

Машинные идентичности в ГИС: как закрыть группу мер ИАФ на практике

Четыре кейса из практики эксплуатации и разбор протоколов по усилению мер

Иван Черников

Руководитель продукта
Рутoken CLM,
компания «Актив»





Что уже действует и куда требования расширяются

01.03.2026

**Приказ ФСТЭК
России №117**

Требования
к защите информации
в ГИС

12.04.2026

**Методический
документ**

Меры, усиления
и группа ИАФ

Проект

**Приказ
вместо №21**

Опубликован
24.07.2026,
пока не подписан

Далее

**Значимые
объекты КИИ**

Тот же подход
к машинной
аутентификации

Требования к сертификатам машин приходят из регуляторики, а не из PKI-моды

Что, если субъект доступа — это машина?



Меры ИАФ написаны для тех и других, практика управления есть только для первых

Люди

Пароль, OTP, токен

Выдача, блокирование, смена и парольная политика являются знакомыми процессами, за которые есть кому отвечать.

Машины

Сертификат X.509, ключ, mTLS

Серверы, сервисы, контейнеры, сетевое оборудование. Управление их факторами доступа чаще всего ручное и не регламентировано.

Аутентификация людей и сервисов живет по разным правилам

Что требуют меры **группы ИАФ**



Методический документ от 12.04.2026: машинная часть требований и то, как она обычно реализована

Мера	Что требует	Как обычно организовано на деле
ИАФ.2	Идентификация устройств: перечень всех идентификаторов и проверка при каждом подключении	Реестры свои у каждой команды: таблицы, вики, скрипты. Сводной картины по инфраструктуре нет
ИАФ.4	Аутентификация устройства при каждом подключении по поддерживаемым протоколам	Единой политики для всех устройств нет: часть узлов пускают по адресу или общему секрету
Усиления ИАФ.4	Смена данных не реже раза в год, корпоративный УЦ, система централизованного управления ЖЦ	Отсутствие централизации управления секретами. Разные УЦ и разные администраторы

ИАФ.2 и ИАФ.4 могут быть определены по результатам моделирования актуальных угроз безопасности: например, УБИ.046, УБИ.125, УБИ.126, УБИ.128, УБИ.131

Усиления мер: что названо прямо



Для идентификации и аутентификации устройств добавлены новые меры



Отдельный технологический УЦ

Свой центр сертификации как источник доверия для машинных идентичностей во внутренней инфраструктуре



Протоколы

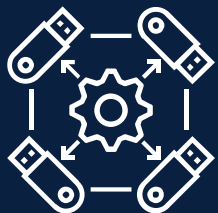
CMP, EST, ACME, MS-WSTEP — это выпуск сертификатов, EAP, 802.1X, TLS — это работа с уже выпущенными



Система управления ЖЦ

Централизованное управление жизненным циклом цифровых сертификатов

Перечень неоднороден: одни протоколы выпускают сертификаты, другие их только предъявляют



**В реальной инфраструктуре тысячи устройств
с разными сроками,
несколько УЦ и сегментов,
но единого реестра сертификатов нет**



Кейс 1. Смена раз в год



ИАФ.4: смена аутентификационных данных не реже раза в год

3 000

сертификатов
в инфраструктуре

÷

250

рабочих дней
в году

=

8

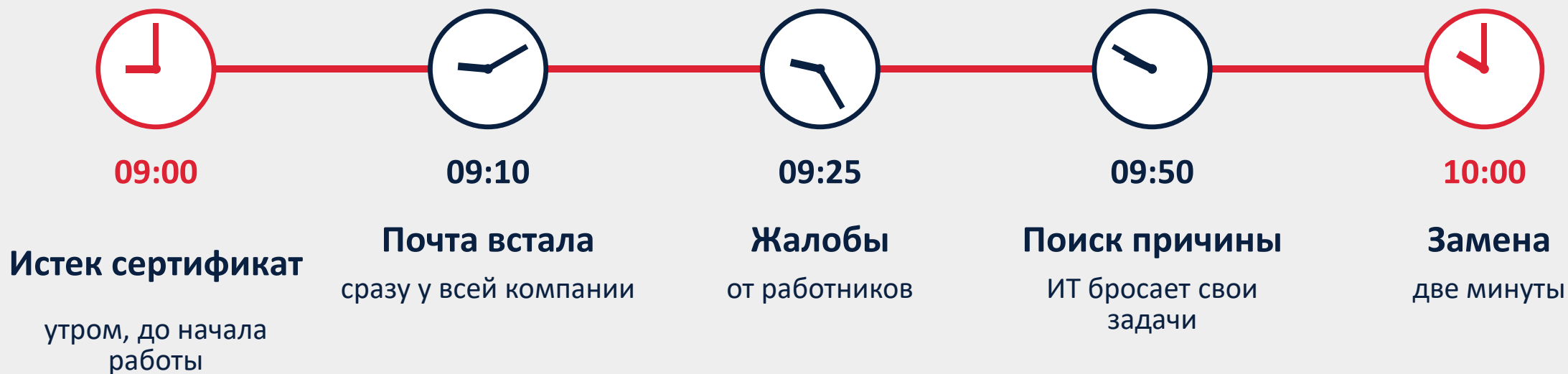
замен каждый
рабочий день

Срок действия — год, но даты выпуска разные, поэтому замены идут неоднородно

«Раз в год» на практике означает каждый день

Кейс 2. Сертификат почтового сервера

ИАФ.4: своевременная замена средств аутентификации.
«Две минуты на замену» — это час, которого нет в отчетах



300

человек без почты весь этот час

Кейс 3. Корневой сертификат VPN

ИАФ.4: действия при компрометации и выводе устройств из эксплуатации

Почему не чинится удаленно



Чтобы обновиться по защищенному каналу, нужен еще действующий сертификат

Что пришлось делать



Разослать новую конфигурацию по почте и попросить каждого перевыпустить свой сертификат самостоятельно

10 минут

на самовыдачу сертификата

350 человек

в компании

58 часов

рабочего времени

Сертификат почты стоил часа. Корневой сертификат VPN стоил недели работы всей компании

Кейс 4. Более 4 УЦ в одной инфраструктуре

ИАФ.2: идентификация устройств

Microsoft CA

серверы и APM в домене

DCOM, WSTEP

Корпоративный УЦ

внутренняя инфраструктура

свой API

Vault PKI

секреты разработки

REST API, ACME

Let's Encrypt

внешний веб-периметр

ACME

УЦ подрядчика

сопровождение систем

Облачный провайдер

внешние сервисы

Тестовый УЦ

стенды разработки

Самоподписанные

то, что сделали руками

И что-то еще

о чем никто не помнит

Сколько технологических сертификатов истекает у вас в следующем месяце?

Свой протокол **под тип узла**



Протокол	Что делает	Где применим
ACME	Выпуск	Внешний веб, Kubernetes Ingress
MS-WSTEP	Выпуск	Узлы в домене Microsoft
EST	Выпуск	Сетевое оборудование, IoT
SCER	Выпуск	Сетевое оборудование без поддержки EST
CMP	Выпуск и отзыв	Промышленные и телеком-системы

Ни один протокол выпуска не покрывает все типы узлов типовой ГИС

Самый частый ответ: «У нас все на ACME»



Возможно, простой и удобный протокол, но его не хватает на все кейсы современной инфраструктуры



Корпоративный УЦ

AD CS штатно ACME не поддерживает: выпуск идет через MS-WSTEP или DCOM



Идентификация

Проверка домена доказывает контроль над именем, а не подлинность устройства



Изолированный контур

Нужна связность с ACME-сервером и работающая DNS-проверка



Инвентаризация

ACME знает только те сертификаты, которые выпустил сам

ACME закрывает публичный веб и Kubernetes. На остальных узлах нужны другие протоколы

Итоги по кейсам



Кейс 1	Срок в год превращается в ежедневную работу	ИАФ.4
Кейс 2	Простой начинается раньше, чем ИТ узнают о проблеме	ИАФ.4
Кейс 3	Истекший корневой сертификат удаленно не восстановить	ИАФ.4
Кейс 4	Несколько УЦ и ни одного общего реестра	ИАФ.2

Все эти проблемы решает единый CLM-слой для выпуска и доставки сертификатов

Что должен уметь CLM-слой



Единое окно ответов на вопросы из четырех кейсов

Что истекает на следующей неделе?

Кейсы 1 и 2



Дашборд сроков по всей инфраструктуре

Откуда этот сертификат и кто владелец?

Кейс 4



Реестр с привязкой к узлу и команде

Ключ скомпрометирован, где он используется?

Кейс 3



Поиск по инфраструктуре и массовый отзыв

Кто и когда менял сертификат на шлюзе?

Кейс 2



Журнал выпуска, установки и отзыва

Именно такую систему методдокумент называет в усилениях мер группы ИАФ

Как построить **управление** сертификатами



1

Кейс 4

Назначить владельца

Сертификаты и ключи во всех контурах

2

Кейс 4

Инвентаризация

Что есть, где стоит, каким УЦ
выпущено

3

Кейсы 2 и 3

Критичные узлы

Корневые сертификаты, VPN, почта,
шлюзы

4

Кейс 1

Описать правила

Сроки, алгоритмы, кто выпускает
и отзывает

5

Кейс 1

Автоматизировать

Выпуск и ротация через подходящий
протокол

6

Кейсы 2 и 3

Контролировать

Единый журнал и уведомления
о сроках

Инвентаризация идет раньше автоматизации

Чем CLM-слой **не должен быть**



Критерии, по которым стоит смотреть на любое решение, включая наше

Вендор-лок

Если слой умеет работать только со своим УЦ, это еще один УЦ, а не управление

Требования к железу

Инвентаризация не должна начинаться с закупки серверов под саму систему

Платформа в нагрузку

Управление сертификатами не должно приезжать вместе с УЦ, хранилищем секретов и мониторингом

Годы вместо недель

Первая картина по инфраструктуре должна появляться за недели, а не за годы внедрения

Эти вопросы стоит задать любому вендору, нам в том числе

Что забрать с собой



Пять вопросов своему ИТ: скорее всего, полной картины нет ни у кого

- 1 Есть ли реестр устройств и сервисов, которые используют сертификаты?
- 2 Что истекает в ближайший месяц и кто узнает об этом первым?
- 3 Как организована смена не реже раза в год и кто ее ведет?
- 4 Какие УЦ выпускают сертификаты для устройств и по каким протоколам?
- 5 Сколько займет восстановление, если истечет корневой сертификат VPN?

С этими вопросами можно за один разговор понять, где вы находитесь

Команда **продукта**



Иван Черников

Руководитель продукта
Рутокен CLM,
компания «Актив»



ich@aktiv-company.ru
info@rutoken.ru



rutoken.ru/products/all/rutoken-clm
www.aktiv-company.ru



+7 925 421-02-61

РУТОКЕН

