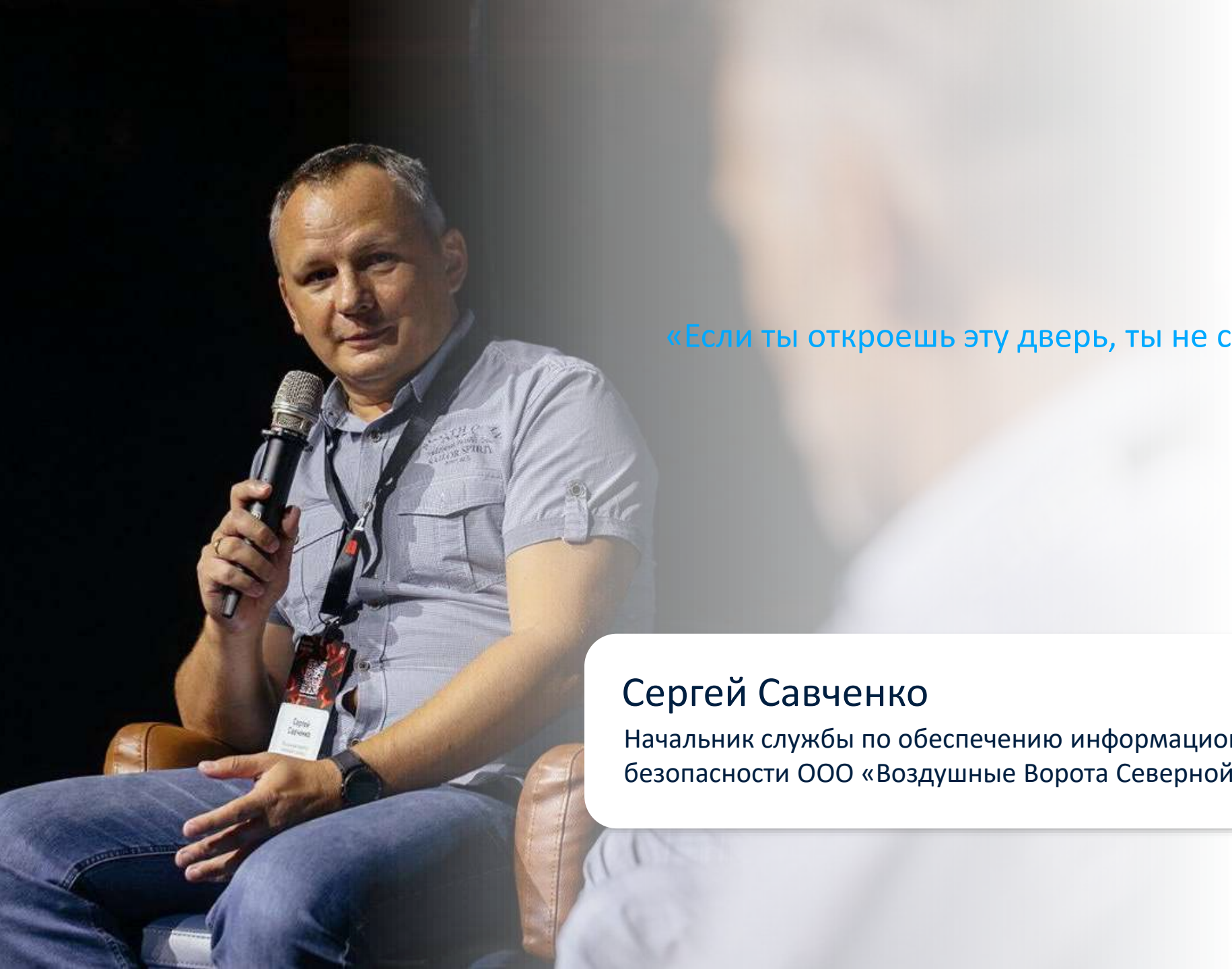
Пулково

Основные отрасли-потребители решений ИБ

Февраль 2026



«Если ты откроешь эту дверь, ты не сможешь контролировать то, что в нее войдет…»

Ганнибал Лектер

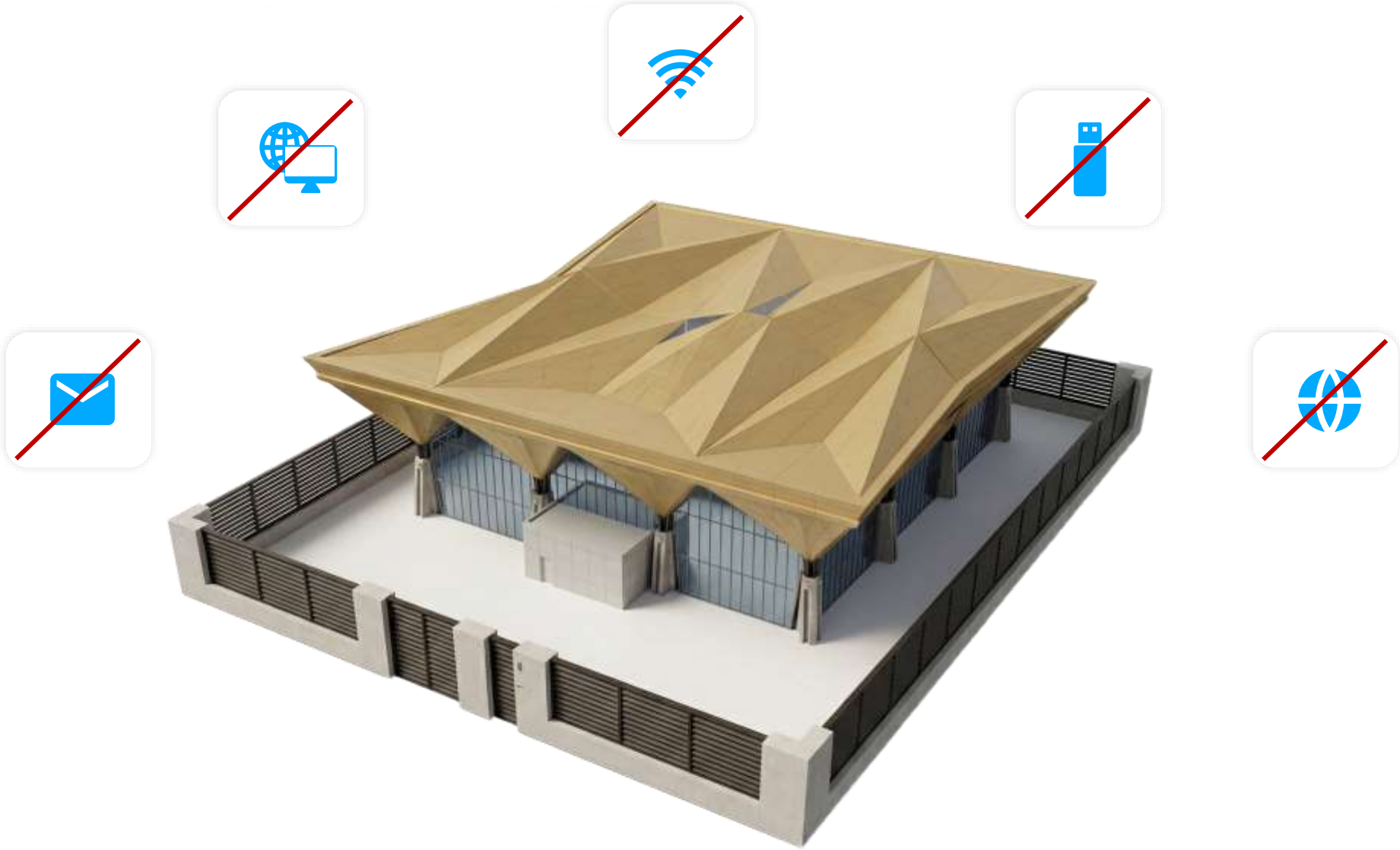
Сергей Савченко

Начальник службы по обеспечению информационной безопасности ООО «Воздушные Ворота Северной Столицы»

КАК БЫЛО РАНЬШЕ ИЛИ «ДОБРО ПОЖАЛОВАТЬ»

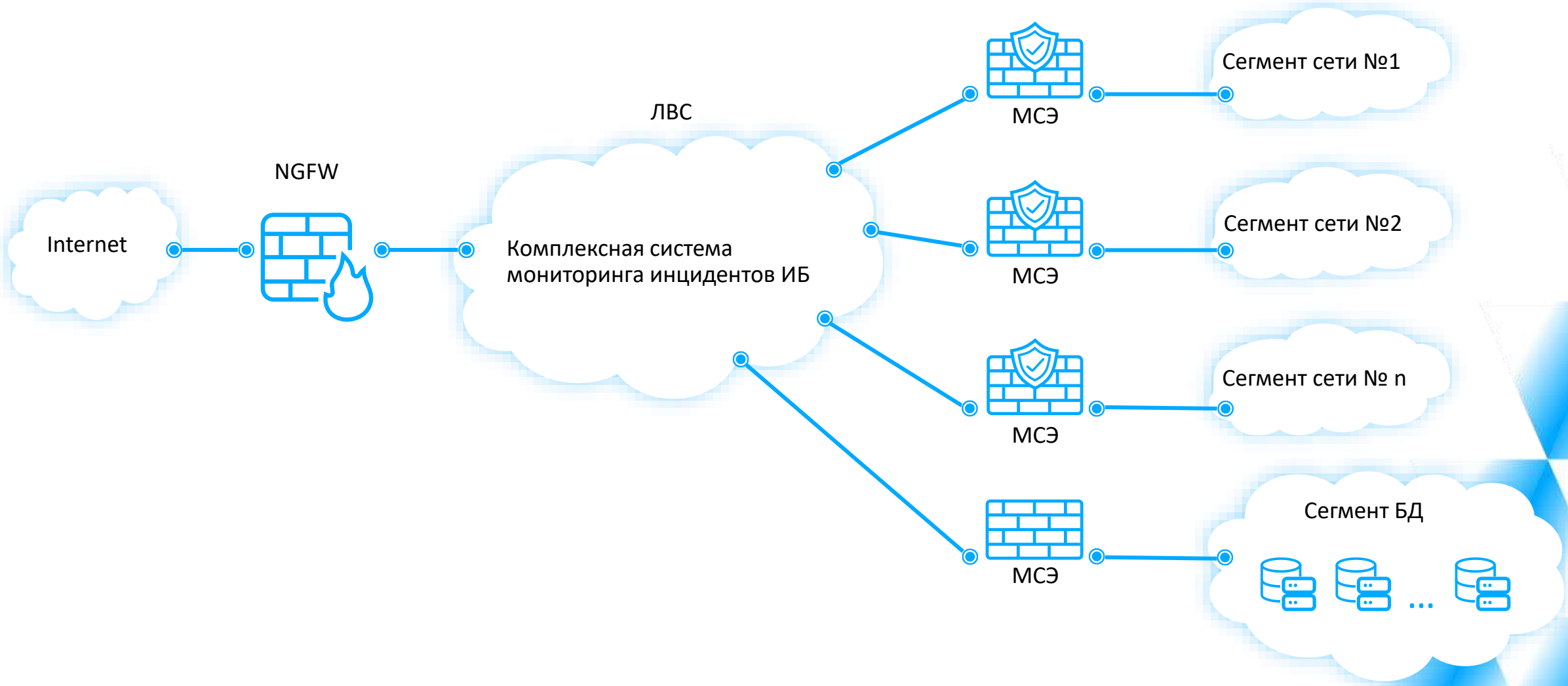
- Получение фишинговых сообщений, отправка конфиденциальной информации
- Бесконтрольный удаленный доступ к ресурсам предприятия
- Использование корпоративной Wi-Fi сети
- Бесконтрольные доступы к USB-портам
- Бесконтрольный прямой доступ в сеть Интернет из корпоративной сети

ТРЕБОВАНИЯ РЕГУЛЯТОРОВ



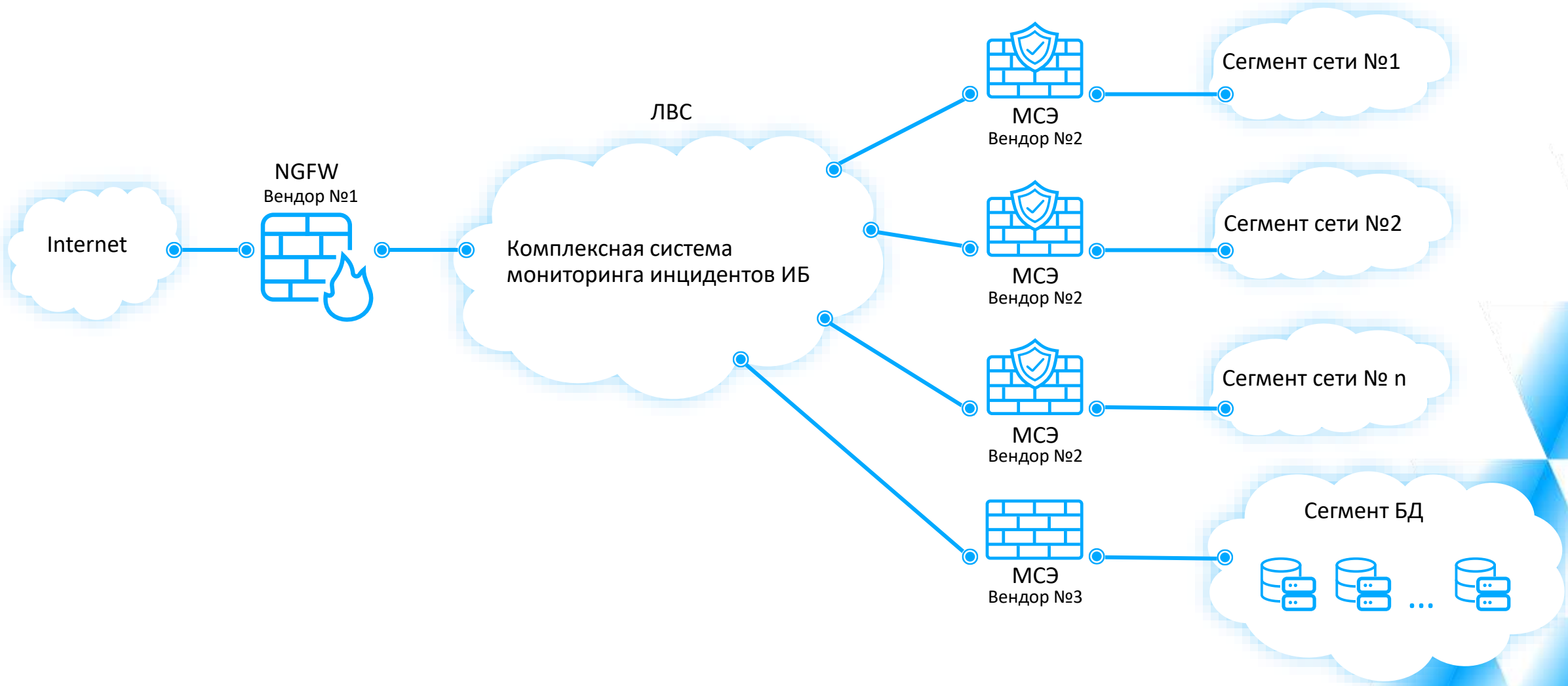
Пример 1

Защита от бесконтрольного прямого доступа в интернет из корпоративной сети



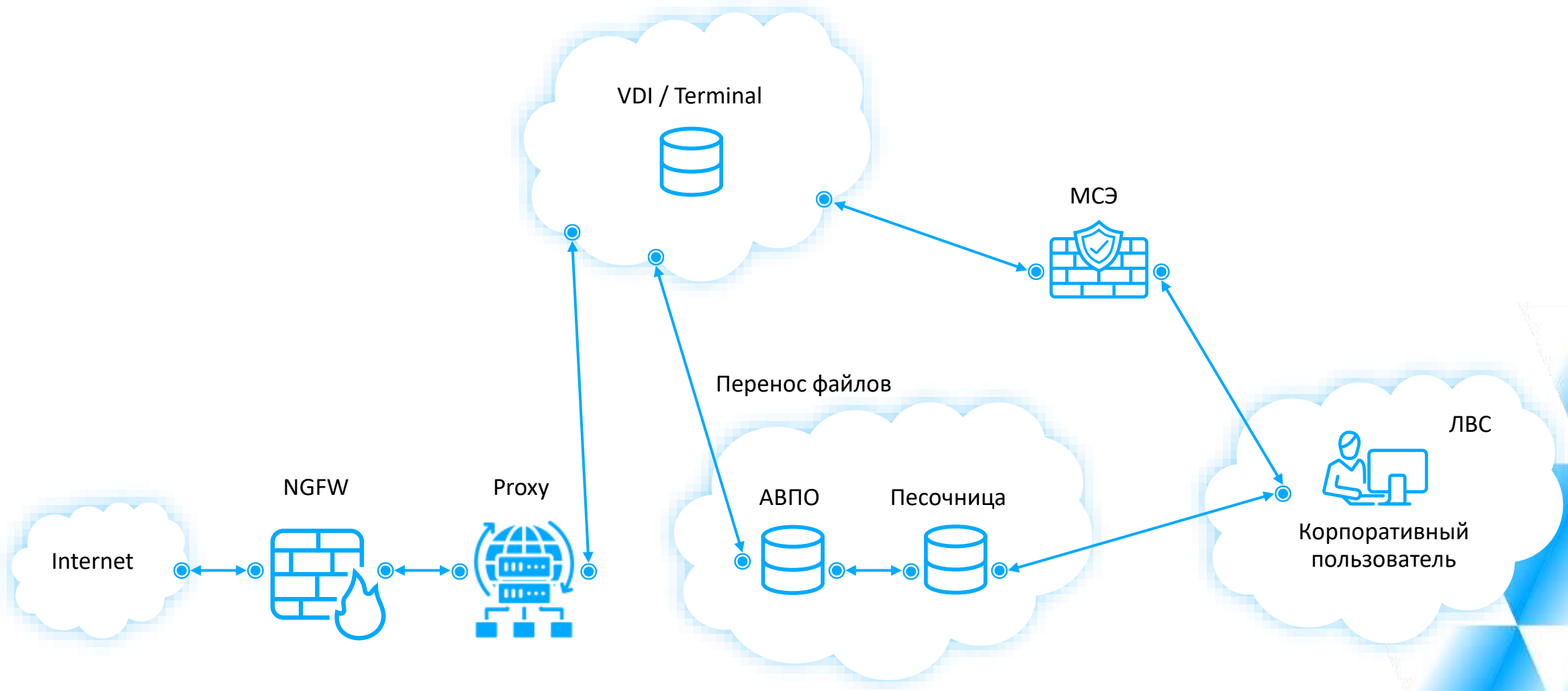
Пример 1

Защита от бесконтрольного прямого доступа в интернет из корпоративной сети



Пример 1

Защита от бесконтрольного прямого доступа в интернет из корпоративной сети



Пример 1

Защита от бесконтрольного прямого доступа в интернет из корпоративной сети

Эффекты от реализации схем защиты ИБ

Контроль интернет-трафика: исключение прямого бесконтрольного выхода в сеть с рабочих мест (АРМ) внутри корпоративной сети

Безопасность вне периметра: ограничение прав пользователей исключает возможность подключения АРМ к сторонним проводным сетям вне офиса

Строгое соблюдение требований ИБ:

Обнуление сессий: все данные и вредоносное ПО удаляются при завершении работы, система возвращается к эталонным настройкам

Изоляция среды: запрет буфера обмена между виртуальным столом и корпоративной сетью блокирует перенос вирусов

Минимизация рисков взлома: доступ злоумышленника к виртуальному рабочему столу не дает входа в корпоративную сеть; по окончании сессии доступ автоматически аннулируется (система обнуляется)

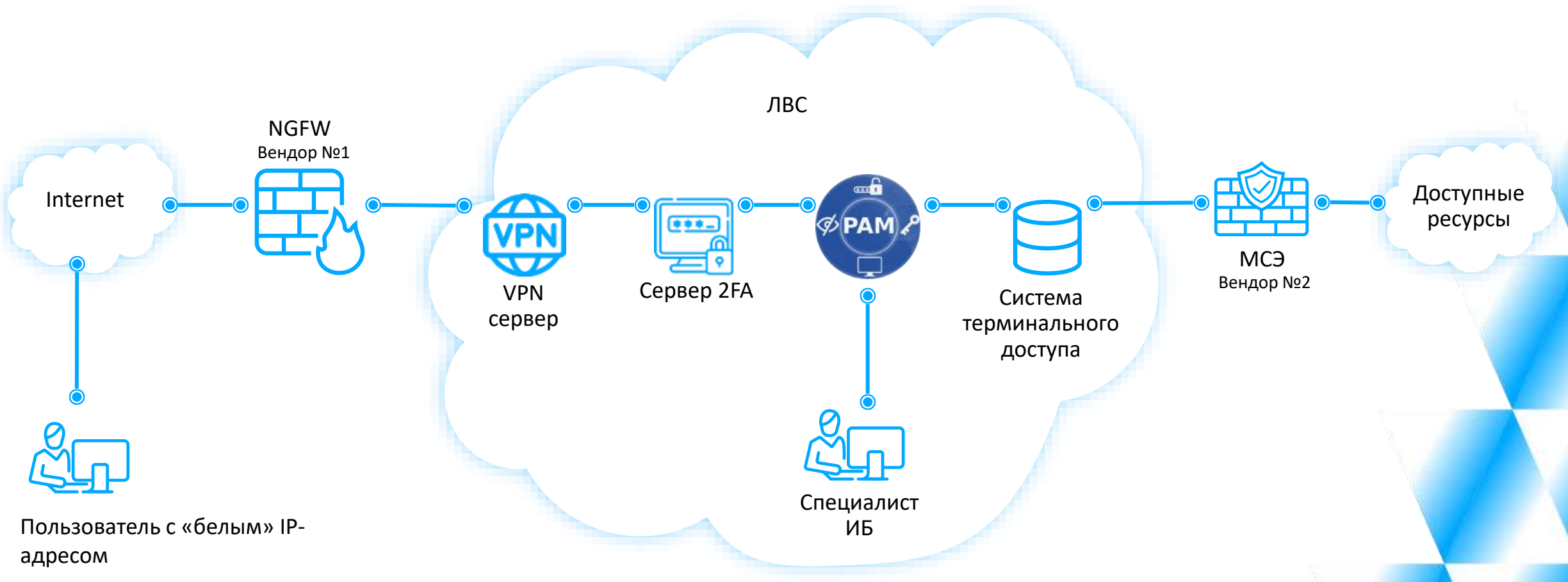
Контентная фильтрация: использование прокси-сервера для ограничения доступа — только к ресурсам, необходимым для выполнения должностных обязанностей

Пример 2

Защита от бесконтрольных доступов к USB-портам

Пример 3

Защита от бесконтрольного удаленного доступа к ресурсам предприятия



Пример 3

Защита от бесконтрольного удаленного доступа к ресурсам предприятия

Регламент организации и требования к удаленному доступу

Согласование доступа: только через подразделения ИТ и ИБ

Минимальные технические требования:

- Статический («белый») IP-адрес
- Актуальный антивирус на АРМ
- Подписанное согласие по защите информации
- VPN-клиент и личный сертификат доступа
- Установленный клиент 2FA

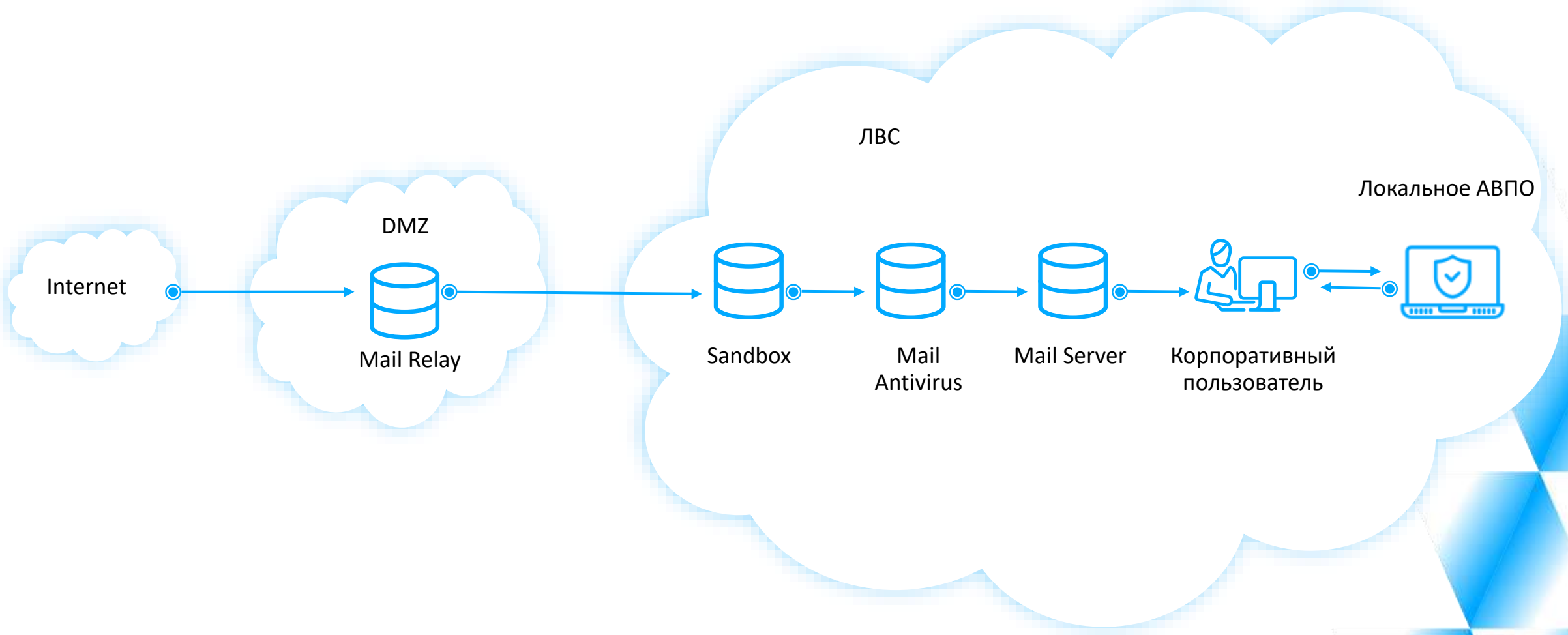
Учетные данные: личное получение логинов/паролей; смена каждые 90 дней

Цепочка аутентификации: VPN → 2FA → PAM-система → Виртуальная машина

Контроль: полное логирование и видеозапись сессий в PAM-системе

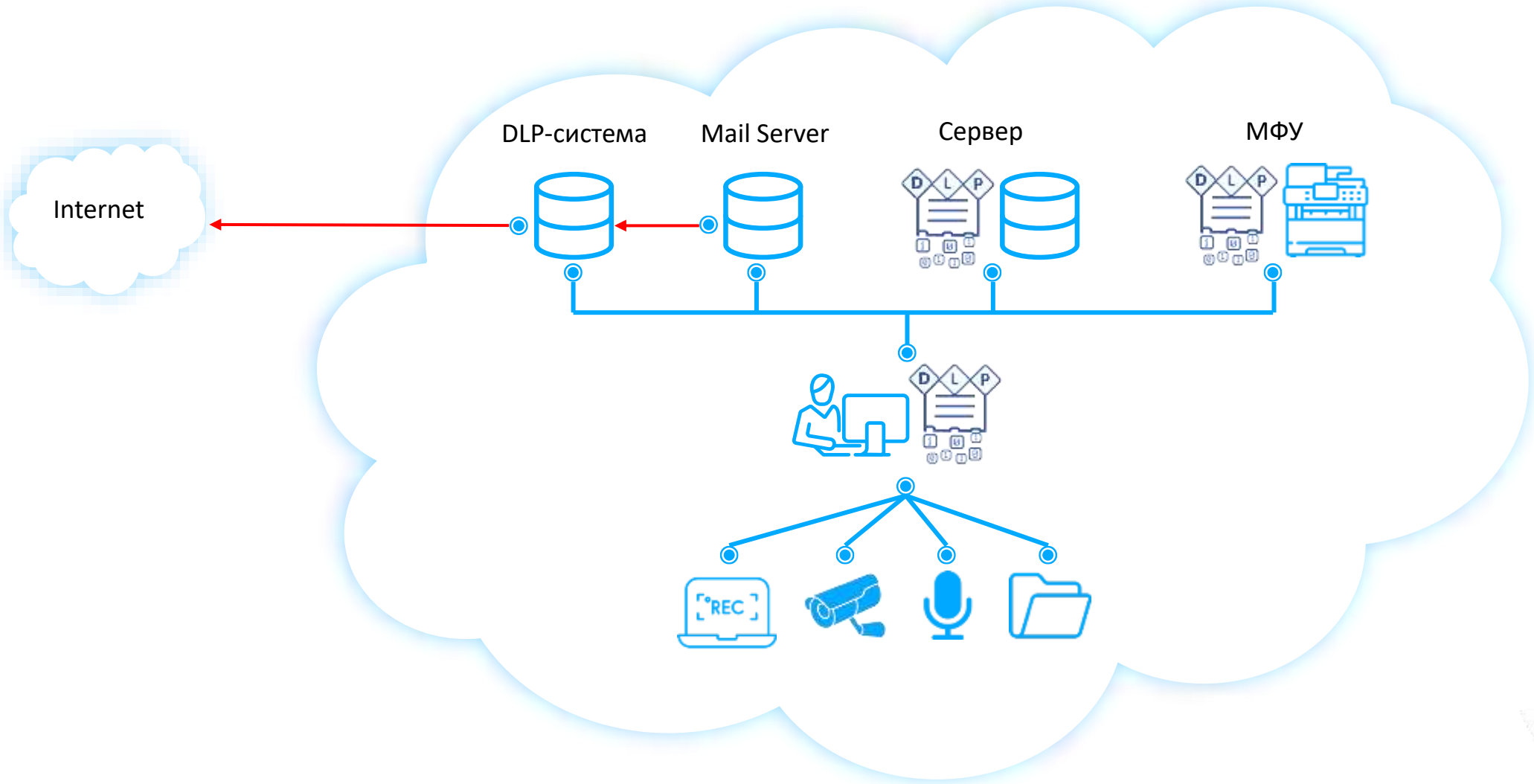
Пример 4

Защита от получения фишинговых сообщений и отправки конфиденциальной информации



Пример 4

Защита от получения фишинговых сообщений и отправки конфиденциальной информации



Пример 4

Защита от получения фишинговых сообщений и отправки конфиденциальной информации

«Песочница» устанавливается «в разрыв», обеспечивая проверку всего почтового трафика на наличие вредоносного ПО в режиме реального времени

Антивирусное ПО работает «в разрыв», что позволяет в реальном времени проверять весь поток сообщений на наличие вирусного ПО

DLP-система для исходящего трафика включается «в разрыв» для глубокого анализа почтовых сообщений на наличие информации конфиденциального характера

Выводы

Соответствие требованиям регуляторов: Учитывая ежегодное ужесточение законодательства, необходимо строить максимально защищенные периметры и системы ИБ, что является критически важным для субъектов КИИ

Гибкость и безопасность коммуникаций: Существующие технологические возможности позволяют реализовать схемы взаимодействия по любым информационным каналам без нарушения требований ИБ

Отраслевая универсальность решений: Современные инструменты защиты применимы в любых отраслях. Их внедрение позволяет гарантировать безопасность предприятий и подтверждает, что сегодня каждая отрасль нуждается в передовых решениях в области информационной безопасности.

Пулково

СПАСИБО ЗА ВНИМАНИЕ!

Начальник службы по обеспечению информационной безопасности
ООО «Воздушные Ворота Северной Столицы»

Савченко Сергей Юрьевич