

Особенности аттестации распределённых информационных систем

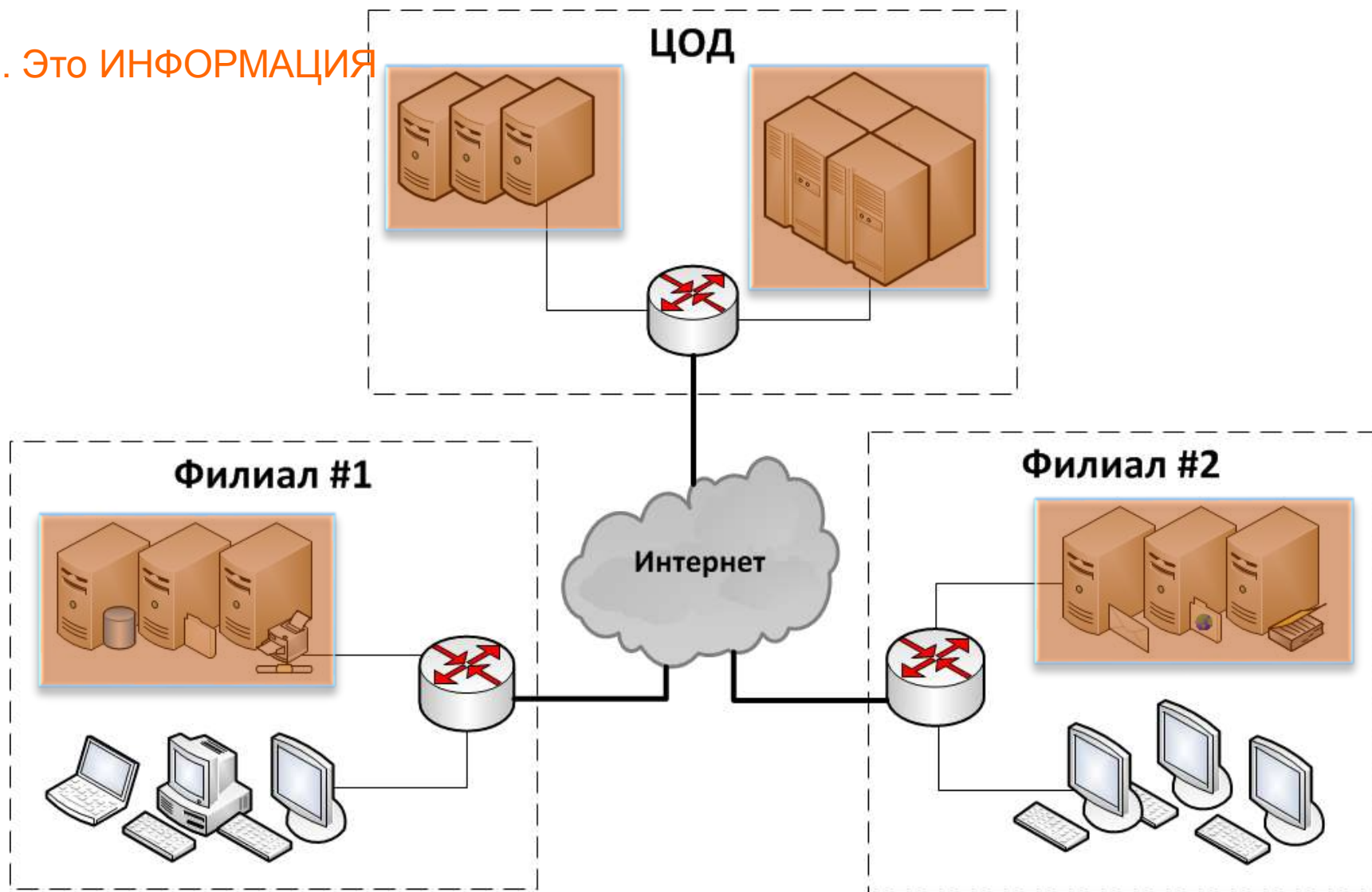
*Заместитель директора по развитию
группы компаний **SaveIT Group**
Яненко Михаил Романович*

Распределённая информационная система

ЧТО ЭТО?

2

1. Это ИНФОРМАЦИЯ



Распределённая информационная система

ЧТО ЭТО?

3

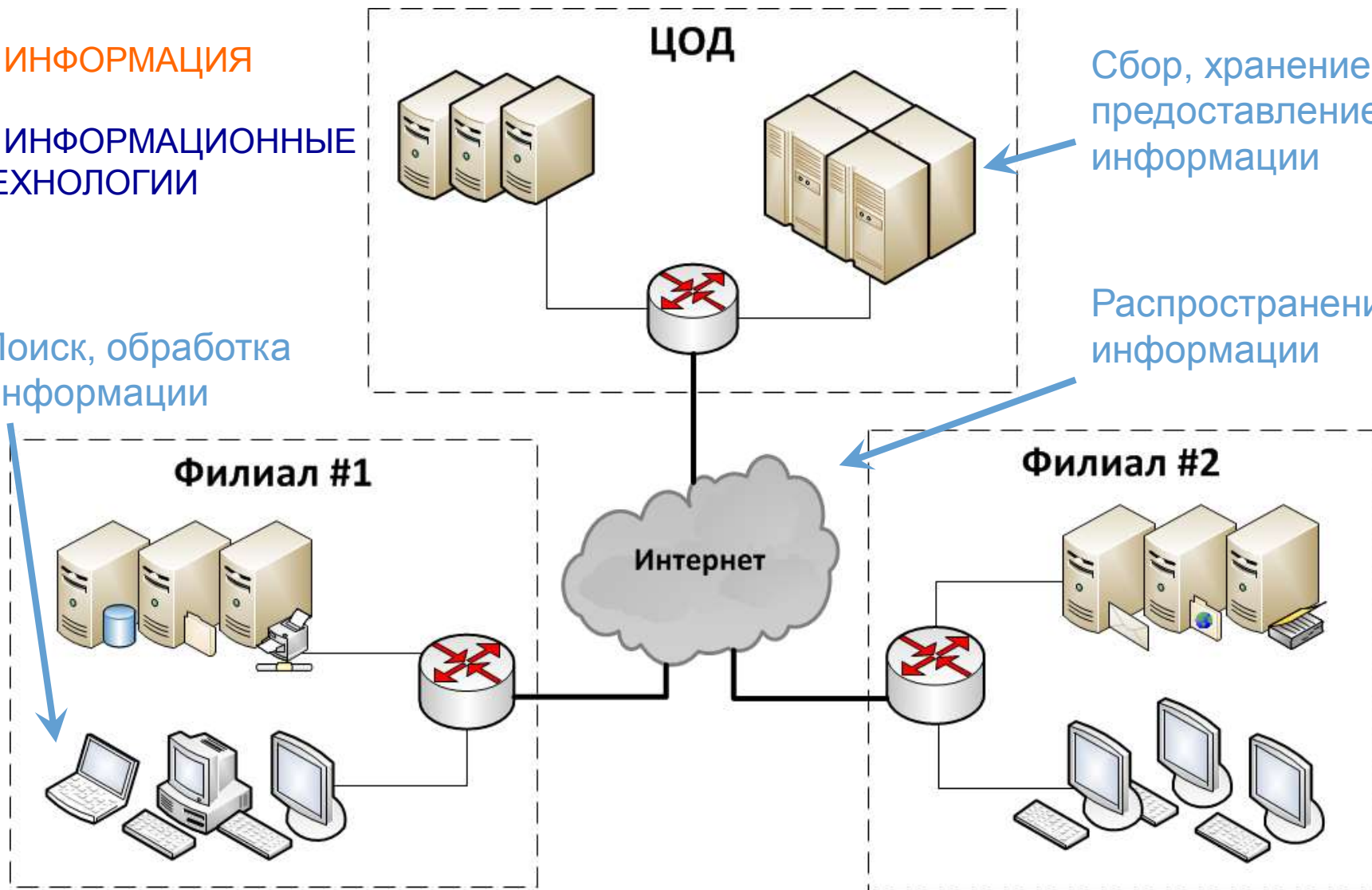
1. ИНФОРМАЦИЯ

2. ИНФОРМАЦИОННЫЕ
ТЕХНОЛОГИИ

Поиск, обработка
информации

Сбор, хранение,
предоставление
информации

Распространение
информации

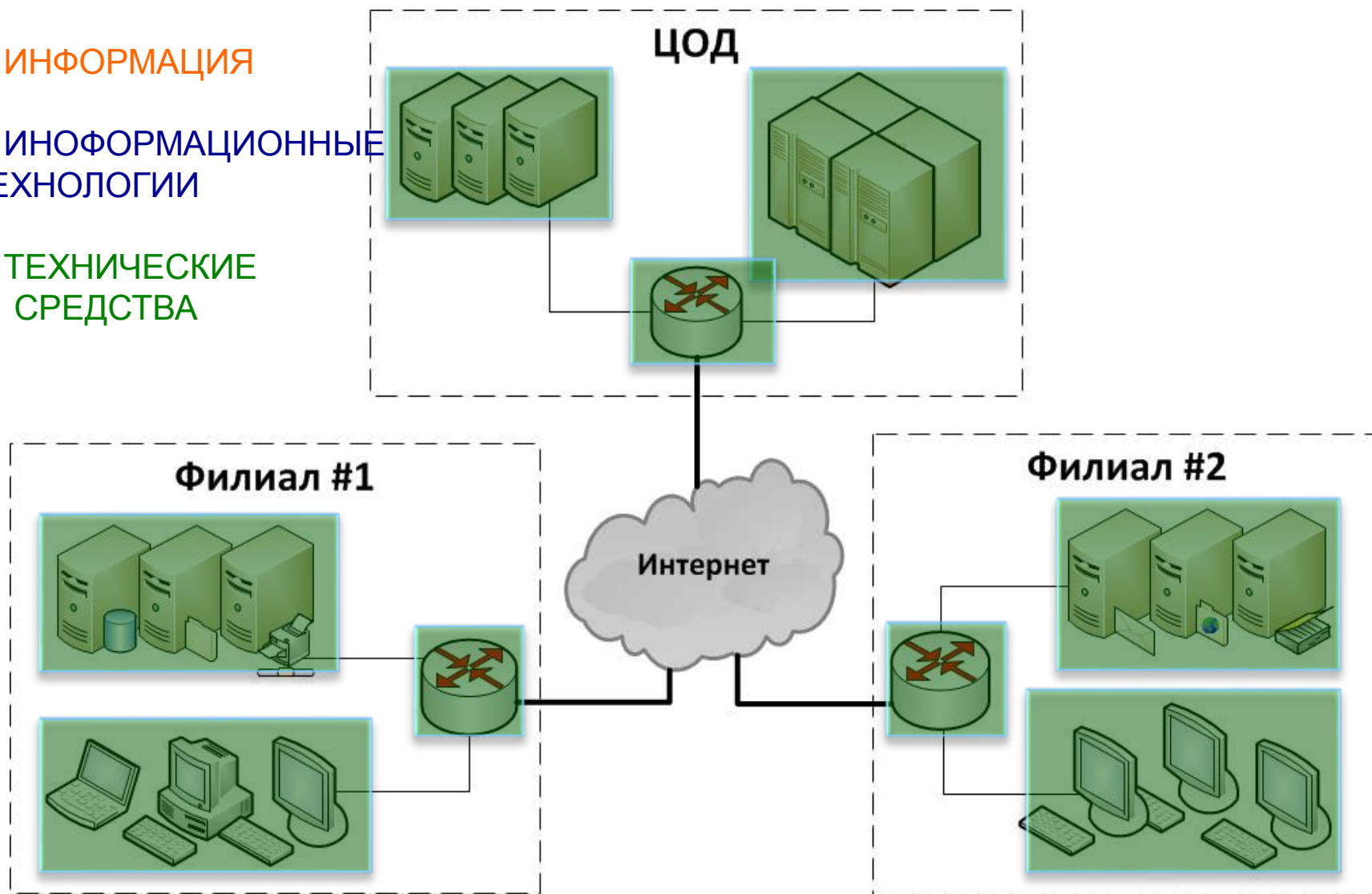


Распределённая информационная система

ЧТО ЭТО?

4

1. ИНФОРМАЦИЯ
2. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
3. ТЕХНИЧЕСКИЕ СРЕДСТВА



Распределённая информационная система

ЧТО ЭТО?

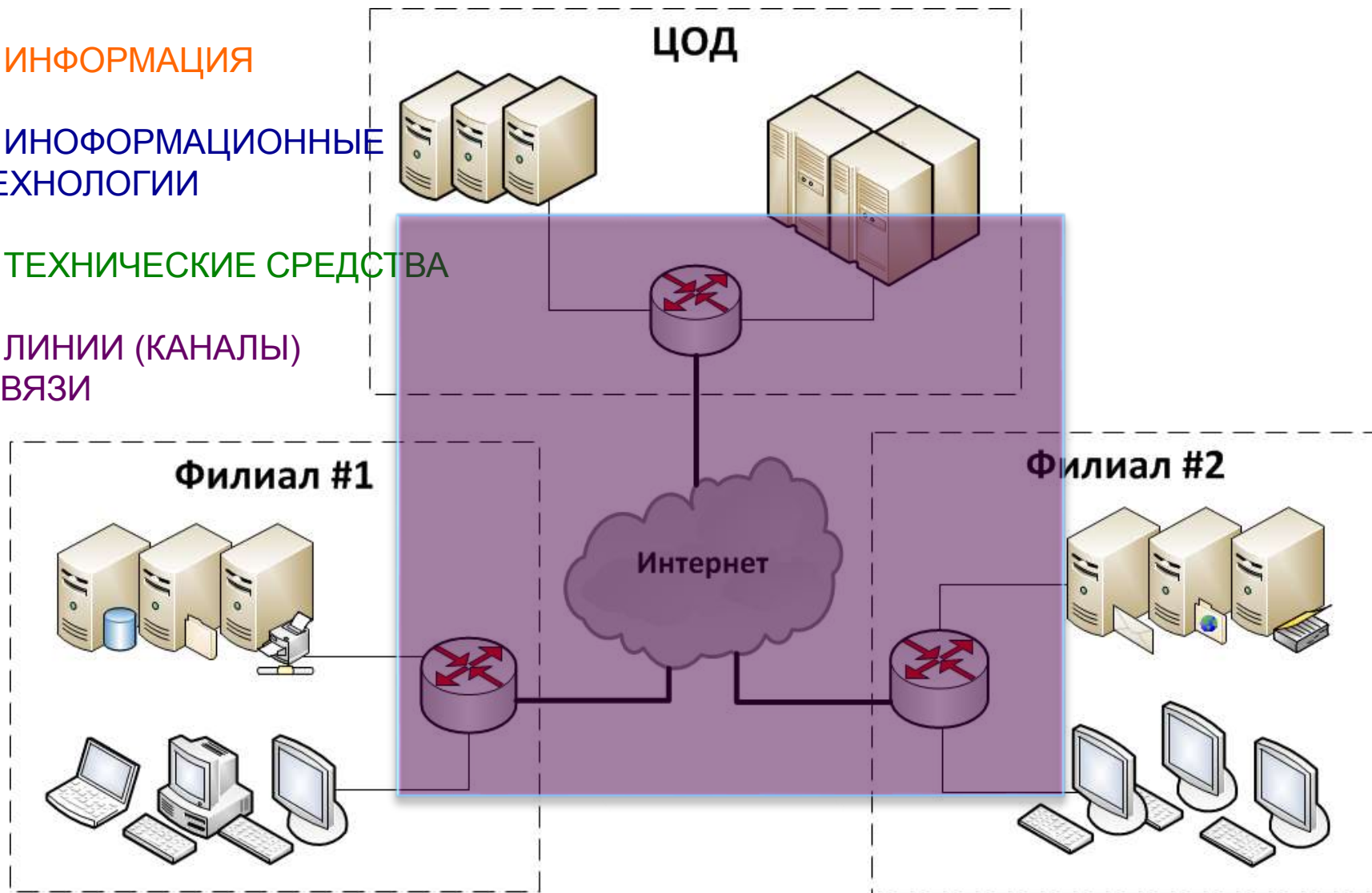
5

1. ИНФОРМАЦИЯ

2. ИНФОРМАЦИОННЫЕ
ТЕХНОЛОГИИ

3. ТЕХНИЧЕСКИЕ СРЕДСТВА

4. ЛИНИИ (КАНАЛЫ)
СВЯЗИ



Распределённая информационная система

ЗАЧЕМ ЗАЩИЩАТЬ и АТТЕСТОВЫВАТЬ?

6

Создание системы защиты информации и проведение аттестации информационной системы является обязательным, если данная система является государственной (муниципальной) информационной системой.



Распределённая информационная система 7

В СООТВЕТСТВИИ С ЧЕМ ЗАЩИЩАТЬ?

Создание СЗИ информационной системы производится в соответствии с требованиями:

Приказа № 17 ФСТЭК России.

Аттестационные испытания проводятся в соответствии с требованиями:

1. ГОСТ РО Аттестация объектов информатизации.
2. ГОСТ РО Программа и методики аттестационных испытаний.

...



А где СТР-К?

8

А где 21-ый приказ ФСТЭК России?

СТР-К:

1. Носит рекомендательный характер;
2. Применяется только в случае определения в качестве актуальных угроз безопасности информации «Угрозы связанные с утечкой информации по техническим каналам»

21-ый приказ ФСТЭК России:

Не применяется для защиты ГИС (МИС).

(приказ 17 ФСТЭК России, раздел «Общие положения», пункт 5)



Походы к аттестации распределённых информационных систем

Известны и используются **3 подхода** к аттестации
распределённых информационных систем (РИС):

Подход 1 «Фиксация системы»

Подход 2 «Сегментирование системы»

Подход 3 «Выделение перечня типовых
сегментов»

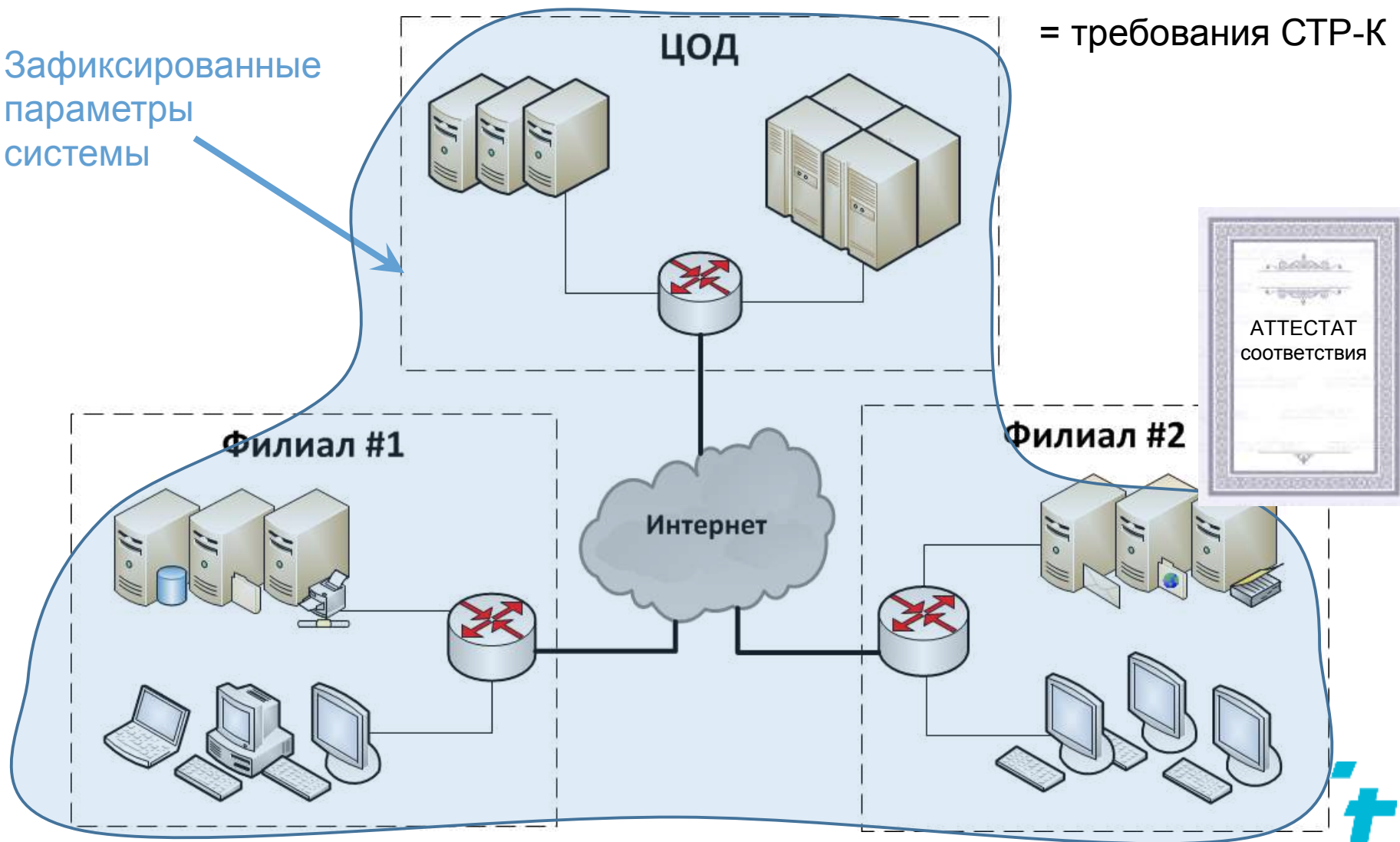


Подход #1 - Фиксация системы

10

«защищаем железо (технические средства)»

Зафиксированные
параметры
системы



«защищаем железо (технические средства)»

Зафиксированные
параметры
системы

ПЕРЕАТТЕСТАЦИЯ

Надо
заменить
сервер?

Надо изменить
технологии
распространения?

Филиал #1

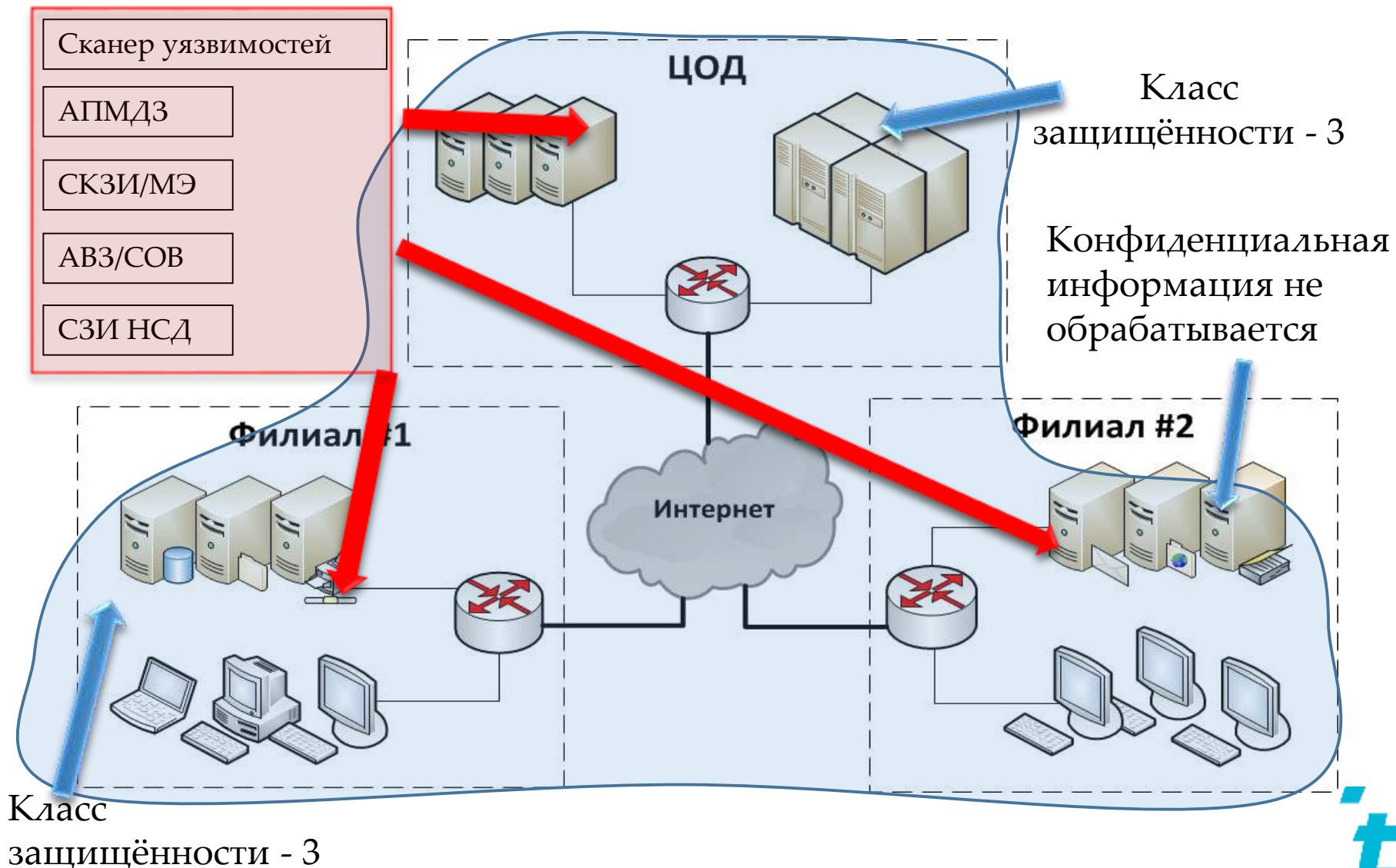
Интернет

Филиал #2

Надо
заменить АРМ?

Надо заменить
маршрутизатор

«защищаем железо (технические средства)»



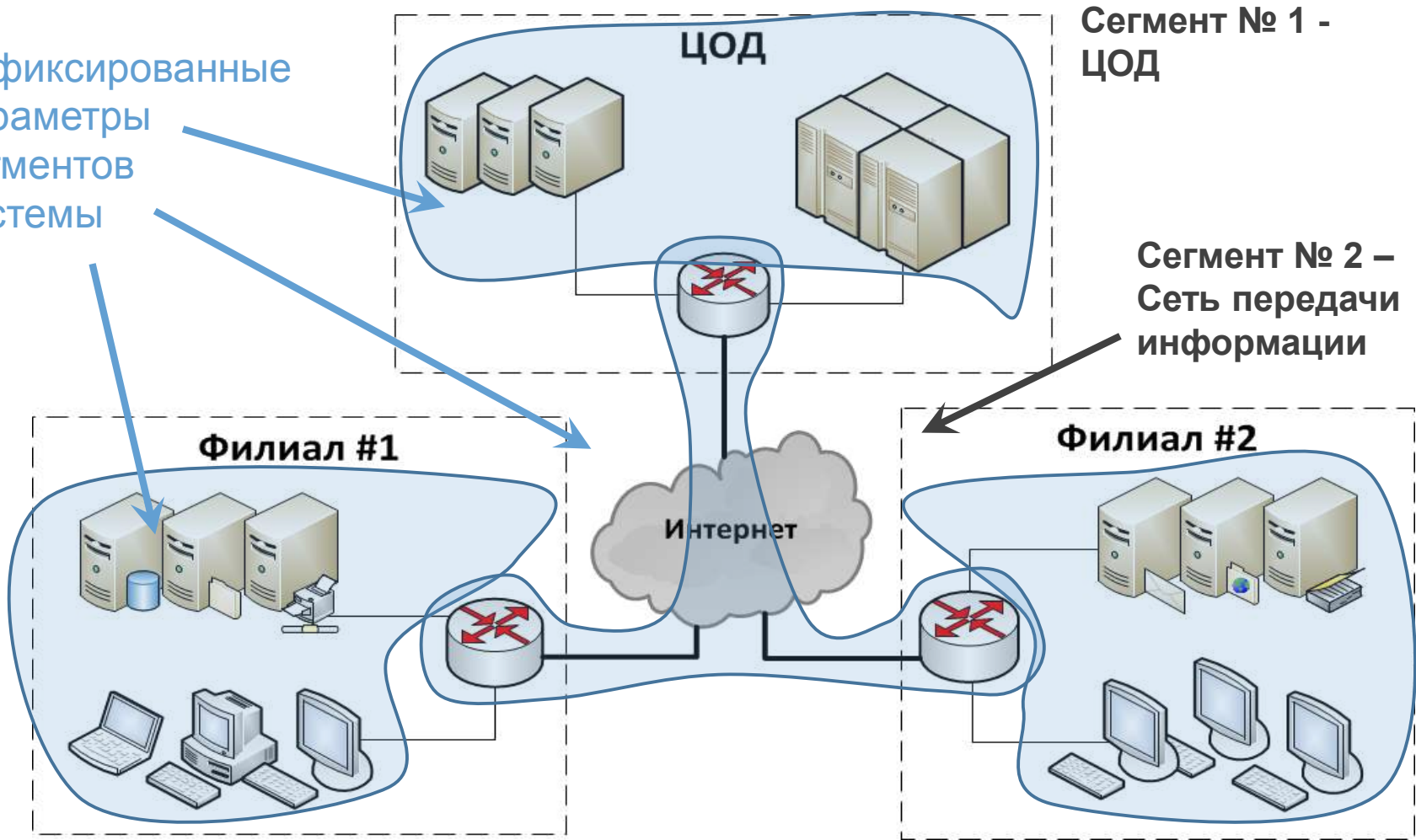
«защищаем железо (технические средства)»

USER	Компьютер	IT специалист	ИБ специалист	Оператор ИС	Лицензиат
					

Подход #2 - Сегментирование системы «защищаем здания/организации»

14

Зафиксированные
параметры
сегментов
системы



Сегмент № 3 – Подведомственная
организация

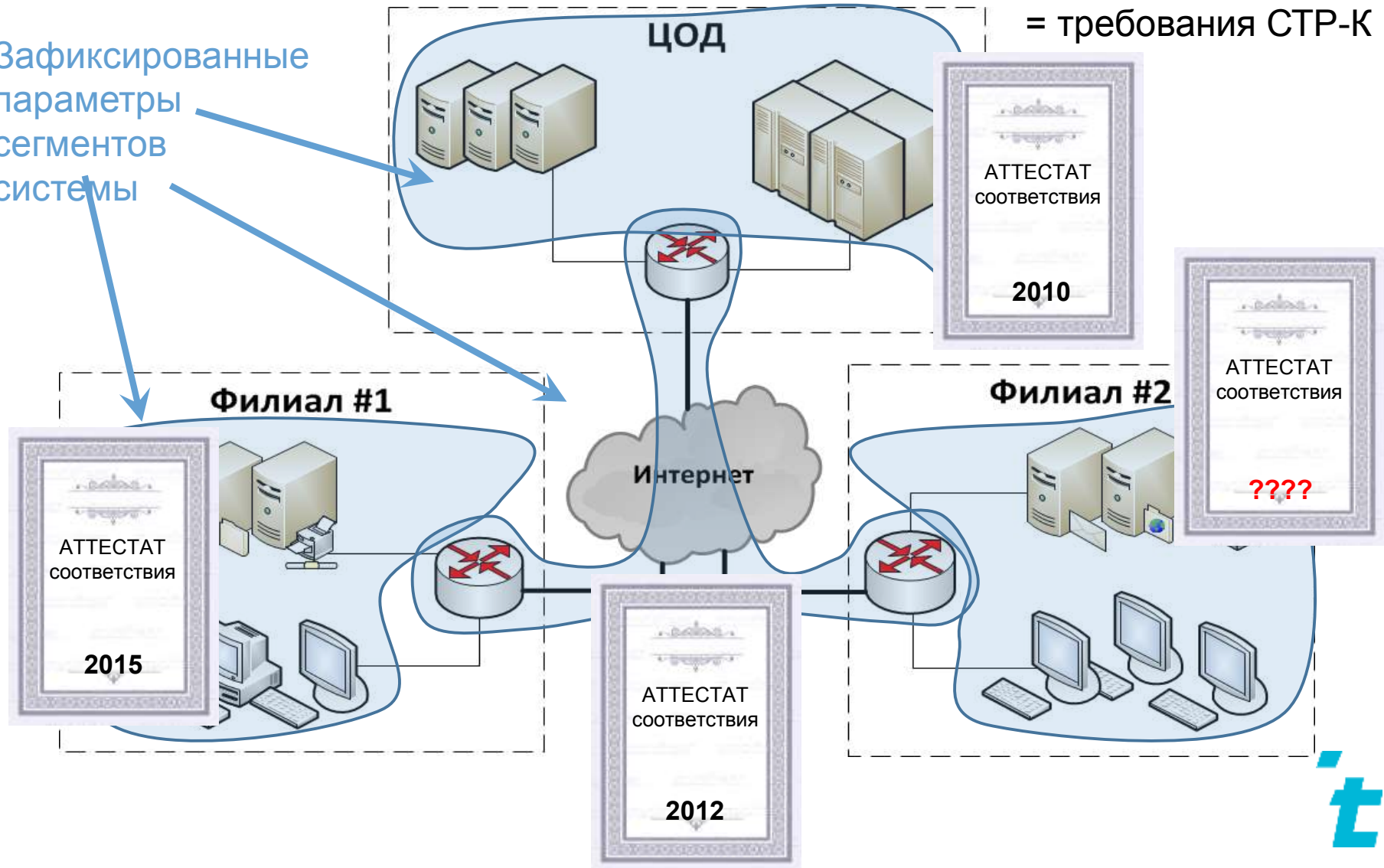
Сегмент № 4 – Филиал
организации



Подход #2 - Сегментирование системы «защищаем здания/организации»

15

Зафиксированные
параметры
сегментов
системы



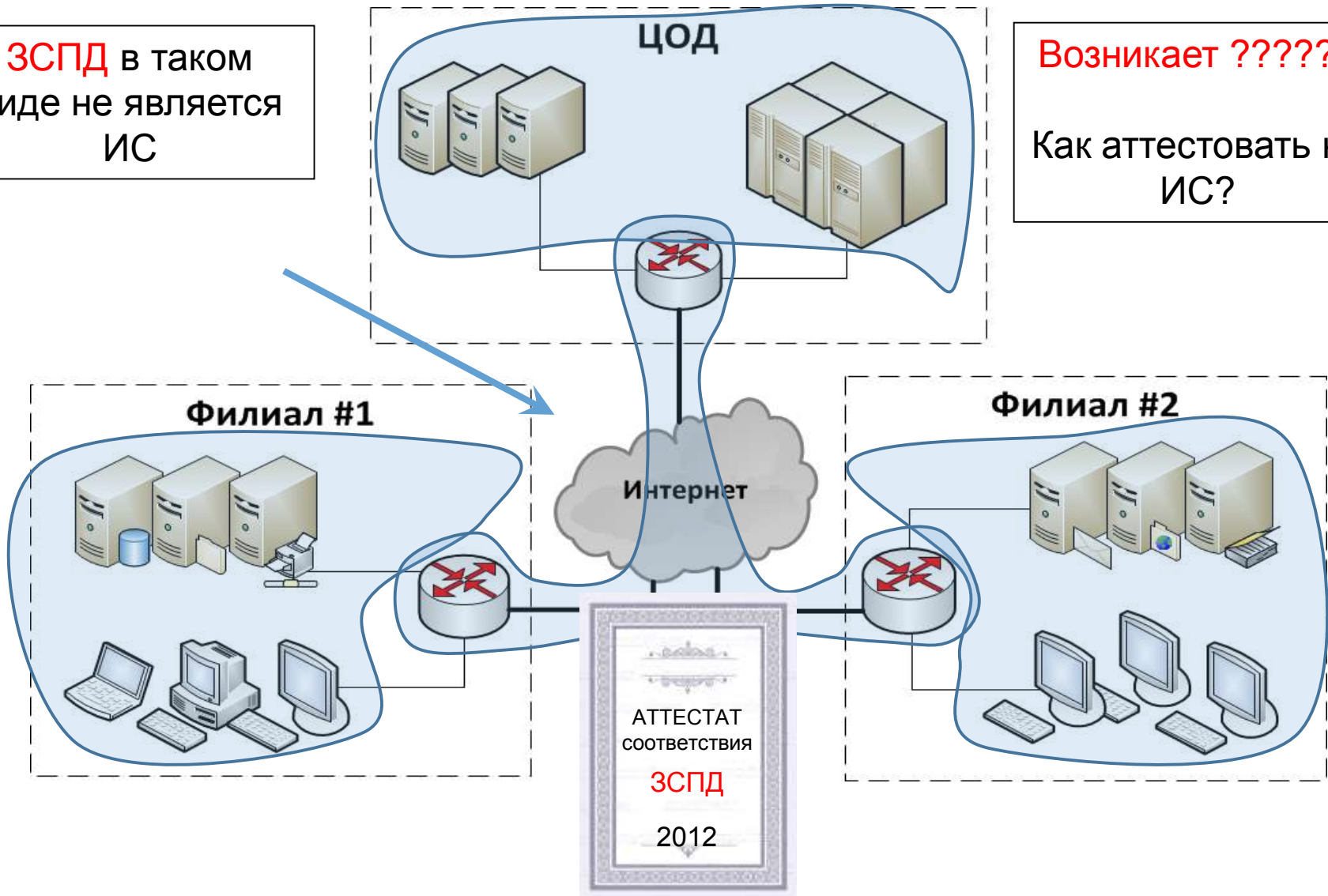
Подход #2 - Сегментирование системы «защищаем здания/организации»

16

ЗСПД в таком
виде не является
ИС

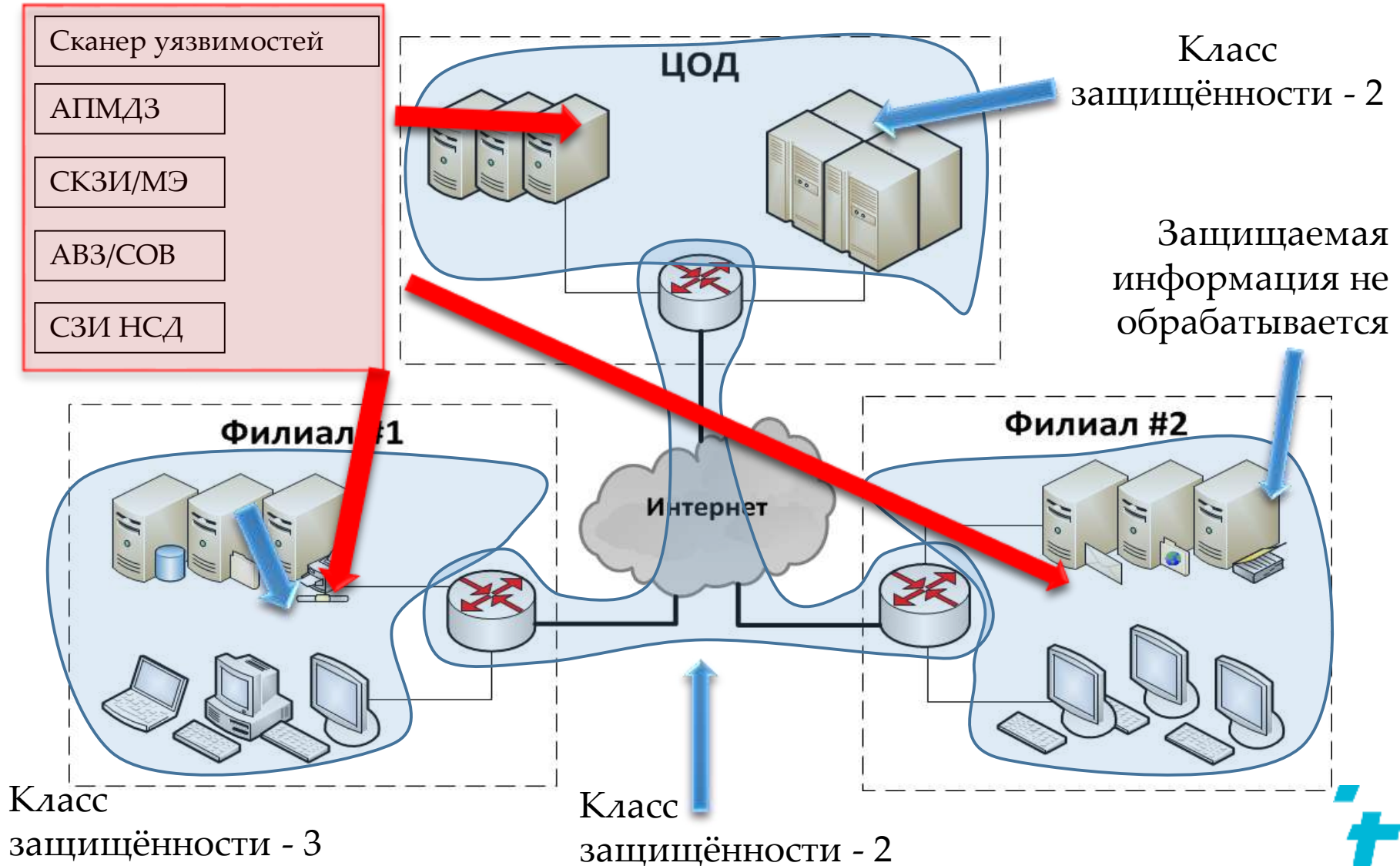
Возникает ??????

Как аттестовать не
ИС?



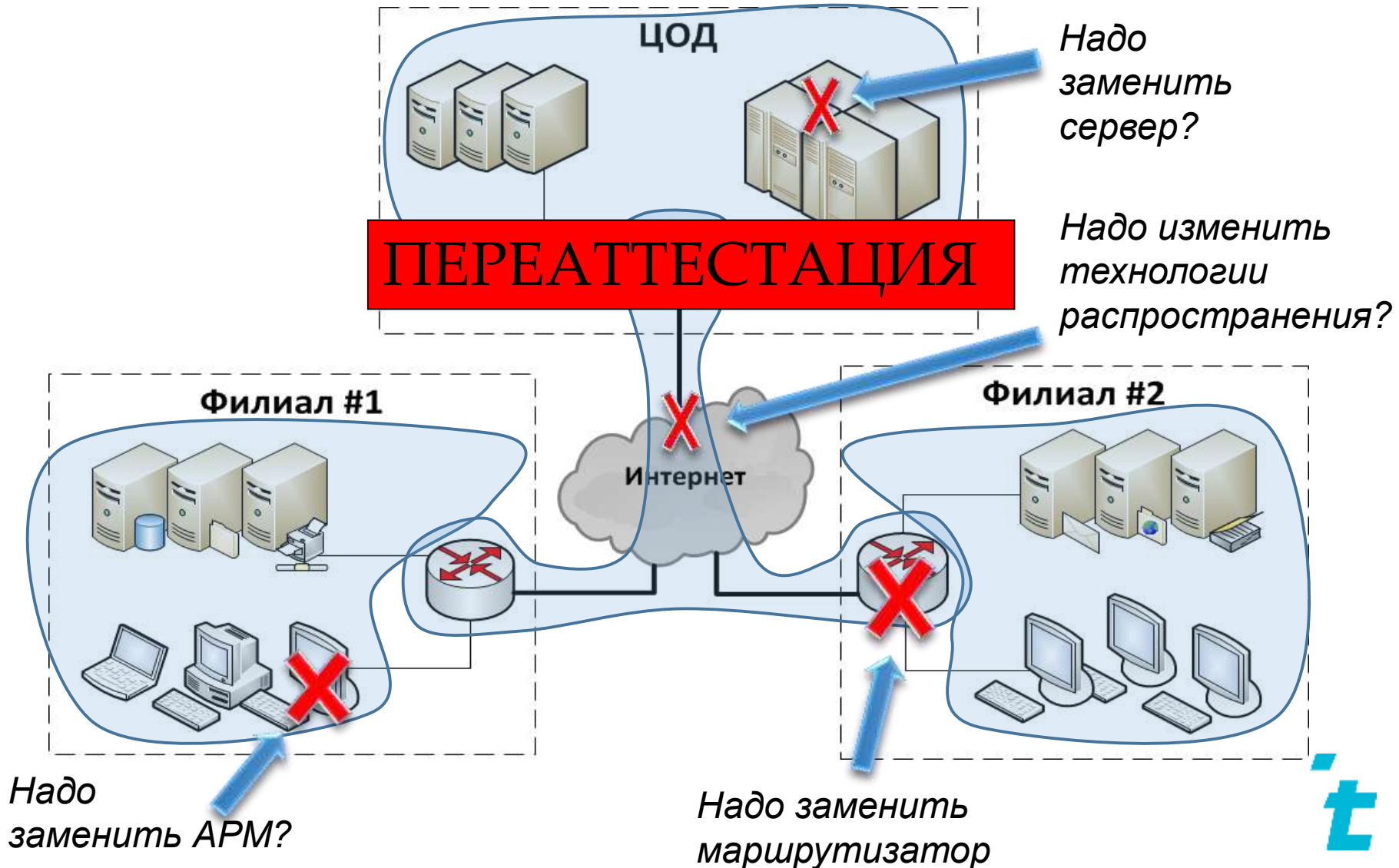
Подход #2 - Сегментирование системы «защищаем здания/организации»

17



Подход #2 - Сегментирование системы «защищаем здания/организации»

18



Подход #2 - Сегментирование системы «защищаем здания/организации»

19

ИНФОРМАЦИОННАЯ
СИСТЕМА

ЦОД

ВЫВОД

Сложно обеспечивать
защищённость СВОЕЙ
информации в
ЧУЖОМ сегменте

Филиал #1

Интернет

Филиал #2

АТТЕСТАТ
СООТВЕТСТВИЯ

???



Подход #2 - Сегментирование системы «защищаем здания/организации»

20

USER	Компьютер	IT специалист	ИБ специалист	Оператор ИС	Лицензиат
					

Подход #3

Выделение перечня типовых
сегментов

«защищаем технологии»

*«IT должно жить!
Спасём IT!»*

Подход #3 - Выделение перечня типовых сегментов «защищаем технологии»

22

Зафиксированные классы защищённости ИС и технологии обработки информации

Типовой сегмент № 2 – Доступ к не перенесённым ресурсам филиала

Типовой сегмент № 3 – Доступ в Интернет

ЦОД

Типовой сегмент № 1 – Удалённая обработка информации

Филиал #1

Филиал #2

Интернет

Типовой сегмент № 4 – Локальная обработка информации

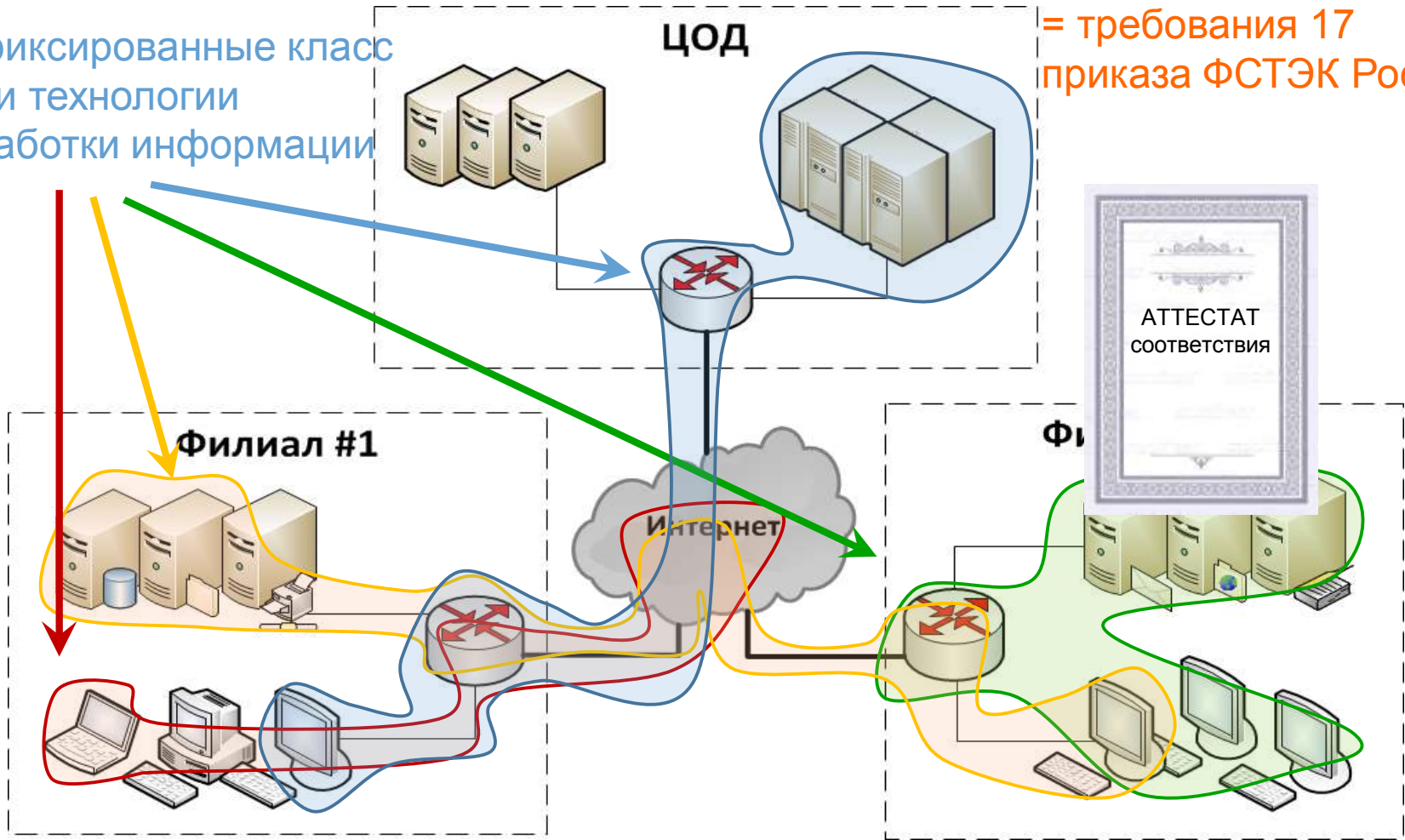


Подход #3 - Выделение перечня типовых сегментов «защищаем технологии»

23

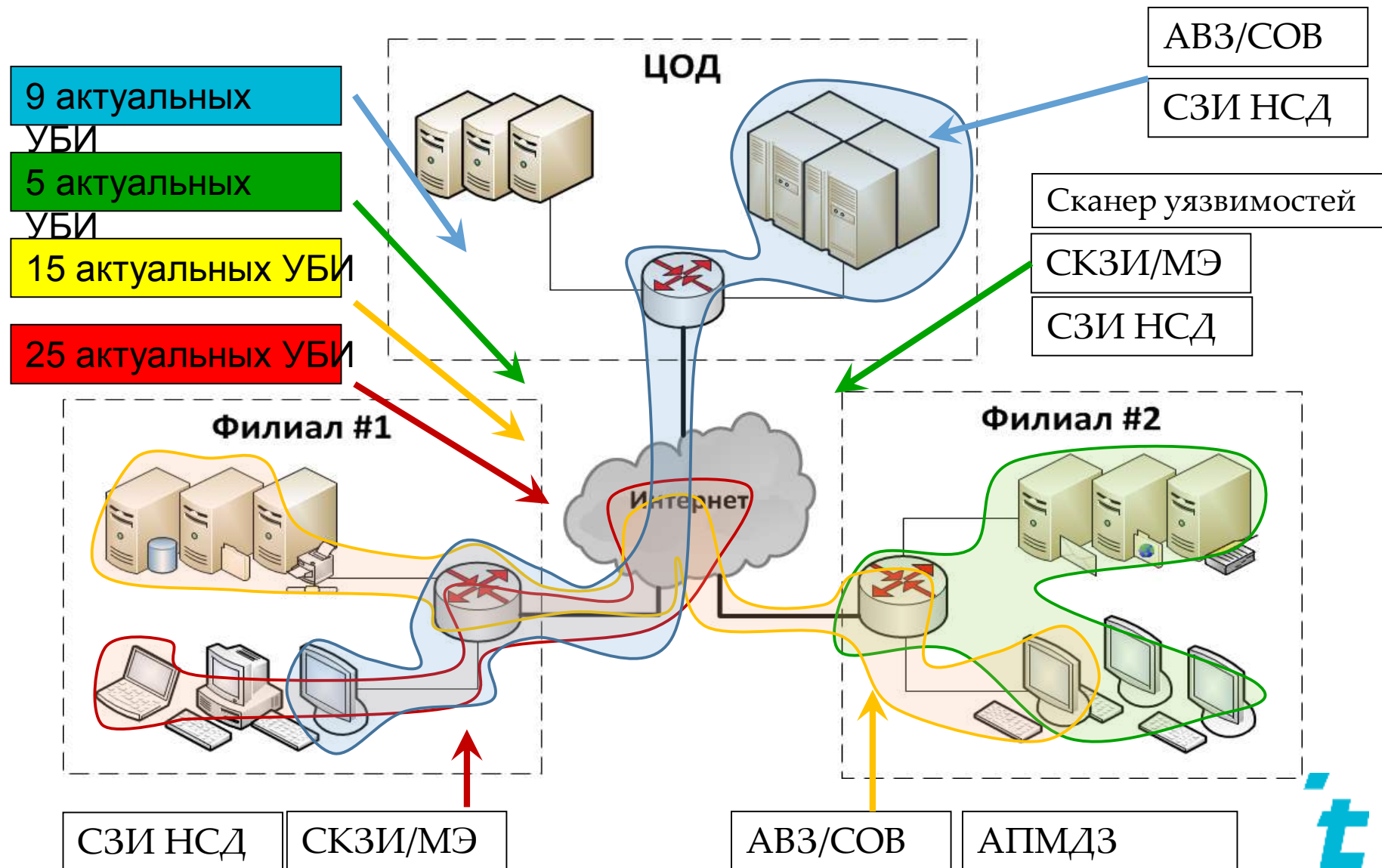
Зафиксированные классы
ИС и технологии
обработки информации

= требования 17
приказа ФСТЭК России



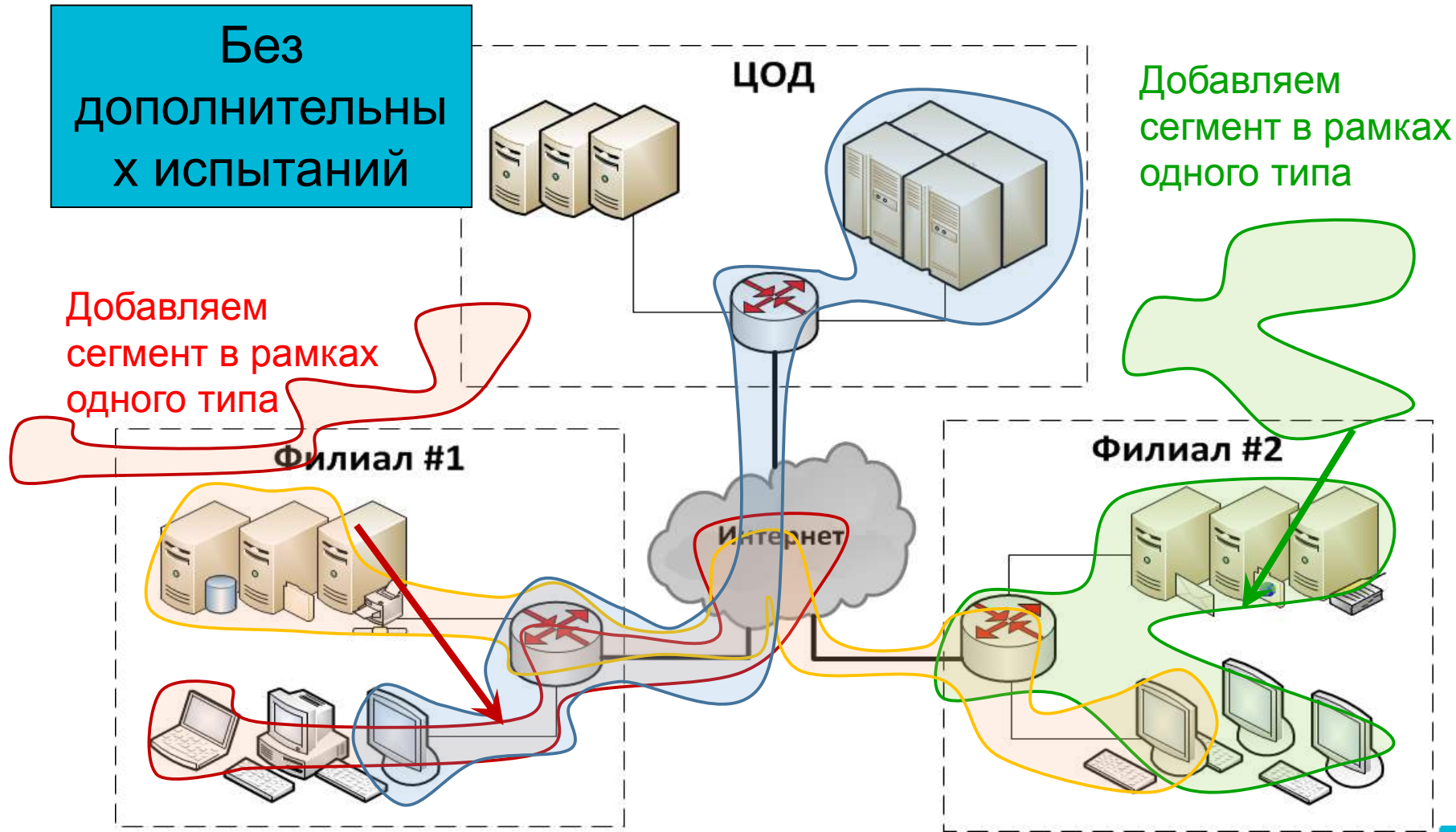
Подход #3 - Выделение перечня типовых сегментов «защищаем технологии»

24



Подход #3 - Выделение перечня типовых сегментов «защищаем технологии»

25



Подход #3 - Выделение перечня типовых сегментов «защищаем технологии»

26

Поменяли
структуру базы
данных

Поменяли линию
связи

Поменяли
операционную
систему

ЦОД

Добавили
информационную
систему

ПЕРЕАТТЕСТАЦИЯ

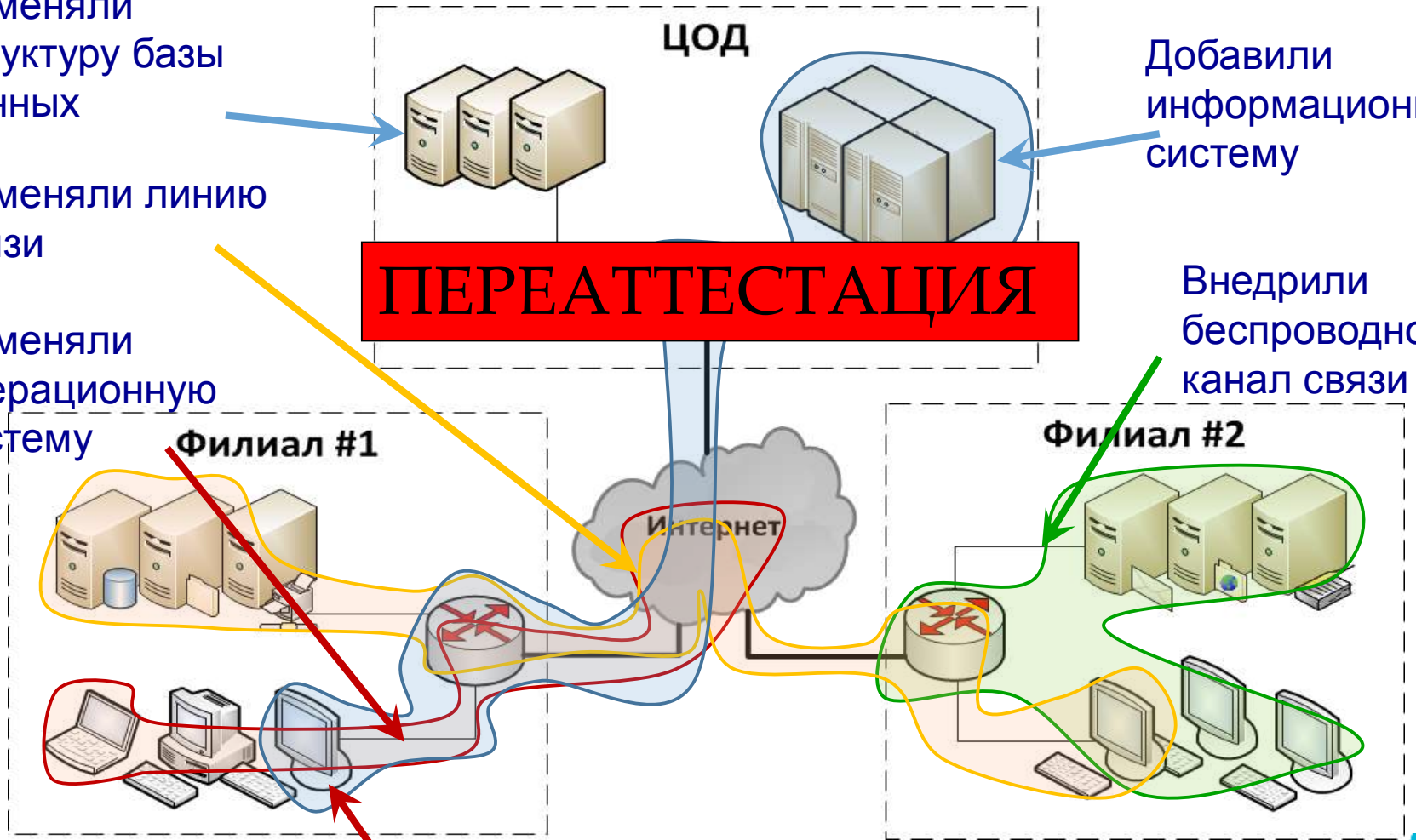
Внедрили
беспроводной
канал связи

Филиал #1

Филиал #2

Интернет

Добавили информационную систему



Подход #3 - Выделение перечня типовых сегментов «защищаем технологии»

27

USER	Компьютер	IT специалист	ИБ специалист	Оператор ИС	Лицензиат
					

А как это сделать?...



Конкретизация подхода #3

Выделение сегментов,
реализующих полную
технологию обработки
информации,
в заданных условиях
эксплуатации

Условия соответствия сегмента типовому сегменту:

1. Одинаковые классы защищённости;
2. Одинаковые угрозы безопасности информации;
3. Одинаковые проектные решения по ИС;
4. Одинаковые проектные решения по СЗИ ИС.



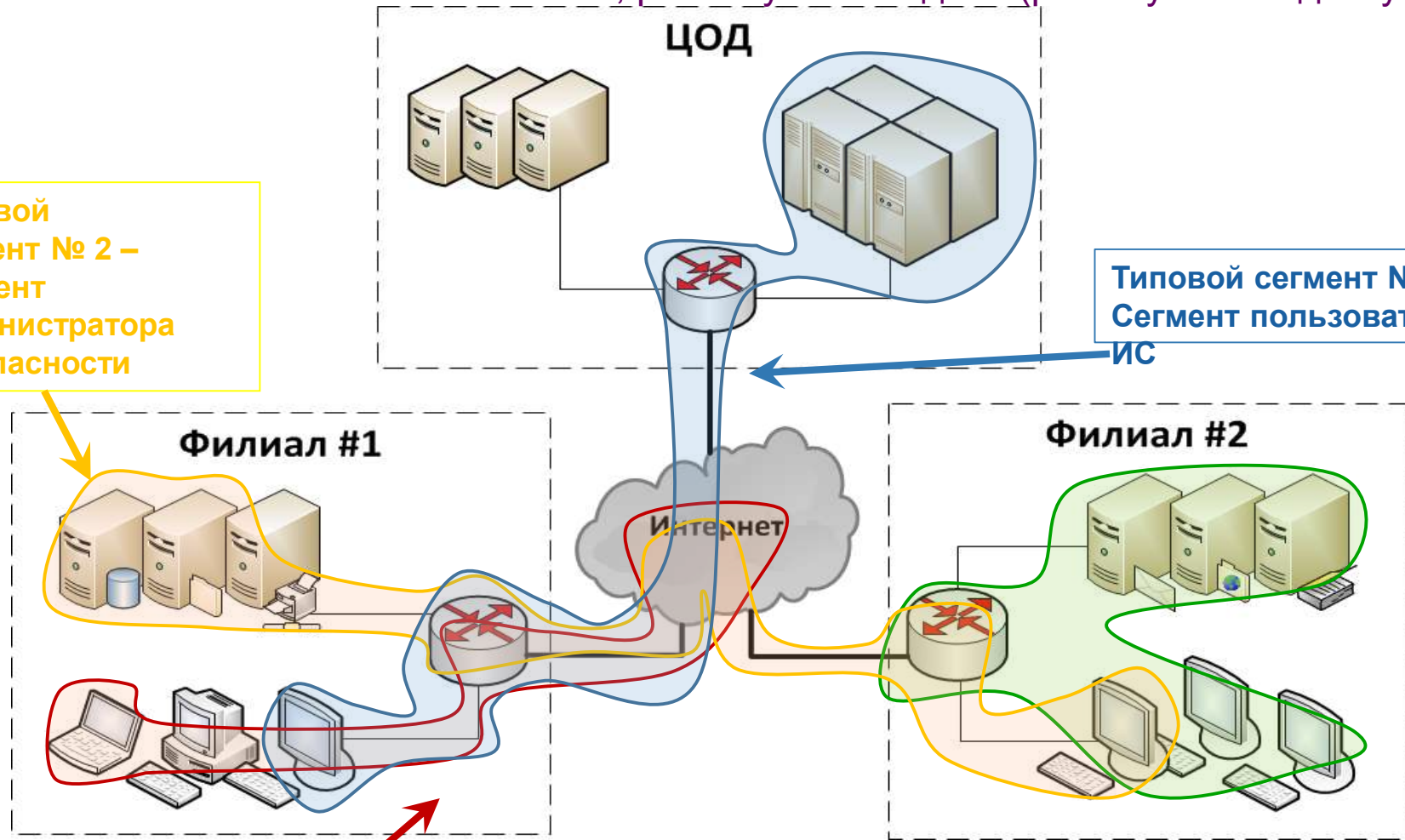
Определяем роли субъектов доступа (перечень типовых сегментов)

31

Тип сегмента – назначение сегмента, реализуемая задача (роль субъекта доступа).

Типовой
сегмент № 2 –
Сегмент
администратора
безопасности

Типовой сегмент № 1 –
Сегмент пользователя
ИС



Типовой сегмент № 3 –
Сегмент доступа в Интернет

Типовой сегмент № 4 –
Сегмент системного
администратора



Какие бывают **Условия эксплуатации** типового сегмента:

- вид и уровень конфиденциальности информации;
- проектные решения по ИС (технологии обработки , хранения, передачи информации)
- проектные решения по СЗИ (технологии защиты информации)



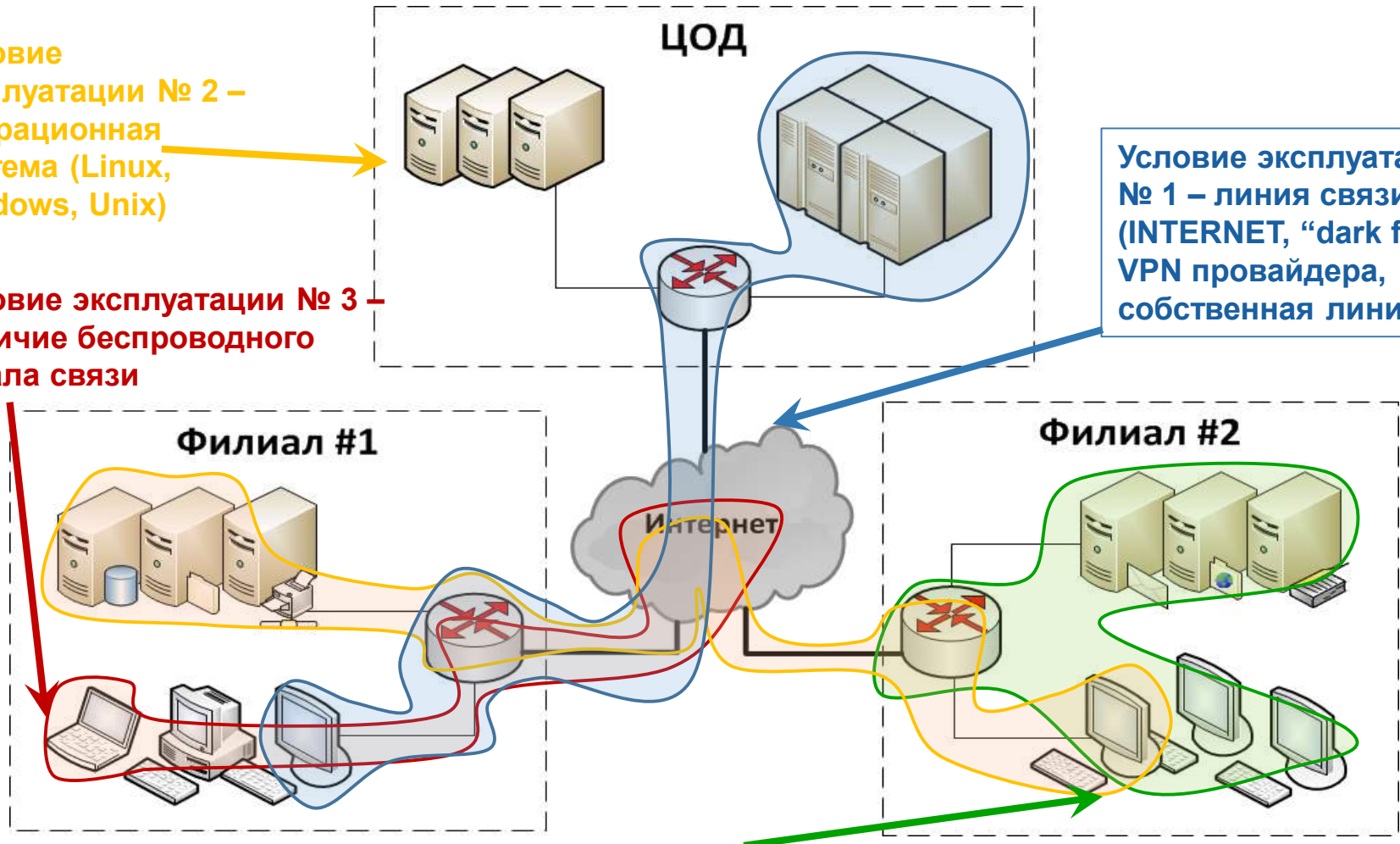
Определяем возможные условия эксплуатации типовых сегментов

33

Условие эксплуатации № 2 –
Операционная
система (Linux,
Windows, Unix)

Условие эксплуатации № 3 –
Наличие беспроводного
канала связи

Условие эксплуатации
№ 1 – линия связи
(INTERNET, “dark fiber”,
VPN провайдера,
собственная линия)



Условие эксплуатации № 4 – тип АРМ пользователя
(ПК, планшет, мобильный телефон)



Стандарт мер по защите информации распределённых информационных систем

34

Стандарт мер
защиты
информации
РИС

Роль субъекта
доступа
(ТИП 1)

Роль субъекта
доступа
(ТИП 2)

Роль субъекта
доступа
(ТИП 3)

Условия
эксплуатации
1.1

Профиль
защиты № 1

Профиль
защиты № 2

Профиль
защиты № 3

Условия
эксплуатации
1.2

Профиль
защиты № 2

Профиль
защиты № 3

Профиль
защиты № 4

Условия
эксплуатации
1.3

Профиль
защиты № 3

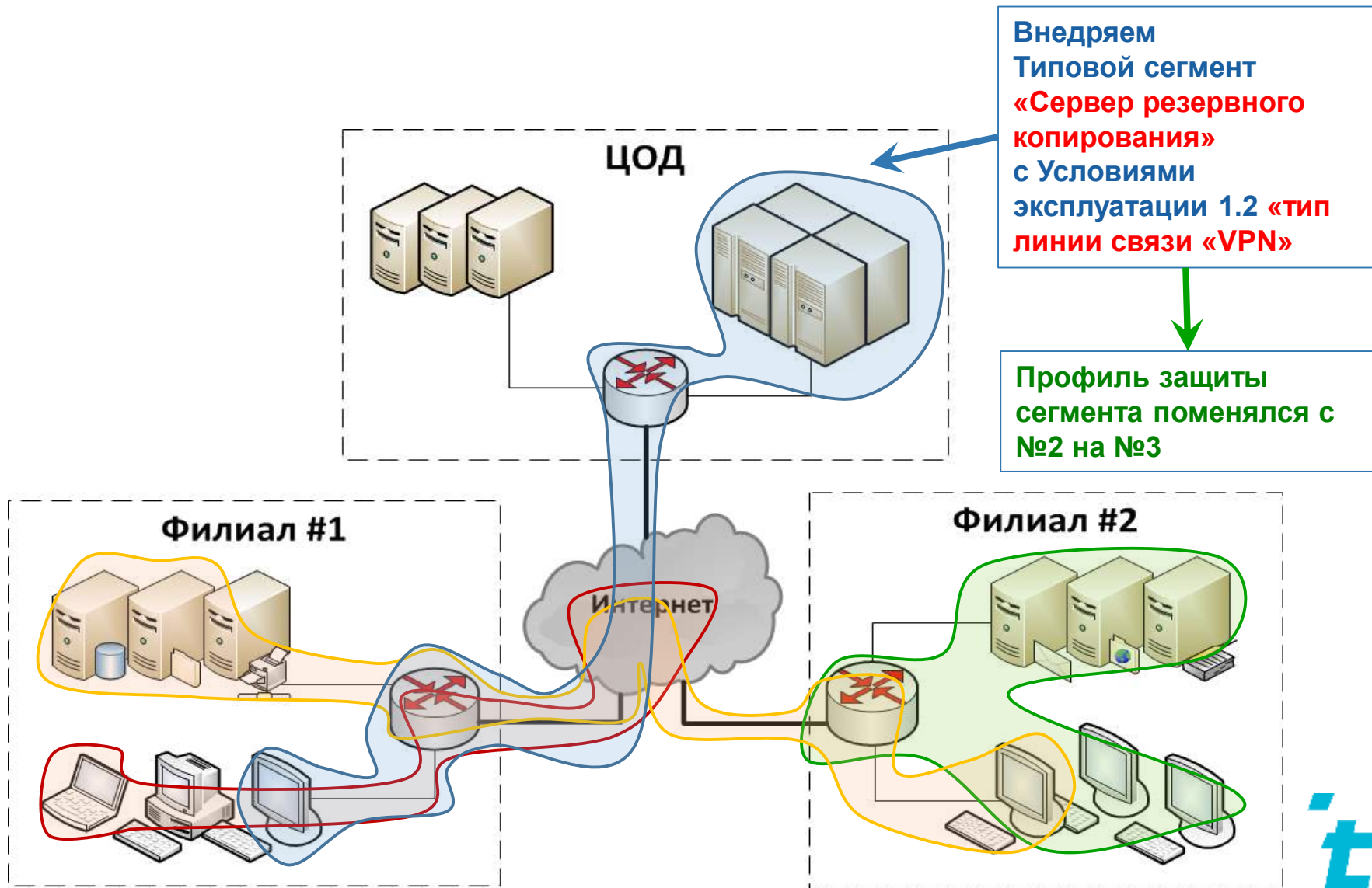
Профиль
защиты № 4

Профиль
защиты № 5



Пример: «Внедряем типовой сегмент с новыми условиями эксплуатации»

35



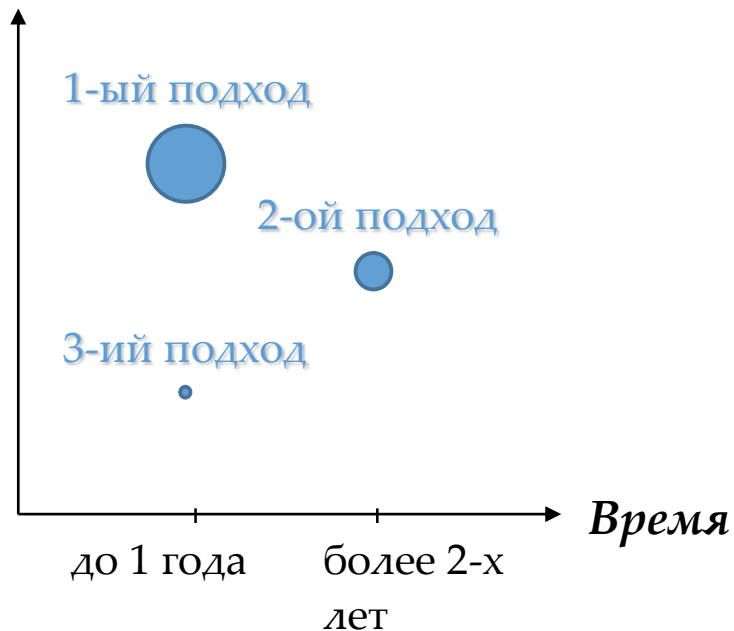
Конкретизация подхода #3 для РИС

36

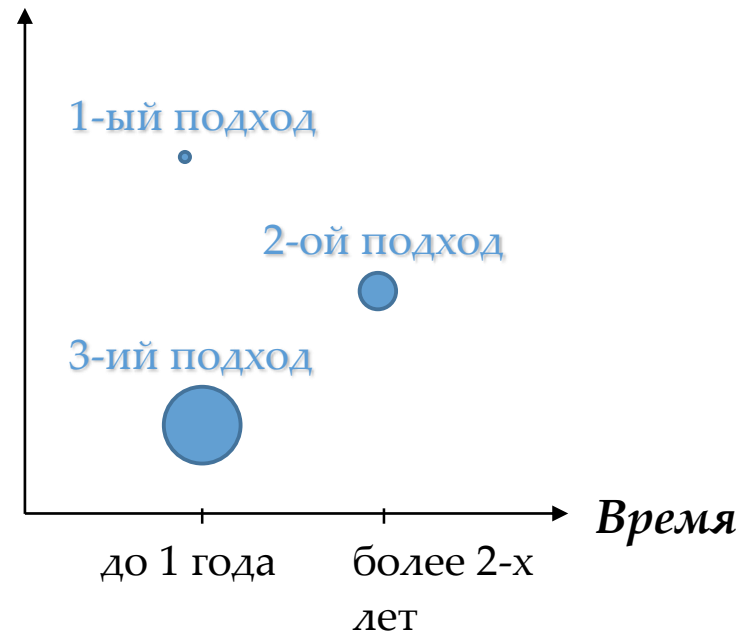
USER	Компьютер	IT специалист	ИБ специалист	Оператор ИС	Лицензиат
					

Преимущества и недостатки подходов 37

Стоимость,
для Заказчика



Затраты,
для Лицензиата



Тезис №1

«Давайте создавать **жизнеспособную** систему защиты информации»

Тезис №2

«Давайте защищать не **Железо**, а **ТЕХНОЛОГИИ** обработки, хранения и передачи информации»



Спасибо за внимание

www.saveit.pro