SAVE group

# Особенности аттестации распределённых информационных систем

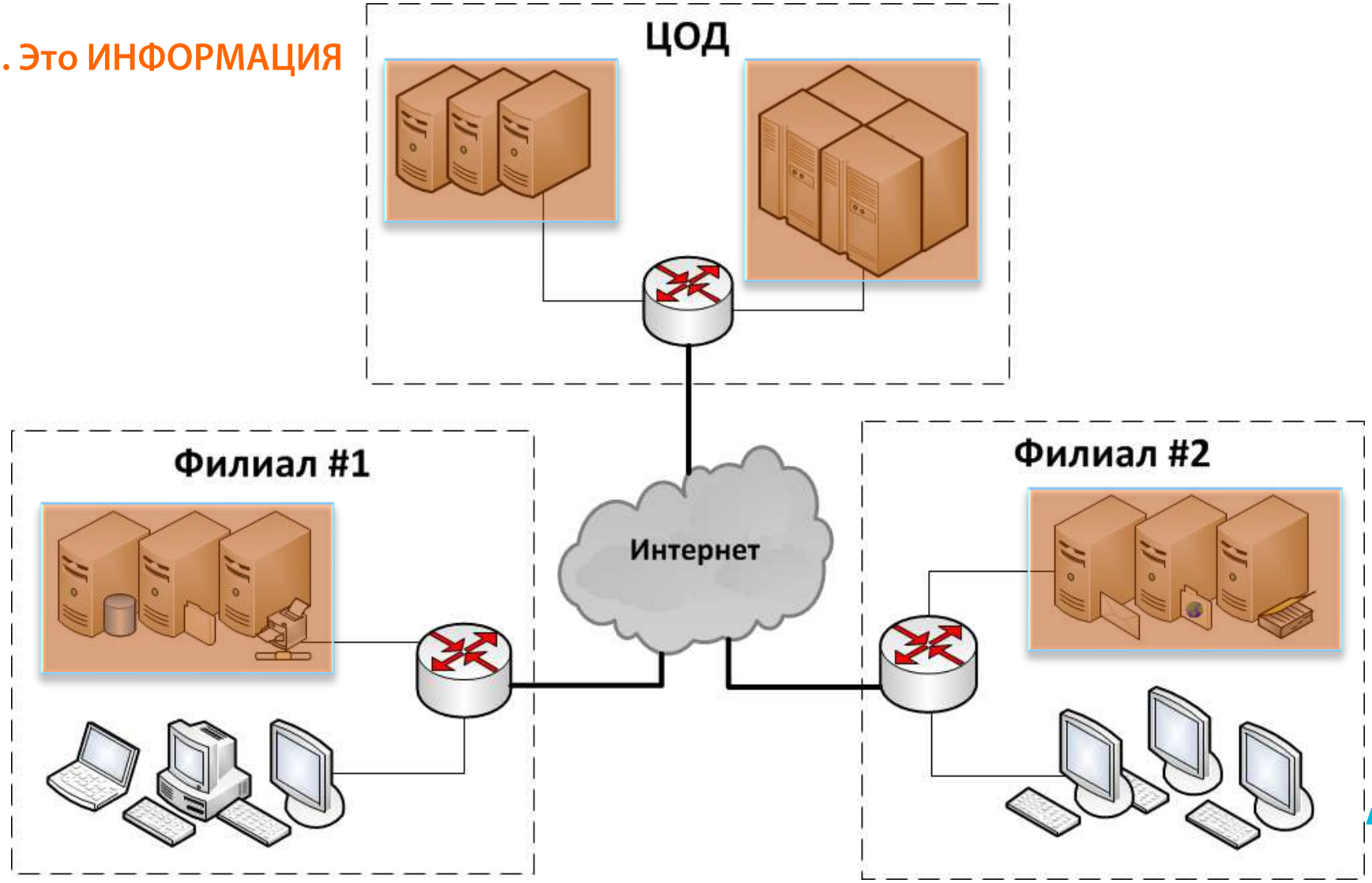
***Директор***
***группы компаний SaveIT Group***
***Рыбьяков Юрий Юрьевич***

# Распределённая информационная система



## ЧТО ЭТО?

1. Это ИНФОРМАЦИЯ



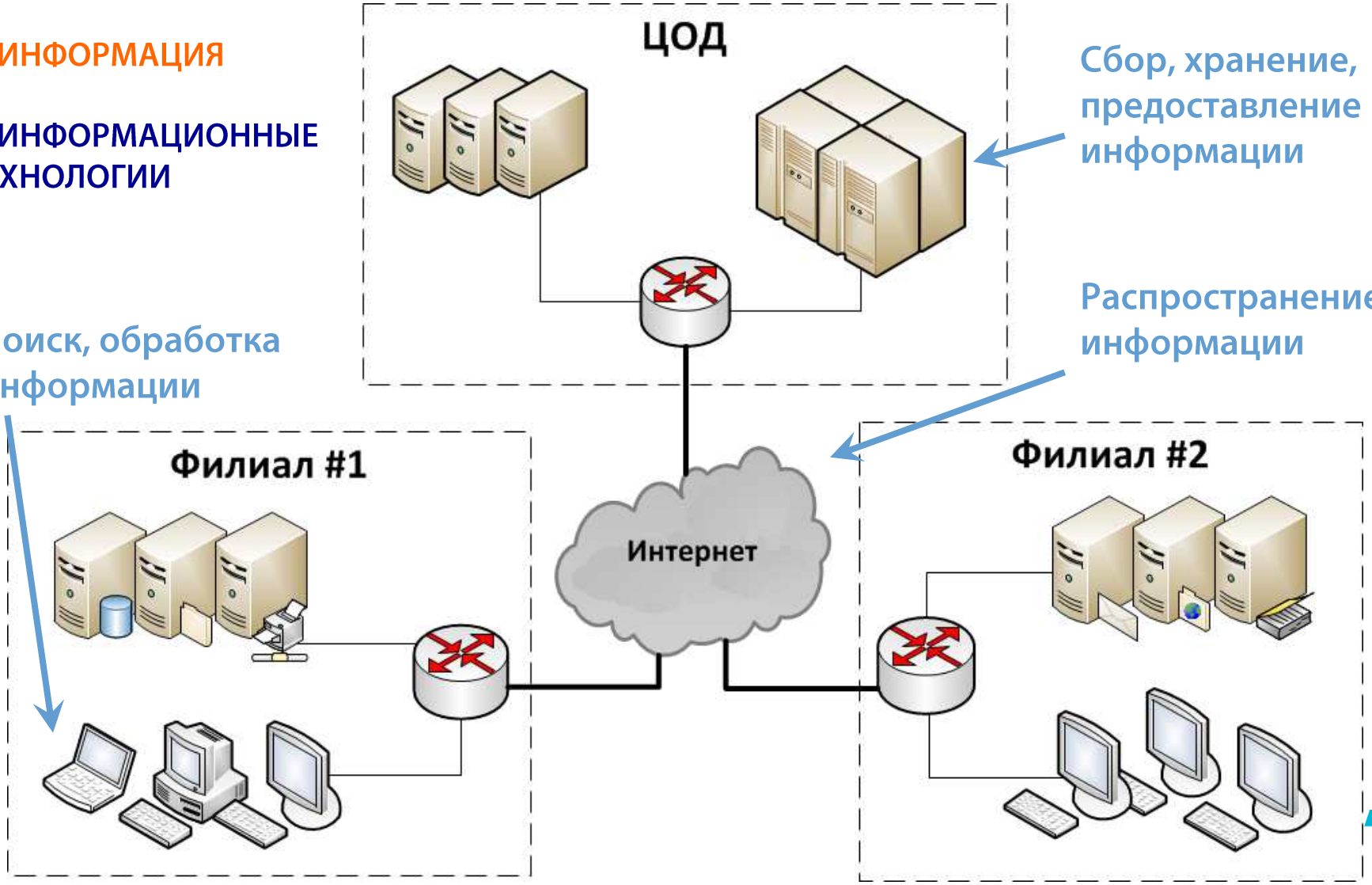
# Распределённая информационная система



## ЧТО ЭТО?

1. ИНФОРМАЦИЯ

2. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ



# Распределённая информационная система

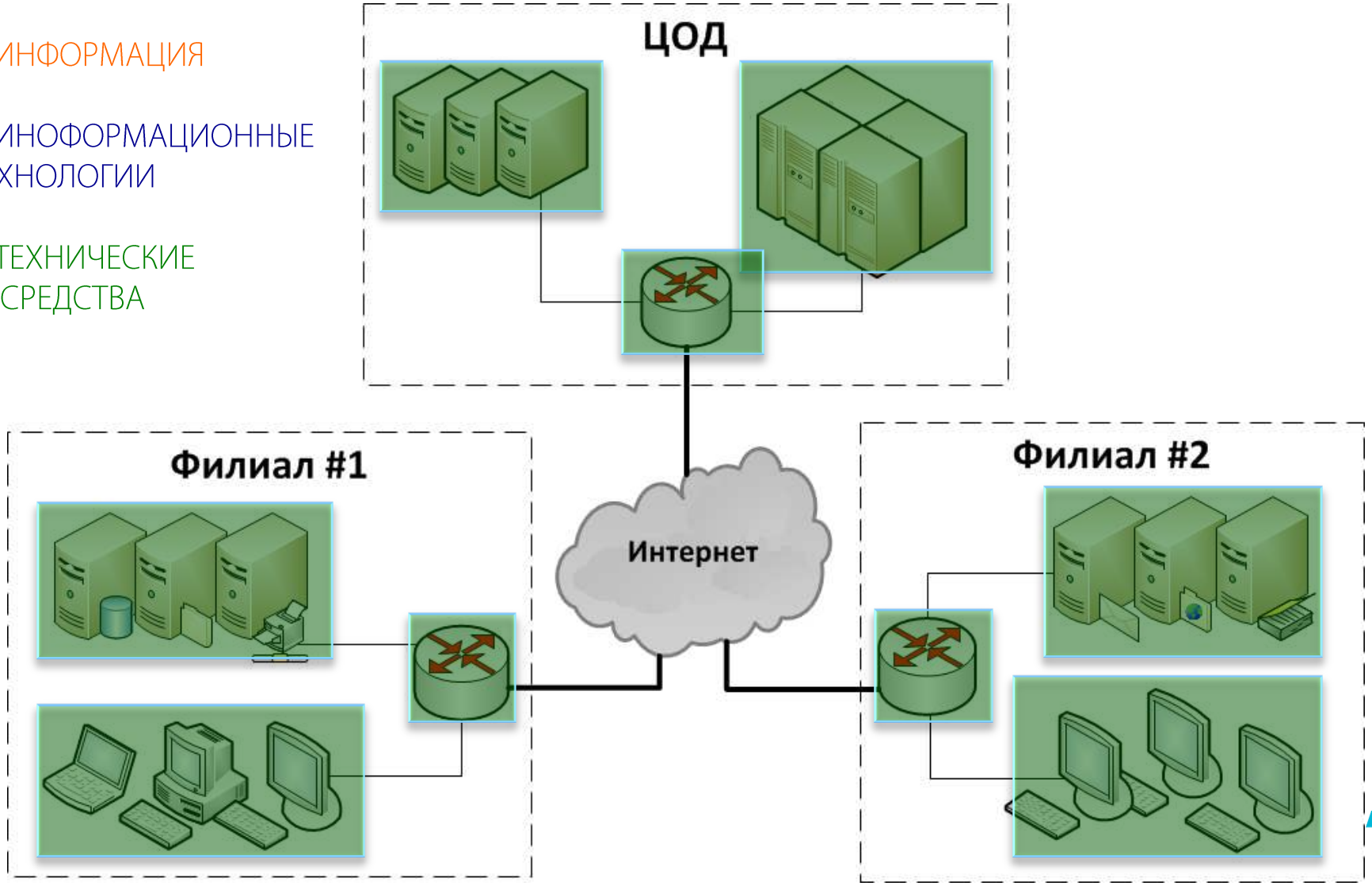


## ЧТО ЭТО?

1. ИНФОРМАЦИЯ

2. ИНОФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

3. ТЕХНИЧЕСКИЕ СРЕДСТВА



# Распределённая информационная система



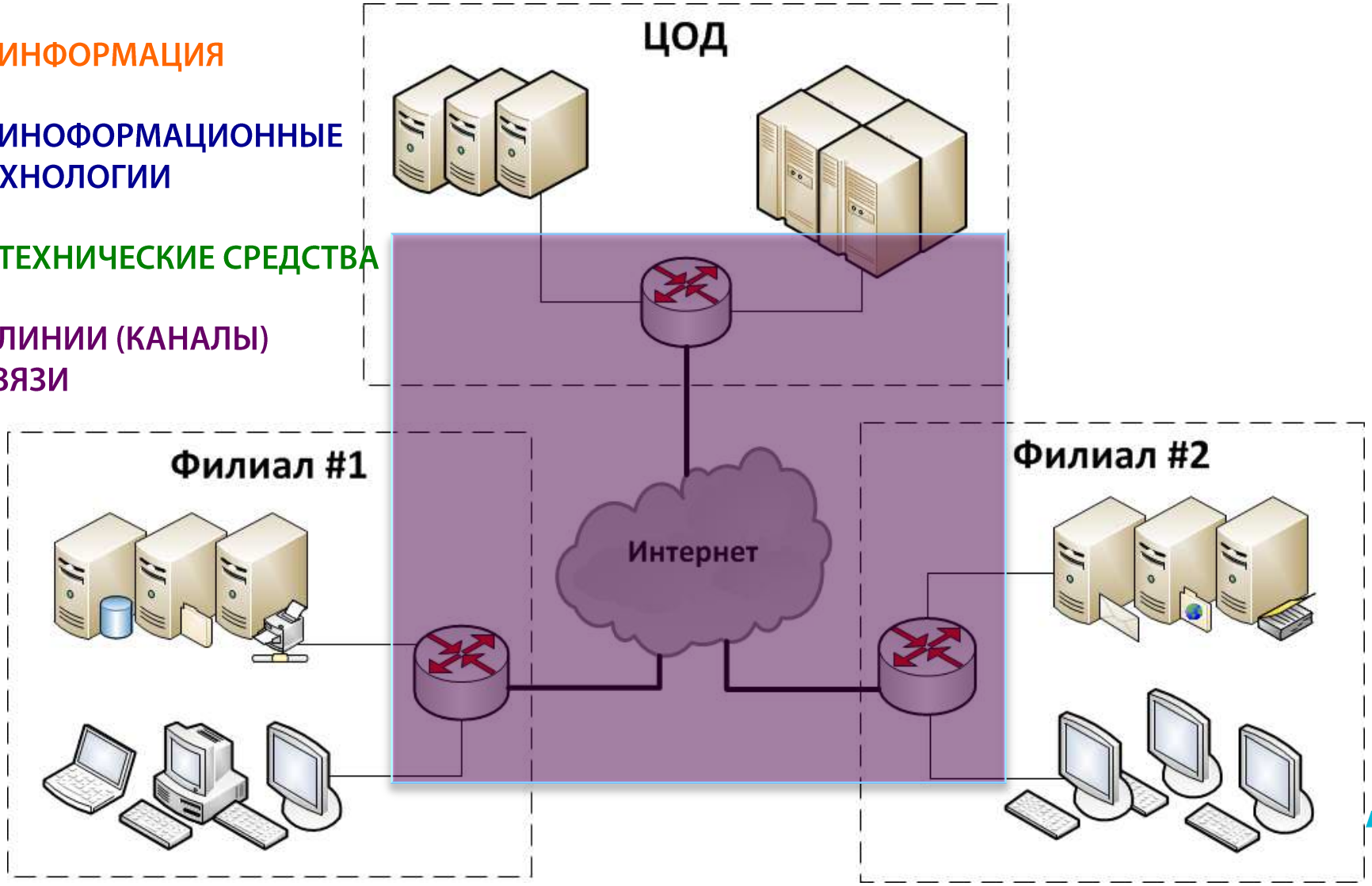
## ЧТО ЭТО?

1. ИНФОРМАЦИЯ

2. ИНОФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

3. ТЕХНИЧЕСКИЕ СРЕДСТВА

4. ЛИНИИ (КАНАЛЫ) СВЯЗИ



# Походы к аттестации распределённых информационных систем



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

**Подход 1** «Фиксация системы»

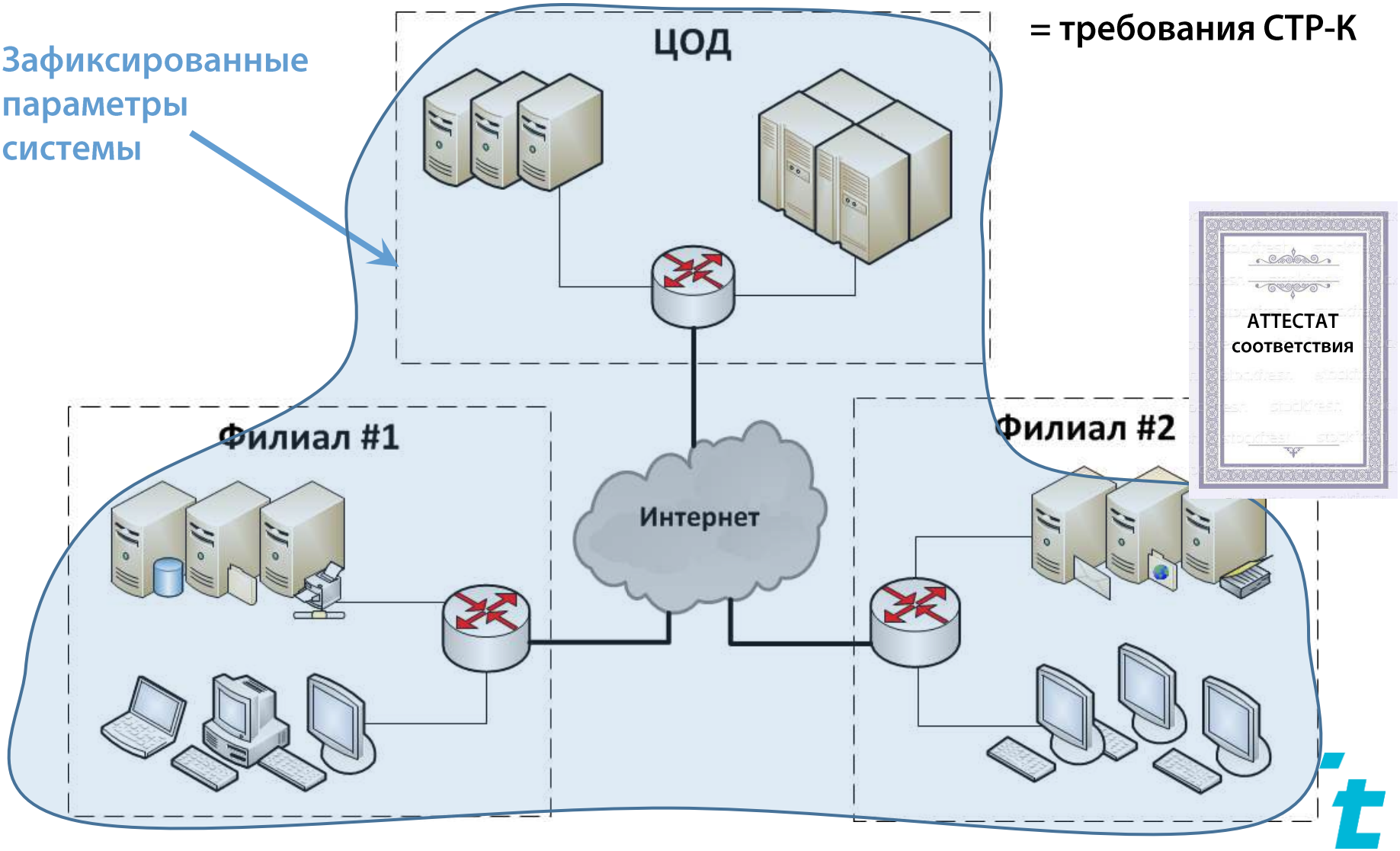
**Подход 2** «Сегментирование системы»

**Подход 3** «Выделение перечня типовых сегментов»

# Подход #1 - Фиксация системы



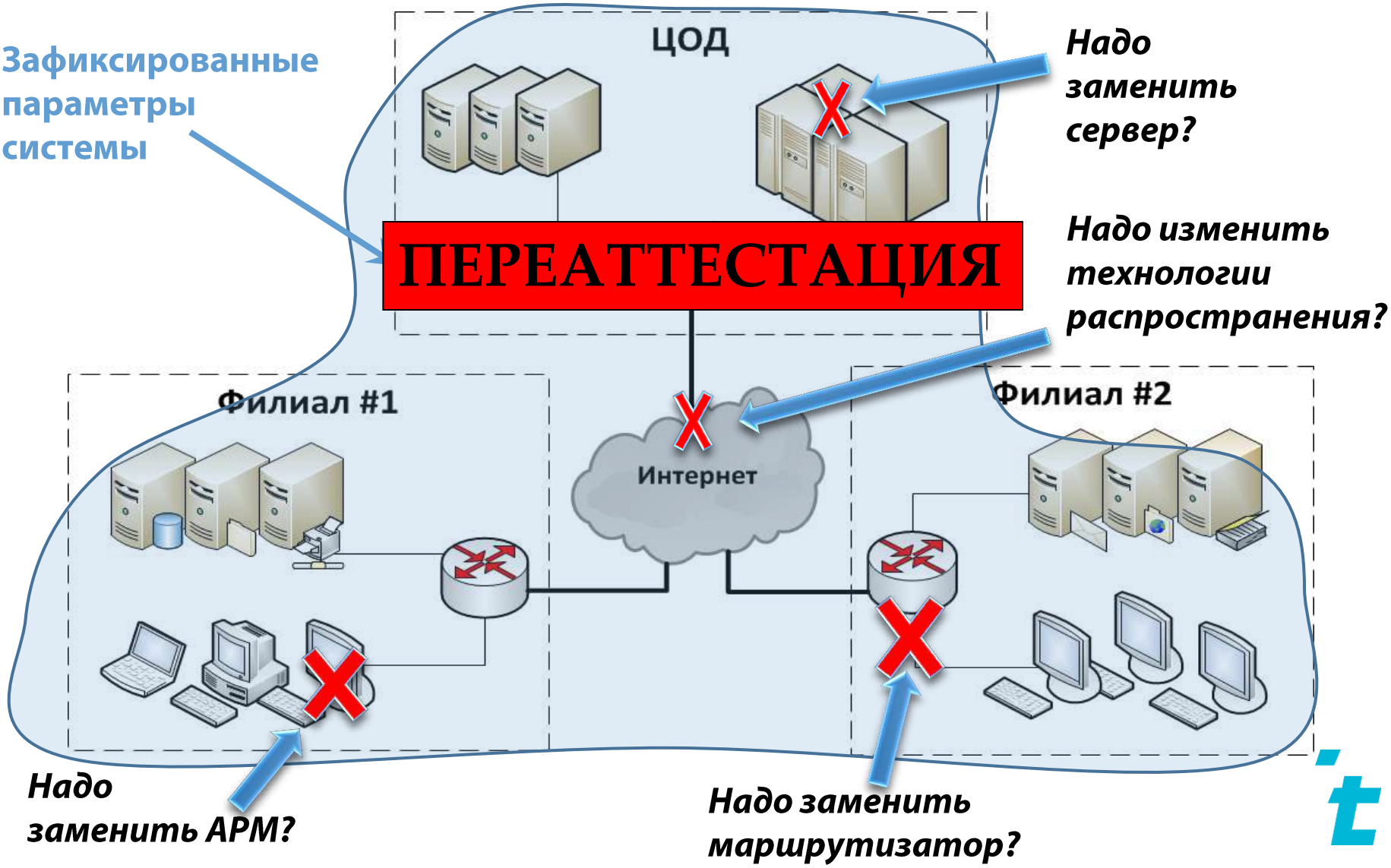
## «защищаем железо (технические средства)»



# Подход #1 - Фиксация системы



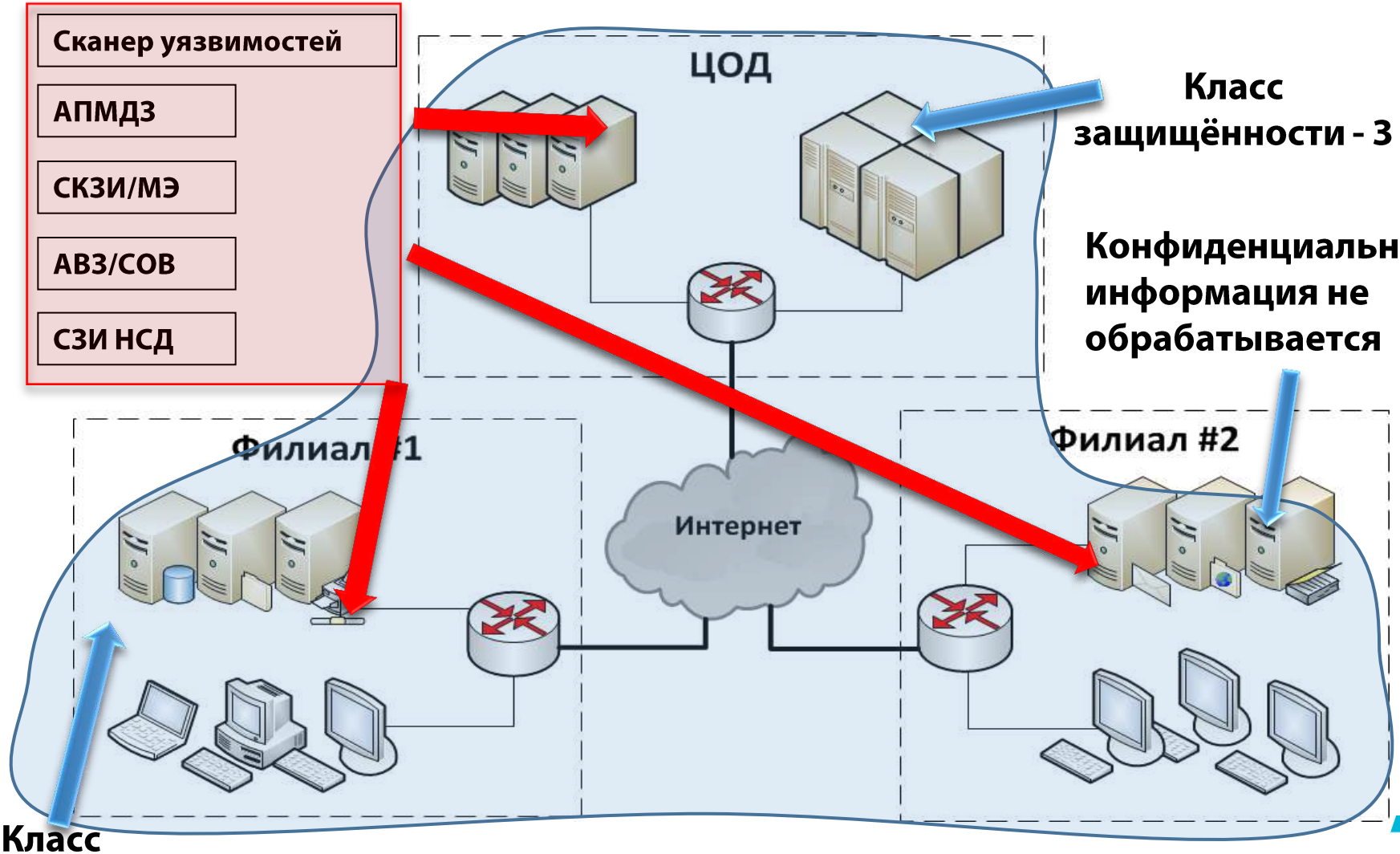
## «защищаем железо (технические средства)»



# Подход #1 - Фиксация системы



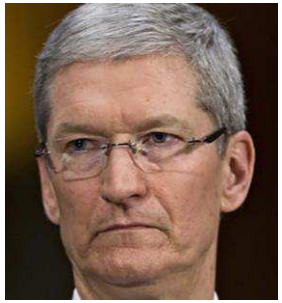
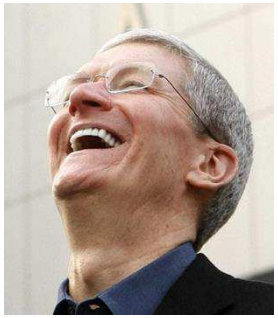
## «защищаем железо (технические средства)»



# Подход #1 - Фиксация системы

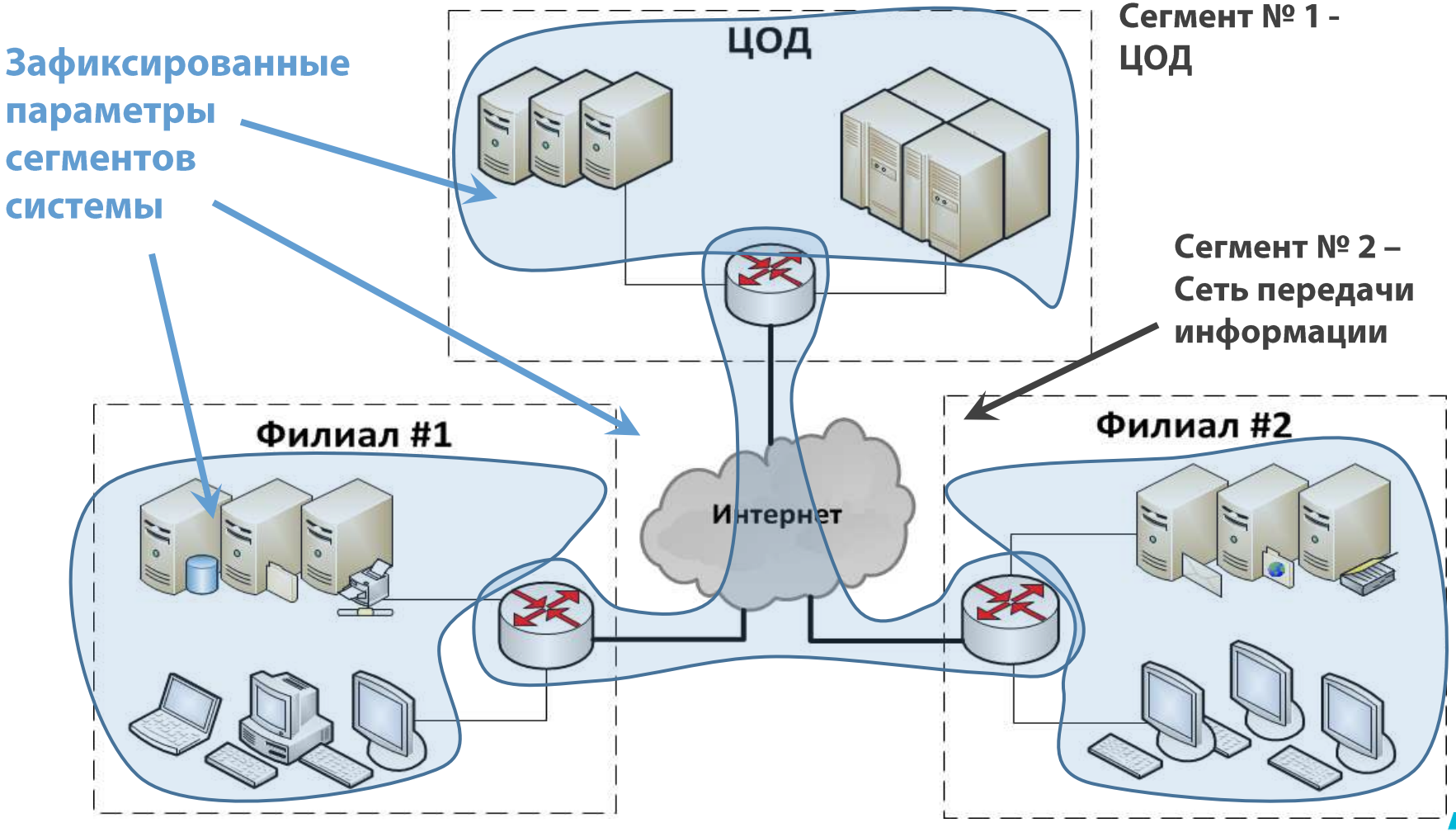


## «защищаем железо (технические средства)»

| USER | Компьютер | IT специалист | ИБ специалист | Оператор ИС | Лицензиат |
|---|---|---|---|---|---|
|  |  |  |  |  |  |

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






Сегмент № 3 – Подведомственная организация

Сегмент № 4 – Филиал организации

# Подход #2 - Сегментирование системы



## «защищаем здания/организации»

= требования СТР-К

Зафиксированные параметры сегментов системы

ЦОД

АТТЕСТАТ соответствия

2010

Филиал #1

АТТЕСТАТ соответствия

2015

Интернет

АТТЕСТАТ соответствия

2012

Филиал #2

АТТЕСТАТ соответствия

????

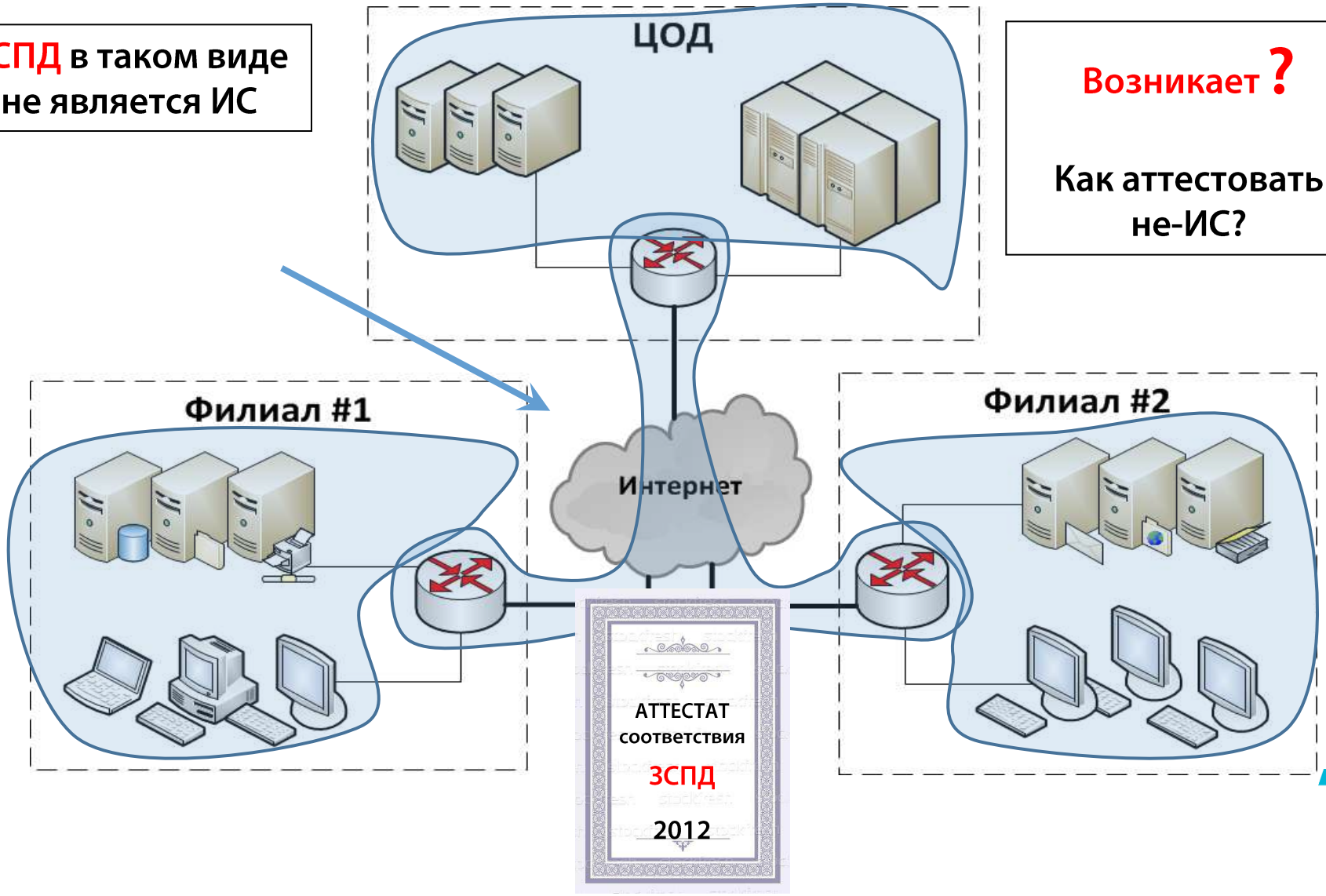
# Подход #2 - Сегментирование системы «защищаем здания/организации»



**ЗСПД в таком виде не является ИС**

**Возникает ?**

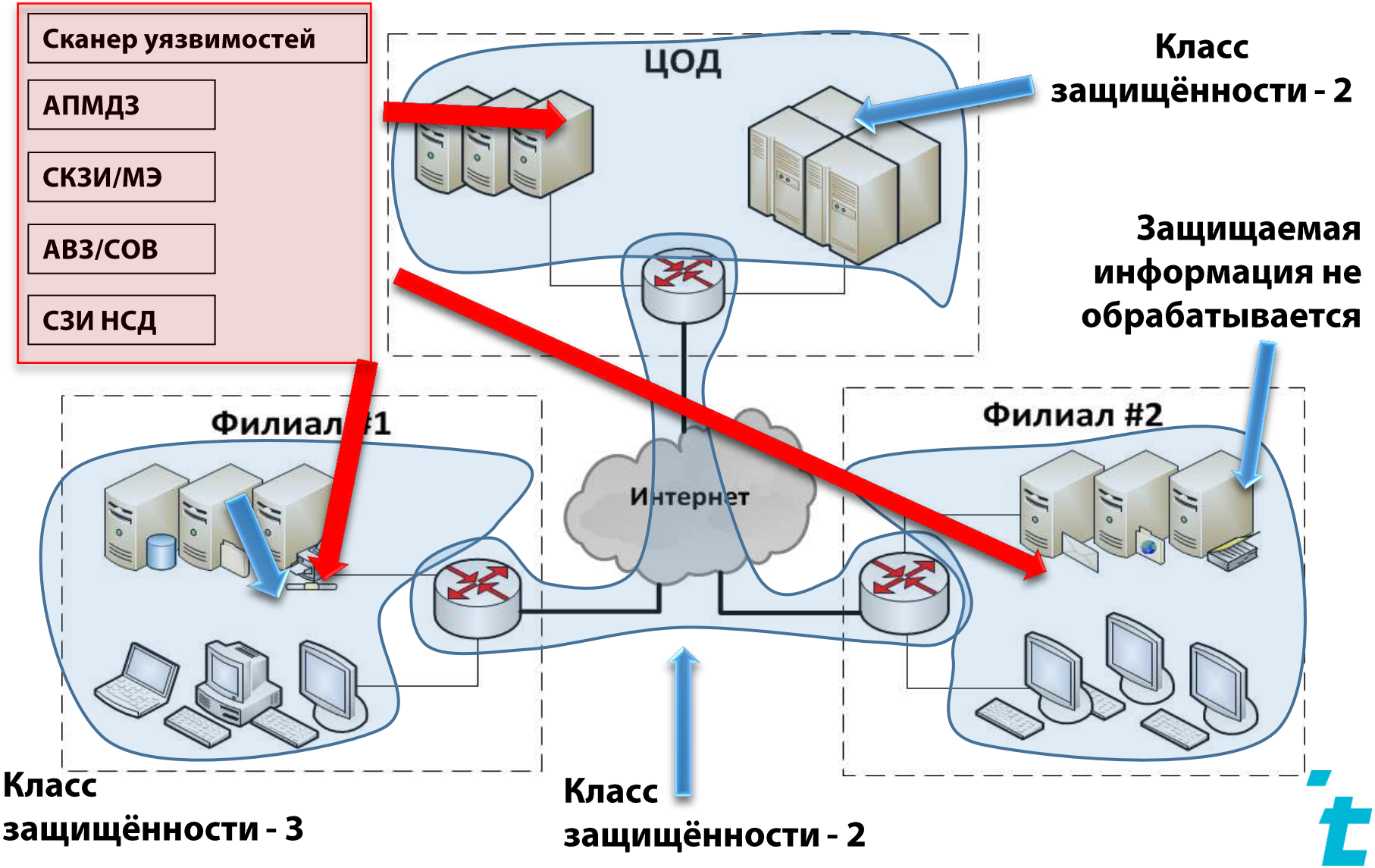
**Как аттестовать не-ИС?**



# Подход #2 - Сегментирование системы



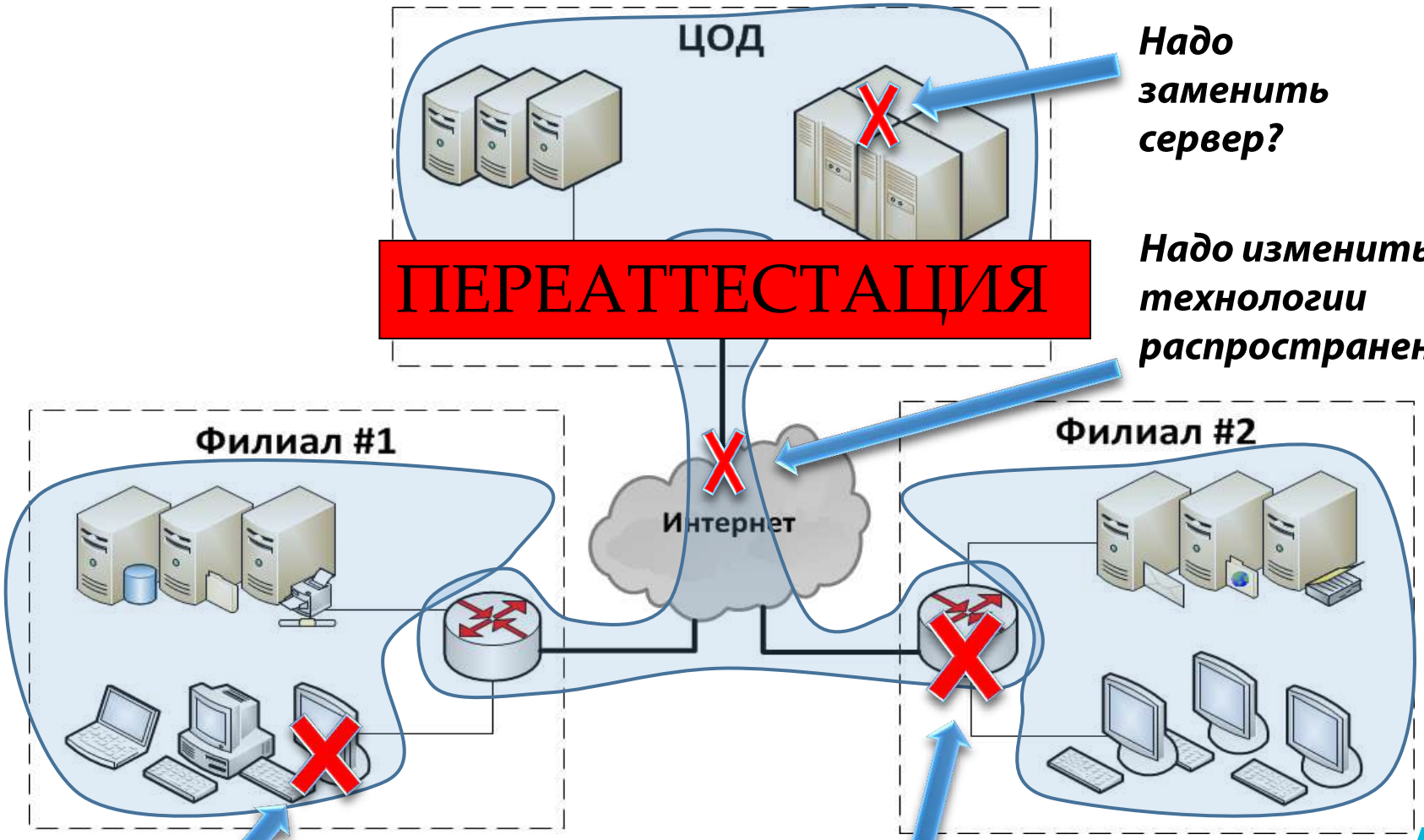
## «защищаем здания/организации»



# Подход #2 - Сегментирование системы

## «защищаем здания/организации»






***Надо заменить сервер?***

***Надо изменить технологии распространения?***

***Надо заменить АРМ?***

***Надо заменить маршрутизатор***

# Подход #2 - Сегментирование системы



## «защищаем здания/организации»

**ИНФОРМАЦИОННАЯ СИСТЕМА**

ЦОД

Филиал #1

Интернет

Филиал #2

АТТЕСТАТ соответствия

????

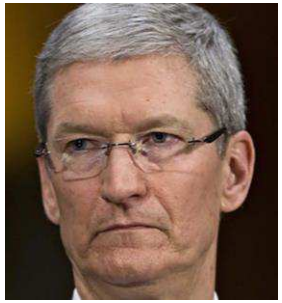
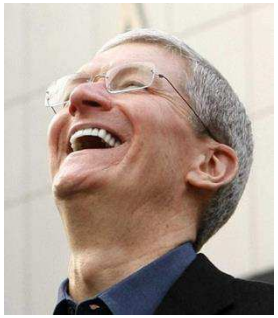
ВЫВОД

Сложно обеспечивать защищённость **СВОЕЙ** информации в **ЧУЖОМ** сегменте

# Подход #2 - Сегментирование системы



## «защищаем здания/организации»

| USER | Компьютер | IT специалист | ИБ специалист | Оператор ИС | Лицензиат |
|---|---|---|---|---|---|
|  |  |  |  |  |  |

# Подход #3

Выделение перечня типовых сегментов

«защищаем технологии»

***«IT должно жить! Спасём IT!»***

# Конкретизация подхода #3 для РИС



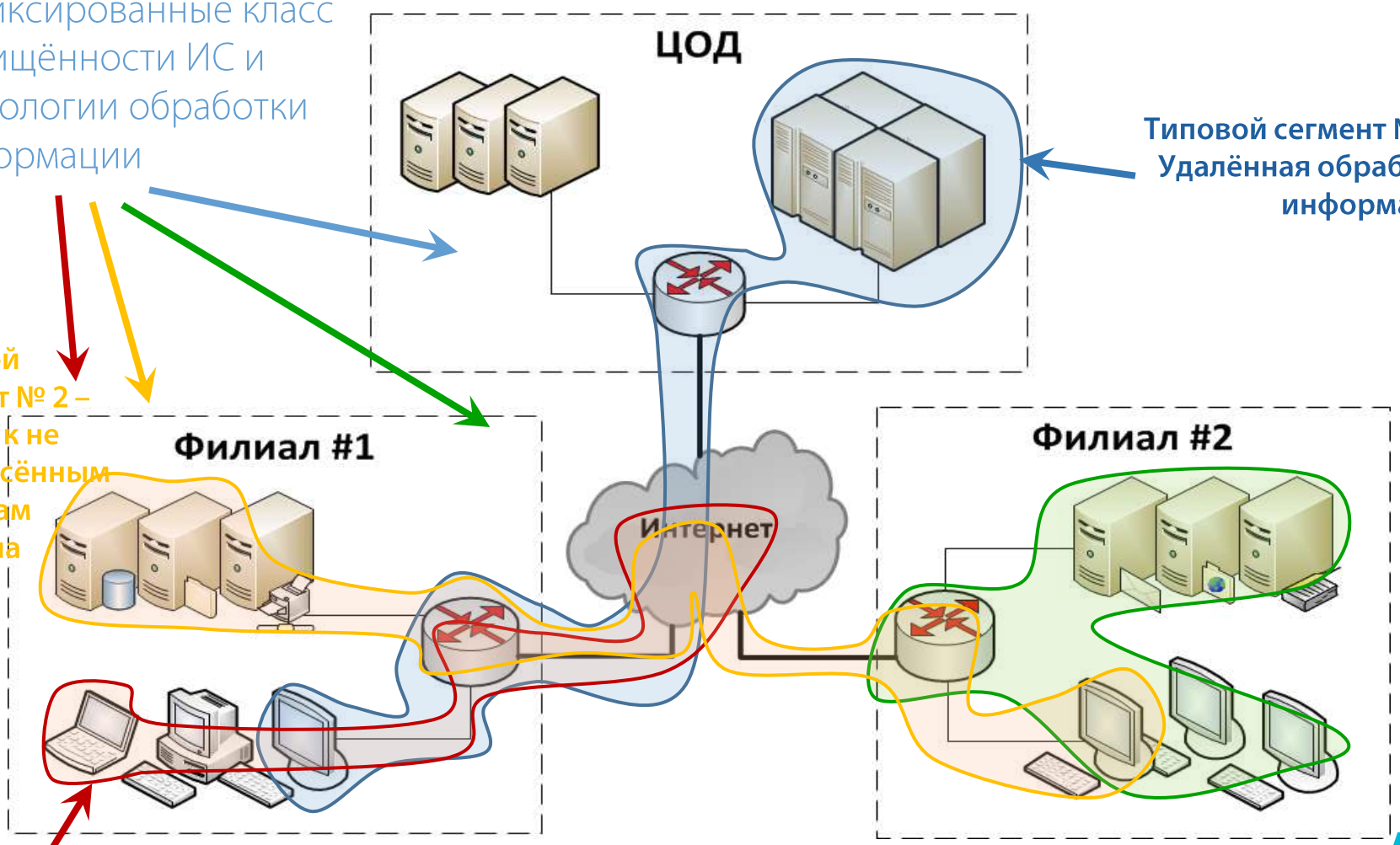
Условия соответствия сегмента *типовому* сегменту:

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

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



Зафиксированные класс защищённости ИС и технологии обработки информации




Типовой сегмент № 1 – Удалённая обработка информации

Типовой сегмент № 2 – Доступ к не перенесённым ресурсам филиала

Типовой сегмент № 3 – Доступ в Интернет

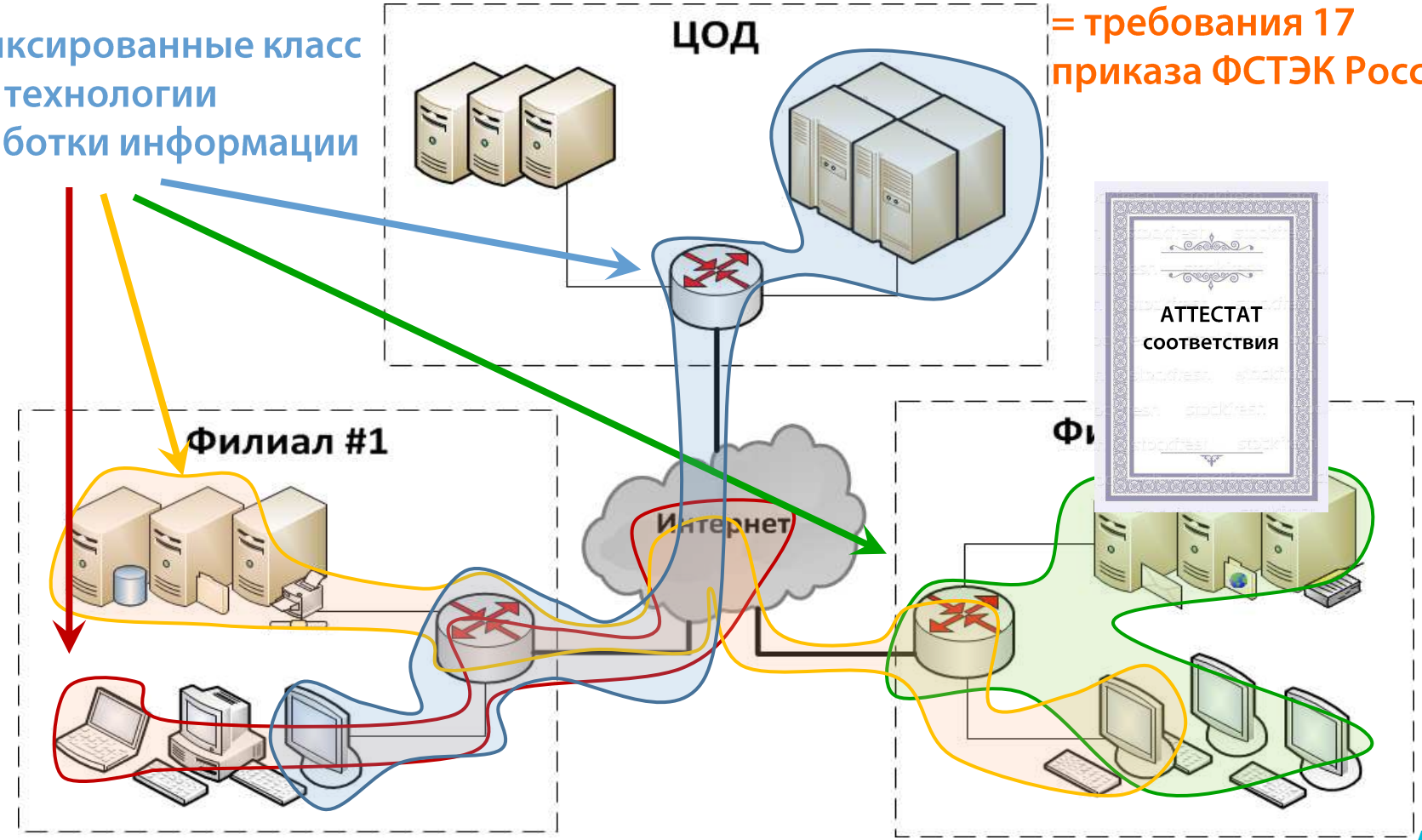
Типовой сегмент № 4 – Локальная обработка информации

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



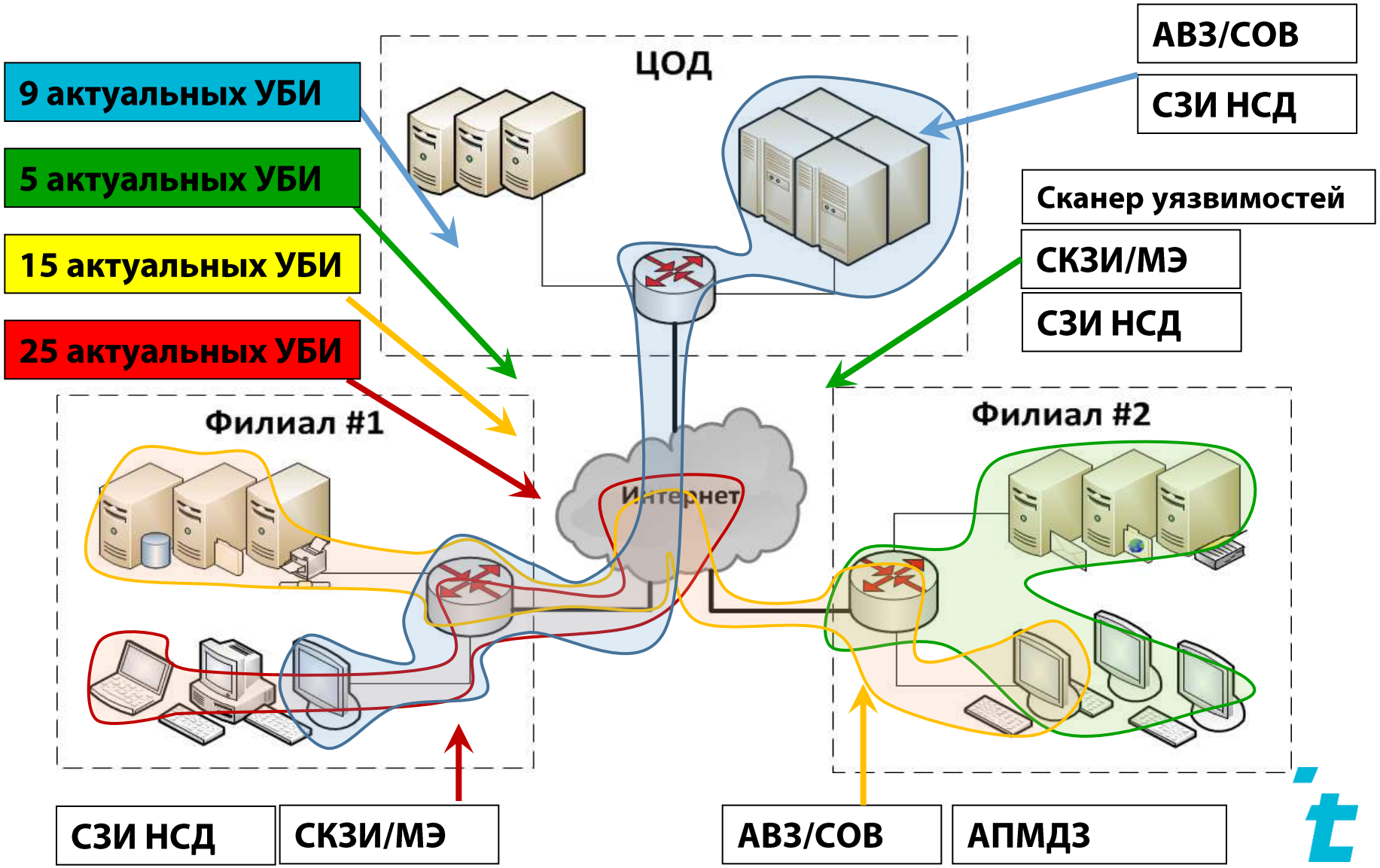
Зафиксированные класс ИС и технологии обработки информации

= требования 17 приказа ФСТЭК России



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

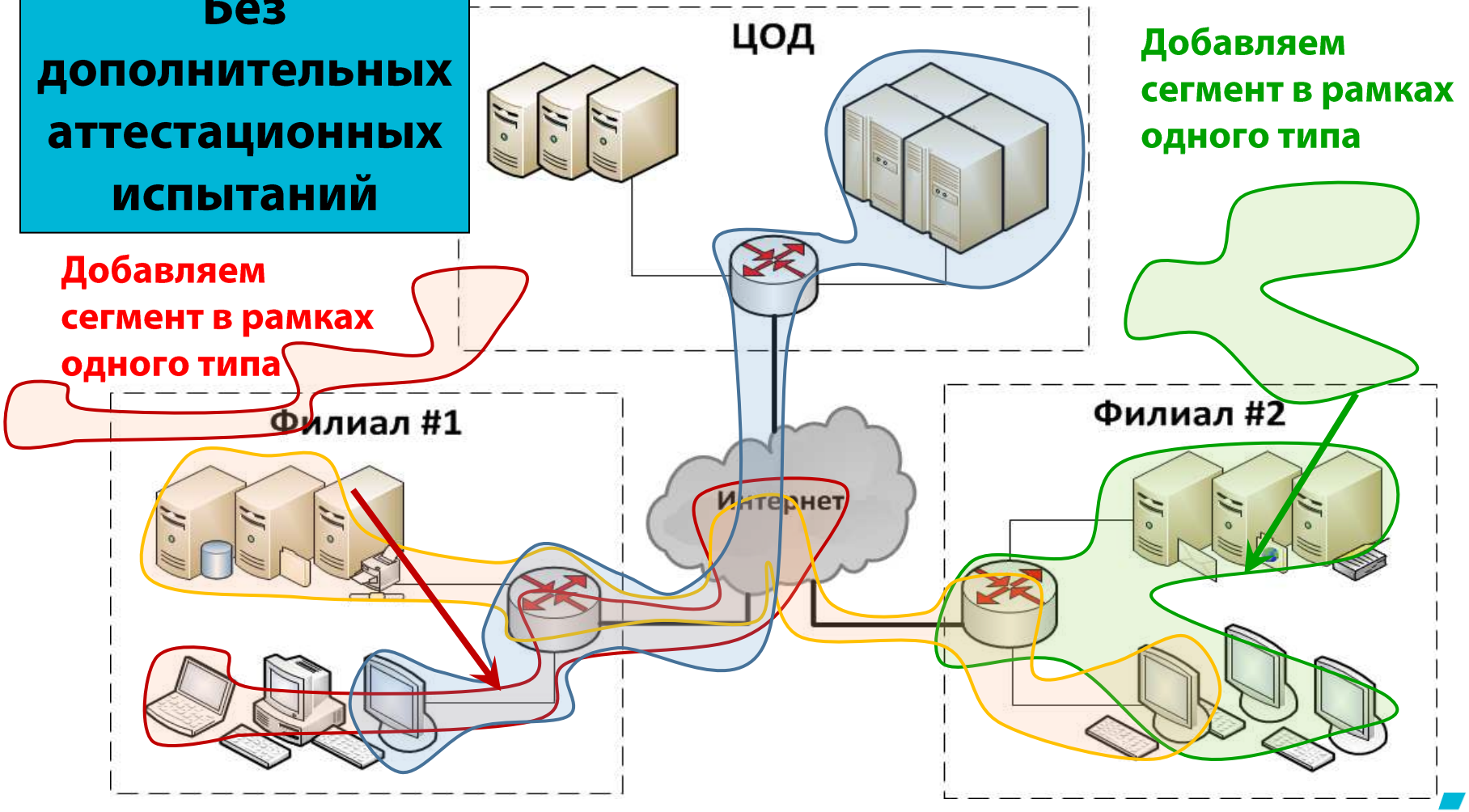




# Подход #3 - Выделение перечня типовых сегментов «защищаем технологии»

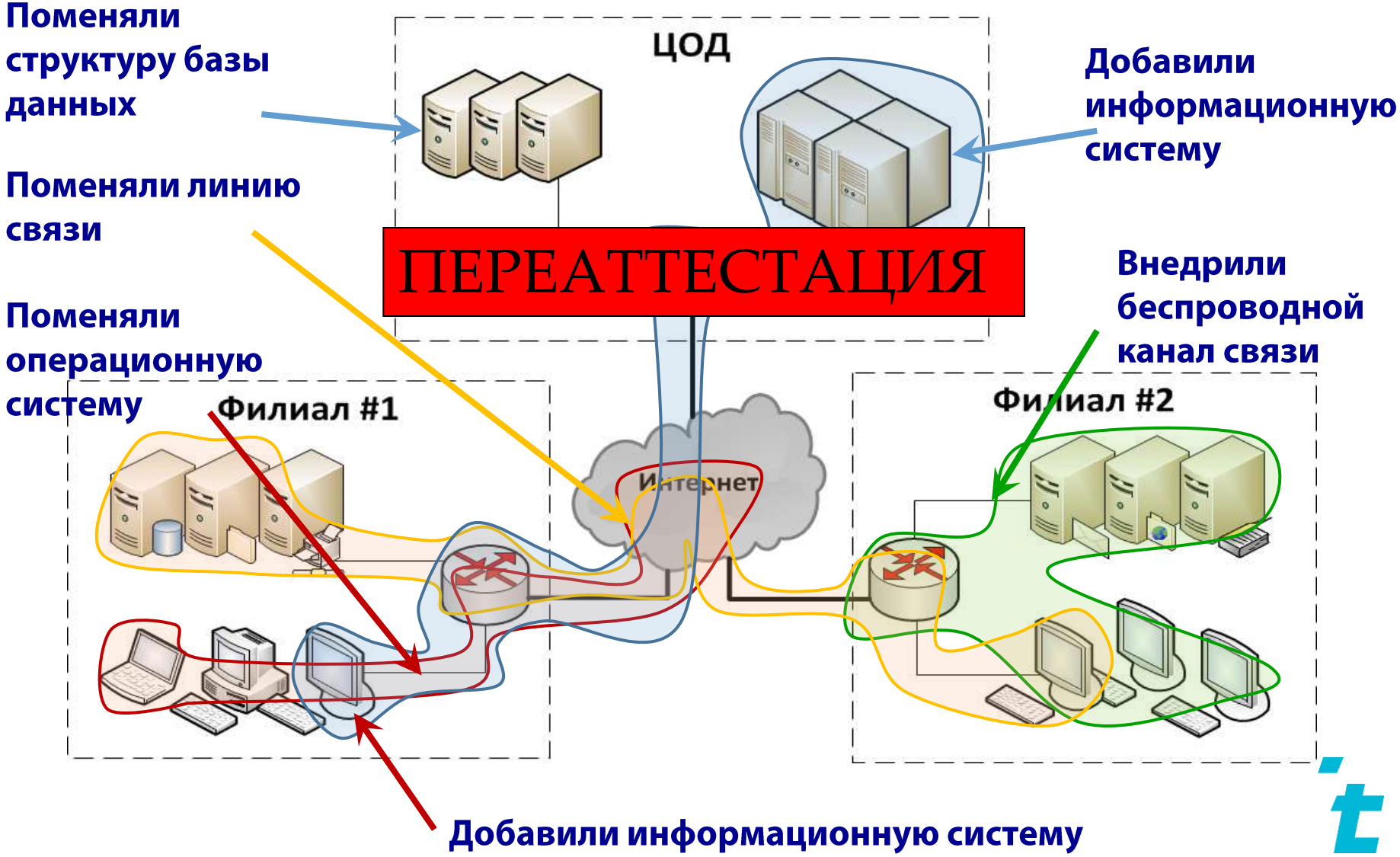


**Без дополнительных аттестационных испытаний**



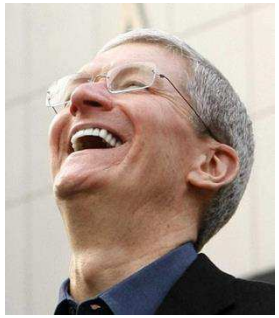
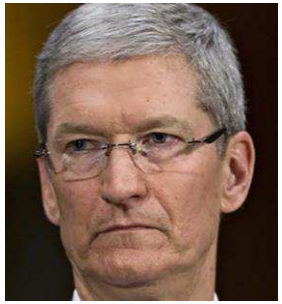
# Подход #3 - Выделение перечня типовых сегментов «защищаем технологии»





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



| 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

# Конкретизация подхода #3 для РИС



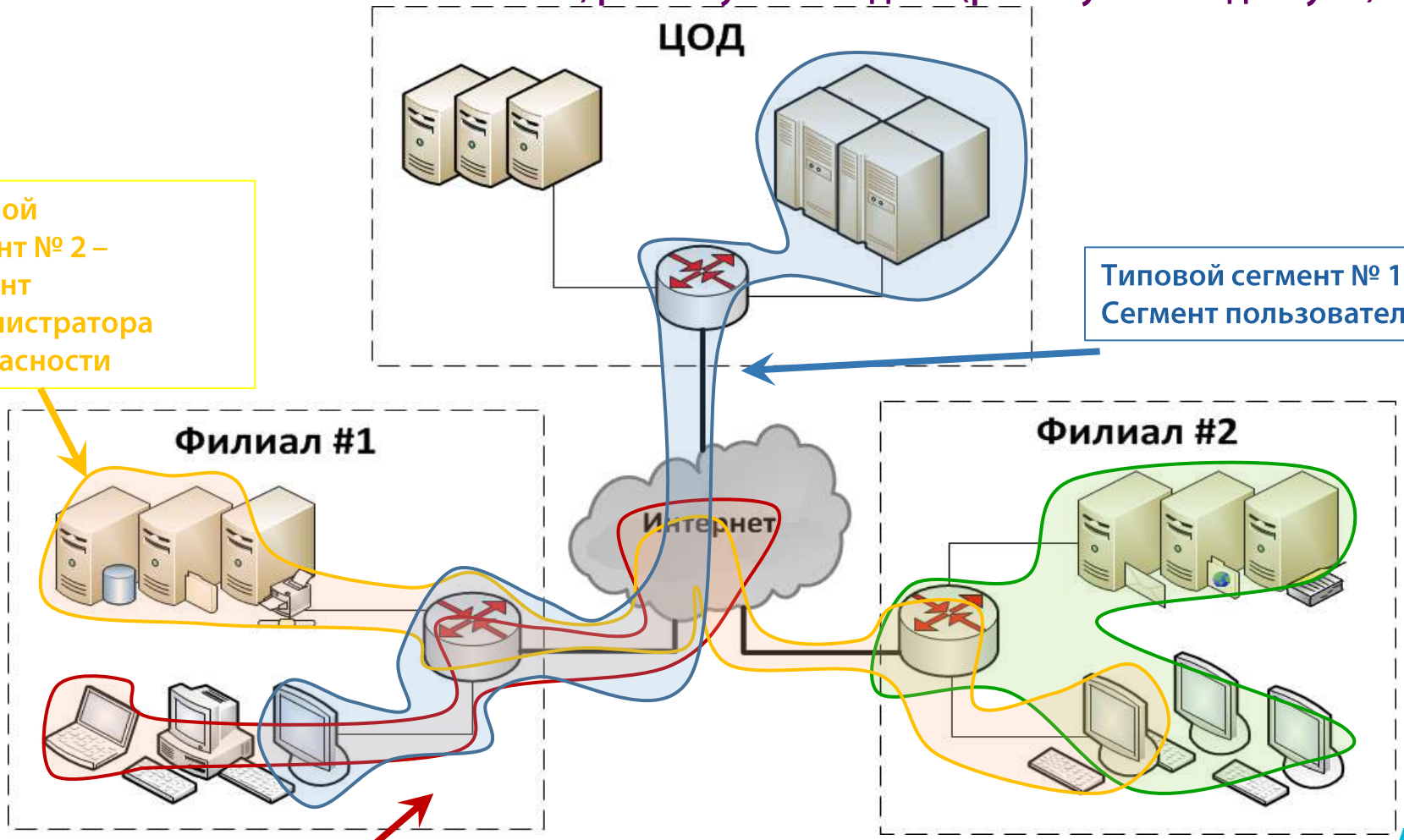
Условия соответствия сегмента *типовому* сегменту:

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 )



**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

# Конкретизация подхода #3 для РИС



Какие бывают Условия эксплуатации типового сегмента:

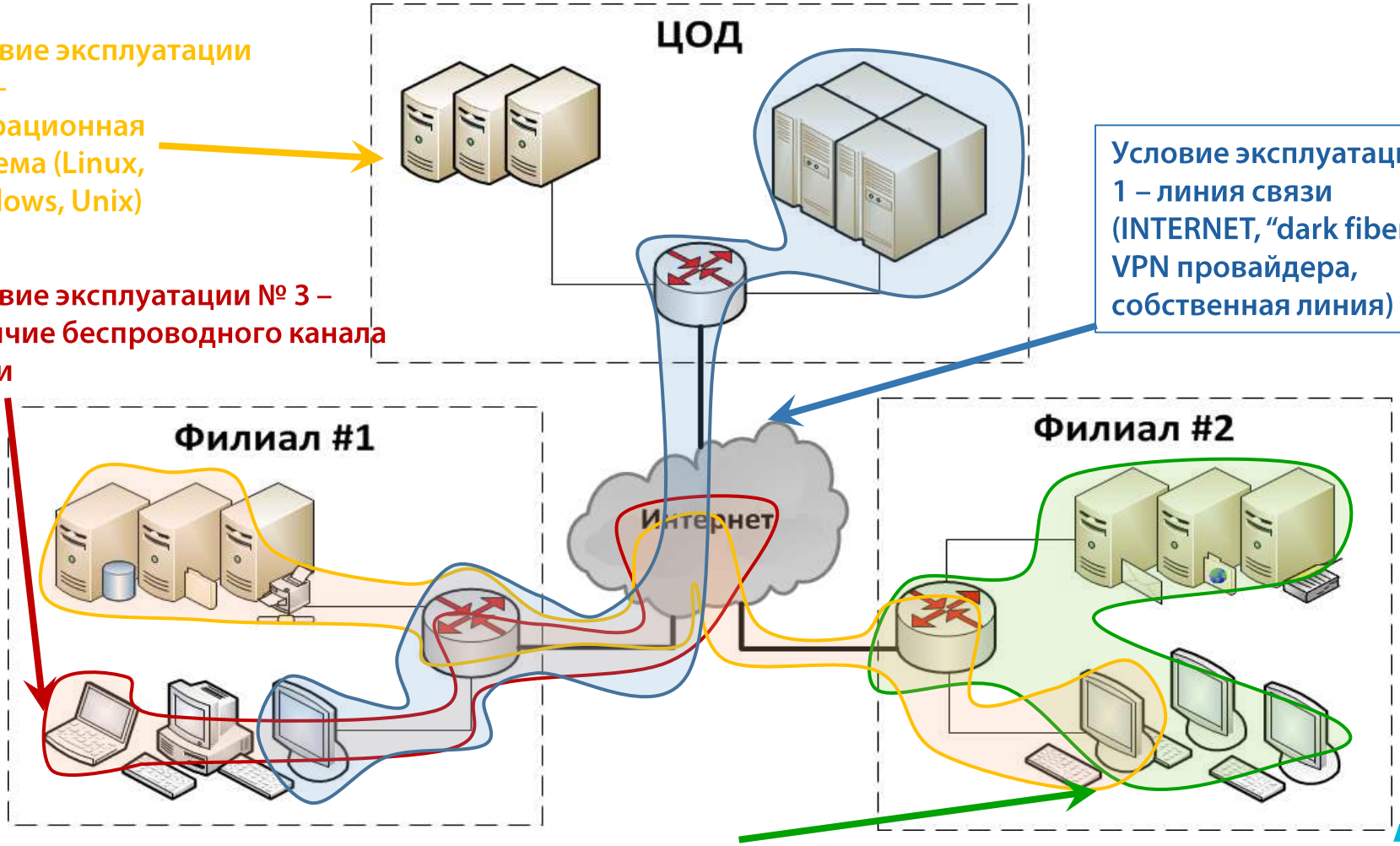
- вид и уровень конфиденциальности информации;
- проектные решения по ИС (технологии обработки , хранения, передачи информации)
- проектные решения по СЗИ (технологии защиты информации)

# Определяем возможные условия эксплуатации типовых сегментов



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



| 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 |

# Порядок разработки СЗИ распределённых ИС по конкретизированному 3-му подходу



**Этап 1** Формирование набора сегментов

(на основе ролей субъектов доступа)

**Этап 2** Определение условий эксплуатации

(в целом с учётом сформированного набора сегментов)

**Этап 3** Составление плана разработки Профилей защиты сегментов (матрицы Профилей)

**Этап 4** Уточнение матрицы (удаление ненужных Профилей)

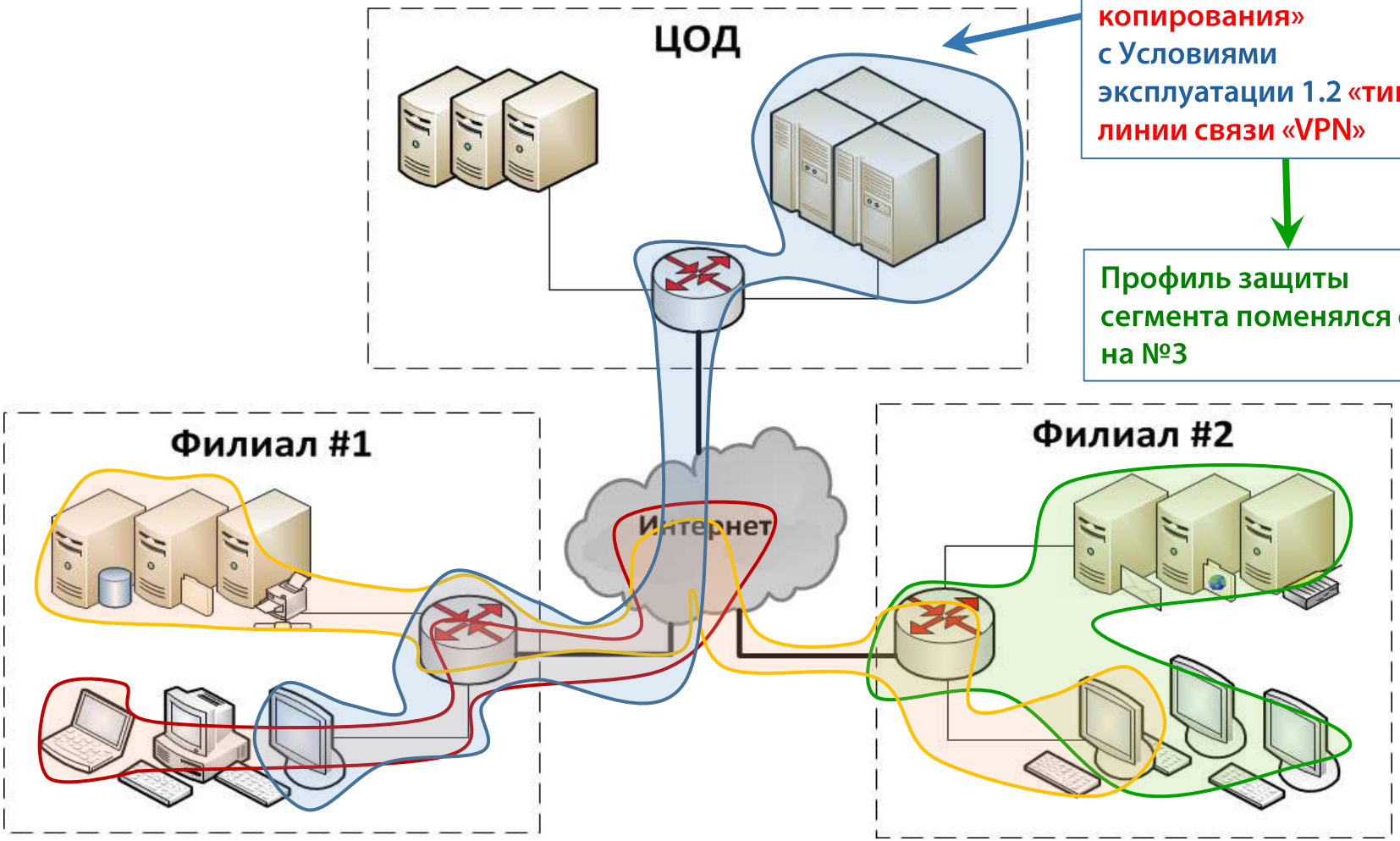
**Этап 5** Разработка Профилей защиты

# Пример: «Внедряем типовой сегмент с новыми условиями эксплуатации»



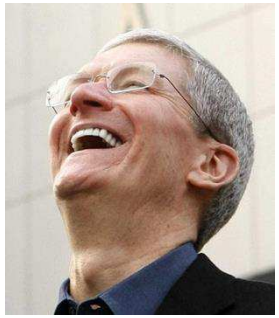
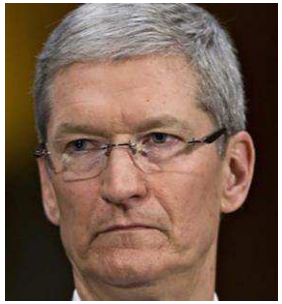
Внедряем Типовой сегмент «Сервер резервного копирования» с Условиями эксплуатации 1.2 «тип линии связи «VPN»

Профиль защиты сегмента поменялся с №2 на №3



# Конкретизация подхода #3 для РИС

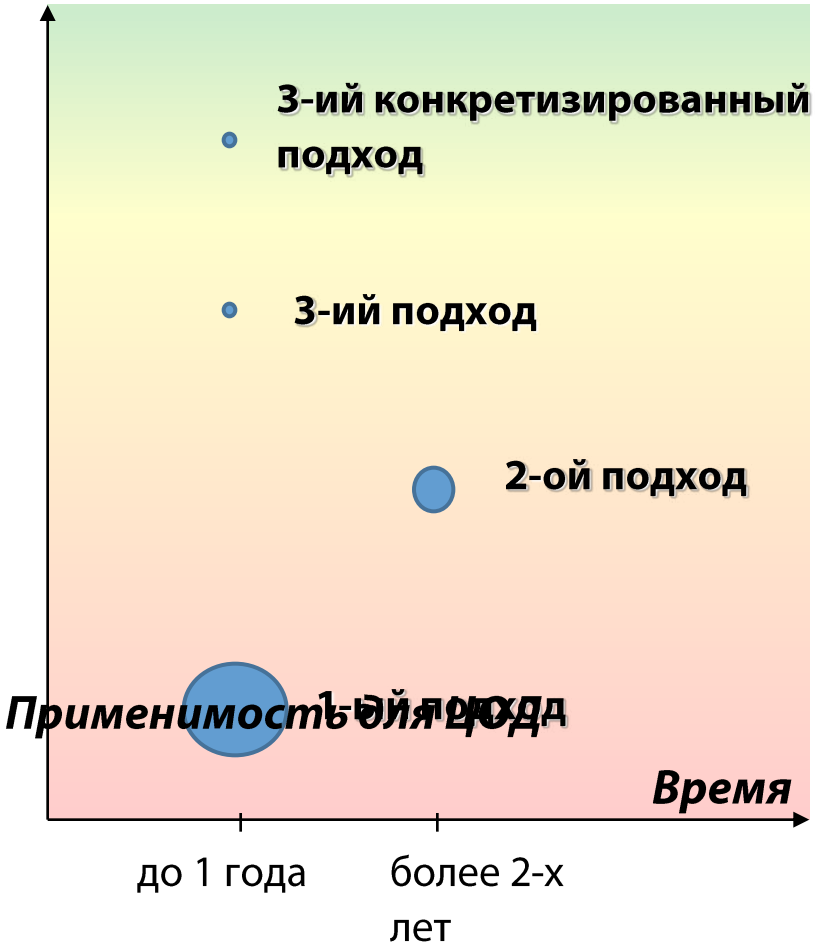


| USER | Компьютер | IT специалист | ИБ специалист | Оператор ИС | Лицензиат |
|---|---|---|---|---|---|
|  |  |  | |  |  |

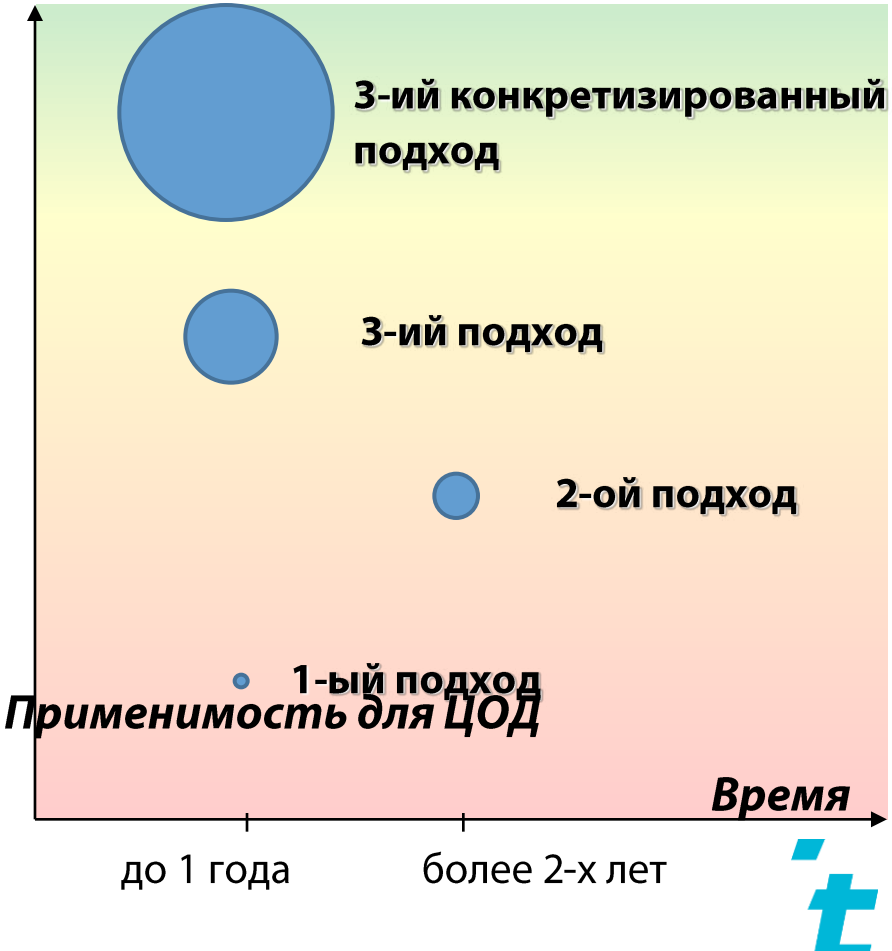
# Преимущества и недостатки подходов



## Затраты Заказчика




## Затраты Лицензиата



**Тезис №1**

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

**Тезис №2**

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

SAVE group

*Спасибо за внимание*

www.saveit.pro