

АТТЕСТАЦИЯ ДЛЯ ДОСТУПА К СМЭВ И ГИС: ТРЕБОВАНИЯ, ОШИБКИ, ПРАКТИКА

Илья Романов
Руководитель отдела консалтинга

Радик Садыков
Специалист группы проектирования отдела
технических решений

Почему отключают от СМЭВ?

- ❖ **СМЭВ – единая платформа для доступа к различным ГИС**
 - В том числе к сервису проверки паспортов МВД.
- ❖ **Как и почему возникают отключения**
 - МВД запрашивает аттестат,
 - При отсутствии – отключают доступ,
 - Блокировка возможна как по сервису проверки паспортов, так и по СМЭВ в целом.
- ❖ **Кого касается**
 - Банки, страховые, операторы связи и все, кто использует СМЭВ.

- ❖ **Базовая норма (ч. 8.1 ст. 14 ФЗ-149)**
 - Нельзя передавать данные из ГИС в системы, не соответствующие требованиям безопасности.
- ❖ **Право владельца ГИС (п. 14.4 Приказа ФСТЭК-17 – утратил силу)**
 - Предъявление дополнительных требований при подключении к системе.
- ❖ **Дополнения с 1 марта 2026 г. (п. 2 Приказа ФСТЭК-117)**
 - Требования ИБ стало больше – и по документам, и по средствам защиты.

Что нужно аттестовать?

- ❖ **Аттестуется система**, которая получает доступ к СМЭВ и осуществляет обмен данными.
- ❖ **Реализация в теории (простой контур):**
 - Адаптер доступа + криптошлюз — фактически единый «шлюз» для взаимодействия.

Что нужно аттестовать?

- ❖ **Аттестуется система**, которая получает доступ к СМЭВ и осуществляет обмен данными.
- ❖ **Реализация в теории (простой контур):**
 - Адаптер доступа + криптошлюз — фактически единый «шлюз» для взаимодействия.
- ❖ **Реализация на практике (сложные контуры):**
 - Несколько ЦОД, распределённая инфраструктура,
 - Несколько серверов и криптошлюзов,
 - Рабочие станции, если они участвуют в процессе взаимодействия.
- ❖ **Важно:** Требования распространяются на все системы, подключённые к ГИС через СМЭВ (не только к сервису проверки паспортов).

Какие документы нужны?

❖ Базовый комплект:

- Модель угроз и нарушителей,
- Техническое задание на защиту,
- Организационно-распорядительные документы (можно дополнить существующие).

Какие документы нужны?

❖ Базовый комплект:

- Модель угроз и нарушителей,
- Техническое задание на защиту,
- Организационно-распорядительные документы (можно дополнить существующие).

❖ Документы аттестации (направляются в ФСТЭК):

- Отчет об анализе уязвимостей,
- Технический паспорт,
- Акт классификации,
- Программа и методики испытаний,
- Протоколы и заключение,
- Аттестат соответствия.

- ❖ **Некорректное наименование системы:**
 - Название в аттестационных документах не совпадает с тем, что было указано при подключении.

- ❖ **Некорректное наименование системы:**
 - Название в аттестационных документах не совпадает с тем, что было указано при подключении.

- ❖ **Неполный учёт требований:**
 - К1, 1-УЗ, 1Г,
 - требования ФСБ, если они применимы.

- ❖ **Некорректное наименование системы:**
 - Название в аттестационных документах не совпадает с тем, что было указано при подключении.

- ❖ **Неполный учёт требований:**
 - К1, 1-УЗ, 1Г,
 - требования ФСБ, если они применимы.

- ❖ **Неполный контур аттестации:**
 - Аттестованы не все системы, участвующие во взаимодействии.

❖ Технические и архитектурные:

- Нет выделенного сетевого сегмента,
- Общая «программная» среда с другими системами,
- Виртуализация и контейнеры, усложняющие выделение контура.

❖ Технические и архитектурные:

- Нет выделенного сетевого сегмента,
- Общая «программная» среда с другими системами,
- Виртуализация и контейнеры, усложняющие выделение контура.

❖ Организационные и процессные:

- Сжатые сроки и необходимость быстро подтверждать соответствие,
- Недостаточное понимание того, что именно является “той самой системой”,
- Особенности взаимодействия с МВД и ФСТЭК (замечания, уточнения).

- ❖ **Не ждать запроса от МВД:**
 - Отключают быстро, реагировать «по факту» поздно.
- ❖ **Определить свой контур:**
 - Какие системы реально участвуют,
 - Что входит в границы аттестации.
- ❖ **Привести систему в соответствие:**
 - Почти всегда требуются доработки: архитектура, СЗИ, документы.
 - Решения должны быть реализуемыми и не ломать процессы,

Техническое обследование Системы

- ❖ **Обследование и технический аудит:**
 - Анализ текущей архитектуры Системы и существующих средств защиты информации.
- ❖ **Анализ существующего парка оборудования:**
 - Оценка возможности использования имеющихся серверов и АРМ;
- ❖ **Подбор нового оборудования:**
 - Определение требований к оборудованию для обеспечения работоспособности Системы

❖ СЗИ от НСД:

- Управление доступом,
- Доверенная загрузка.

❖ Сетевая безопасность:

- Межсетевые экраны (персональные или периметровые),
- Обнаружение вторжений,
- Шифрование при необходимости.

❖ Защита инфраструктуры:

- Антивирусная защита,
- Защита виртуализации / контейнеризации.

❖ Контроль защищенности:

- Сетевые сканеры и средства анализа защищённости.

❖ Все используемые средства защиты должны быть сертифицированы.

❖ Совместимость предлагаемых СДЗ

- Тестирование совместимости программных и аппаратных СДЗ с существующим оборудованием

❖ Выбор оборудования:

- Помощь в подборе нового оборудования, совместимого с СДЗ

❖ Геораспределенная Система:

- Исключение взаимодействия компонентов Системы, размещенных на разных площадках;
- Организация защищенных каналов связи

❖ Наличие уязвимостей:

- Минимизация взаимодействий;
- Обновление ПО;
- Устранение в соответствии с рекомендациями разработчика ПО

г. Москва,
1-й Нагатинский проезд, д.10, стр.1,
БЦ «Ньютон Плаза»

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

<http://www.DialogNauka.ru>
e-mail: info@DialogNauka.ru

