



**ИТ-инфраструктура ЦОД:
ляпы, которые обходятся дорого**



Олег Абанкин

Генеральный директор компании intact

- 11 лет в ИТ и ИБ
- МГУ им. М.В. Ломоносова, математика и механика
- MBA, стратегический менеджмент



Цели

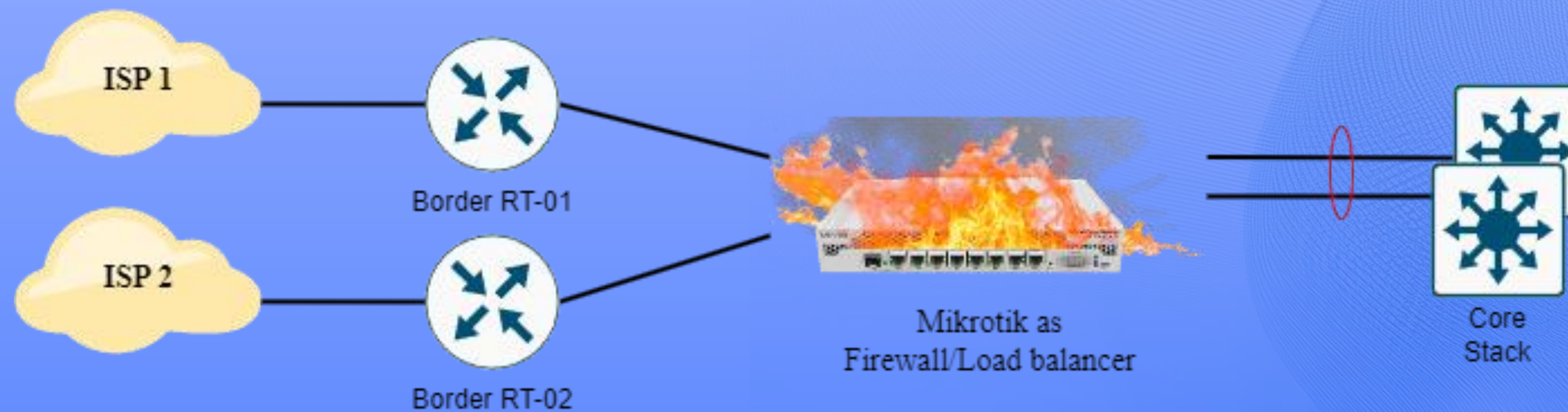
- ✓ Повод задуматься нет ли у меня типовых ошибок
- ✓ Составить план, как работать с типовыми ошибками



Структура

- ✓ Не выявлены узкие места в системе
- ✓ Не организована защита данных
- ✓ Ляпы в информационной безопасности

Выявление узких мест



- Два маршрутизатора (BGP+HSRP)
- Два коммутатора уровня ядра в стеке
- Две линии связи к внешнему миру (резервирование интернета)
- **Одно устройство Mikrotik**, через которое проходит весь трафик



Проблема

- ✓ В системе резервируется/
модернизируются не все компоненты

Реальный показатель надежности

- ✓ определяется «самым слабым
элементом»



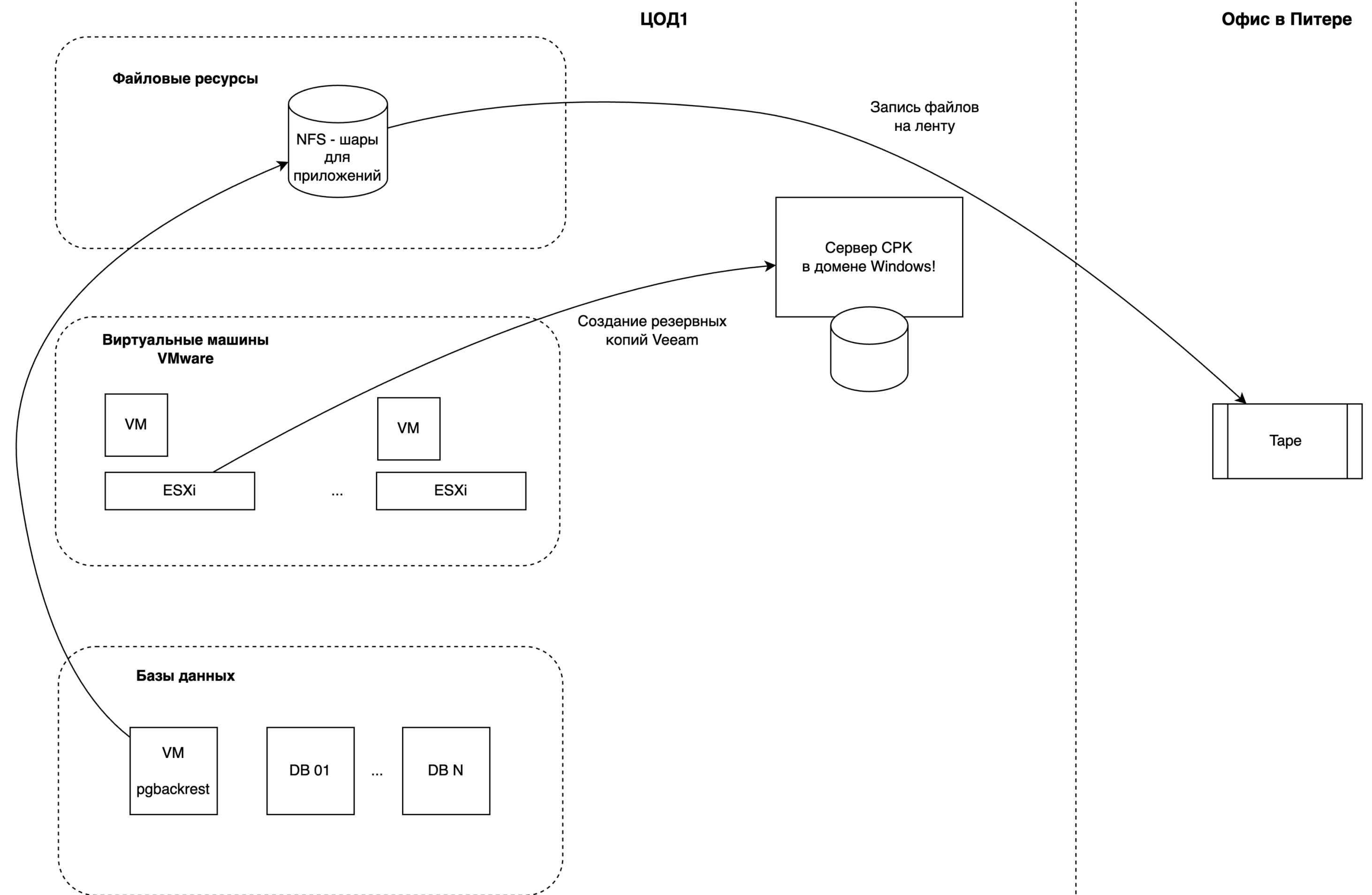
Решение

- ✓ Наладить практику регулярных
аудитов ИТ-инфраструктуры
- ✓ Требуется архитектор в составе
команды обслуживания



Защита данных

- Резервное копирование не всей инфраструктуры
- Наличие RDM-дисков и NFS-шар вне виртуализации
- Сервер Veeam в домене
- Копирование баз данных на ту же СХД





Проблема

- ✔ Смешение понятий DR и backup
- ✔ Отсутствие тестирования резервных копий
- ✔ Неконсистентные резервные копии
- ✔ Отсутствие отчуждаемых носителей

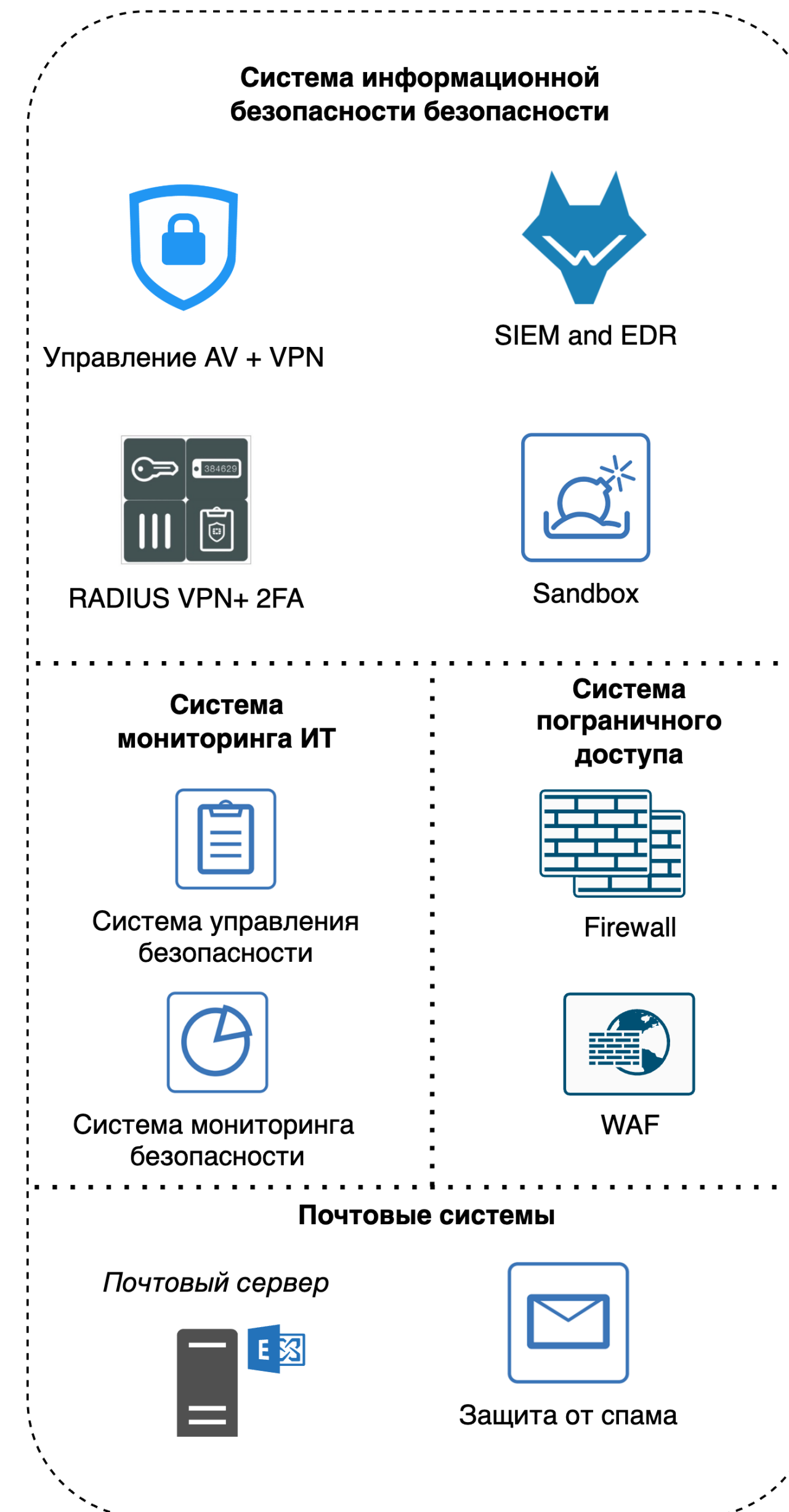


Решение

- ✔ Хранение по схеме 3-2-1
- ✔ Использование отчуждаемых носителей
- ✔ Регулярное восстановление (до записи на ленту)
- ✔ Использование application aware или СРК БД

Информационная безопасность

- Внедрены системы ИБ: FW, WAF, EDR, Anti-Spam, SIEM, EPP, Sandbox, NTA
- В организации 500 АРМ
- В компании нет сотрудника ИБ, в ИТ подразделении 5 админов





Проблема

- ✓ Акцент делается на средства защиты, а не на людей и процессы
- ✓ Не соблюдаются лучшие практики ИБ в ИТ инфраструктуре
- ✓ Не внедрены базовые средства защиты (EPP, Anti-spam, IPS, 2FA и т.д.)

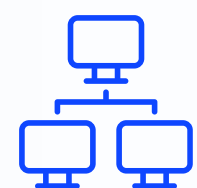


Решение

- ✓ Наладить практику регулярных аудитов ИТ-инфраструктуры
- ✓ Сформировать выделенную команду ИБ или внешний SOC
- ✓ Внедрение базовых средств защиты



Инженерные
системы



Сети передачи
данных



Объединенные
коммуникации



Мультимедийные
системы



Вычислительные
системы



ИТ-сервисы



Информационная
безопасность



Импортозамещение

Услуги компании

- Аудит
- Проектирование
- Поставка оборудования и ПО
- Монтажные и пусконаладочные работы
- Техническая поддержка

15+
лет на рынке

1500+
реализованных
проектов

100+
сотрудников



Спасибо!
Вопросы?

121609, г. Москва, Осенний бульвар, д.23
+7 495 989 40 49 | info@intact.ru | intact.ru

