



**КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ**

04 октября 2018 г.  
г. Красноярск

**#CODEIB  
#RESHETNEV**

# ЗАПИСКИ НА МАНЖЕТАХ БЕЗОПАСНИКА



**АО «ИСС»**

Роман Лебедев  
УИВТ, сектор защиты информации

**ТЕЛЕФОН:** +7 (3919) 73-29-05

**EMAIL:** [rl@iss-reshetnev.ru](mailto:rl@iss-reshetnev.ru)

# Анонс доклада

ЧАСТЬ 1:  
Защищенная виртуализация

ЧАСТЬ 2:  
Антивирус в корпоративной сети

# Объекты внимания

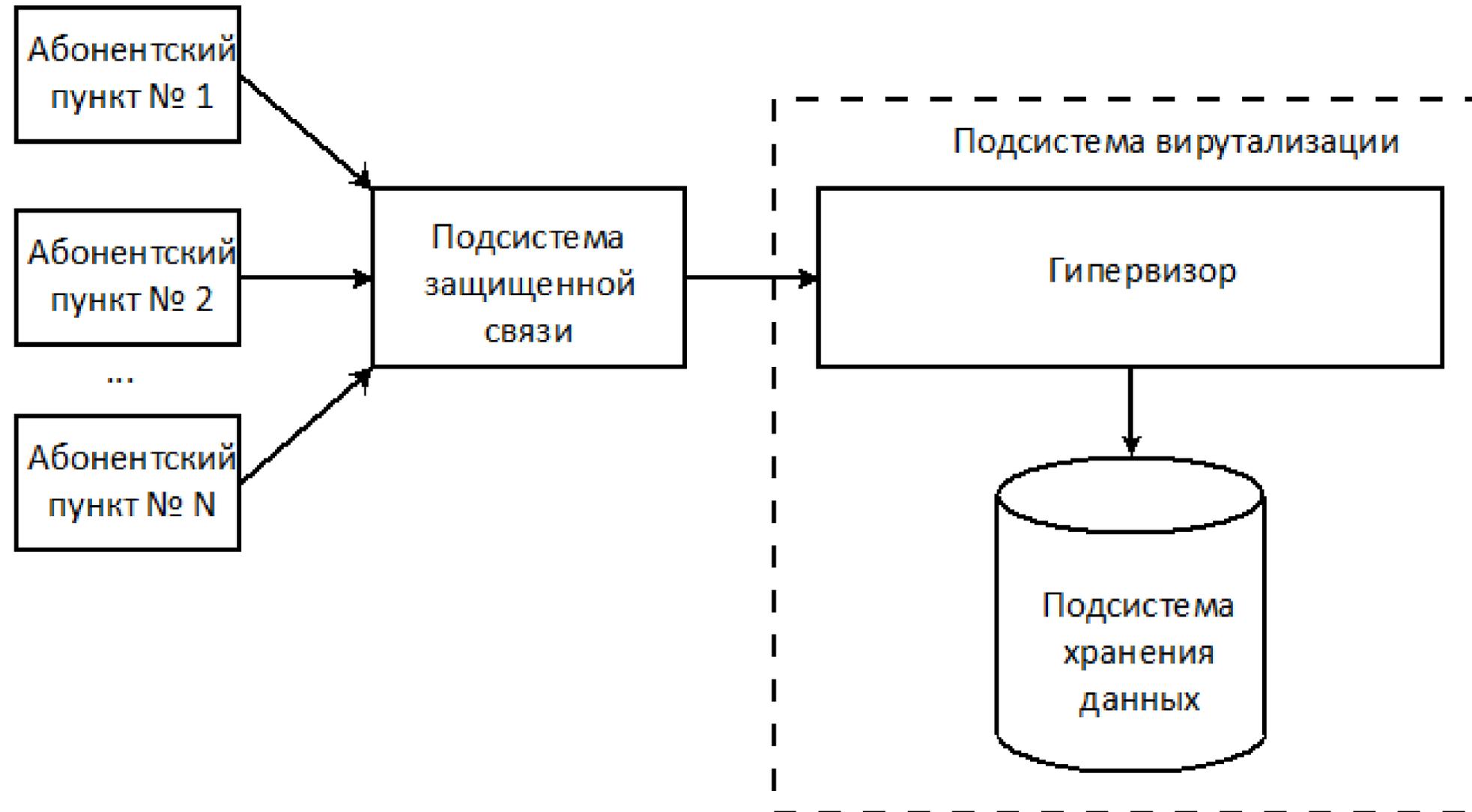
Ведомственные ГИС

Отраслевые ИС

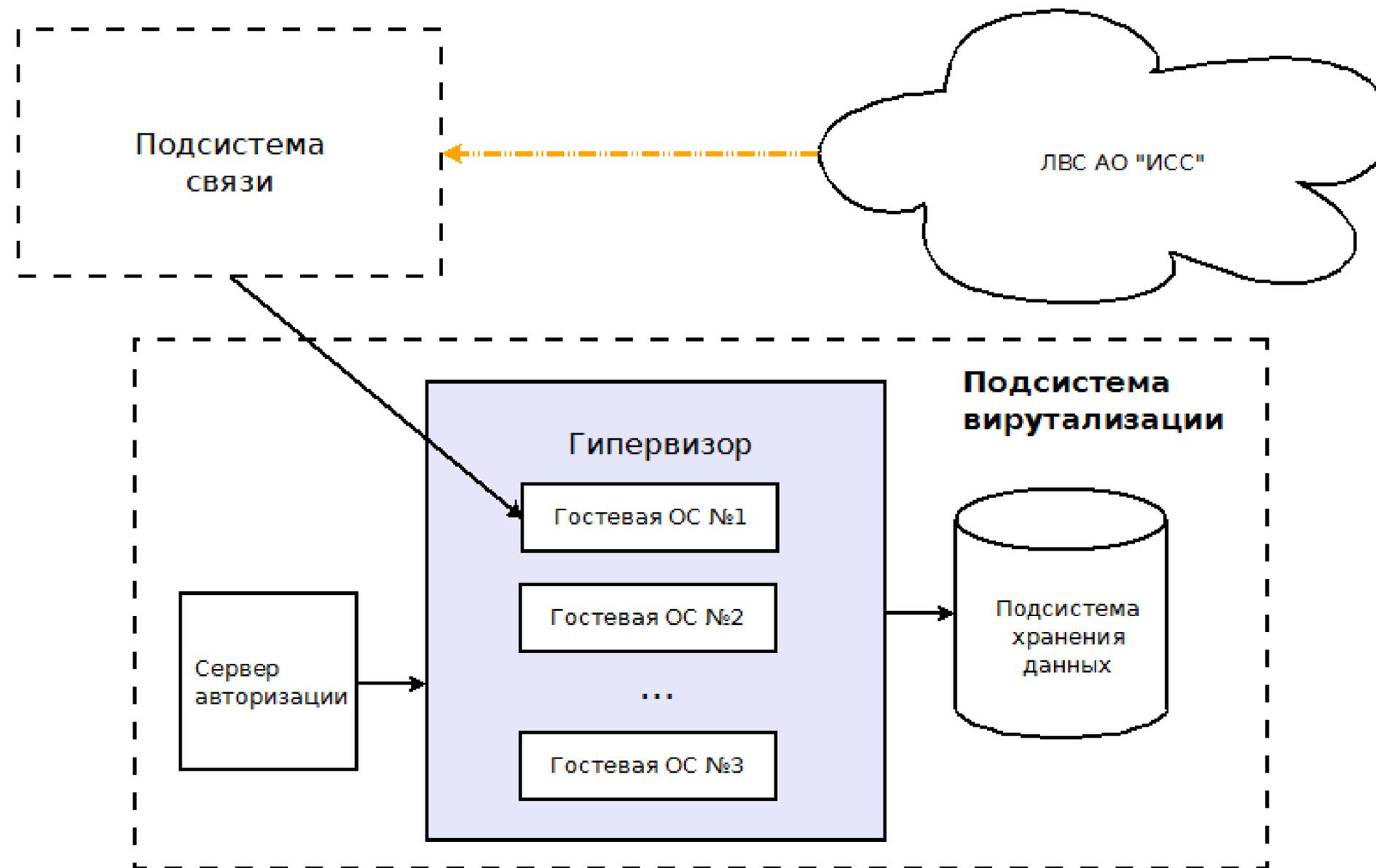
Системы ДБО

АРМ ДСП

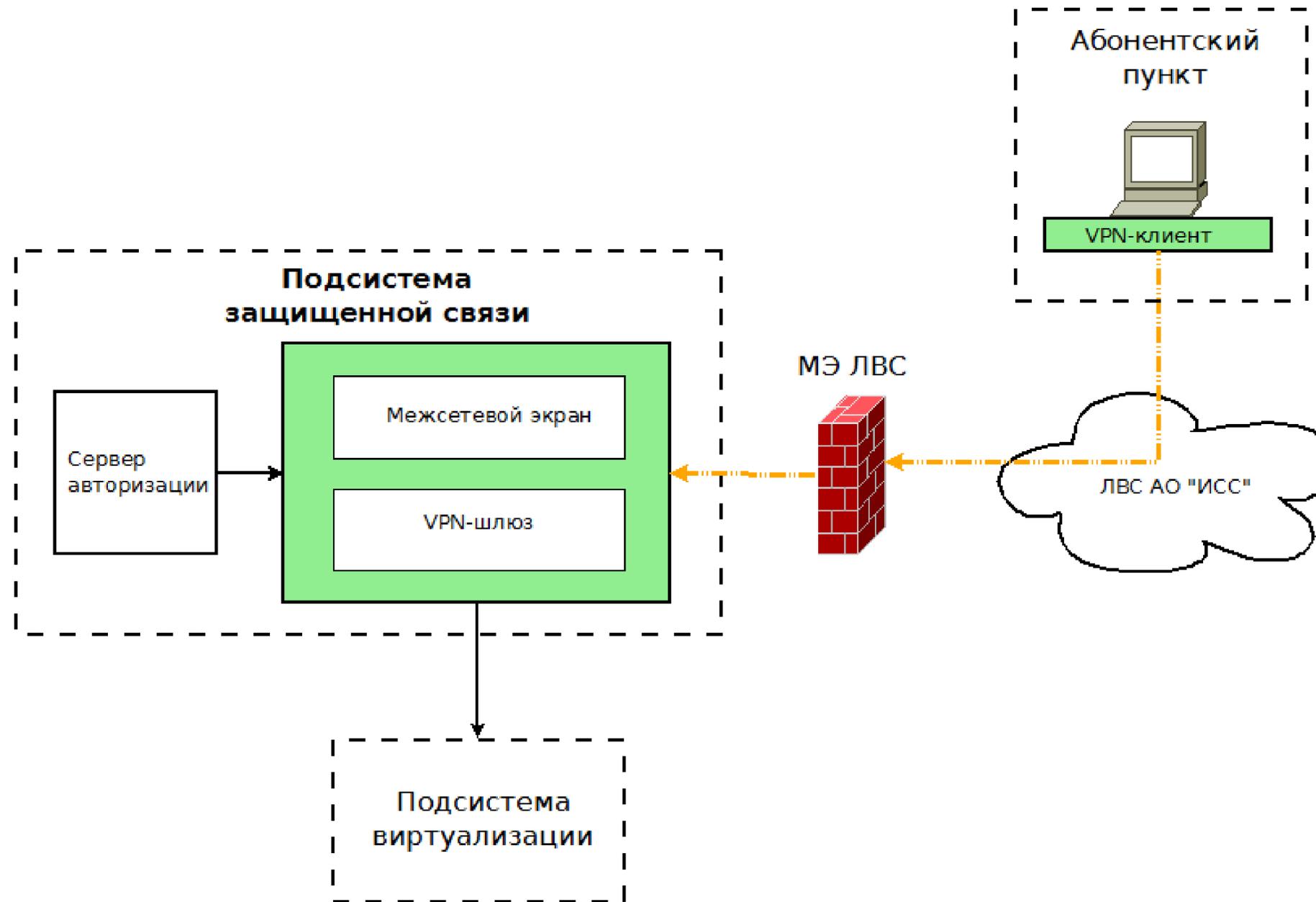
# Виртуализация ДСП!



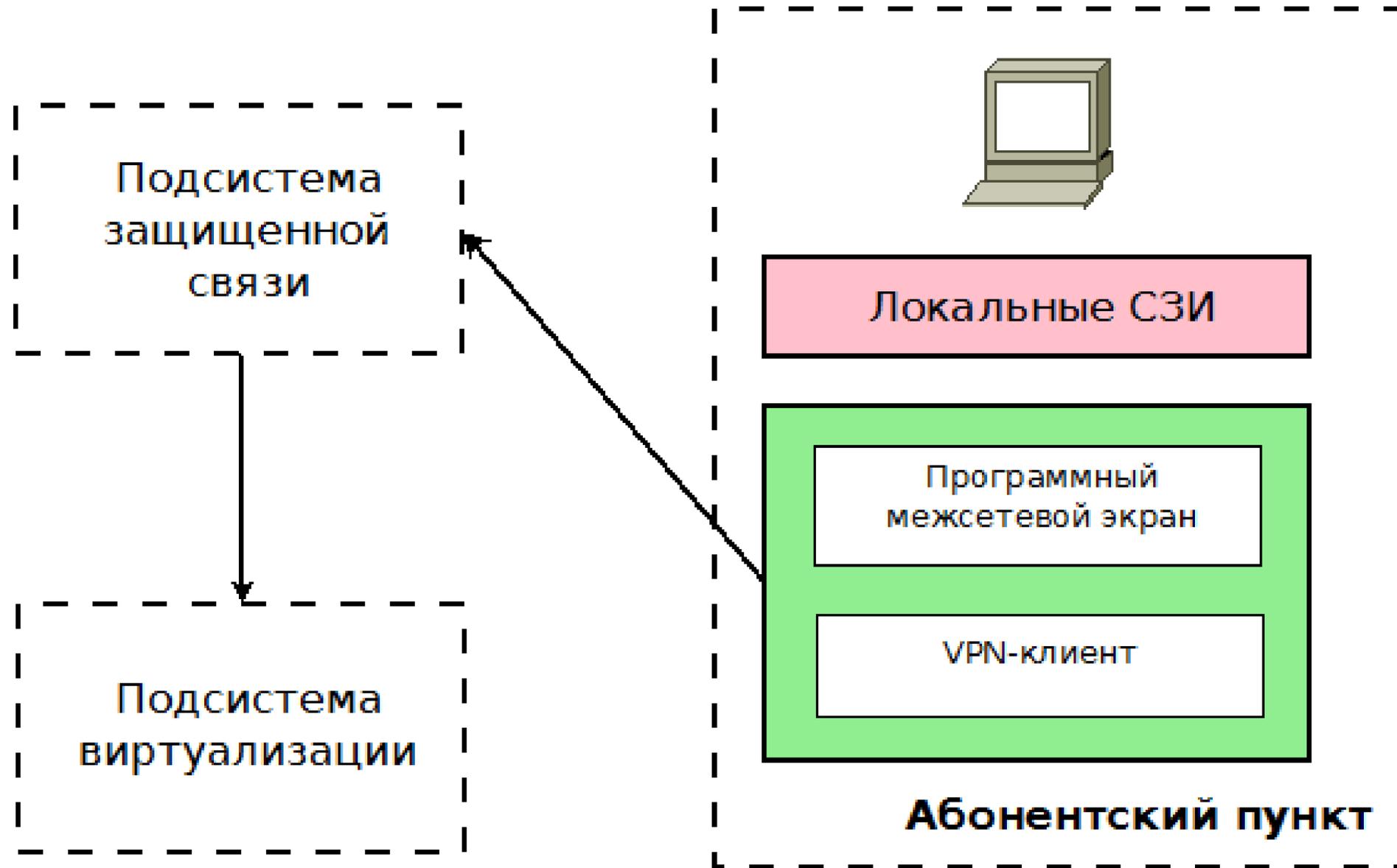
# Подсистема виртуализации



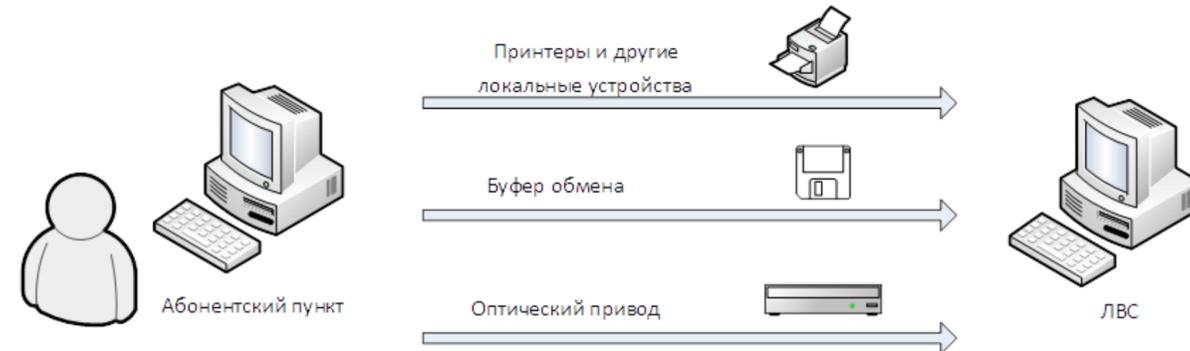
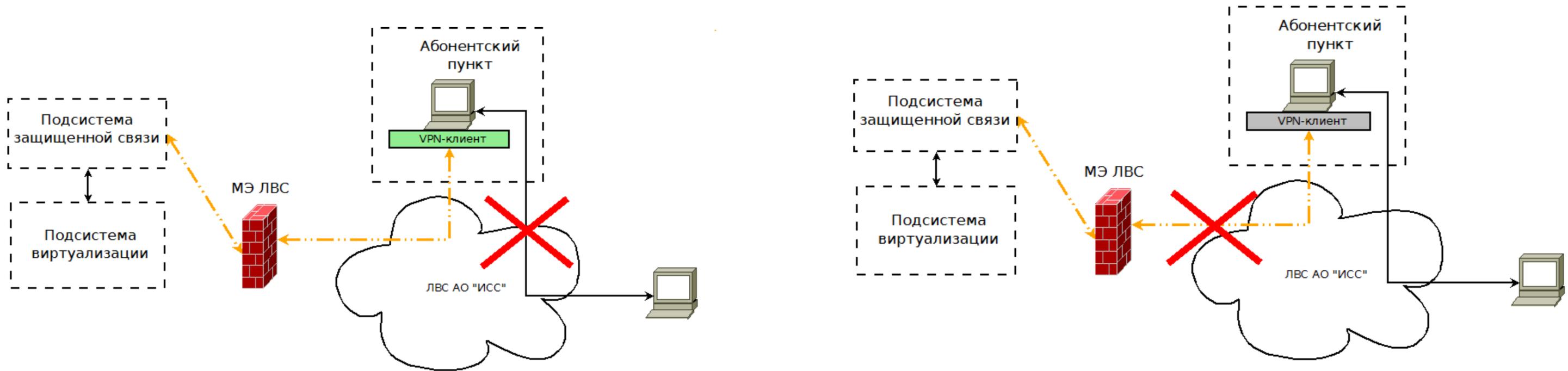
# Подсистема связи



# Абонентские пункты



# Режимы работы АП



# Решение ФСТЭК



ФСТЭК РОССИИ

УПРАВЛЕНИЕ  
ФЕДЕРАЛЬНОЙ СЛУЖБЫ  
ПО ТЕХНИЧЕСКОМУ  
И ЭКСПОРТНОМУ КОНТРОЛЮ  
ПО СИБИРСКОМУ ФЕДЕРАЛЬНОМУ  
ОКРУГУ

Красный проспект, д. 41, г. Новосибирск, 630091  
тел./ факс: (383) 203-54-07  
E-mail: sfo@fstec.ru  
ОКПО 56009786, ОГРН 1025401918761  
ИНН/КПП 5405213849/540601001

ИД № 13.98

На № 160-4/183 деп от 22.09.2016

О рассмотрении концепции

Уважаемый Николай Алексеевич!

Направленная в наш адрес концепция автоматизированной системы обработки информации с пометкой «ДСП» с технологией терминального доступа Управлением ФСТЭК России по Сибирскому федеральному округу рассмотрена.

Считаю возможным реализацию данного проекта с учетом следующего.

В указанной автоматизированной системе предполагается обработка информации ограниченного доступа и в соответствии с «Положением о государственной системе защиты в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» такая информация должна обрабатываться с использованием технических и программных средств защиты, сертифицированных в установленном порядке, а также должна проводиться аттестация на предмет соответствия требуемому уровню безопасности информации.

19.12.16  
Генеральному директору  
АО «Информационные спутниковые  
системы»  
имени академика М.Ф.Решетнёва»

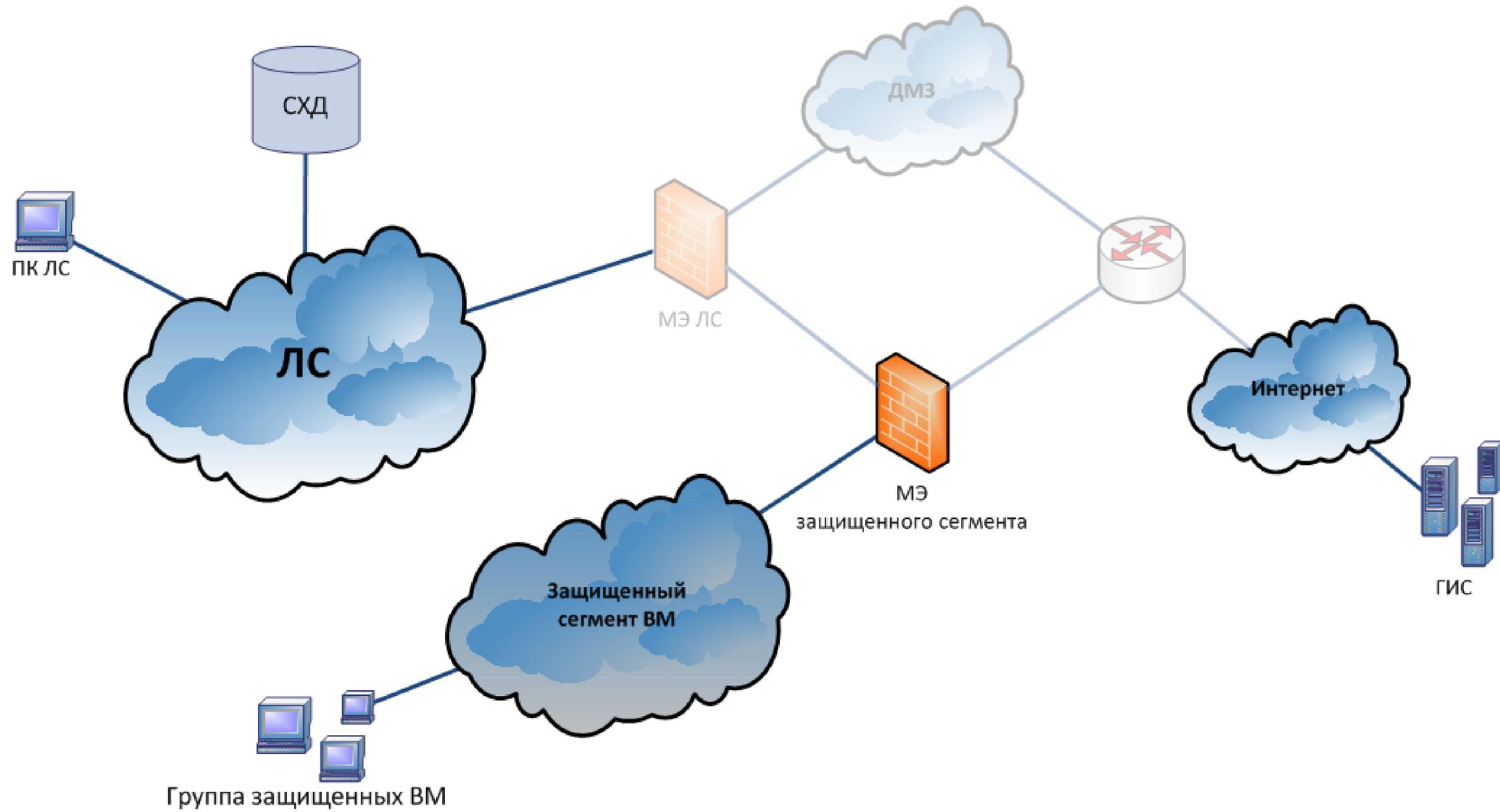
Н.А.ТЕСТОЕДОВУ

ул. Ленина, д. 52, г. Железногорск,  
Красноярский край, 662972

Рогов Г.А.

20.12.16

# На сегодняшний день



# Планы на будущее

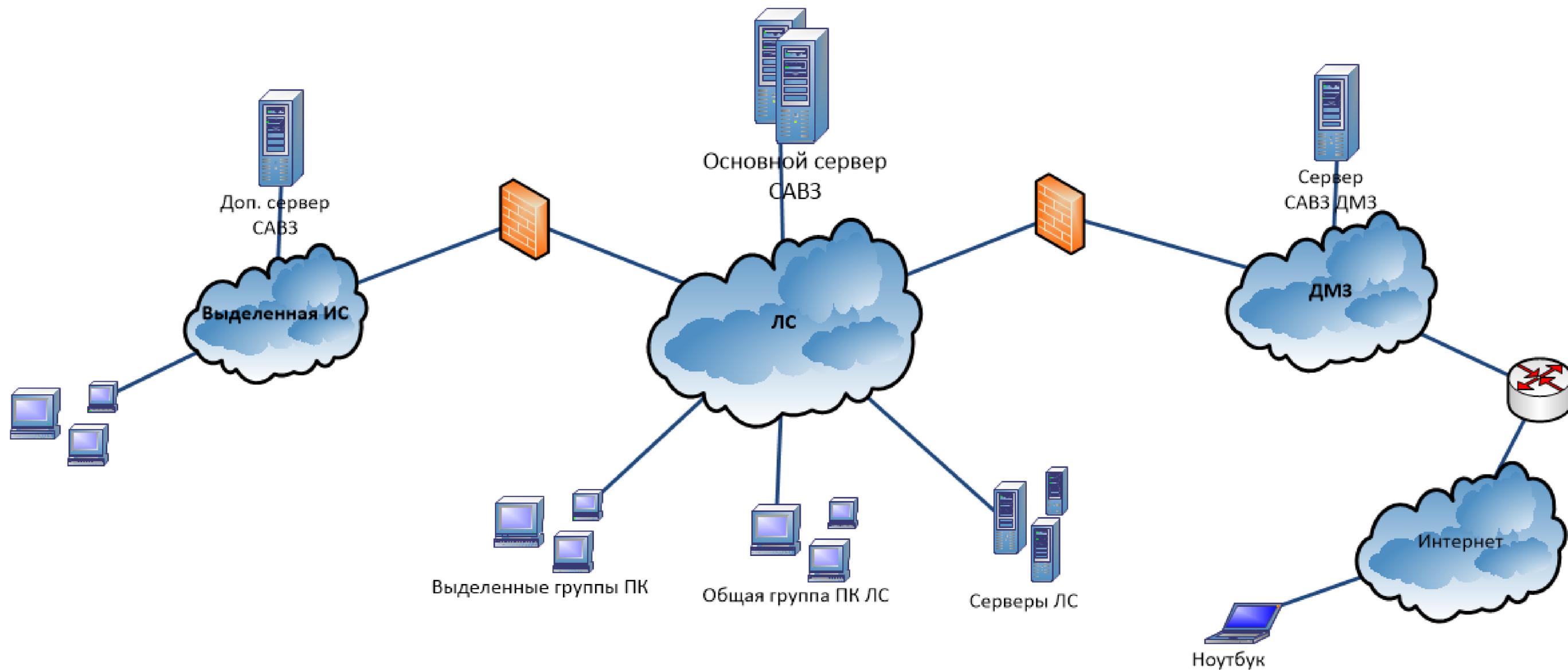
- 1 Отработка СЗИ виртуализации на стенде
- 2 Аттестация по СТР-К (пр. 17)
- 3 Проработка концепции виртуализации ГТ

# Корпоративный антивирус

МНОГО КЛИЕНТОВ  
> 5000

РАЗНЫЕ ВЕНДОРЫ  
≥ 2

УСЛОВИЯ ИСПОЛЬЗОВАНИЯ  
10 типовых сборок

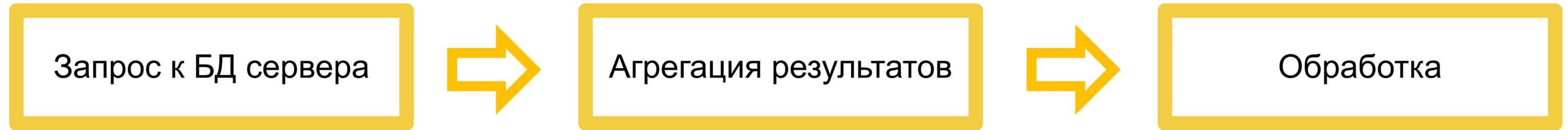


# Требования к антивирусу

1 АНТИВИРУС ДОЛЖЕН РАБОТАТЬ

2 БАЗЫ ДОЛЖНЫ ОБНОВЛЯТЬСЯ

# Мониторинг



Полная идентификация клиента антивируса

Обнаружение коллизий

Интеграция с системами управления ИБ

# Типизация политик

Определяющий фактор – полномочия пользователя

- Только наблюдение
- Изменение режима работы
- Изменение объектов защиты
- Отключение (удаление) модулей



**СПАСИБО ЗА  
ВНИМАНИЕ!**



**#КОТИБ**