22 ноября 2018

Безопасность облачных сервисов

Андрей Прошин
Менеджер по развитию бизнеса

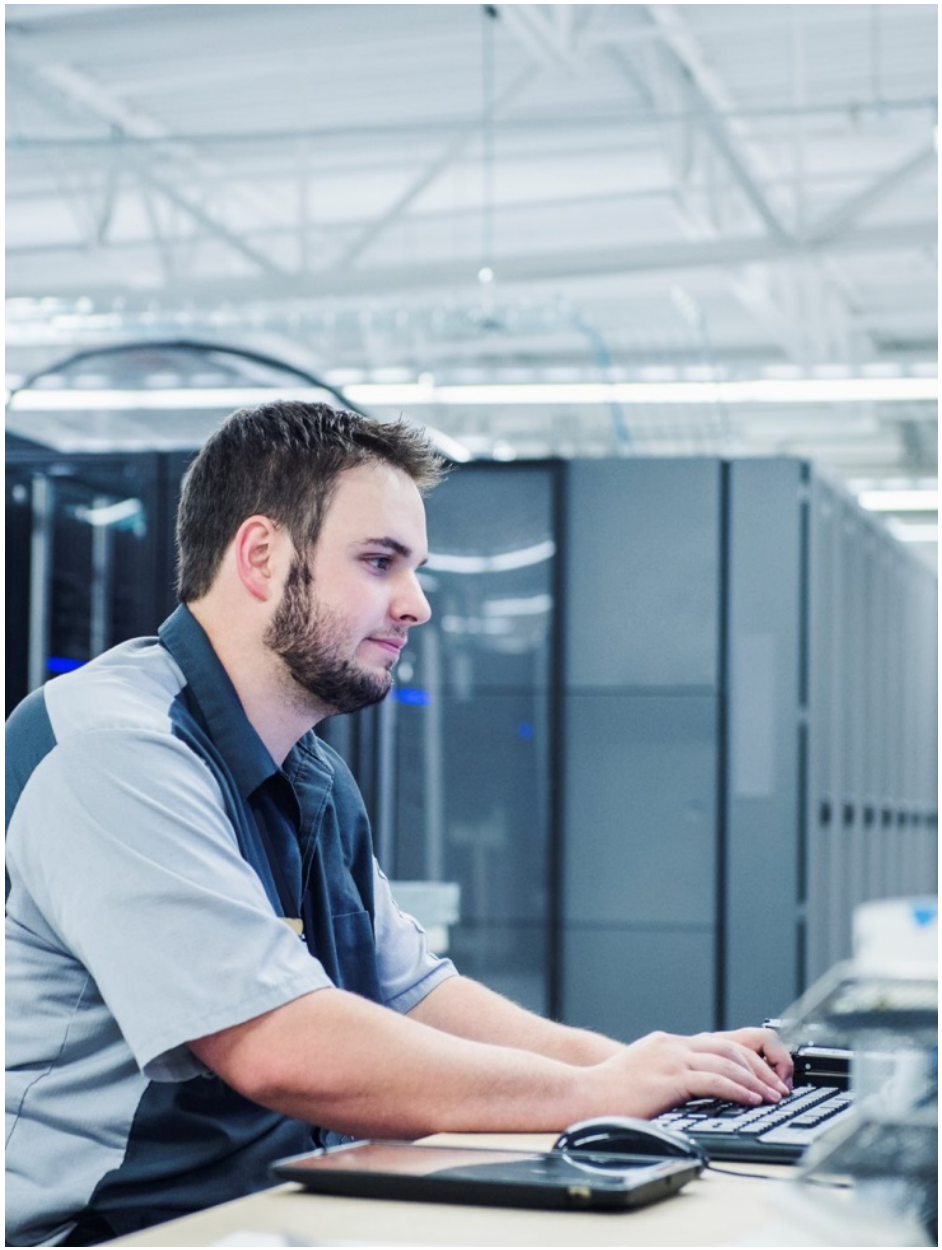
orange™ Business Services

IaaS / PaaS / SaaS

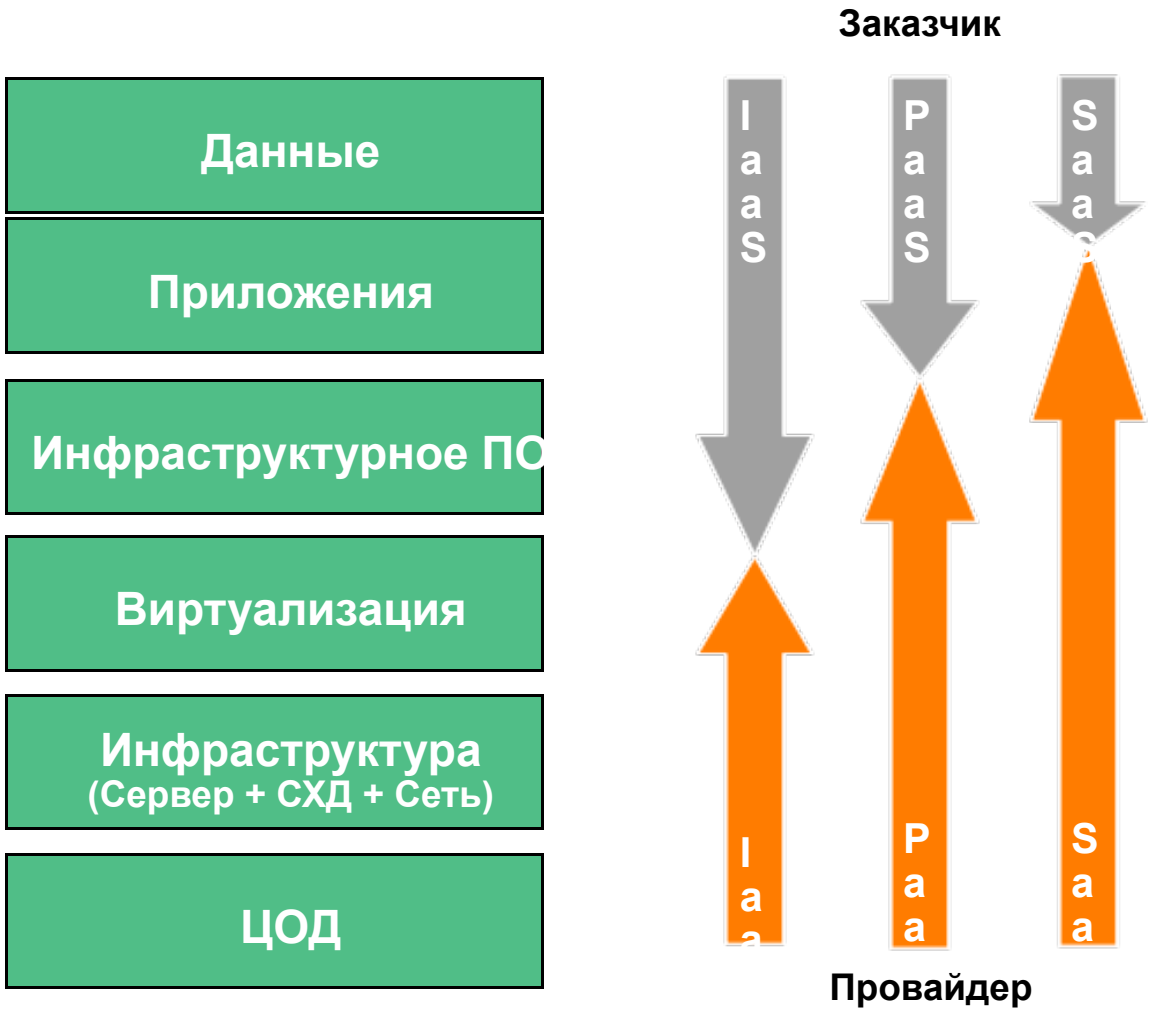
Infrastructure as a Service (IaaS)
вычислительная инфраструктура (серверы, хранилища данных, сети, операционные системы) для создания собственных приложений
Пример: Виртуальный ЦОД

Platform as a Service (PaaS)
информационно-технологические платформы: операционные системы, СУБД, связующее программное обеспечение, средства разработки и тестирования, размещённые у облачного провайдера
Пример: Облачный контакт-центр

Software as a Service (SaaS)
Готовое прикладное программное обеспечение, полностью обслуживаемое облачным провайдером
Пример: Аутентификация из облака



Зоны ответственности

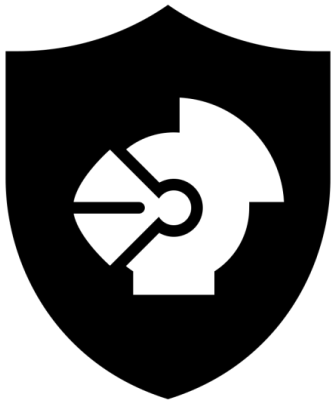


Безопасность для облачных сервисов

Compliance (требования законодательства)

- Закон о Персональных Данных
- Закон о Критической Информационной Инфраструктуре
- Отраслевые стандарты и рекомендации

Общие требования по ИБ



- Корпоративные политики
- NIST SP 800-144 “Guidelines on Security and Privacy in Public Cloud Computing”

Провайдеру необходимо подготовить облачный сервис под оба типа требований ИБ

Compliance: пример реализации

Заказчик планирует размещать и обрабатывать персональные данные в облаке

Провайдеру необходимо:

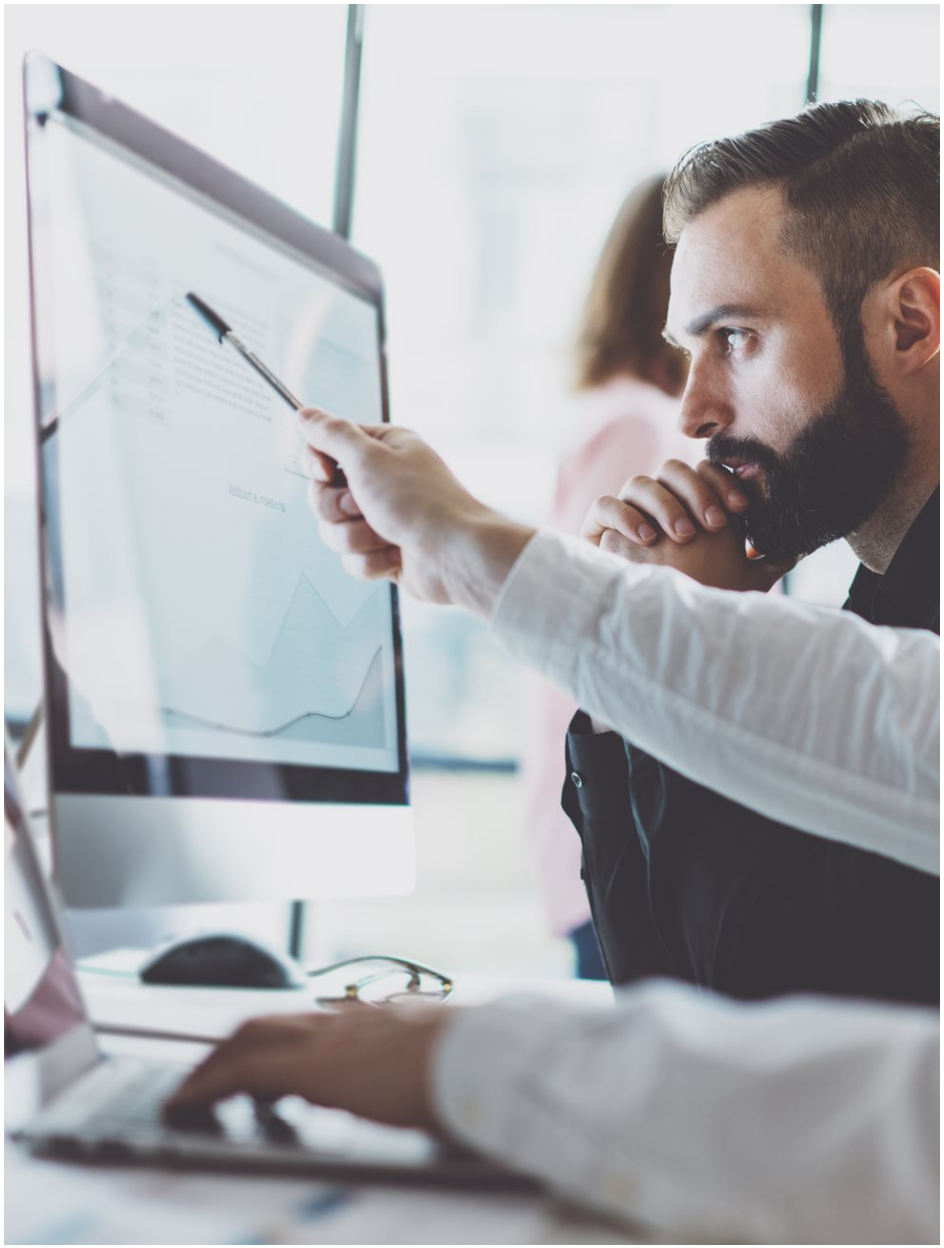
- Подготовить типовой набор документов (в том числе, модель угроз), который может быть использован Заказчиком для проекта СЗПДн;
- Иметь в составе сервиса необходимые средства ИБ (сертифицированные), которые могут быть использованы в СЗПДн;
- Наличие необходимых лицензий ФСТЭК, ФСБ для работы.

Общие требования ИБ: пример реализации

Заказчик запрашивает необходимые меры защиты в соответствии со соответствии со своими корпоративными требованиями

Провайдеру необходимо:

- Использовать риск-ориентированный подход при проектировании облачного сервиса;
- Использовать необходимые средства ИБ для защиты инфраструктуры (МЭ, IPS, DDoS, 2FA, защита виртуализации и др)
- Иметь возможность предложить дополнительные средства ИБ для выполнения специфичных требований
- Обеспечивать мониторинг и реагирование на инциденты ИБ



Требования клиентов (IaaS/SaaS)

Размещение приложений в облачном ЦОД + полностью управляемый сервис

Требования Заказчика

1. Подготовка и предоставление необходимых документов (политики, регламенты, технические схемы) в области обеспечения ИБ
2. Сегментация между сетями и между разными Заказчиками
3. Подключение к ЦОДам Заказчика через VPN или MPLS
4. Всегда использовать шифрование при передаче данных
5. Наличие процедуры Patch Management
6. Требования к парольной политике
7. Необходимость проводить периодические аудиты и пен тесты
8. Требования к бэкапированию (шифрование, отдельное хранение, доступ персонала)
9. Мониторинг и уведомление об инцидентах ИБ, касающихся инфраструктуры

Решение

- ISO 27001 аудиты
- Использование МЭ и др средств ИБ как часть решения
- Использование криптосредств
- Процесс патч-менеджмента
- Процесс создания резервных копий
- 24x7 мониторинг и реагирование на инциденты ИБ
- Использование различных систем безопасности в самом ЦОД
- Использование IDM / PAM для администраторов

Требования клиентов (PaaS)

Подключение к платформе Контакт Центра

Требования Заказчика:

1. Защита периметра + предоставить диаграмму
2. Использование IPS, WAF, DDoS
3. Использование шифрование при передаче и хранении данных
4. Использование парольной политики
5. Использование средств защиты рабочих станций администраторов
6. Анализ защищенности
7. Работа с подрядчиками (если есть)
8. Мониторинг и реагирование на инциденты

Решение

- ISO 27001 аудиты
- Использование МЭ и др средств ИБ как часть решения
- Использование криптосредств
- Процесс патч-менеджмента
- Процесс создания резервных копий
- 24x7 мониторинг и реагирование на инциденты ИБ
- Использование различных систем безопасности в самом ЦОД
- Использование IDM / PAM для администраторов

Решение о выборе провайдера принимается на основе анализа и обсуждения рисков

Совместные усилия

На стороне провайдера
[Защита инфраструктуры]

1. Проектирование облака с учетом требований ИБ, использование СЗИ
2. Периодический анализ защищенности
3. 24x7 Мониторинг (включая долгосрочное хранение) и реагирование на инциденты
4. Использование threat intelligence (данных о новых атаках и уязвимостях)
5. Периодические аудиты (включая ISO 27001)

На стороне Заказчика
[защита/контроль данных в облачных средах]

1. Анализ рисков и модель угроз (в том числе для внутреннего нарушителя)
2. Разграничение доступа сотрудников для работы с облачными сервисами
3. Контроль и мониторинг работы с данными в облаке (CASB)

Спасибо!

orange™ Business Services