

Forest OS Global

Подготовка информационного взаимодействия с ФГИС ЛК

Техническое описание · модель данных · регламент · безопасность · тест-план · проект обращения
оператору

ТЕХНИЧЕСКИ ГОТОВО К СОГЛАСОВАНИЮ

Промышленный обмен не активирован. Подключение возможно только после решения оператора,
соглашения, утверждения схемы и выдачи реквизитов тестового контура.

Дата фиксации

13 августа 2026 года

Правовой контур

ПП РФ № 1378, раздел XVII, пункты 334–347

Профиль обмена

XML / JSON / GeoJSON; REST / SOAP 1.2

Статус документа

Проект для согласования с оператором ФГИС ЛК

Документ не является подтверждением промышленного подключения и не содержит секретов, ключей или сертификатов.

Состав пакета

Комплект собран как единый воспроизводимый пакет для технического и правового согласования. Исходные Markdown-файлы, OpenAPI, XSD и примеры обмена поставляются отдельно вместе с этим документом.

1. Готовность Forest OS к информационному взаимодействию с ФГИС ЛК
2. Техническое описание интеграции
3. Схема передаваемых данных
4. Регламент информационного обмена
5. Описание мер безопасности
6. План тестирования интеграции
7. Персональные данные
8. Проект обращения оператору ФГИС ЛК
9. Матрица требований и реализации
10. Протокол подключения к тестовому контуру
11. Внешние шаги, которые нельзя выполнить автономно
12. Официальные источники

Ключевой принцип

Аналитические наблюдения Forest OS не выдаются за юридически значимые записи ГЛР; схема и полномочия фиксируются соглашением с оператором.

Готовность Forest OS к информационному взаимодействию с ФГИС ЛК

Дата фиксации: 13.08.2026. Версия адаптера: 0.1.0.

Итоговый статус

Forest OS технически подготовлена к согласованию как «другая информационная система» по разделу XVII Правил ведения государственного лесного реестра, утверждённых постановлением Правительства РФ от 25.08.2023 № 1378.

Закрытый staging-адаптер развёрнут на production-host: 127.0.0.1:8896, service/timer активны, outbound=disabled. Для промышленного обмена нужны решение и соглашение оператора, утверждённая схема, endpoint/WSDL, сертификаты и профиль защищённого канала.

Что реализовано

1. REST API для формирования, получения, проверки и подтверждения пакетов.
2. SOAP 1.2 интерфейс Forest OS для согласования операций и последующей привязки к WSDL оператора.
3. XSD forest-os-observation-1.0 для NDVI, LST, влажности и активных пожаров.
4. Реестр официальных схем с выбором версии по дате.
5. Установлены и компилируются действующие официальные XSD:
 - ForestFire 2.3.4, действует с 05.05.2026; - ForestFireSecurity 3.0.7, действует с 05.05.2026 по 31.08.2026; - common 3.4, общие под-схемы.
6. Учтена опубликованная будущая версия ForestFireSecurity 3.1.0, вступающая в силу 01.09.2026; автоматическое преждевременное переключение исключено.
7. HMAC-SHA256, защита от повторного nonce, mTLS напрямую или через доверенный loopback proxy.
8. SQLite outbox, идемпотентность, SHA-256 каждого payload, аудит операций, состояния доставки и подтверждения.
9. Fail-closed контроль электронной подписи: outbound не отправляет пакет без detached-подписи, связанной с SHA-256 payload.
10. Автоматическая выгрузка из ops_map_preview.json с сохранением provenance и QA.
11. Форматы XML, JSON и GeoJSON.
12. Systemd service/timer и пример nginx mTLS-периметра.

Проверенный объём

На production-снимке из 17 185 точек сформирован XML-пакет из 14 342 фактических наблюдений. Размер 11 348 944 байта; SHA-256 payload: c99b2255b2a836085327345bfa7d2969c637d9ac0caaa1cfe554ea46dbc71fdb. XSD-валидация завершилась без ошибок. Пропущенные значения не заменялись нулями.

Что намеренно не заявляется

- Forest OS ещё не подключена к промышленному контуру ФГИС ЛК.
- XSD аналитических наблюдений ещё не утверждена оператором.
- SOAP namespace и операции Forest OS не выдаются за официальный WSDL ФГИС ЛК.
- Спутниковое наблюдение пожара не является актом о лесном пожаре.
- mTLS/HMAC не выдаются за электронную подпись документа.
- Обычный OpenSSL/nginx не выдаётся за сертифицированное ГОСТ-шифрование.
- Пакеты не вносятся напрямую в ГЛР до определения состава сведений, полномочий и подписанта.

Техническое описание интеграции

1. Назначение

Адаптер `forest-os-fgis-adapter` отделяет аналитический контур Forest OS от юридически значимого контура ГЛР. Он обеспечивает воспроизводимую подготовку спутниковых и климатических наблюдений, их проверку, подписание внешним одобренным криптопровайдером, безопасную доставку и подтверждение приёма.

2. Архитектура

Поток данных:

1. Материализованный production-снимок Forest OS `ops_map_preview.json` поступает в read-only источник адаптера.
2. Экспортёр фильтрует наборы, дату и bbox, проверяет диапазоны и создаёт детерминированные `observation_id`.
3. Кодек формирует XML, JSON или GeoJSON.
4. XML проходит XSD-валидацию.
5. Outbox атомарно сохраняет payload, SHA-256, идемпотентный ключ и статус `READY`.
6. Уполномоченный криптопровайдер формирует УНЭП/УКЭП; адаптер прикрепляет detached-подпись к неизменному SHA-256.
7. Delivery worker отправляет подписанный envelope только при включённом оператором endpoint.
8. Ответ сохраняется как `DELIVERED`, затем операторское подтверждение переводит пакет в `ACKNOWLEDGED`.

3. REST API

- GET `/health` - доступность процесса;
- GET `/ready` - база, источник и XSD;
- GET `/v1/capabilities` - форматы и наборы;
- GET `/v1/schemas` - версии схем;
- POST `/v1/batches` - создать неизменяемый пакет;
- GET `/v1/batches/{id}` - статус и хеши;
- GET `/v1/batches/{id}/payload` - payload с ETag и X-Payload-SHA256;
- POST `/v1/validate?profile=...` - XSD-валидация;
- POST `/v1/batches/{id}/ack` - подтверждение доставки;
- GET `/metrics` - внутренние Prometheus-метрики.

POST `/v1/batches` требует Idempotency-Key. Повтор того же запроса возвращает существующий пакет. Использование ключа с иным телом возвращает конфликт.

4. SOAP 1.2

POST `/soap/v1` поддерживает операции `GetCapabilitiesRequest` и `CreateExportRequest`. Интерфейс используется как проверяемая переговорная реализация. После получения WSDL оператора меняются namespace, SOAPAction, операции и envelope без изменения ядра экспортёра.

5. Входная и выходная валидация

- JSON-запрос проверяется по whitelist наборов и форматов.
- Bbox принимается только в EPSG:4326 и в допустимых диапазонах.
- Период принимает YYYY-ММ или YYYY-ММ-DD.
- NDVI ограничен диапазоном [-1; 1].
- LST ограничена диапазоном [-100; 100] °C как технический sanity-check.

- Влажность ограничена диапазоном $[0; 1]$ м³/м³.
- Счётчики пожаров не могут быть отрицательными.
- null, NaN и бесконечности не преобразуются в ноль.
- Ограничение записей отражается полями truncated и omittedDueLimit; скрытого усечения нет.

6. Официальные документы

Официальные ForestFire и ForestFireSecurity валидируются отдельно. Адаптер не строит их из спутникового сигнала, потому что XSD требует юридически значимые сведения: составителя и наблюдателей, организацию, причину, локализацию и ликвидацию, ущерб, ответственных лиц, вложения и иные реквизиты.

Преобразование аналитического наблюдения в официальный документ допускается только после поступления недостающих сведений от уполномоченного органа и подписания правомочным лицом.

7. Развёртывание

Приложение запускается отдельным systemd-сервисом на 127.0.0.1:8896. Внешняя публикация выполняется только через согласованный mTLS/VPN-периметр. Автоматический timer создаёт новый пакет только при изменении SHA-256 входного снимка.

Схема передаваемых данных

1. Профиль аналитических наблюдений

Профиль: forest-os-observation-1.0.

Юридический статус: advisory_observation_not_glr_record. Профиль предлагается оператору для утверждения либо отображения в согласованную оператором схему.

2. Заголовок пакета

Поле	Тип	Назначение
schemaProfile	string	Версия согласованной схемы
batchId	string	Неизменяемый идентификатор fos-batch-*
createdAt	dateTime UTC	Время формирования
producer	string	Forest OS Global
legalStatus	enum/string	Аналитический, не запись ГЛР
coordinateReferenceSystem	string	EPSG:4326
spatialIndex	string	НЗ
sourceSnapshotSha256	SHA-256	Хеш исходного production-снимка
sourceGeneratedAt	string/dateTime	Время материализации источника
sourceStatus	string	QA/статус источника
truncated	boolean	Было ли ограничение результата

3. Наблюдение

Поле	Обязательность	Описание
observationId	да	Детерминированный SHA-256-based ID
dataset	да	ndvi, lst, soil_moisture, active_fire, burn_history
observedAt	да	Дата или месяц наблюдения
value	да	Числовое значение; отсутствующее не создаётся
unit	да	1, Cel, m3/m3, count
latitude, longitude	да	EPSG:4326
h3	условно	Индекс НЗ, если присутствует в источнике
sourceId	да	Машинный идентификатор источника
sourceProduct	да	Публично понятное название продукта
qualityStatus	да	Например, observed_event, materialized_guarded
legalStatus	да	Не является самостоятельной записью ГЛР
metadata	нет	FRP, AM/PM-влажность и другие метаданные

4. Наборы и периодичность

Набор	Текущее поле	Единица	Номинальная периодичность	Текущий экспорт
NDVI	ndvi	1	по доступному месячному слою	при обновлении снимка
LST	lst_c	°C	по доступному месячному слою	при обновлении снимка
Влажность	soil	м³/м³	месячная агрегация SMAP	при обновлении снимка
Активные пожары	fire	count	наблюдаемые события FIRMS	при обновлении снимка
История выгорания	burn_12m	count	скользящие 12 месяцев	только по отдельному запросу

5. Пространственная привязка

Передаются Point-координаты EPSG:4326 и НЗ. Привязка к субъекту, лесничеству, участковому лесничеству, кварталу и выделу должна выполняться по согласованным справочникам ФГИС ЛК. Forest OS не подменяет официальные юридические границы.

6. No-data

null, NaN, отсутствующее поле или некорректный период не создают наблюдение. Для каждого набора пакет содержит:

- records - реально выданные записи;
- missing - отсутствующие значения в выбранном контуре;
- invalid - значения, отклонённые sanity-check;
- omittedDueLimit - валидные записи, не включённые из-за лимита.

Регламент информационного обмена

1. Роли

- Поставщик: владелец/лицензиат Forest OS, реквизиты уточняются в обращении.
- Оператор ФГИС ЛК: Федеральное агентство лесного хозяйства либо назначенная организация в пределах полномочий.
- Подписант: правомочное лицо владельца Forest OS, сертификат и тип подписи согласуются.
- Технические контакты: ответственные за эксплуатацию и информационную безопасность с обеих сторон.

2. Режимы

1. Pull: оператор запрашивает формирование пакета по набору, периоду и bbox.
2. Push: Forest OS формирует пакет при изменении production-снимка и отправляет его в согласованное окно.
3. File fallback: подписанный пакет передаётся через согласованный защищённый канал без автоматического вызова API.

Выбор режима фиксируется соглашением.

3. Частота

- активные пожары - целевой режим от 15 минут до суток в зависимости от согласованной оперативности;
- NDVI/LST - после появления проверенной агрегации, обычно ежемесячно;
- влажность SMAP - ежемесячно;
- повторная передача - только при изменении payload либо по запросу оператора.

Текущий безопасный timer проверяет источник четыре раза в сутки, но создаёт пакет только при новом SHA-256.

4. Идемпотентность

Каждый запрос содержит Idempotency-Key. Один ключ и один канонический запрос дают один batchId. Смена тела при том же ключе отклоняется. Оператор может безопасно повторить запрос после сетевой ошибки.

5. Состояния

- READY - пакет сформирован и проверен;
- SENDING - попытка доставки;
- DELIVERED - transport-level приём подтверждён;
- FAILED - ошибка, назначено время повторной попытки;
- ACKNOWLEDGED - оператор присвоил идентификатор подтверждения.

6. Повторы и ошибки

Повтор выполняется с экспоненциальной задержкой от 60 секунд, максимум один час. Ошибка сохраняется без payload и секретов. Повторы не меняют payload, batchId и SHA-256.

Категории:

- 400/422 - ошибка данных, автоматический повтор блокируется до исправления;
- 401/403 - ошибка сертификата, подписи или полномочий;
- 409 - конфликт идемпотентности/версии;

- 429 - повтор по Retry-After;
- 5xx/timeout - автоматический повтор;
- XSD failure - пакет не переходит в доставку.

7. Мониторинг

Контролируются количества пакетов по статусам, возраст старейшего READY/FAILED, ошибки XSD, повтор поппе, ошибки подписи, время ответа и число подтверждений. Alert-пороги и контакты фиксируются в соглашении.

8. Изменение схем

Новая версия схемы устанавливается в четыре этапа: публикация оператором, локальная проверка и компиляция, контрактные тесты в песочнице, переключение в дату вступления в силу. Автоматическое использование future-dated XSD запрещено.

9. Отзыв и исправление

Payload неизменяем. Исправление формирует новый пакет со ссылкой на заменяемый batchId после согласования поля связи. Удаление/перезапись ранее переданного пакета без оператора не выполняется.

Описание мер безопасности

1. Принципы

Минимальные полномочия, fail-closed, неизменяемость payload, разделение транспортной аутентификации и электронной подписи, отсутствие секретов в коде и журналах.

2. Сетевой периметр

- процесс слушает только loopback;
- внешний вход разрешается через выделенный mTLS/VPN-периметр;
- TLS не ниже 1.2;
- клиентский сертификат проверяется по CA и, при необходимости, allowlist SHA-256 fingerprint;
- размер запроса ограничен 32 МБ;
- production без аутентификации запрещён конфигурацией.

3. Аутентификация

Основной профиль - mTLS. HMAC-SHA256 предназначен для песочницы или дополнительного application-level контроля. Подпись HMAC включает метод, полный path, timestamp, nonce и SHA-256 тела. Допуск времени - 300 секунд. Nonce одноразовый.

4. Электронная подпись

Для негосударственной «другой информационной системы» пункт 337 Правил ведения ГЛР предусматривает УНЭП. Адаптер:

- не выдаёт mTLS/HMAC за УНЭП;
- принимает detached-подпись только с профилем UNEP или UKER;
- связывает подпись с SHA-256 конкретного payload;
- запрещает outbound при отсутствии/несоответствии подписи;
- не реализует криптографию самодельными средствами.

Создание и криптографическая проверка выполняются сертифицированным, согласованным оператором средством. Формат CAdES/XAdES, алгоритмы, контейнер и цепочка сертификатов фиксируются соглашением.

5. ГОСТ и VPN

Раздел XVII постановления № 1378 разрешает для других ИС сети общего пользования и web-сервисы, но не задаёт в этих пунктах конкретный ГОСТ/VPN-профиль. Если оператор требует ГОСТ TLS или защищённый канал, он организуется через согласованный сертифицированный шлюз/криптопровайдер (например, выбранный оператором класс решения). Пример nginx не считается сертифицированной ГОСТ-реализацией.

6. Хранение

- state directory и outbox создаются с UMask=0077;
- systemd ограничивает файловую систему ProtectSystem=strict;
- источник и код read-only, запись разрешена только в state directory;
- payload проверяется по SHA-256 при каждом чтении;
- SQLite работает в WAL, все ключевые операции попадают в audit log;
- секреты находятся в /etc/forest-os/fgis-adapter.env с доступом root-only.

7. Журналирование

Записываются субъект, действие, объект, исход, время и безопасные метаданные. Не записываются HMAC-секреты, bearer tokens, приватные ключи, полные документы и персональные данные.

8. Управление уязвимостями

- зависимости минимальны: Python stdlib и lxml;
- XML разбирается без entity resolution и сетевых загрузок;
- ZIP официальных XSD проверяется на path traversal и SHA-256;
- обновления XSD и зависимостей проходят тесты до production;
- ключи и сертификаты ротируются по регламенту оператора.

9. Реагирование

При компрометации сертификата: заблокировать fingerprint/ключ, выключить outbound, сохранить аудит, уведомить оператора, выпустить новый сертификат, повторно подписать только непереданные payload. Переданные документы не переписываются.

План тестирования интеграции

1. Цель

Подтвердить корректность данных, совместимость схем, безопасность, идемпотентность, устойчивость и наблюдаемость до подключения к промышленному контуру.

2. Уровни

Локальные автоматизированные тесты

ID	Сценарий	Ожидаемый результат
UT-01	null NDVI	запись не создаётся, missing увеличивается
UT-02	значение вне диапазона	запись не создаётся, invalid увеличивается
UT-03	bbox/период	только записи внутри контура
UT-04	XML профиль Forest OS	XSD valid
UT-05	официальные XSD и common 3.4	обе схемы компилируются offline
UT-06	HMAC	корректная подпись принимается
UT-07	повтор nonce	401, событие не исполняется
UT-08	идемпотентный повтор	тот же batchId, новый payload не создаётся
UT-09	конфликт ключа	409
UT-10	unsigned outbound	доставка запрещена
UT-11	подпись другого payload	доставка запрещена
UT-12	REST create/get	SHA-256 скачанного payload совпадает
UT-13	SOAP capabilities	валидный SOAP 1.2 ответ
UT-14	запрос без auth	401

Проверка production-снимка

Исходный снимок: 17 185 точек. Ожидается полный пакет фактических ненулевых/нулевых наблюдений при исключении null, XSD valid, совпадающие SHA-256 до и после чтения.

Фактический контрольный результат 13.08.2026: 14 342 наблюдения, 11 348 944 байта, XSD valid, 0 ошибок.

Песочница оператора

ID	Проверка	Критерий приёма
ST-01	mTLS handshake	обе стороны проверяют цепочки сертификатов
ST-02	УНЭП	оператор подтверждает формат и валидность
ST-03	минимальный XML	принят и получен ask ID
ST-04	JSON-аналог	семантика совпадает с XML
ST-05	пакет с null статистикой	нет подмены нулём
ST-06	дубликат	один документ/пакет в принимающей стороне
ST-07	некорректная XSD	структурированный отказ
ST-08	просроченный/отозванный сертификат	отказ

ID	Проверка	Критерий приёмки
ST-09	timeout/5xx	безопасный повтор без дубля
ST-10	смена версии XSD	old/new работают по согласованной дате
ST-11	32 МБ	согласованный лимит и поведение
ST-12	аудит	трассировка по batchId с обеих сторон

3. Нагрузочная проверка

Профили: 1, 10 и 50 параллельных запросов; пакет 1 000, 10 000 и 100 000 записей; повторное скачивание payload. Измеряются p50/p95/p99, CPU, память, размер WAL, время XSD и скорость outbox.

4. Безопасность

Проверяются XML entity attack, ZIP traversal, oversized body, replay, timestamp skew, подмена payload после подписи, неизвестный fingerprint, отсутствие подписи, утечка секретов в логах и доступ к пути вне outbox.

5. Протокол результата

Для каждого теста фиксируются дата, версия адаптера, версия XSD, request ID/batch ID, обезличенный запрос, код ответа, ask ID, фактический результат, логи и решение. Выход в production допускается только при закрытии дефектов уровня critical/high.

Персональные данные

1. Текущий профиль

Пакет forest-os-observation-1.0 не содержит ФИО, телефонов, email, СНИЛС, паспортных данных, учётных записей, адресов проживания или иных идентификаторов физических лиц. Координаты относятся к наблюдениям природной территории, а не к местоположению физического лица.

Отдельное согласие на обработку персональных данных для текущего машинного пакета не требуется, поскольку персональные данные в нём не передаются. Окончательная правовая оценка выполняется владельцем Forest OS и оператором.

2. Технические контакты

ФИО, должности и телефоны ответственных лиц, требуемые пунктами 343/344 или соглашением, передаются как организационные реквизиты обращения, а не внутри набора наблюдений. Доступ к ним ограничивается участниками согласования.

3. Если состав будет расширен

До добавления персональных данных необходимо:

1. определить оператора/обработчика и правовое основание;
2. зафиксировать цели и минимальный состав;
3. оформить поручение/соглашение и уведомления при необходимости;
4. установить сроки хранения и удаления;
5. провести модель угроз и оценку требований 152-ФЗ;
6. обновить API, XSD, журналирование и тесты;
7. запретить персональные данные в метаданных свободного текста.

До выполнения этих действий API отклоняет произвольные пользовательские поля и работает по закрытому whitelist.

Проект обращения оператору ФГИС ЛК

В Федеральное агентство лесного хозяйства Оператору федеральной государственной информационной системы лесного комплекса

От: _____ ОГРН/ИНН:

_____ Адрес:

_____ Контакт (ФИО, должность, телефон, email): _____

Поля выше заполняются владельцем информационной системы перед официальным направлением.

Об организации информационного взаимодействия Forest OS Global с ФГИС ЛК

В соответствии с пунктами 334-347 Правил ведения государственного лесного реестра, утверждённых постановлением Правительства Российской Федерации от 25.08.2023 № 1378, просим рассмотреть возможность организации информационного взаимодействия информационной системы Forest OS Global с ФГИС ЛК.

1. Наименование информационной системы

Forest OS Global.

2. Цели создания и назначение

Автоматизированное формирование воспроизводимых аналитических наблюдений о состоянии лесной растительности и факторах риска на основе открытых спутниковых и климатических данных. Предлагаемый обмен включает NDVI, температуру поверхности земли, поверхностную влажность почвы и наблюдаемые активные пожары с пространственной привязкой, provenance и QA-статусом.

3. Описание системы

Forest OS формирует версионированные неизменяемые XML/JSON-пакеты, валидирует их по XSD, обеспечивает идемпотентность, SHA-256, журнал аудита, mTLS/HMAC, detached-электронную подпись и подтверждение доставки. Аналитические наблюдения не выдаются за юридически значимые записи ГЛР или акты о лесных пожарах.

4. Сведения о собственнике/лицензиате

Заполняется владельцем перед направлением: правообладатель, ОГРН/ИНН и адрес.

5. Документ о праве собственности или лицензионный договор

Указать номер и наименование документа, подтверждающего право на информационную систему.

6. Предлагаемый автоматизированный процесс

1. Формирование пакета после обновления проверенного production-снимка либо по запросу оператора.
2. XSD-валидация и фиксация SHA-256.
3. Подписание УНЭП/УКЭП согласованным криптопровайдером.
4. Передача через web-сервис по mTLS/VPN в согласованном формате.
5. Получение технического и прикладного подтверждения.
6. Безопасный повтор по идемпотентному ключу при транспортной ошибке.

7. Состав предлагаемых сведений

- идентификатор и время пакета;
- версия схемы и SHA-256 источника/payload;
- тип показателя;
- период наблюдения;

- значение и единица измерения;
- EPSG:4326 и НЗ;
- источник/продукт;
- QA-статус;
- статистика пропусков и усечения;
- статус «аналитическое наблюдение, не самостоятельная запись ГЛР».

Просим сообщить:

1. допустим ли прямой обмен указанным аналитическим профилем;
2. какой XSD/JSON Schema следует использовать либо согласовать;
3. URL тестового контура, WSDL/OpenAPI и порядок выдачи доступа;
4. требования к УНЭП/УКЭП, формату CAdES/XAdES и сертификатам;
5. требования к VPN, mTLS и ГОСТ-алгоритмам;
6. допустимые справочники и идентификаторы территории;
7. лимиты, SLA, коды ошибок и формат ask;
8. порядок заключения соглашения об информационном взаимодействии.

Приложения: техническое описание, схема данных, OpenAPI, XSD, регламент, меры безопасности, план тестирования, сведения о персональных данных, результаты тестов, документ о праве на ИС.

Подпись уполномоченного лица: _____ Дата: _____

Матрица требований и реализации

Основание/требование	Реализация Forest OS	Статус
ПП №1378, п. 334: другие ИС входят в контур	отдельный адаптер внешней ИС	готово технически
п. 336: полнота и достоверность	whitelist, диапазоны, provenance, QA, no-data статистика	готово
п. 336: конфиденциальность	mTLS/VPN-периметр, минимизация данных, закрытые секреты	готово к согласованию
п. 337: XML или JSON	XML/JSON, дополнительно GeoJSON	готово
п. 337: УНЭП для другой ИС	fail-closed detached signature binding	интерфейс готов, сертификат внешний
п. 338: схемы оператора	versioned registry, официальные XSD с SHA-256	готово
п. 340: web-сервисы	REST и SOAP 1.2	готово, контракт согласуется
п. 341: соглашение	проект регламента и обращения	подготовлено
п. 342: форматы в соглашении	XSD, OpenAPI, примеры XML/JSON	подготовлено
п. 344: наименование/цели/описание	разделы обращения	подготовлено
п. 344: собственник/право	placeholders и перечень приложений	нужны реквизиты владельца
п. 344: процесс автоматического обмена	push/pull, outbox, ack, retries	подготовлено
п. 344: состав сведений	словарь данных	подготовлено
п. 346: рассмотрение 14 рабочих дней	контрольная точка процесса	внешний шаг
XSD совместимость	ForestFire 2.3.4, FireSecurity 3.0.7, common 3.4	тесты проходят
Нет дублирования	idempotency key, immutable batch, ack	готово
Актуальность	source SHA-256 и timer по изменению снимка	готово
Защищённый канал	loopback app, mTLS/VPN gateway template	нужен профиль оператора
ГОСТ	только через сертифицированное согласованное средство	внешний выбор/закупка
Песочница	тест-план и сценарии	запросить доступ

Протокол подключения к тестовому контуру

До выдачи доступа

Передать оператору обращение и пакет документов. Получить:

- endpoint и DNS/IP;
- REST OpenAPI или SOAP WSDL;
- XSD/JSON Schema и справочники;
- тестовый CA, серверные и клиентские сертификаты;
- профиль УНЭП/УКЭП;
- VPN/mTLS/ГОСТ требования;
- тестовые идентификаторы субъектов, лесничеств, кварталов;
- лимиты payload/rate и SLA;
- контакты NOC/ИБ/разработчиков.

Последовательность

1. Проверить цепочки сертификатов и время на узлах.
2. Поднять отдельный staging endpoint без доступа к owner-контуру.
3. Выполнить health/capabilities.
4. Передать минимальный подписанный пакет из одной записи.
5. Сверить XSD, подпись, координаты и единицы.
6. Повторить тот же пакет и подтвердить отсутствие дубля.
7. Передать пакет с намеренной XSD-ошибкой и получить структурированный отказ.
8. Передать NDVI/LST/SMAP/FIRMS по отдельности.
9. Проверить пакет с missing, но без подмены нулём.
10. Выполнить негативные тесты сертификата, подписи, nonce и лимита.
11. Сверить audit trail по batchId и ack ID.
12. Подписать протокол тестов и только затем согласовать production.

Критерий выхода

Все обязательные тесты пройдены, критические/высокие дефекты закрыты, версии схем закреплены, владелец данных и подписант подтверждены, регламент и порядок отзыва сертификата подписаны.

Внешние шаги, которые нельзя выполнить автономно

1. Указать юридического владельца/лицензиата Forest OS и приложить документ о праве на ИС.
2. Назначить уполномоченного подписанта и технических/ИБ-контактов.
3. Направить обращение оператору по пункту 344 Правил №1378.
4. Получить решение о возможности взаимодействия и заключить соглашение.
5. Получить тестовый endpoint/WSDL/OpenAPI, CA и сертификаты.
6. Согласовать XSD аналитических наблюдений или точное отображение в схему оператора.
7. Выбрать и настроить сертифицированный криптопровайдер для УНЭП/УКЭП.
8. Если требуется, организовать VPN/ГОСТ-шлюз.
9. Провести совместные тесты и подписать протокол.
10. Получить письменное разрешение на production и окно ввода.

До выполнения пунктов 1-10 outbound остаётся disabled; это контролируемое безопасное состояние, а не техническая недоработка.

Официальные источники

Проверено 13.08.2026.

1. Рослесхоз: ФГИС ЛК. Информационные материалы

<https://rosleshoz.gov.ru/information-systems/fgis-lk-information/>

2. Рослесхоз: нормативно-правовые акты ФГИС ЛК

<https://rosleshoz.gov.ru/information-systems/fgis-lk-information/acts/>

3. Рослесхоз: постановление Правительства РФ от 25.08.2023 №1378, Правила ведения ГЛР

<https://rosleshoz.gov.ru/documents/other-documents/pravila-vedeniya-glir/>

4. Рослесхоз: образцы документов XSD-схем

<https://rosleshoz.gov.ru/information-systems/fgis-lk-information/sampledoc-xsd/>

5. Рослесхоз: техническая информация ФГИС ЛК

<https://rosleshoz.gov.ru/information-systems/fgis-lk-information/technical-info/>

6. Официальный текст постановления Правительства РФ от 06.07.2015 №676

<http://publication.pravo.gov.ru/Document/View/0001201507080013>

Контрольные суммы официальных пакетов:

- ForestFire_2.3.4.zip: d03b0529b5c18c299bf3aa59fc5f727cf3412221976d5b61d75264f1184c2e73;
- ForestFireSecurity_3.0.7_.zip:
4a6b6fe2820818ce2474ced611afc256106acdcfeac70518d49be61354e114ad;
- common_3.4.zip: ec6ef2a0f6fea2675956592ef1aa23678f2a73624f9a95f8bf1e4f329fb16bf0.

Нормативное уточнение: постановление №676 задаёт общие требования к созданию и эксплуатации государственных ИС. Непосредственная процедура взаимодействия ФГИС ЛК с другими ИС для данного проекта подтверждается разделом XVII Правил №1378, пункты 334-347.

Машиночитаемые приложения

Следующие файлы входят в поставку и являются нормативно-техническими приложениями к настоящему документу.

Файл	Назначение
openapi.yaml	OpenAPI 3.1: REST-контракт адаптера
schemas/forest-os-observation-1.0.xsd	XSD аналитического профиля Forest OS
schemas/manifest.json	Версии и SHA-256 официальных XSD
examples/observation-batch-example.xml	Пример XML-пакета
examples/observation-batch-example.json	Пример JSON-пакета
examples/observation-batch-example.geojson	Пример GeoJSON-пакета
deploy/nginx-mtls.example.conf	Шаблон mTLS-периметра
deploy/forest-fgis-adapter.service	Systemd unit адаптера
deploy/forest-fgis-export.timer	Регламентная выгрузка

Контроль версии

Перед официальным направлением следует заполнить реквизиты владельца, приложить документ о праве на ИС, зафиксировать SHA-256 архива поставки и подписать обращение уполномоченным лицом.