НАЦИОНАЛЬНЫЙ ИННОВАЦИОННЫЙ ЦЕНТР
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Теория и практика аттестации ГИС. Особенности создания систем защиты информации в условиях дефицита сертифицированных по уровням доверия средств защиты информации

АО «НИЦ»

Создана

Q2.2006

Направления деятельности

- Создание комплексных СОИБ
- Консалтинг в области ПДн и КИИ
- Анализ уязвимостей и аттестация
- Организация сертификации
- Производство сертифицированных СрЗИ

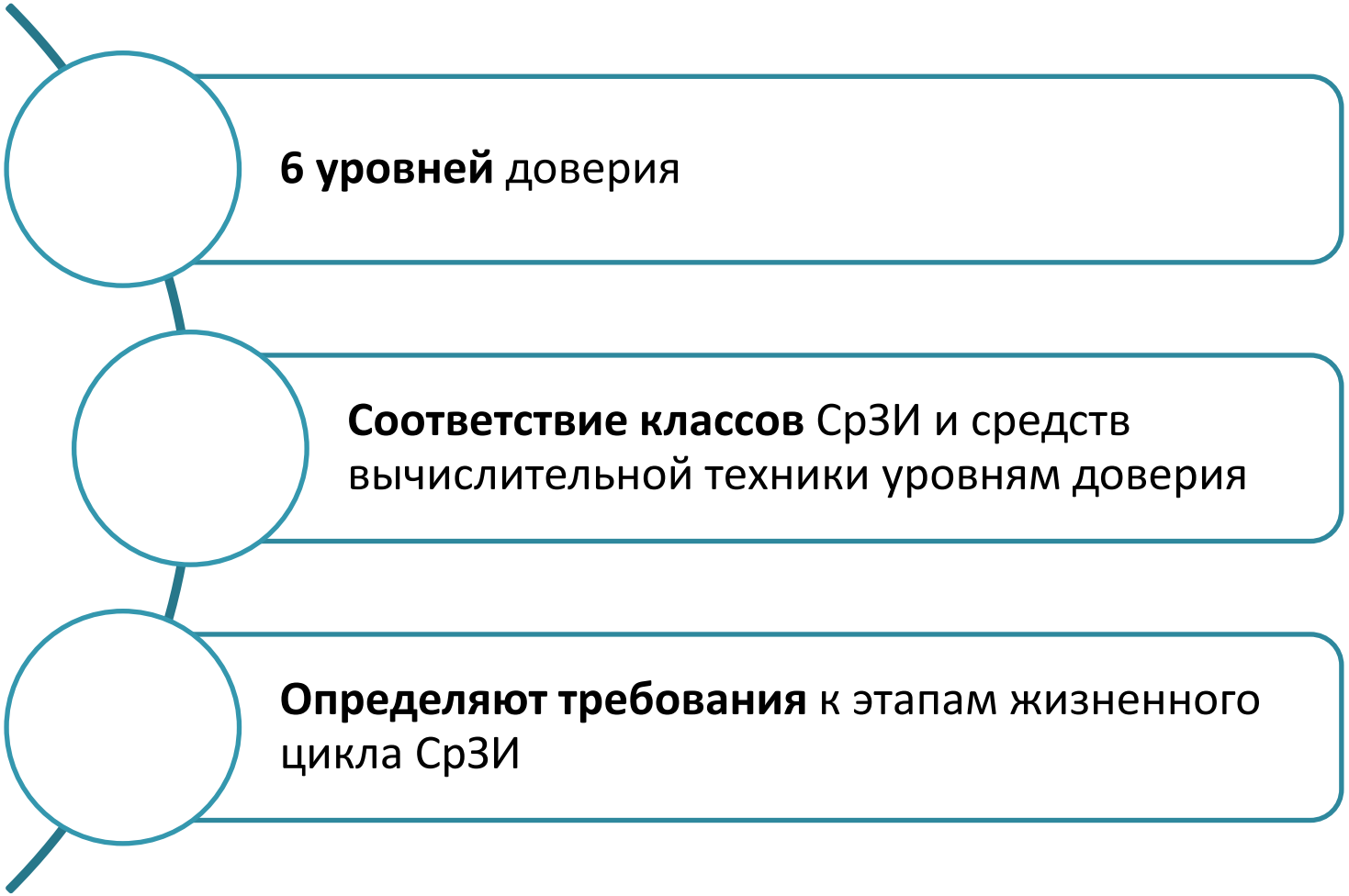
Уровни доверия

Общие критерии
Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий) — международный стандарт (ISO/IEC 15408, ИСО/МЭК 15408-2002)

Приказ ФСТЭК России от 30 июля 2018 г. № 131
«Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»

Приказ ФСТЭК России от 2 июня 2020 г. № 76 новая редакция «Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»

Уровни доверия



Уровни доверия (начало)

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
1.	Требования к разработке и производству средства:			
1.1.	требования к разработке модели безопасности средства			+
1.2.	требования к проектированию архитектуры безопасности средства	+	=	=
1.3.	требования к разработке функциональной спецификации средства	+	+	+
1.4.	требования к проектированию средства	+	=	=
1.5.	требования к разработке проектной (программной) документации	+	+	+
1.6.	требования к средствам разработки, применяемым для создания средства	+	=	=
1.7.	требования к управлению конфигурацией средства	+	+	+
1.8.	требования к разработке документации по безопасной разработке средства	+	=	+
1.9.	требования к разработке эксплуатационной документации	+	=	=

Уровни доверия (продолжение)

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
2.	Требования к проведению испытаний средства:			
2.1.	требования к тестированию средства	+	+	+
2.2.	требования к испытаниям по выявлению уязвимостей и недекларированных возможностей средства	+	+	+
2.3.	требования к проведению анализа скрытых каналов в средстве			+
3.	Требования к поддержке безопасности средства:			
3.1.	требования к устранению недостатков средства	+	+	+
3.2.	требования к обновлению средства	+	+	+
3.3.	требования к документированию процедур устранения недостатков и обновления средства	+	=	=
3.4.	требования к информированию об окончании производства и (или) поддержки безопасности средства	+	=	=

Требования к средствам защиты информации

Обязательная сертификация

- Государственные информационные системы (Приказ ФСТЭК России от 11 февраля 2013 года №17)

Оценка соответствия

- Информационные системы персональных данных (Приказ ФСТЭК России от 18 февраля 2013 года №21)
- Объекты критической информационной инфраструктуры (Приказ ФСТЭК России от 25 декабря 2017 года №239)
- Автоматизированные системы управления производственными и технологическими процессами (Приказ ФСТЭК России от 14 марта 2014 года №31)

Формы оценки соответствия

ИСПДн и автоматизированные системы управления

- Любая форма оценки в соответствии с Федеральным законом «О техническом регулировании» от 27.12.2002 №184-ФЗ, например, испытания или приемка

Значимые объекты КИИ

- Формы оценки соответствия: испытания или приемка
- **С 1 января 2023 г.:**
  - Соответствие УД6 или выше для СрЗИ, не встроенных в общесистемное и прикладное ПО;
  - К прикладному ПО предъявляются требования по безопасности:
    - Процедуры безопасной разработки ПО
    - Выявление уязвимостей:
      - Статический анализ **исходного кода**
      - Фаззинг-тестирование
      - Для ЗОКИИ 1 категории – динамический анализ исходного кода
    - Процедуры поддержки безопасности ПО

Условия испытаний

Условия испытаний:

- Испытания (приемка) СЗИ на соответствие требованиям к уровню доверия и требованиям к функциям безопасности проводятся на этапе предварительных испытаний;
- Испытания (приемка) проводятся отдельно или в составе объекта;
- Программа и методики испытаний (приемки) утверждаются оператором в случае самостоятельного проведения испытаний. В случае проведения испытаний иным лицом, программа и методики испытаний (приемки) утверждаются этим лицом по согласованию с оператором;
- Протокол испытаний утверждается оператором в случае самостоятельного проведения испытаний. В ином случае протокол испытаний утверждается лицом, проводившим испытания

Содержание протокола:

- По результатам испытаний (приемки) средства защиты информации оформляется протокол испытаний, в котором указываются:
  - дата и место проведения испытаний (приемки);
  - описание испытываемого средства защиты информации;
  - описание проведенных испытаний;
  - результаты испытаний по каждому испытываемому параметру (характеристике);
  - выводы о соответствии (несоответствии) средства защиты информации требованиям по безопасности информации.

Рекомендации по составу проверок

№ п/п	Наименование проверки	Пункт требований ЧТЗ	Содержание испытаний	Критерий достижения положительного результата
А 1	**Проверка функций защиты информации**			
А 1.1	**Идентификация и аутентификация субъектов доступа и объектов доступа**			
А 1.1.1	Идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1) и Защита обратной связи при вводе аутентификацион-ной информации (ИАФ.5)	п.1 Приложения 1	1. В веб-браузере перейти по адресу Системы. Должна отобразиться форма приглашения на авторизацию. 2. В поле **Логин** ввести логин пользователя с правами администратора, в поле **Пароль** ввести действующий пароль. Убедиться, что при вводе пароля вводимые символы пароля отображаются условными знаками «•». 3. При успешном входе в Систему перейти в панель администрирования Системы и в меню навигации перейти в Настройки > Инструменты > Журнал событий. Удостовериться, в журнале аудита имеется запись о входе в Систему администратора с отображением даты и времени события, субъекта события (логин), типа и описания события.	1. При выполнении действий по п.2 доступ в Систему осуществляется посредством идентификации и аутентификации пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей. 2. При выполнении действий по п.2 аутентификация пользователей осуществляется с использованием паролей. В процессе ввода аутентификационной информации осуществляется ее защита от возможного использования лицами, не имеющими на это полномочий, посредством отображения для пользователя действительного значения аутентификационной информации (пароля) в виде условных знаков «•». 3. При выполнении действий по п. 3 подтверждено, что в Системе обеспечена

Требования к оценке эффективности мер

Обязательная аттестация

- Государственные информационные системы:
  - Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 г. Москва «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
  - Приказ ФСТЭК России от 11 февраля 2013 года №17

Добровольная аттестация или иная форма

- Информационные системы персональных данных
  - Приказ ФСТЭК России от 18 февраля 2013 года №21
- Объекты критической информационной инфраструктуры
  - Приказ ФСТЭК России от 25 декабря 2017 года №239
- Автоматизированные системы управления производственными и технологическими процессами
  - Приказ ФСТЭК России от 14 марта 2014 года №31

Условия оценки эффективности мер

Состав испытаний:

- Предварительные испытания;
- Опытная эксплуатация;
- Анализ уязвимостей;
- Приемочные испытания
  - В ходе приемочных испытаний объекта и СЗИ должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие объекта и его СЗИ требованиям

Состав проверок:

- Оценка документации:
  - модель угроз безопасности информации, акт классификации, ТЗ на создание и (или) ТЗ (ЧТЗ) на создание СЗИ, проектная и эксплуатационная документация на СЗИ, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы предшествующих предварительных испытаний
- Оценка условий функционирования;
- Оценка реализации мер защиты информации

Изменения с 1 января 2021 г.

Изменения с 1 января 2021 г.

- В информационных системах 1 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 4 или более высокому уровню доверия. В информационных системах 2 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В информационных системах 3 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.

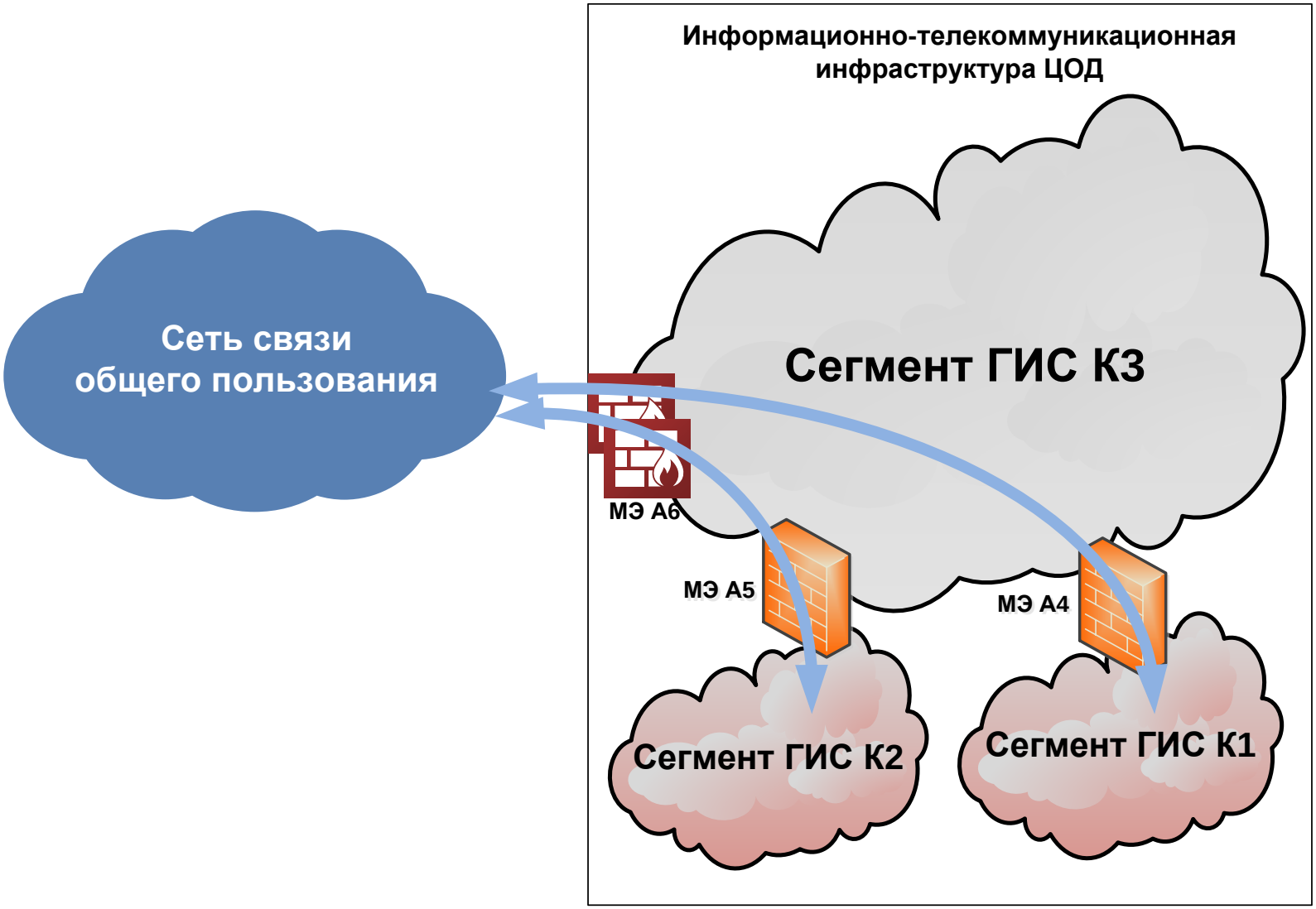
Вопросы рынка

- Можно ли продолжать использовать, доустанавливать средства защиты не приведенные в соответствие Требованиям доверия после 1 января 2021 года, если:
  - Средства защиты были установлены до 1 января 2021 года;
  - Средства защиты устанавливаются для совместимости с установленными до 1 января 2021 года средствами защиты информации при масштабировании информационных систем;
  - При управлении конфигурацией (модернизации) ранее аттестованных информационных систем:
    - Смена мест размещения компонент;
    - Изменение конфигурации системы (количества компонент систем и сетей, состава и(или) версий используемого ПО);
    - Доработка прикладного программного обеспечения;
    - Иные изменения не влекущие появление новых актуальных угроз, на противодействие которым направлено использование ранее установленных средств защиты информации

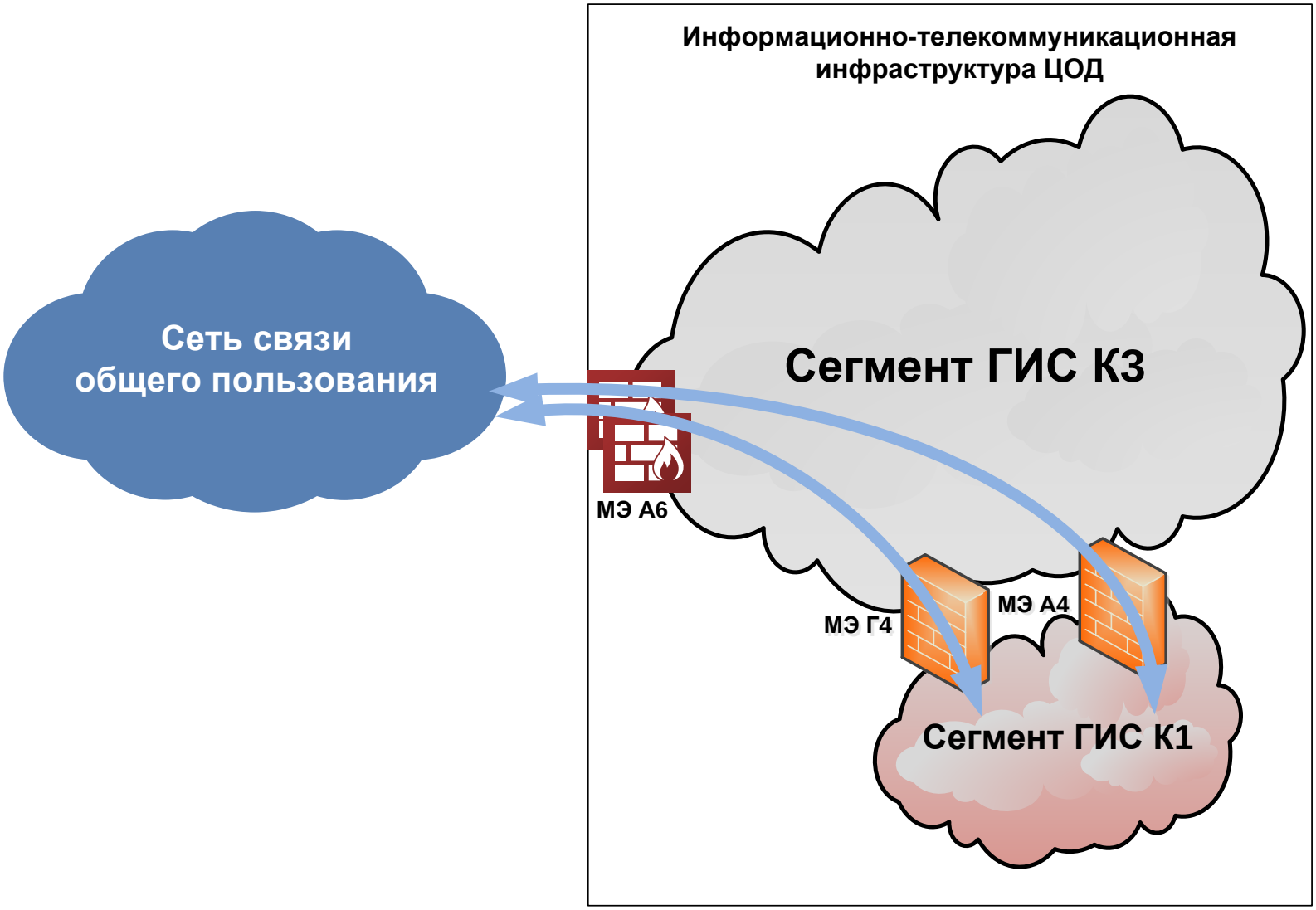
Действия в условиях дефицита

- Максимальное использование допустимых сценариев применения СрЗИ, не приведенных в соответствие Требованиям доверия
- Сегментирование информационных систем, с выделением сегментов, требующих защиты по классу ГИС К3
- Использование иной формы оценки средств защиты информации, отличной от обязательной сертификации (не применимо для ГИС)

Варианты сегментирования



Варианты сегментирования



НАЦИОНАЛЬНЫЙ ИННОВАЦИОННЫЙ ЦЕНТР
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Спасибо за внимание!

АО «НИЦ»
Тел.: +7 (495) 204-20-86
E-mail: info@centin.ru