

Обеспечение информационной безопасности в облачных бизнес-приложениях и дата-центрах (на примере ЦОД SAP CIS)

Шабанов Алексей,
Эксперт по Информационной Безопасности

- ✓ Снижение совокупной стоимости владения
- ✓ Автоматические обновления
- ✓ Быстрый результат
- ✓ Надежность
- ✓ Безопасность
- ✓ Масштабируемость
- ✓ Интеграция
- ✓ Простота в использовании



Ключевые ценности SAP Cloud

■ Чтобы завоевать доверие наших клиентов, мы...

- ❑ Защищаем Ваши данные также хорошо, как это делаете Вы, и даже лучше;
- ❑ Оберегаем персональные данные Ваших сотрудников также хорошо, как это делаете Вы, и даже лучше;
- ❑ Гарантируем надежность, которую ожидаете Вы, и даже выше;
- ❑ Обеспечиваем открытость и прозрачность наших процессов, политик, методик и сервисов на уровне Вашего ИТ-подразделения и даже выше;
- ❑ Предлагаем гибкий подход к обеспечению Ваших будущих потребностей;
- ❑ Не создаем преград для управления изменениями.



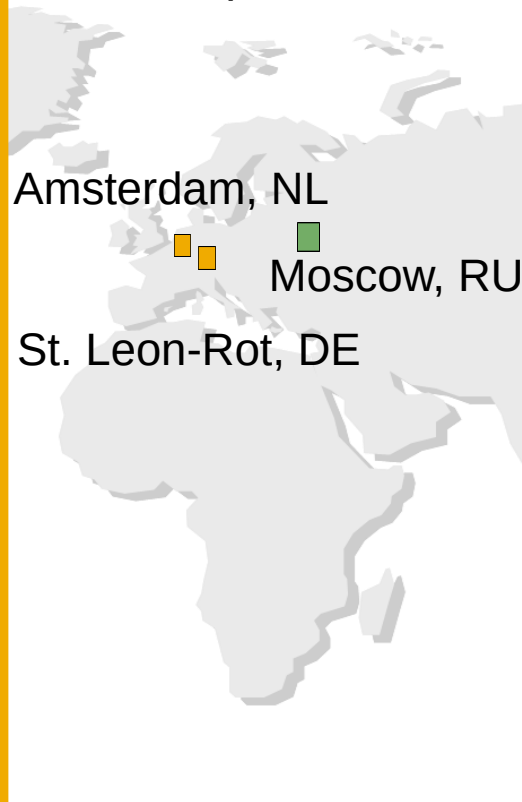
Центры обработки данных SAP



US Operations



EU Operations



APJ Operations



■ Data center location

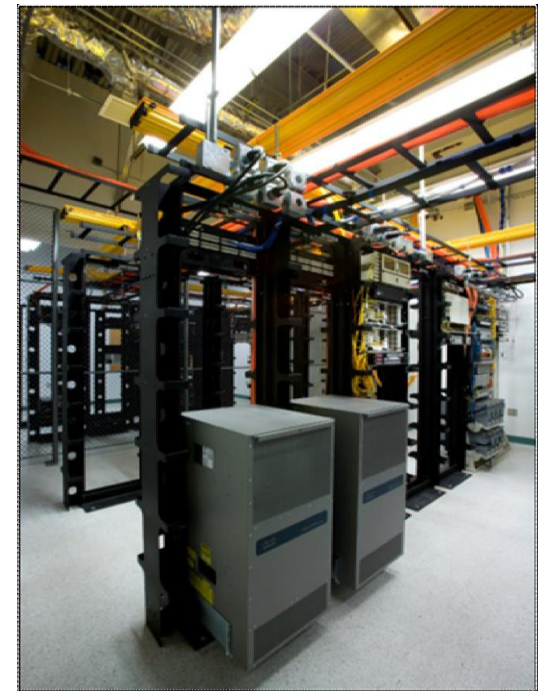
Стандарты SAP

❑ Система информационной безопасности:

- ❑ Политика ИБ базируется на стандартах ISO27002 и Safe Harbor
- ❑ **Сертификаты решений SAP**
 - ❑ ISO/IEC 27002 менеджмент ИБ
 - ❑ ISO/IEC 20000 менеджмент ИТ-сервисов
 - ❑ BS 10012 менеджмент персональных данных
- ❑ **Требования SAP к ЦОДам**
 - ❑ Tier Level III, III+ or IV уровень отказоустойчивости
 - ❑ ISO 9001:2008 система управления качеством
 - ❑ ISO/IEC 27001:2005 система менеджмента ИБ
 - ❑ PCI-DSS v2.0 безопасность платежных систем
- ❑ **Аудит ИБ согласно SSAE16-SOC2* Type 2**
 - ❑ раз в 6 месяцев

*Statements on Standards for Attestation Engagements No. 16 - Service Organization Control Audit

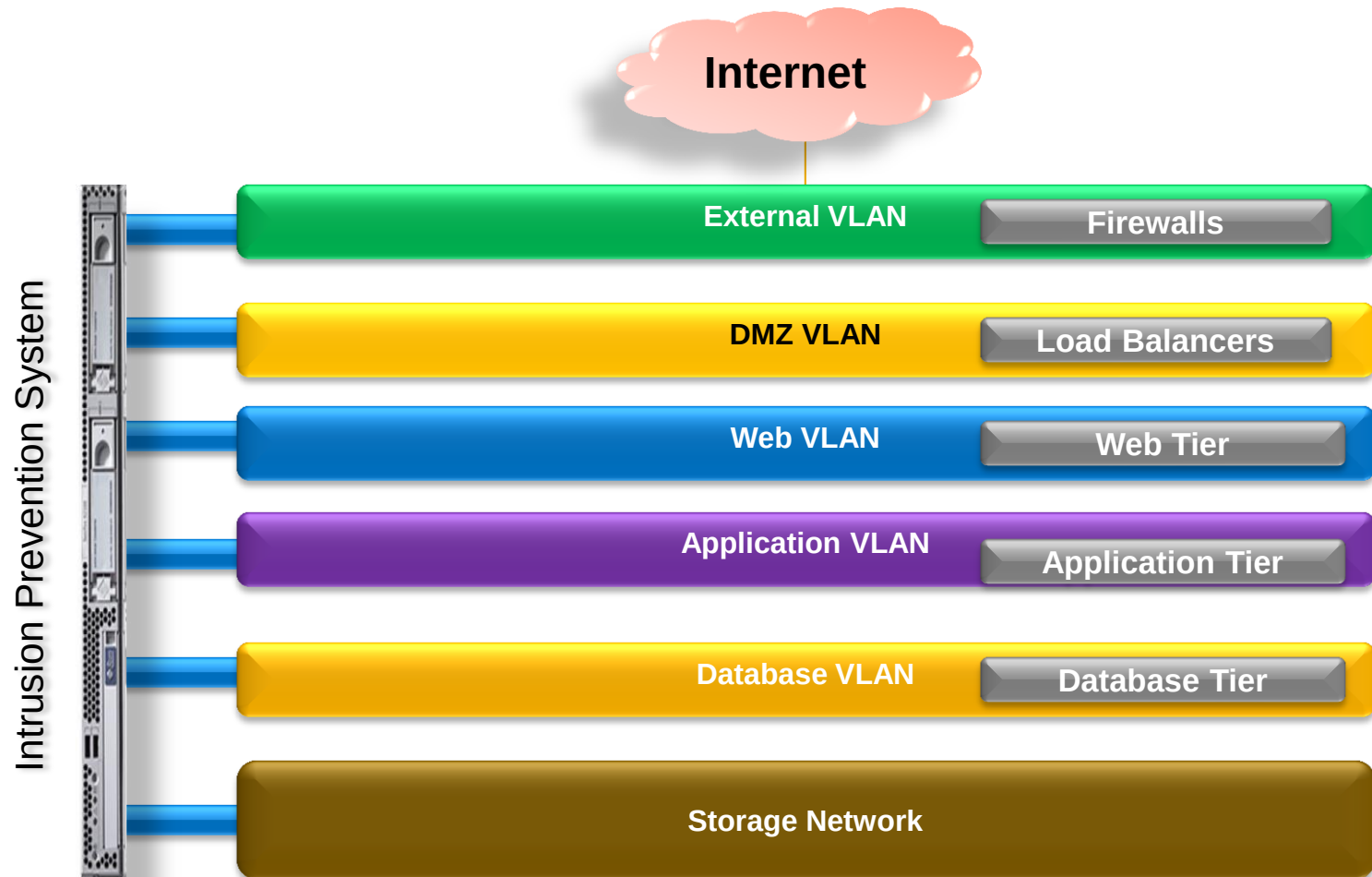
SAP CLOUD: DATA CENTER SECURITY REQUIREMENTS





Безопасность в Cloud-решениях SAP

Public Cloud: Сетевая модель



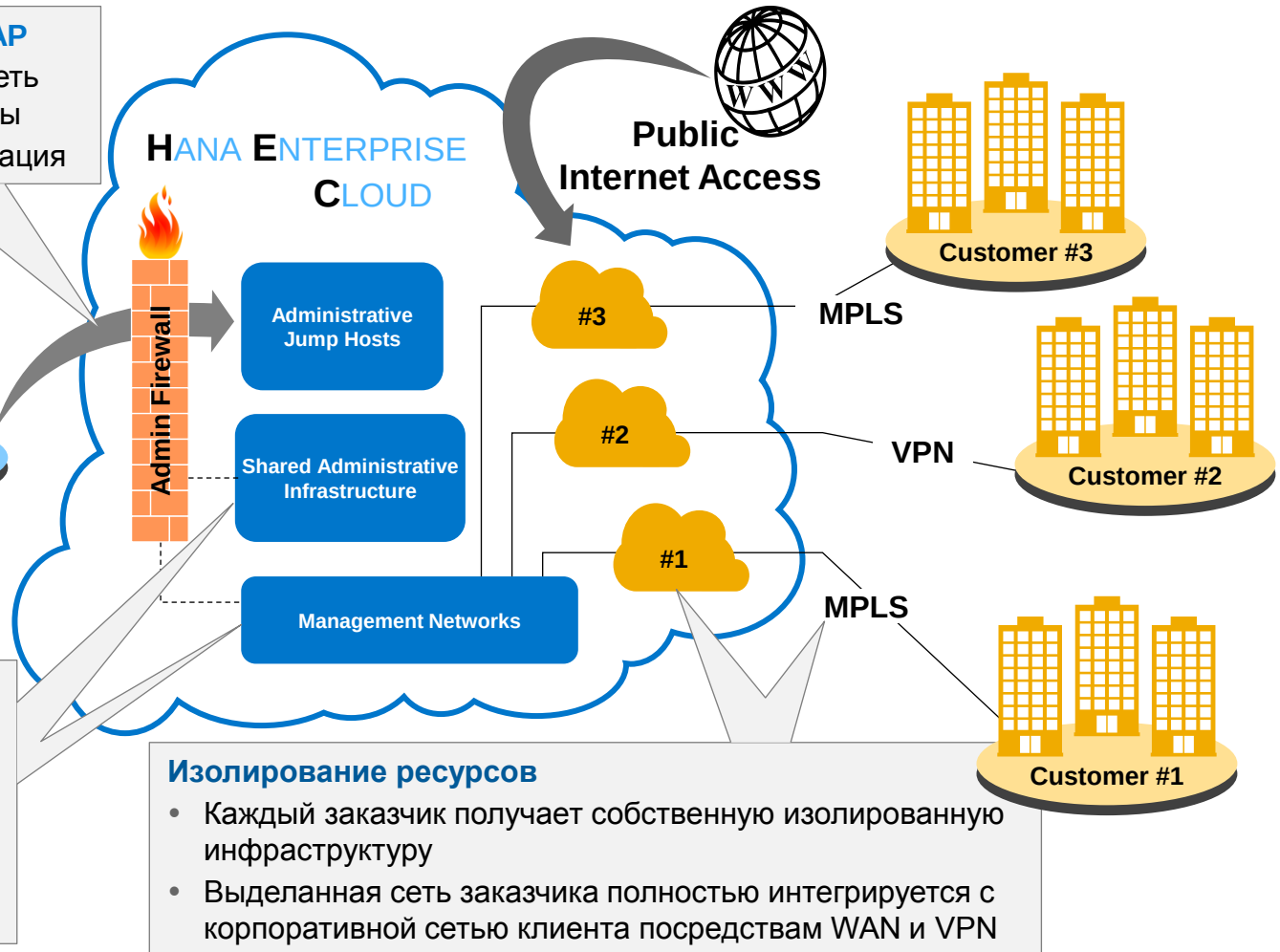
Public Cloud: Архитектура решения



Private Cloud: Архитектура HANA Enterprise Cloud

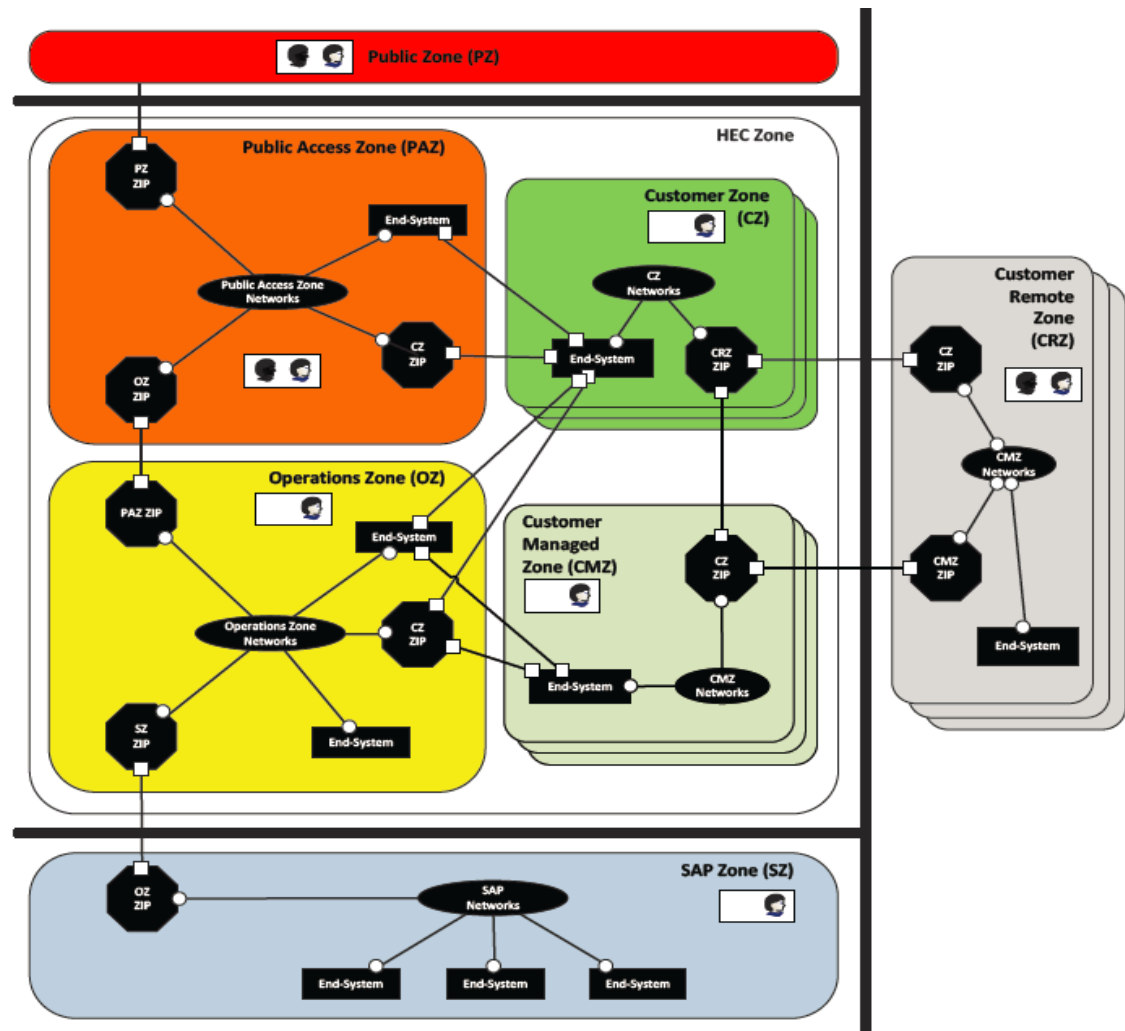
Интеграция облака HEC и SAP

- Сеть DC и корпоративная сеть SAP полностью изолированы
- Двухфакторная аутентификация

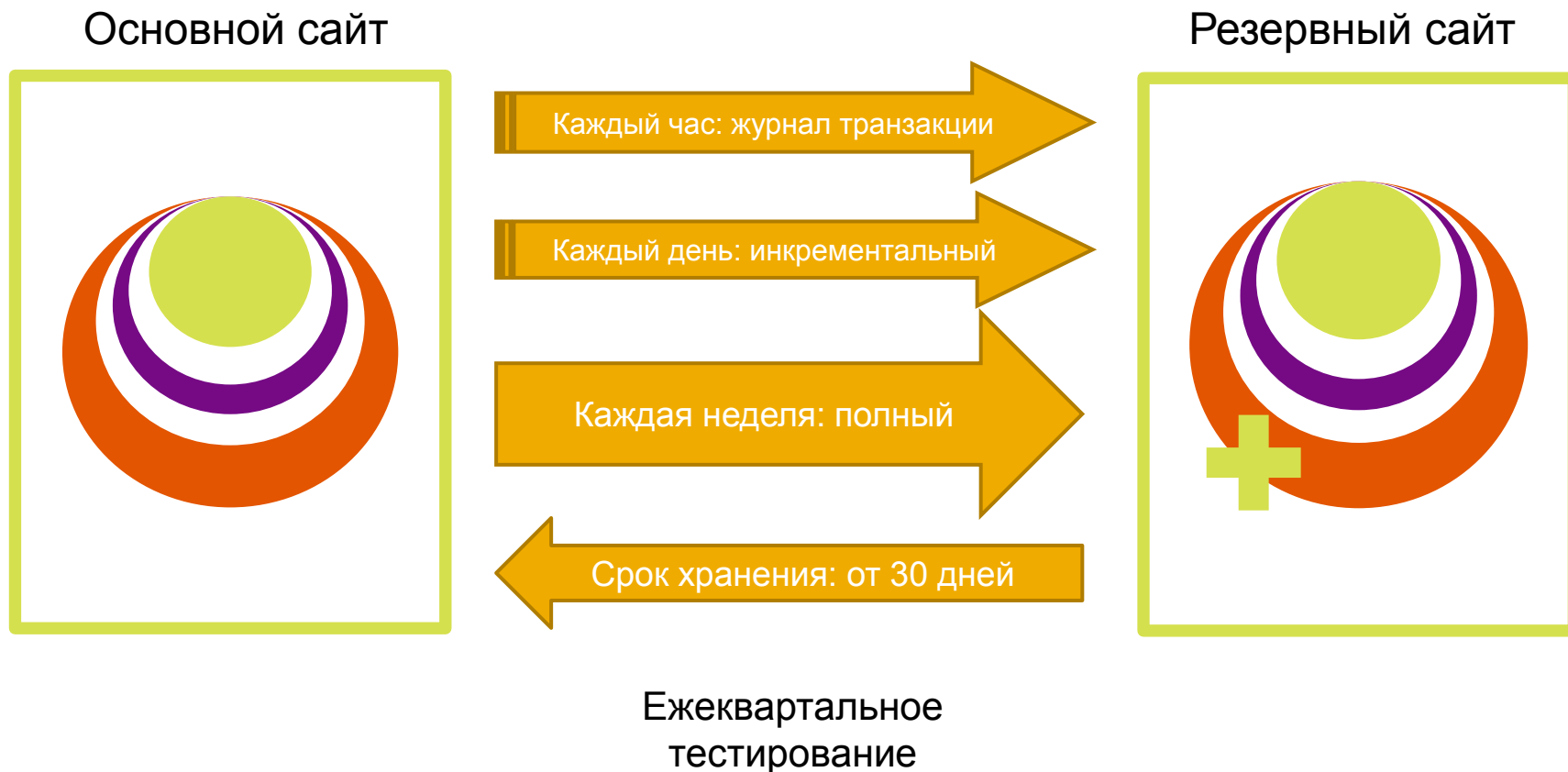


Private Cloud: Модель зон безопасности

- ✓ Каждая зона имеет свой уровень безопасности
- ✓ Принцип матрешки
- ✓ Контроль полномочий пользователя на каждом пограничном устройстве



Резервное копирование



Резервное копирование: в пределах 24 часов

Среднее время восстановления: в пределах 72 часов

Процесс резервного копирования подтвержден аудитом SSAE-16 SOC-2

Мониторинг

Сканер безопасности



Клиенты



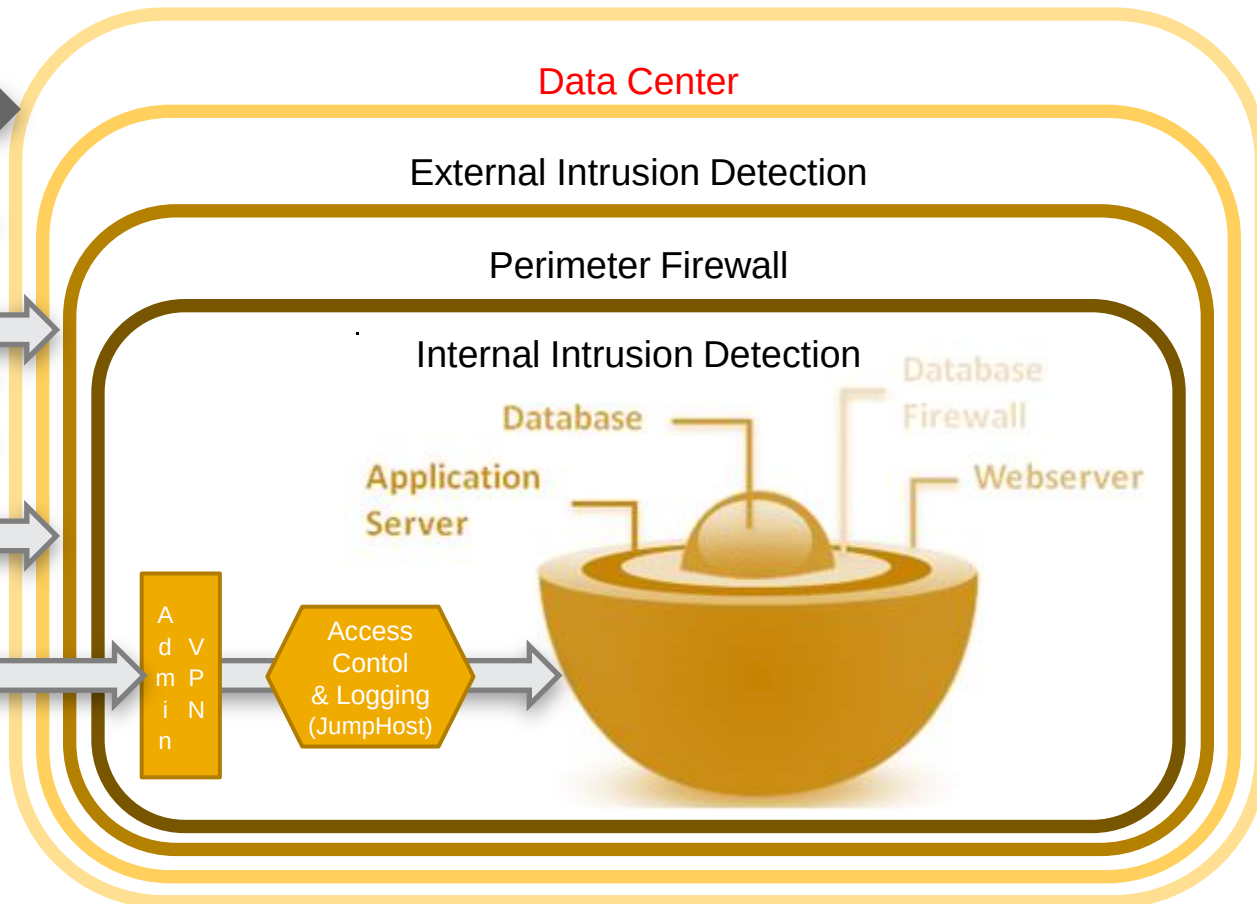
Операторы SAP

Ежемесячное
сканирование
инфраструктуры

Еженедельные
тесты на
проникновение

Тесты на
проникновение

Двухфакторная
аутентификация





Центр обработки данных SAP в России

Открыт 23 декабря 2014



Соответствие Cloud-решений SAP

требованиям Российского законодательства

- ❑ Сертификация всех функций безопасности, встроенных в ПО, а также наложенных средств защиты информации по требованиям ФСТЭК России
- ❑ Аттестация каждого решения ЦОД по 2-му уровню защищенности ПДн и классу 1Г для ИС, обрабатывающих конфиденциальную информацию, включая коммерческую тайну.
- ❑ Регистрация ЦОДа в Роскомнадзоре
- ❑ Сертификация решений ЦОД по ISO 27001 и ISO 9001



Лицензии САП СНГ:



Бессрочная лицензия ФСБ России №0010533,
рег. №13685Н от 26.06.2014г.

на 12 видов деятельности, включая
**распространение (продажу), установку,
техническое обслуживание шифровальных
(криптографических) средств, предоставление
услуг в области шифрования информации.**

Позволяет:

- соответствовать требованиям законодательства в вопросах получения по электронным каналам и продажи продуктов SAP, имеющий функции шифрования;
- предоставлять услуги, включая облачные, на территории РФ по использованию продуктов SAP, имеющий функции шифрования;
- соответствовать тендерным требованиям заказчиков при создании защищенных информационных систем.

Лицензии САП СНГ:



Бессрочные лицензии ФСТЭК России №005836, рег. № 2429 и №005837, рег. № 1312 от 17.09.2014г.

- на деятельность по разработке и производству средств защиты конфиденциальной информации
- на деятельность по технической защите конфиденциальной информации

Позволяют:

- предоставлять услуги, включая облачные, на территории РФ по использованию продуктов SAP по технической защите конфиденциальной информации, включая персональные данные;
- соответствовать тендерным требованиям заказчиков при создании защищенных информационных систем.



Спасибо!



Алексей Шабанов
Эксперт по информационной безопасности

САП СНГ
Космодамианская наб., 52/7
115054 Москва

T +7 495 755 9800
M +7 966 311 2329
E Alexey.Shabanov@sap.com
www.sap.com/cis



Backups

Перечень разрешенных видов деятельности:



12. Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств.
13. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем.
14. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
15. Монтаж, установка (инсталляция), наладка средств изготовления ключевых документов.
17. Ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств информационных систем.
18. Ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
20. Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
21. Передача шифровальных (криптографических) средств.
22. Передача защищенных с использованием шифровальных (криптографических) средств информационных систем.
23. Передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
25. Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.
26. Предоставление услуг по имитозащите информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.

Infrastructure Security Requirements – Datacenter

Cloud hosted customer environments need to be operated in an

SAP Tier Level III, III+ or IV classified Datacenter

to meet the physical security and operational compliance requirements of the customer industries.

For co-location data center (non-SAP DC), access to SAP Cloud infrastructure needs to be physically separated from other DC customers, e.g. using cages

Minimum Security Requirements	Tier I	Tier II	Tier III	Tier III+	Tier IV
Stand alone Building necessary	no	no	no	yes	yes
available external el. service lines	1	1	1	1	2
Redundancy Transformers (n / n + 1)	n	n	n+1	n+1	2(n+1)
UPS Battery System	no	yes	yes	yes	yes
Minutes UPS must provide power	0	5	>10	>10	>10
Redundancy of the UPS Systems	n	n	n+1	n+1	2(n+1)
(Diesel-) Generators	no	no	yes	yes	yes
Redundancy of Cooling Systems	n	n	n+1	n+1	2(n+1)
Cooling independent from Office Building	no	no	yes	yes	yes
Fire Detection System	yes	yes	yes	yes	yes
Fire-extinguishing system	no	yes	yes	yes	yes
Security Fences and Perimeter defense	no	no	no	yes	yes
Security Guards for Data centers	no	no	yes	yes	yes
Biometrical access controls	no	no	no	no	yes
Electronic Access cards (card readers)	yes	yes	yes	yes	yes
Access logging	no	no	yes	yes	yes
Video surveillance (CCTV) main entry	no	yes	yes	yes	yes
Video surveillance (CCTV) server room	no	no	yes	yes	yes
Video Recordings needed	no	no	yes	yes	yes
Burglar Alarm System and Sensors	no	no	yes	yes	yes
facility on site response time	<48h	<8h	1h	1h	1h
WAN Network connection lines	1	n+1	redundant	redundant	fully
LAN Network connection	n	n+1	n+1	2(n+n)	2(n+n)

Cloud-системы и персональные данные

Законодательная и нормативная база РФ

- ❑ **Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»**
- ❑ **Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»**
- ❑ **Постановление Правительства от 26.06.1995 № 608 «О сертификации средств защиты информации»**
- ❑ **Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»**
- ❑ **Нормативно-методические и руководящие документы ФСТЭК России и ФСБ России**
- ❑ **Проект приказа Минкомсвязи, определяющего требования к ЦОД**

Cloud-системы и конфиденциальная информация

Законодательная и нормативная база РФ

- ❑ **Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»**
- ❑ **Федеральный закон от 29.07.2006 № 98-ФЗ «О коммерческой тайне»**
- ❑ **Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»**
- ❑ **Постановление Правительства от 26.06.1995 № 608 «О сертификации средств защиты информации»**
- ❑ **Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»**
- ❑ **Нормативно-методические и руководящие документы ФСТЭК России и ФСБ России**
- ❑ **ГОСТы**
- ❑ **Приказы Минкомсвязи**