

АБИСС

Приказ ФСТЭК № 117 - новые правила игры для госсектора с 1 марта 2026 года

Модератор: Александр Хонин, директор центра консалтинга, Angara Security

Спикер: Андрей Рябов,
руководитель группы по обеспечению комплексной безопасности, Angara Security

Спикер: Александр Осипов,
Руководитель направления комплаенса и методологии,
РАД КОП

Ассоциация пользователей стандартов по ИБ АБИСС

Объединяем профессионалов для создания
цивилизованного рынка аудита
информационной безопасности

О нас

Ассоциация пользователей стандартов по информационной безопасности АБИСС – это сообщество профессионалов, основной задачей которого является развитие и совершенствование сферы применения стандартов информационной безопасности за счет постоянного взаимодействия членов, партнеров и поднадзорных организаций.

Мы объединяем

- ✓ Регуляторов ИБ
- ✓ Поднадзорные организации
- ✓ ИТ/ИБ компании
- ✓ Ассоциации и СМИ

АБИСС

Пятая межотраслевая конференция по регуляторике в сфере информационной безопасности, объединяющая на своей площадке специалистов, деятельность которых сопряжена с обеспечением соответствия ИБ-требованиям.



Сегодня обсудим

01

Кто подпадает под действие нового приказа

02

Ключевые отличия от Приказа ФСТЭК № 17

03

Особенности при взаимодействии с внешними организациями

04

Вопросы аттестации

05

Анализ уязвимостей как обязательный элемент системы защиты ИС

06

Взаимодействие с ГосСОПКА и ЦМУ ССОП

07

Требования к персоналу

08

Чек-лист: что сделать в ближайшее время

Новый Приказ ФСТЭК № 117:

- ✔ Приказ ФСТЭК № 117 Вступил в силу с 01 марта 2026 года и полностью заменил Приказ ФСТЭК № 17
- ✔ Методический документ ФСТЭК от 12 апреля 2026 г.
- ✔ Расширяется перечень организаций, на которые распространяется действие приказа (по сравнению с приказом №17)
- ✔ Абсолютно новый подход по защите информации в ГИС и ИС Госсектора



Кто подпадает под действие нового приказа:

Приказ ФСТЭК № 17

- ✓ Государственные информационные системы

Приказ ФСТЭК № 117

- ✓ Государственные информационные системы
- ✓ ИС государственных органов
ИС государственных унитарных предприятий
ИС государственных учреждений
Муниципальные информационные системы
- ✓ ИС подрядчиков (разработчиков и интеграторов)
ИС организаций, взаимодействующих с вышеперечисленными ИС

Ключевые отличия от Приказа № 17

- ✓ **Меры ЗИ:** Приказ № 117 больше не содержит итоговой таблицы защитных мер (Меры ЗИ «перетекли» в Методический документ ФСТЭК от 12 апреля 2026 г.)
- ✓ **Требования к наличию ОРД:** Приказ № 117 устанавливает трехуровневую систему документации, включающую политику защиты информации, внутренние стандарты и внутренние регламенты
- ✓ **Отчетность перед ФСТЭК:** Две сквозные метрики: Кзи (раз в полгода) + Пзи (раз в 2 года)
- ✓ **Сроки по устранению уязвимостей:** Критические — 24 часа, высокие — 7 дней. Новые уязвимости (не в базе ФСТЭК) → сообщить регулятору за 5 рабочих дней
- ✓ **Контроль подрядчиков:** Обязательные требования в договорах — подрядчик под надзором
- ✓ **Кадровые требования:** Не менее 30% сотрудников ИБ — профильное образование или переподготовка

Ключевые отличия от Приказа № 17

- ✓ **Контекст современных технологий:** ИИ, контейнеризация, облачные технологии, IoT
- ✓ **Инфраструктурные меры ЗИ:** акцент на «современных» NGFW, WAF, EDR, защиты конечных точек, усиленной аутентификации/MFA
- ✓ **Информирование:**
 - ГосСОПКА об инцидентах
 - ФСТЭК о новых уязвимостях
 - Центр мониторинга и управления сетью связи общего пользования в части DDOS-атак

Технические меры защиты

✓ В приказе № 117 выделяется 17 ключевых базовых мер, включая новые технологические аспекты:

- Идентификация и аутентификация
- Управление доступом
- Регистрация событий безопасности
- Защита виртуализации и облачных вычислений **(New)**
- Защита технологий контейнерных сред и их оркестрации **(New)**
- Защита сервисов электронной почты **(New)**
- Защита веб-технологий **(New)**
- Защита программных интерфейсов взаимодействия приложений **(New)**
- Защита конечных устройств **(New)**
- Защита мобильных устройств **(New)**
- Защита технологий интернета вещей **(New)**
- Защита точек беспроводного доступа **(New)**
- Антивирусная защита
- Обнаружение и предотвращение вторжений на сетевом уровне
- Сегментация и межсетевое экранирование
- Защита от компьютерных атак, направленных на отказ в обслуживании
- Защита каналов передачи данных и сетевого взаимодействия

Требования к безопасной разработке ПО

- ✓ Единый стандарт — ГОСТ Р 56939-2024 (Разделы 4 и 5): При самостоятельной разработке обязательно следовать Разделам 4 и 5 этого ГОСТа, который описывает 25 процессов безопасной разработки (РБПО)
- ✓ Внедрение практик DevSecOps и использование инструментов анализа кода (SAST/DAST).
- ✓ Строгие требования к подрядчикам: Ответственность за безопасность конечного ПО лежит на госзаказчике, поэтому в договорах с подрядчиками требования по ГОСТ Р 56939-2024 уже должны быть включены в ТЗ
- ✓ Обязательный внутренний регламент (п. 14д): Организации, самостоятельно разрабатывающие ПО, обязаны создать и утвердить внутренний регламент. Этот документ детально прописывает порядок безопасной разработки

Особенности при взаимодействии с внешними организациями

- ✓ Приказ впервые закрепляет необходимость защищать госинформацию на всей цепочке поставщиков
- ✓ Требования распространяются на подрядчиков, которые разрабатывают, сопровождают, администрируют системы заказчика или получают доступ к его данным и инфраструктуре
- ✓ Обязательная разработка политик информационной безопасности у организаций-партнеров
- ✓ Включение в договоры обязательств по обеспечению безопасности информации
- ✓ Фиксация ответственности внешних организаций за соблюдение требований; безопасности при взаимодействии с критическими информационными системами

Новые механизмы контроля со стороны регулятора



Контроль состояния защищенности осуществляется ФСТЭК России по 2-ум показателям, помимо классического контроля при аттестации ГИС .



Показатели ФСТЭК России:

- показатель защищенности (Кзи) (проводится не реже одного раза в шесть месяцев.).
- показатель уровня зрелости (Пзи) (не реже одного раза в два года).



Методика оценки КЗИ утверждена ФСТЭК России 11 ноября 2025 года.



Оценку защищенности может проводить как **оператор ИС**, так и **лицензиат ФСТЭК**.

Новые механизмы контроля со стороны регулятора



Методика расчета показателя уровня зрелости (Пзи) на данный момент не утверждена

Информационное сообщение ФСТЭК России от 22 мая 2026 г. N 240/92/3506

МЕТОДИЧЕСКИЙ ДОКУМЕНТ
(ПРОЕКТ)

МЕТОДИКА
ОЦЕНКИ УРОВНЯ ЗРЕЛОСТИ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ
ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ
СИСТЕМАХ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ
ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ



Оценку уровня зрелости может проводить как **оператор ИС**, так и **лицензиат ФСТЭК**.

Вопросы аттестации

- ✓ Аттестаты соответствия, выданные до 1 марта 2026 года, продолжают действовать. Но если вы планируете создание новой ГИС или модернизацию существующей - проектировать систему защиты информации придется уже по новым требованиям
- ✓ Аттестовывать надо ГИС, остальные ИС на усмотрение Оператора или если есть дополнительные отраслевые требования
- ✓ Инфраструктура ЦОД, где планируется размещать ГИС, также должна быть аттестована на соответствие требованиям Приказа ФСТЭК № 117
- ✓ Информационные системы, аттестованные на соответствие требованиям приказа ФСТЭК № 17, после вступления в силу приказа ФСТЭК № 117 переаттестации не подлежат. Однако последующая аттестация ИС при модернизации будет производиться уже по новым требованиям
- ✓ В рамках аттестации выполняется анализ защищённости с учетом Методического документа ФСТЭК России «Методика анализа защищенности информационных систем» (утв. от 25 ноября 2025 года)
- ✓ В рамках аттестации для ГИС и других ИС госорганов **1 и 2 классов защищенности, которые имеют подключение к сети Интернет**, выполняется тестирование на проникновение (пентест) по методике ФСТЭК

Анализ защищенности по методике ФСТЭК России от 25.11.2025

- ✓ В рамках аттестации выполняется анализ защищённости с учетом Методического документа ФСТЭК России «Методика анализа защищенности информационных систем» (утв. от 25 ноября 2025 года).
- ✓ **Процедура включает:**
 - Инвентаризация ИС (сетевые адреса/порты, ПО, СЗИ, пользователи).
 - Внешний анализ уязвимостей: Сканирование периметра ИС из сети Интернет.
 - Внутренний анализ уязвимостей: Сканирование изнутри периметра (внутренняя инфраструктура).
 - Оценка выявленных уязвимостей: Экспертная оценка критичности на основе угроз
 - Устранение выявленных уязвимостей
 - Повторное сканирование
 - Подготовку отчета
- ✓ Анализ защищенности по Методике может проводить как оператор ИС, так и лицензиат ФСТЭК.

Тестирование на проникновение (пентест) по методике ФСТЭК России

- ✓ Тестирование на проникновение (пентест) проводится по «Методике испытаний систем защиты информации информационных систем методами тестирования на проникновение». Соответствующее информационное сообщение № 240/24/4734 было опубликовано 8 сентября 2025 г.
- ✓ Методика становится **обязательной** для ГИС и других систем госорганов, госпредприятий и госучреждений 1 и 2 классов защищенности, которые имеют подключение к сети Интернет и (или) взаимодействуют с иными ИС, в том числе с ИС подрядных организаций (за исключением случаев, когда такое взаимодействие реализовано с использованием VPN ГОСТ (с применением сертифицированных СКЗИ)).
- ✓ В остальных случаях операторы и владельцы ИС могут принимать решение о применении методики самостоятельно
- ✓ Пентест по Методике может проводить как оператор ИС, так и лицензиат ФСТЭК
- ✓ Пентест проводится как завершающий этап после анализа уязвимостей

Контроль уровня защищенности

✓ Контроль уровня защищенности — это комплексная оценка того, насколько эффективно реализованные меры защиты противостоят реальным угрозам

✓ **Виды и методы контроля:**

1. Автоматизированное/ручное выявление уязвимостей с экспертной оценкой возможности их использования.
2. Выявление несанкционированных подключений устройств к информационным системам.
3. Тестирование путем моделирования актуальных угроз (пентест).
4. Тренировки по отработке действий в условиях реализации угроз.

✓ **Периодичность:** не реже 1 раза в 3 года или после компьютерного инцидента.

✓ По результатам составляется отчет, который подписывается проводившими контроль лицами и в течение 3 рабочих дней представляется руководителю. Отчет также направляется в ФСТЭК.

✓ Для контроля уровня защищенности может привлекаться лицензиат ФСТЭК

Взаимодействие с ГосСОПКА и ЦМУ ССОП

- ✓ Абзац 2 пункта 59 Приказа № 117 обязывает всех операторов (госорганы, ГУП, госучреждения) обеспечить взаимодействие с ГосСОПКА и в автоматизированном режиме — с ЦМУ ССОП
- ✓ **Каналы передачи информации ГосСОПКА:**
 - Средства автоматизированного обмена информацией (API).
 - Личный кабинет ГосСОПКА в технической инфраструктуре НКЦКИ.
 - Электронная почта.
 - Почтовые отправления.
 - Телефонная связь (в качестве дополнительного канала).
- ✓ Взаимодействие с ЦМУ ССОП должно осуществляться в автоматизированном режиме

Требования к персоналу

- ✓ Не менее 30% специалистов по ИБ должны иметь профильное ИБ-образование (или пройти переподготовку)
- ✓ Изменения потребуют от многих организаций и их подрядчиков пересмотреть состав и квалификацию своих ИБ-команд
- ✓ Проведение мероприятий по повышению уровня знаний и информированности пользователей ИС

Практический чек-лист: что сделать в ближайшее время

- ✓ Составить реестр всех ИС организации, подпадающих под требования приказа
- ✓ Оценить класс защищённости каждой системы.
- ✓ Провести аудит текущего состояния ИС и СОИБ, сравнить их с обязательными пунктами из Приказа № 117, Методического документа ФСТЭК от 12 апреля 2026 г.
- ✓ Заложить бюджеты на закупку новых сертифицированных СЗИ и услуг (построение/модернизацию СОИБ, пентест, анализ уязвимостей, аттестацию и т.д.)
- ✓ Актуализировать внутренние стандарты и регламенты защиты информации
- ✓ Организовать взаимодействие с ГосСОПКА и ЦМУ ССОП
- ✓ Провести кадровую инвентаризацию и обучение
- ✓ Привести договоры с подрядчиками в соответствие

АБИСС

Контактная информация



a.riabov@angarasecurity.ru



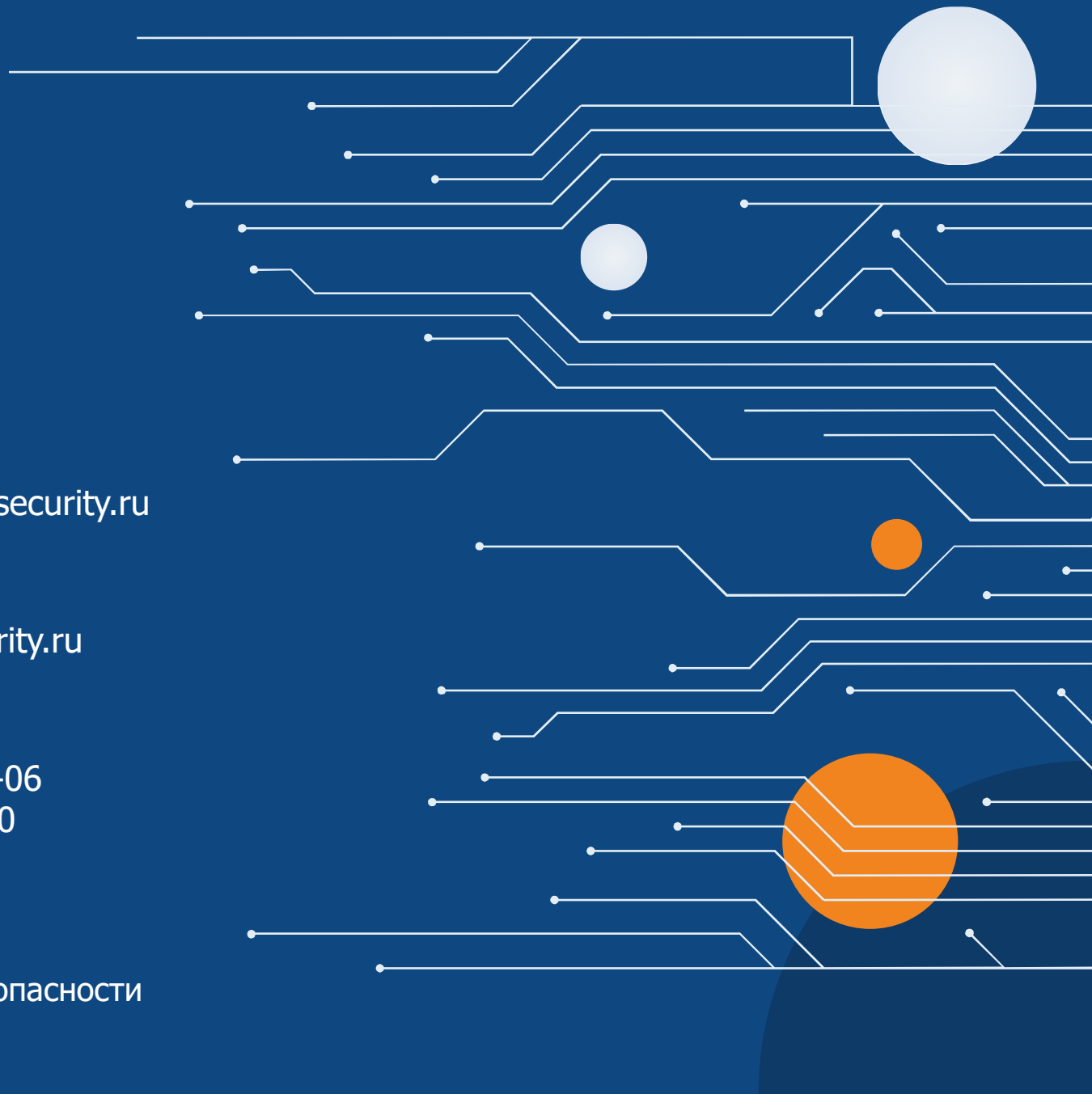
www.angarasecurity.ru



+7 (495) 269-26-06
+7 964 876-90-00

Рябов Андрей,

Руководитель группы по обеспечению комплексной безопасности
Angara Security



АБИСС

Аттестация ИС по требованиям Приказа 117 для подключения к СМЭВ и прикладные аспекты защиты

Александр Осипов,
Руководитель направления комплаенса и методологии, РАД КОП

АБИСС

Кто я ?



15

+ лет в ИБ

10

+ лет руковожу командами

50

+ реализованных проектов



Александр Осипов,

Руководитель направления комплаенса и методологии

О чём поговорим ?

01

Чем обусловлена необходимость проводить аттестацию при подключении к СМЭВ ?

02

Какой контур подлежит аттестации ?

03

Какие средства защиты необходимо применять ?

04

Какие варианты размещения аттестуемого контура ?

Чем обусловлена необходимость проводить аттестацию при подключении к СМЭВ ?

Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»



5. **Требования** о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, **устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации**, в пределах их полномочий. При создании и эксплуатации государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений применяемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Чем обусловлена необходимость проводить аттестацию при подключении к СМЭВ ?

Приказ ФСТЭК от 11 апреля 2025 г. № 117
«Об утверждении Требований о защите информации,
содержащейся в государственных информационных
системах, иных информационных системах
государственных органов, государственных унитарных
предприятий, государственных учреждений»



2. **В случае передачи из государственной информационной системы информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации** (далее - информация ограниченного доступа), **информационная система, в которую передается информация ограниченного доступа, должна соответствовать требованиям о защите информации, установленным в соответствии с частью 5 статьи 16** Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Состав передаваемой информации ограниченного доступа, цели ее защиты и **уровень защищенности** в соответствии с Требованиями **должны устанавливаться** обладателем информации, заказчиком, заключившим контракт на создание информационных систем, **оператором** информационных систем (далее - оператор (обладатель информации)).

Чем обусловлена необходимость проводить аттестацию при подключении к СМЭВ ?

Установленные МВД России требования для информационных систем, получающих сведения «Проверка действительности паспортов для банков»

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Необходимо привести заявку на предоставление доступа в полное соответствие с Пунктом 5.4 «Шаблон заявки на предоставление (изменение) доступа к информации в Единой системе межведомственного электронного взаимодействия (обязателен для заполнения)» Руководства пользователя вида сведений в единой системе межведомственного электронного взаимодействия Сведения «Проверка действительности паспорта для банков». 2. В соответствии с Федеральным законом от 8 августа 2024 г. № 216-ФЗ частью 8.1 статьи 14 Федерального закона от 27 июля 2006 г. № 149-ФЗ установлен запрет на передачу сведений из государственных информационных систем в иные информационные системы, не соответствующие требованиям о защите информации, указанным в статье 16 Федерального закона № 149-ФЗ. Приказом ФСТЭК России от 11 апреля 2025 г. № 117 (ранее от 11 февраля 2013 г. № 17) утверждены Требования о защите информации. Согласно пункту 2 Требований информационная система, в которую передается информация, должна соответствовать требованиям о защите информации, установленным в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ. При этом состав передаваемой информации, цели ее защиты и уровень защищенности в соответствии с Требованиями устанавливаются обладателем информации. Обращаем внимание, что информационная система МВД России имеет класс защищенности – К1, уровень значимости – У31, класс автоматизированной системы – 1Г, первый уровень защищенности персональных данных и аттестована в соответствии с требованиями о защите информации ФСТЭК России, как государственная информационная система. Учитывая изложенное, принимая во внимание положения части 8.1 статьи 14 Федерального № 149-ФЗ, информационная система потребителя должна соответствовать требованиям нормативных правовых актов в сфере защиты информации с учетом вышеуказанной классификации. В этой связи просим приложить копию аттестата соответствия информационной системы требованиям по защите информации класса защищенности К1.

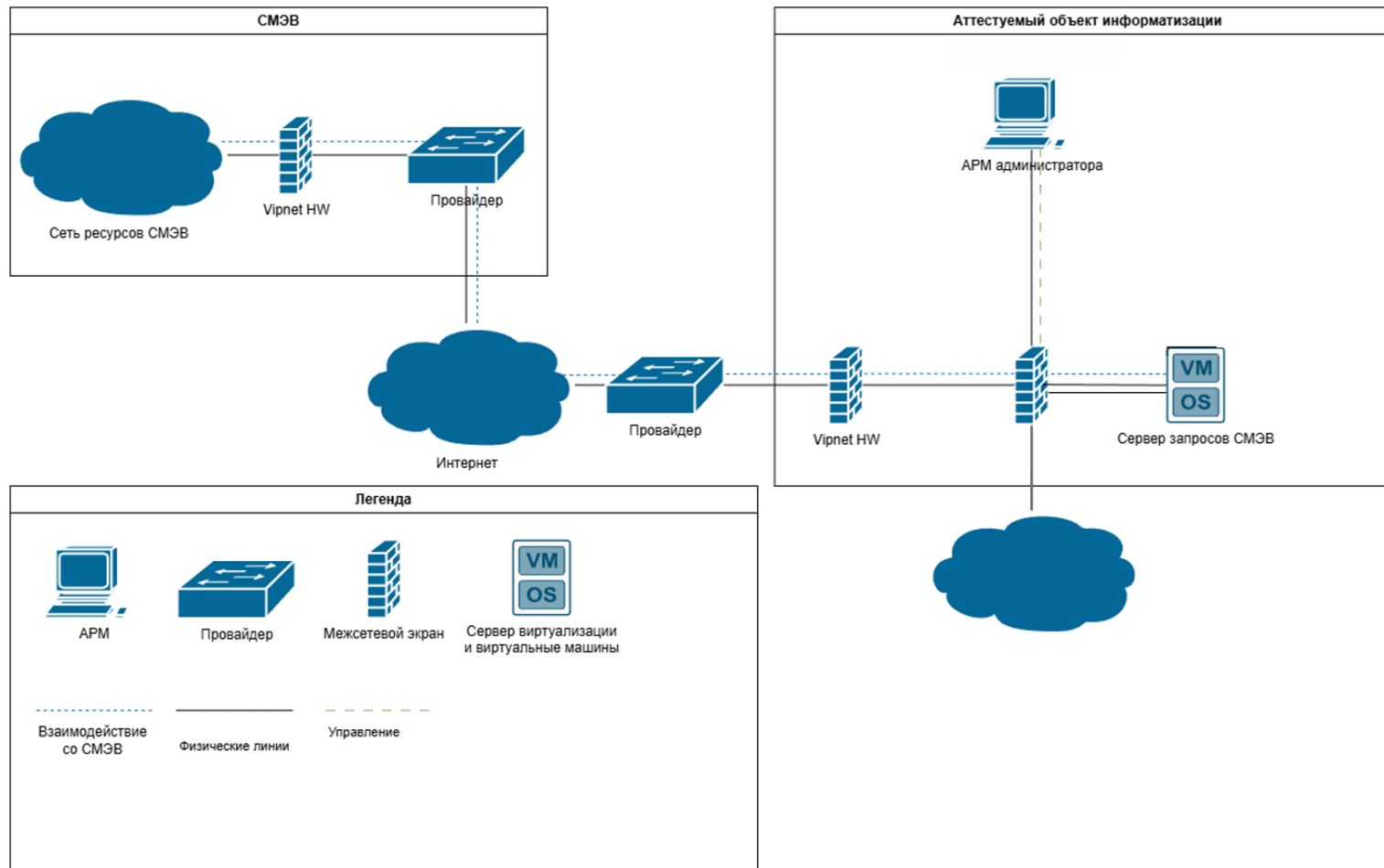


Как осуществляется аттестация ?

- 01** Лицензиатом ФСТЭК (с буквой «г» в лицензии) в соответствии с Приказом ФСТЭК 77
- 02** Аттестация включает подготовку объекта информатизации к аттестации его владельцем
- 03** Предоставление в орган по аттестации необходимых документов и сведений для подготовки программы и методики аттестационных испытаний
- 04** Проведение аттестационных испытаний и выдачу Аттестата соответствия (в случае отсутствия недостатков, которые невозможно устранить)



Какой контур подлежит аттестации ?



Какие документы необходимо подготовить ?

III. Проведение работ по аттестации объектов информатизации

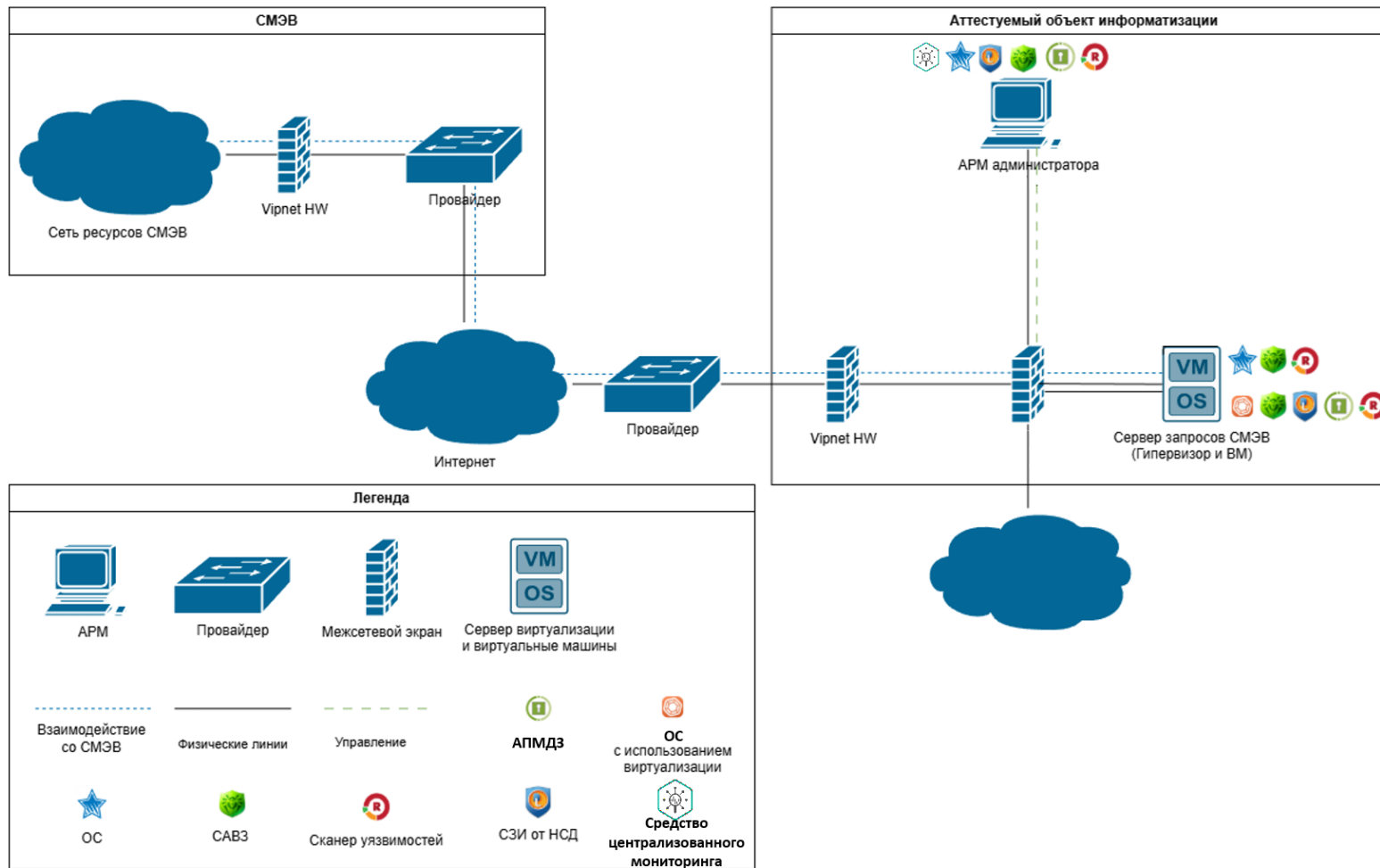
11. Для проведения работ по аттестации владелец объекта информатизации представляет в орган по аттестации следующие документы или их копии:

- а) технический паспорт на объект информатизации по форме согласно приложениям N 1, 2 к настоящему Порядку;
- б) акт классификации информационной (автоматизированной) системы по форме согласно приложению N 3 к настоящему Порядку, акт категорирования значимого объекта критической информационной инфраструктуры Российской Федерации (далее - акт категорирования значимого объекта);
- в) модель угроз безопасности информации (в случае ее разработки в соответствии с требованиями по защите информации);
- г) техническое задание на создание (развитие, модернизацию) объекта информатизации и (или) частное техническое задание на создание (развитие, модернизацию) системы защиты информации объекта информатизации (для объекта информатизации, входящего в состав объекта капитального строительства, задание на проектирование (реконструкцию) объекта капитального строительства) (в случае их разработки в ходе создания объекта информатизации);
- д) проектную документацию на систему защиты информации объекта информатизации (в случае ее разработки в ходе создания объекта информатизации);
- е) эксплуатационную документацию на систему защиты информации объекта информатизации и применяемые средства защиты информации;
- ж) организационно-распорядительные документы по защите информации владельца объекта информатизации, регламентирующие защиту информации в ходе эксплуатации объекта информатизации, в том числе план мероприятий по защите информации на объекте информатизации, документы по порядку оценки угроз безопасности информации, управлению (администрированию) системой защиты информации, управлению конфигурацией объекта информатизации, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации (далее - документы по защите информации владельца объекта информатизации);
- з) документы, содержащие результаты анализа уязвимостей объекта информатизации и приемочных испытаний системы защиты информации объекта информатизации (в случае проведения анализа и испытаний в ходе создания объекта информатизации).

По решению владельца объекта информатизации указанные в настоящем пункте документы (их копии) представляются в орган по аттестации в виде электронных документов.

12. На основе анализа документов, предусмотренных пунктом 11 настоящего Порядка, и предварительного ознакомления с объектом информатизации в условиях его эксплуатации орган по аттестации разрабатывает программу и методики аттестационных испытаний.

Какие средства защиты необходимо применить ?



Итоги

Требования
устанавливаются
оператором (обладателем
информации) ГИС



Могут быть установлены
требования по защите информации
при передаче информации в
сторонние информационные
системы, в том числе требования по
аттестации информационной
системы

Уже сейчас стоит
проверить и уточнить
требования, которые будут
установлены



Информация о тех требованиях,
которые необходимо соблюдать
может поступить неожиданно и
лучше подготовиться заранее,
чтобы продолжать получать
информацию из ГИС

После уточнения требований
необходимо привести
подключаемую
информационную систему в
соответствие



В случае необходимости провести
аттестацию подключаемой
информационной системы –
выбрать и подготовить объект
информатизации и его
документацию к аттестации

АБИСС

Спасибо!



АБИСС

Контактная информация

Демидова Алина Юрьевна,

Администратор Ассоциации



+7 (495) 925-77-90 доб. 242



www.abiss.ru



abiss@abiss.ru

