ДЕПАРТАМЕНТ
ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
ГОРОДА МОСКВЫ

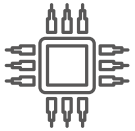
Практические аспекты проведения аттестации в государственных информационных системах

Начальник управления информационной безопасности отраслевых проектов
А. Е. Бутов

Москва: цифры и факты

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

Информационных систем



169

Визитов на mos.ru в месяц

50 млн

Ежедневно пользуются электронными услугами и сервисами на mos.ru

~ 8,5 млн

Электронных услуг оказывается ежечасно

30 тыс.

Получателей городских сервисов удовлетворены качеством оказания госуслуг

95%

Услуг доступно в электронном виде

340+

Особенности размещения ГИС

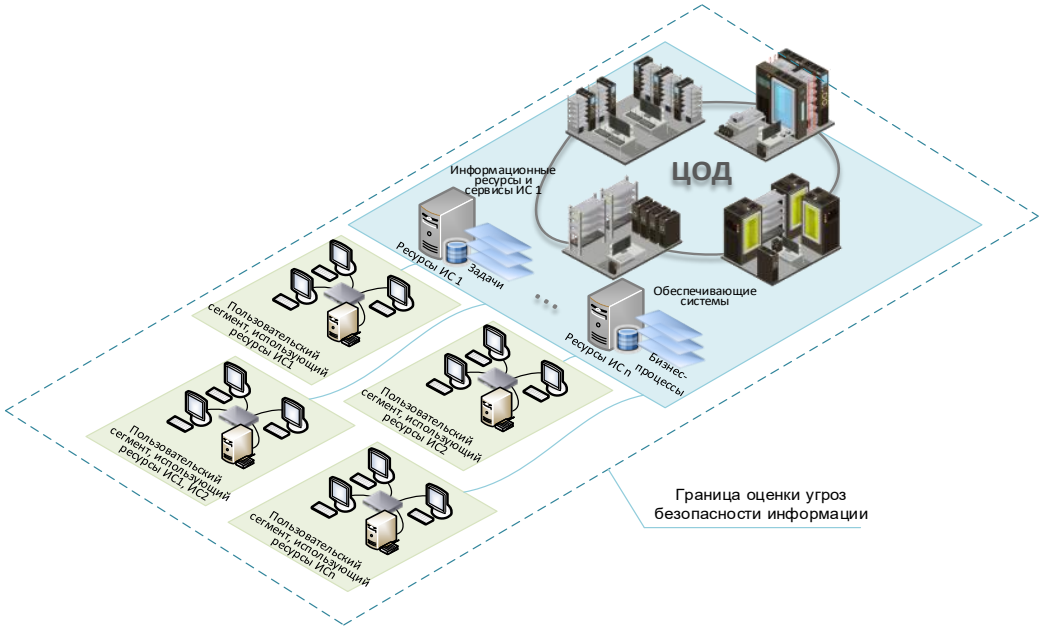
ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

Размещение на базе общей информационно-телекоммуникационной инфраструктуры ЦОД по разным моделям размещения ИС города Москвы:

ИС органов исполнительной власти города Москвы и подведомственных им организаций, в том числе ИС, обеспечивающих предоставление государственных и муниципальных услуг

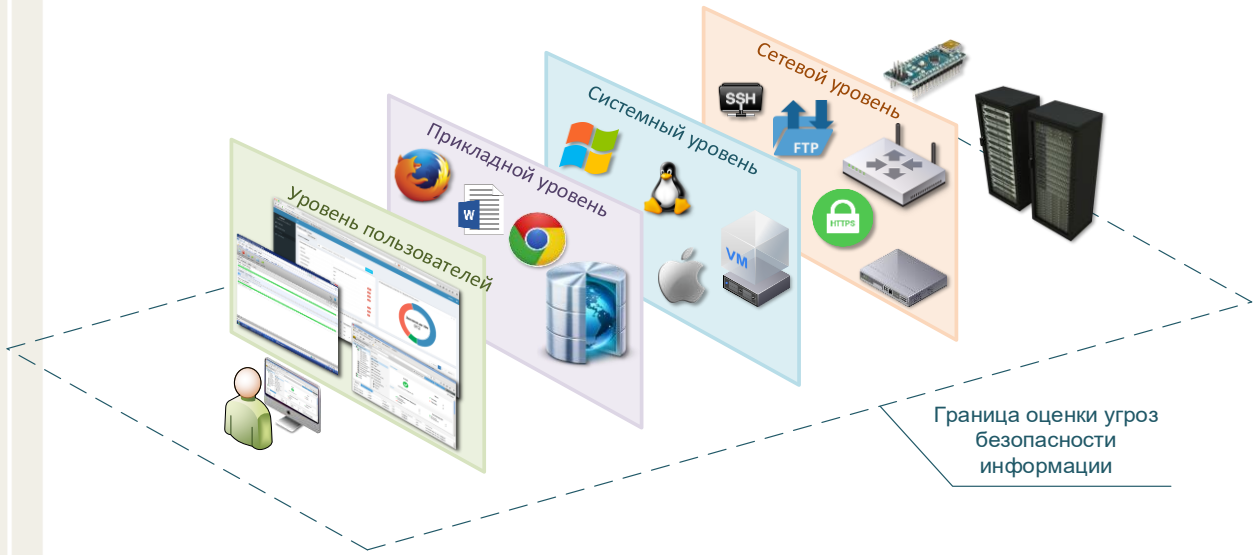
Единый оператор ЦОД

ВИ ЦОД аттестована для возможности размещения на ее базе ГИС до класса защищенности К1 включительно



Оценка угроз при размещении ГИС в ВИ ЦОД

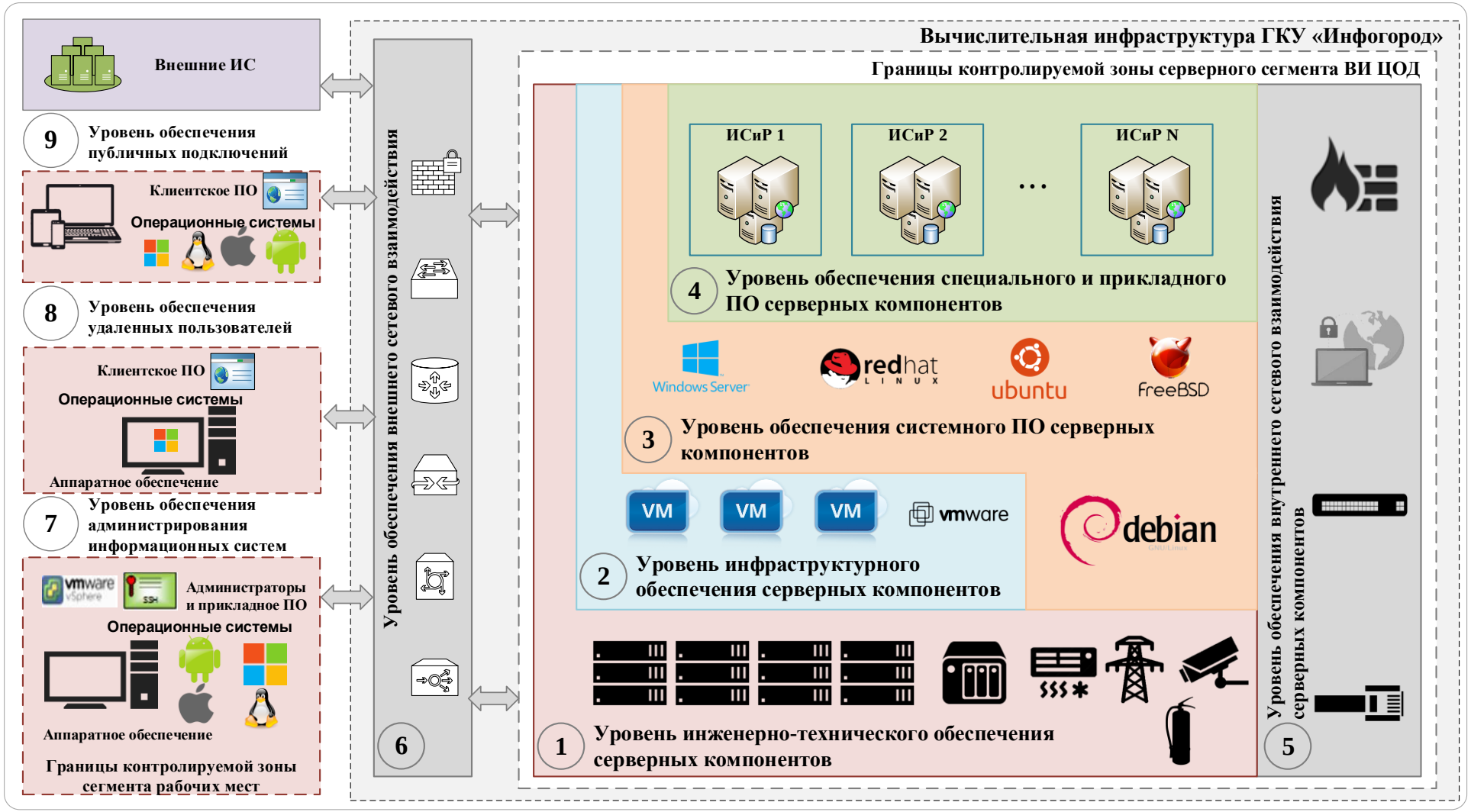
ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ



Дополнительно

- сетевой уровень декомпозируется:
  - сетевой внутренний
  - сетевой внешний
- системный уровень декомпозируется:
  - уровень инфраструктурного обеспечения
  - уровень системного ПО серверных компонент (гостевых ОС);
- уровень пользователей декомпозируется:
  - уровень обеспечения рабочих мест администраторов
  - уровень удаленных подключений (функциональных пользователей)
  - уровень обеспечения публичных подключений (публичных пользователей, граждан)

Технологические (архитектурные) уровни



Угрозы безопасности информации, декомпозированные по технологическим (архитектурным) уровням

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

УБИ	Наименование УБИ	Технологические (архитектурные) уровни								
		1	2	3	4	5	6	7	8	9
ДОП.001	Угрозы, связанные с наличием недекларированных возможностей в системном ПО	-	-	+	-	-	-	+	+	+
ДОП.002	Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО	-	-	-	+	-	-	+	+	+
ДОП.003	Угрозы утечки информации по каналу ПЭМИН	+	-	-	-	+	+	+	+	+
ДОП.004	Природные угрозы	+	-	-	-	-	-	+	+	+
…	…	…	…	…	…	…	…	…	…	…
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	+	+	-	-	-	-	-	-	-
УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	-	-	-	-	+	+	-	-	-
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации	-	-	+	+	-	-	+	+	+
УБИ.004	Угроза аппаратного сброса пароля BIOS	+	-	-	-	+	+	+	+	+

Способы реализации мер защиты для технологических (архитектурных) уровней

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

Наименование технологического (архитектурного) уровня	Модель (способ) размещения серверных компонент ИС		
	Colocation	IaaS	PaaS
	Способы реализации мер защиты для технологического (архитектурного) уровня		
1 – Уровень инженерно-технического обеспечения серверных компонент	СЗИ ВИ ЦОД / Система защиты информации ГИС	СЗИ ВИ ЦОД	
2 – Уровень инфраструктурного обеспечения серверных компонент	Система защиты информации ГИС	СЗИ ВИ ЦОД	
3 – Уровень обеспечения системного программного обеспечения серверных компонент	Система защиты информации ГИС		СЗИ ВИ ЦОД
4 – Уровень обеспечения специального и прикладного программного обеспечения серверных компонент	Система защиты информации ГИС		
5 – Уровень обеспечения внутреннего сетевого взаимодействия серверных компонент	СЗИ ВИ ЦОД / Система защиты информации ГИС	СЗИ ВИ ЦОД	
6 – Уровень обеспечения внешнего сетевого взаимодействия		СЗИ ВИ ЦОД	
7 – Уровень обеспечения администрирования информационных систем	Система защиты информации ГИС	СЗИ ВИ ЦОД	
8 – Уровень удаленных подключений	Система защиты информации ГИС		
9 – Уровень обеспечения публичных подключений	Система защиты информации ГИС		

Особенности мероприятий по защите информации

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

Наименование мероприятия	Отчетные документы
1. Формирование требований к защите информации	• … • **Акт определения области проведения аттестации** • **Аналитическое обоснование необходимости создания СЗИ ГИС** • Модель угроз безопасности информации • Акт классификации • Частное техническое задание на создание СЗИ
2. Разработка СЗИ	• … • Проектная и эксплуатационная документация на СЗИ • Организационно-распорядительные документы по защите информации
3. Сертификация ППО по требованиям безопасности информации	• … • **Сертифицированное прикладное программное обеспечение** • Сертификат соответствия в системе сертификации средств защиты информации ФСТЭК России • Технические условия • Формуляр
4. Внедрение СЗИ	• … • Результаты анализа уязвимостей • Материалы предварительных испытаний, опытной эксплуатации и приемочных испытаний СЗИ
5. Аттестация по требованиям защиты информации	• … • Аттестат соответствия требованиям по защите информации (с учетом аттестата ВИ ЦОД)

Дополнительные мероприятия

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

- Углубленный анализ защищенности (тестирование на проникновение) с привлечением нескольких команд Red Team
- Анализ исходного кода
- Анализ защищенности системы со стороны общественности и специалистов / хакатон / программы Bug Bounty
- Киберучения

ДЕПАРТАМЕНТ
ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
ГОРОДА МОСКВЫ

Всегда на связи!