# Мировой опыт обеспечения конфиденциальности, безопасности и соответствия требованиям в Office 365

Андрей Шереметинский
Эксперт по технологиям
Microsoft Corporation

Office 365

# Доверие к провайдеру основывается…

## Неприкосновенности

Что значит неприкосновенность данных для Microsoft?

Используете ли вы мои данные для подготовки и продажи аналитических отчетов?

## Прозрачности

Где хранятся мои данные?

Кто имеет доступ к моим данным?

## Соответствии нормам

Какие сертификаты соответствия нормам есть у Microsoft?

Какие документы Microsoft предоставляет для соответствия нормам?

## Безопасность

Безопасно ли хранить данные в облаке?

Безопасна ли инфраструктура Microsoft Online Services?

Какие дополнительные возможности дает Office 365 сотрудникам СБ?

Office 365

# История дата-центров Microsoft


1989 — Первый центр обработки данных Microsoft

1995 — Hotmail, msn

1995 — Центр отзывов по безопасности компании Microsoft (MSRC)

2000 — Active Directory

2000 — Центр обновления Windows

2000 — Xbox Live

2000 — Подразделение Global Foundation Services (GFS)

2000 — Меморандум Билла Гейтса

2000 — Инициатива Trustworthy Computing (TwC)

2005 — Центр инженеров по безопасности Microsoft (MSEC) / Жизненный цикл разработки безопасного ПО (SDL)

2005 — Центр защиты от вредоносного программного обеспечения

2005 — Сертификация SAS-70

2005 — Microsoft Online Services

2010 — Сертификация ISO 27001

2010 — Windows Azure

2010 — Microsoft Security Essentials

2010 — Сертификация FISMA

Office 365

# Безопасность Office 365

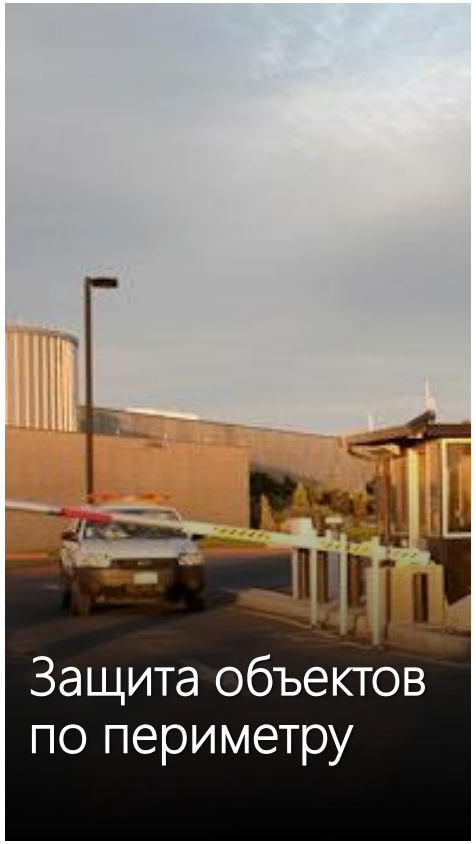
Встроенные средства безопасности Office 365

Средства и системы, контролируемые заказчиками Office 365

Независимое тестирование Office 365 и обеспечение соответствия нормативным требованиям


Office 365

# Физическая защита оборудования







Сейсмическая защита

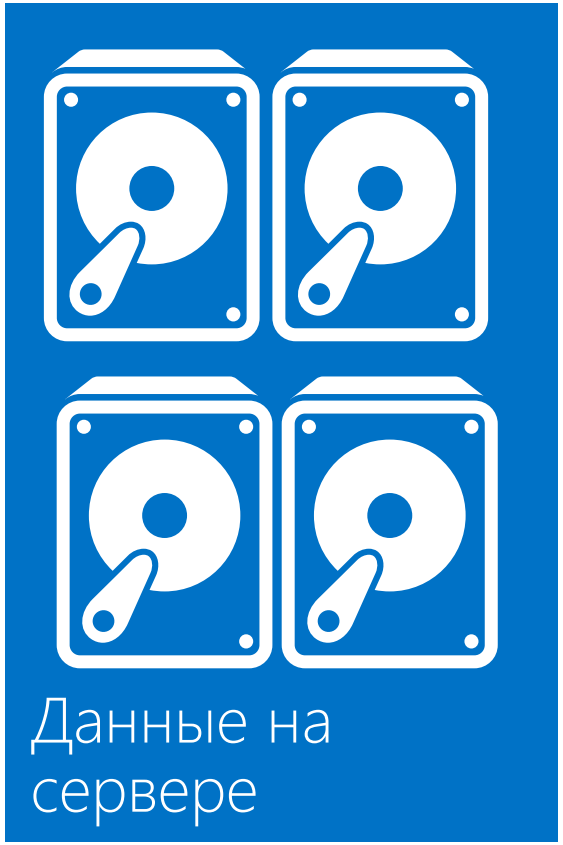
Круглосуточная охрана объектов

Электроснабжение от резервных источников в течение нескольких дней

Десятки тысяч серверов

Office 365

# Изолированные данные клиентов




Логическая изоляция данных на одном и том же физическом оборудовании

Невозможность преднамеренного или случайного доступа к данным другого клиента

Физическая изоляция данных корпоративных клиентов от частных

Office 365

# Безопасная сеть


Сети в центрах обработки данных Office 365 разделены на сегменты.
Обеспечивается физическая изоляция критически важных внутренних серверов и устройств хранения данных от общедоступных интерфейсов.
Средства безопасности пограничных маршрутизаторов позволяют выявлять попытки вторжения и признаки уязвимости системы.

Office 365

# Шифрование данных

## Шифрование данных в местах хранения (Encryption at Rest)

Все жесткие диски зашифрованы с использованием технологии BitLocker

Возможно использовать сторонние решения для предварительного шифрования передаваемой информации (Encryption gateway)

## Шифрование передаваемых данных

Для всех коммуникаций используются протоколы Transport Layer Security (TLS) и Secure Sockets Layer (SSL).

Exchange Online поддерживает RMS, S/MIME и технологии сторонних разработчиков, например PGP.

Office 365

# Автоматизация операций

**Зарегистрировано как заявка на обслуживание**

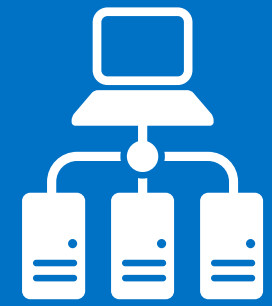
1. Контролируемые функции.
2. Возможность самостоятельного составления отчетов.

Администратор O365 запрашивает доступ

Блокировка: контроль доступа на основе ролей

Сеть ЦОД Office 365

Предоставление временных привилегий



Корпоративная сеть Microsoft

**Предоставляются минимальные привилегии, необходимые для выполнения задачи. Проверка наличия прав будет пройдена успешно, если:**

1. завершена проверка анкетных данных,
2. завершено снятие отпечатков пальцев,
3. завершено обучение мерам безопасности.

Office 365

# Функционал обеспечения безопасности Office 365

Office 365

# Функциональные возможности

## Контроль данных

## Поиск

### Транспортные правила и DLP

Применение правил к передаваемой почте

Отправка писем через согласующего

Запрет отправки писем по критериям

Контроль или запрет передачи персональных данных

### Удержание и контроль данных

Двухфакторная аутентификация

Использование не доменных учетных записей

Удержание данных по критериям

Сохранение удаленных или измененных сотрудником писем, документов SharePoint и активностей из Lync

### Шифрование почты

Шифрование почтового трафика до партнера

Шифрование писем с применением правил

Защита писем от прочтения в случае утери письма

Правила для писем
-только прочтение
-запрет печати
-запрет снимка экрана

### Сквозной поиск

Поиск информации по всем ящикам

Делигирование полномочий для СБ

Поиск удержанных или измененных сообщений

Поиск по персональным архивам сотрудников

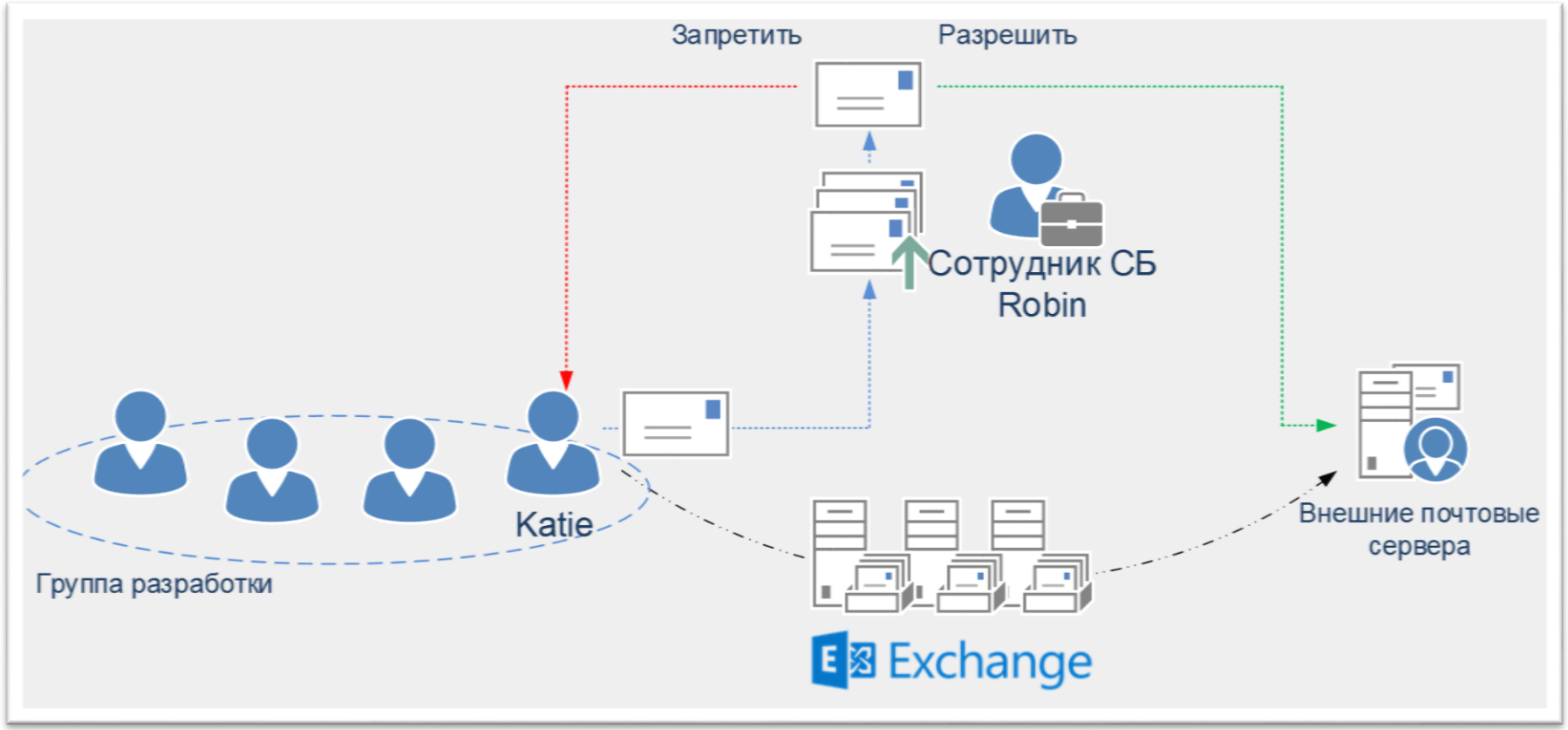
Система отчетов

Office 365

# Реализация контуров безопасности

С применением транспортных правил можно управлять потоками электронной почты по различным критериям

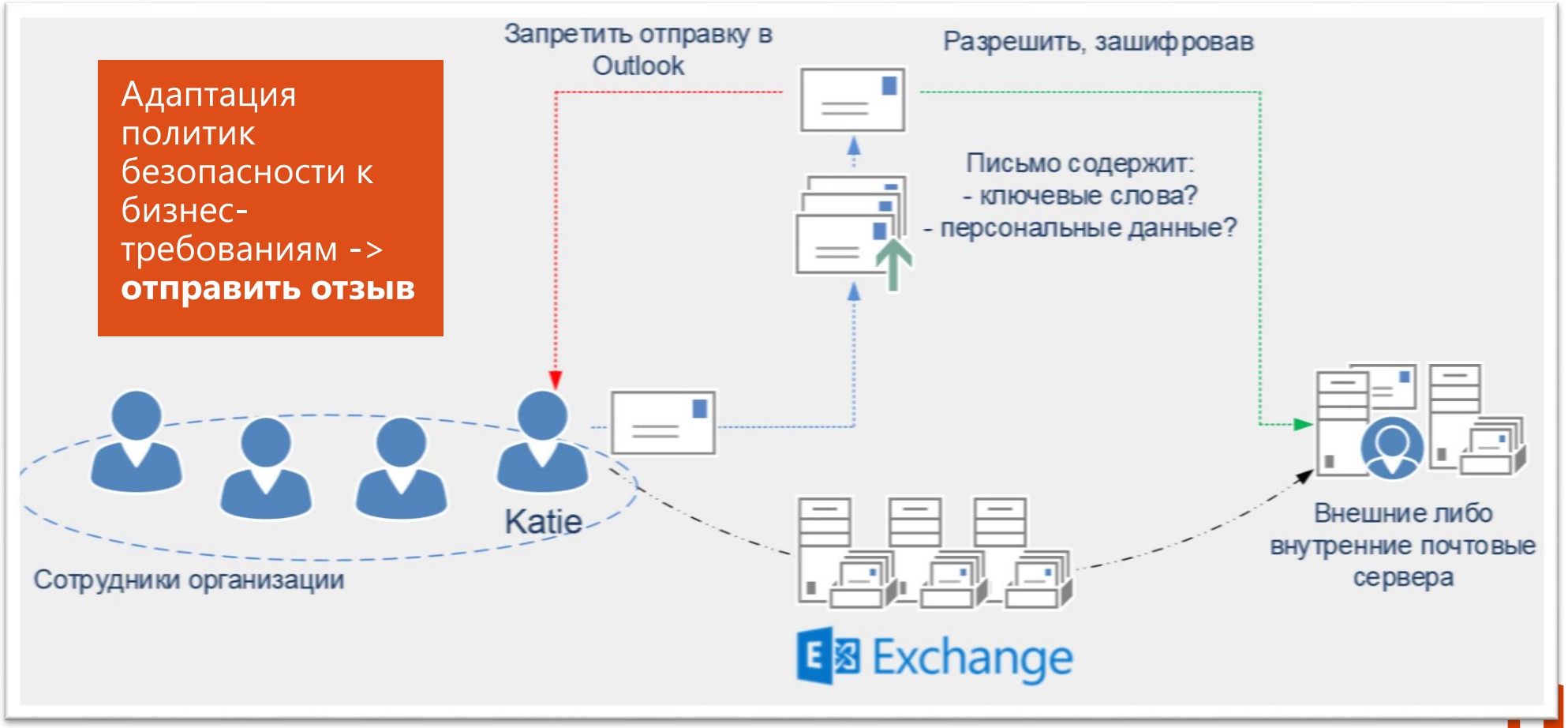
Пример - отправка писем во внешнюю сеть группой сотрудников через согласующего




Office 365

# Предотвращение утечек информации

С применением транспортных правил и DLP функционала возможна шифрация писем, содержащих ключевые слова либо отказ в отправке письма, содержащего персональные данные




Office 365

# Сквозной поиск (eDiscovery)

Office 365

# Новый Rights Management Service

Поддержка файлов любых типов файлов

Возможность работы с защищёнными файлами на различных платформах (ОС) через соответствующие SDK/мобильные приложения

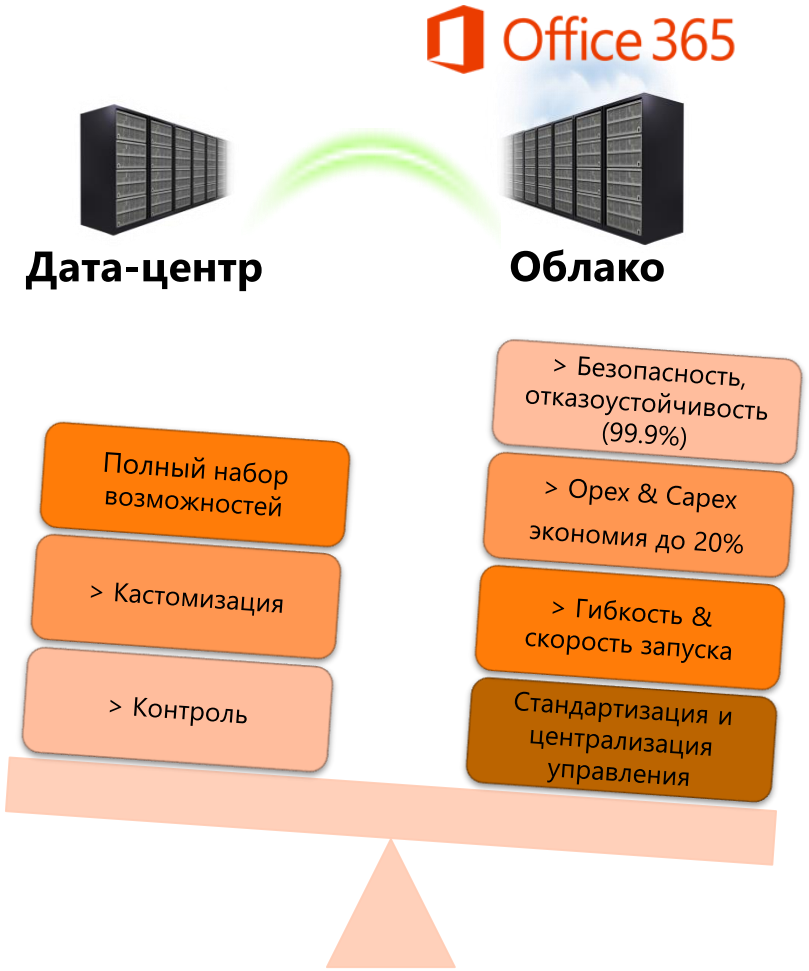
Возможность передачи защищённых файлов за пределы своей организации (т.н. “business to business” или “business to labour” file sharing) – внешние пользователи смогут открывать эти файлы бесплатно

Возможность использования собственного приватного ключа*


*Функционал ограничен при использовании с Exchange Online

Office 365

# Основания для перехода в «облако»




- Безопасное хранение данных в облаке
- Надежная и безопасная инфраструктура Microsoft Online Services
- Большое количество дополнительных возможностей для сотрудников СБ

Office 365

# Q&A

Office 365

Microsoft