддержка всех браузеров
- Аудит использования Интернет
- Автоматическая установка лимитов трафика
- Разграничение доступа к ресурсам Интернет



Контроль доступа SQUID



Идентификация

Squid поддерживает несколько видов идентификации пользователей:

- По IP-адресу (или доменному имени узла)
- По переданным реквизитам (логин/пароль)
- По идентификатору пользовательского агента (браузера)
- Для идентификации по логину/паролю возможно использовать:
- Обычные логин/пароль
- NTLM-авторизацию через DSfW
- Интеграцию с DLP- системами

Благодарю за внимание!