Технические требования (ТЗ)

Приложение №1 к Договору

1. Общие сведения

Предмет работ: разработка программного обеспечения (далее — «ПО») для зеркалирования трафика протокола SIP с возможностью дублирования связанного медиатрафика (RTP/RTCP), фиксации и передачи данных на один или несколько целевых узлов (далее — «Приёмники»), а также локальной записи и предоставления интерфейсов управления.

Цель: обеспечить надёжное зеркалирование SIP/RTP-трафика, **автоматическое переключение на резервное оборудование (failover)**, **расширенное управление правами доступа (RBAC)** и **автоматическую очистку данных** по политикам хранения.

Основание разработки: пункт 1.1 Договора.

Стороны: - Заказчик: ___ **- Исполнитель:** _____

2. Термины и сокращения

- **SIP** — Session Initiation Protocol (RFC 3261 и сопутствующие).
- **RTP/RTCP** — Real-time Transport Protocol / Real-time Transport Control Protocol (RFC 3550 и сопутствующие).
- **SIP-TLS** — SIP поверх TLS.
- **PCAP/PCAPNG** — форматы файлов сетевых захватов.
- **SPAN/Mirror-порт** — режим зеркалирования на коммутаторе/маршрутизаторе.
- **Приёмник** — удалённый узел, получающий зеркалируемый трафик.

3. Назначение и область применения

ПО применяется в сетевой инфраструктуре Заказчика для пассивного контроля и анализа сигнализации SIP и, опционально, медиапотоков, инициируемых SIP-сессиями. ПО не вмешивается в рабочий трафик и не изменяет его.

4. Требования к архитектуре

4.1. **Архитектурная модель** — модульная, включает: - Модуль захвата (Capture): получение пакетов с интерфейса(ов) ОС и/или через SPAN/mirror. - Модуль корреляции SIP↔RTP: парсинг SIP/SDP, определение адресов/портов медиапотоков. - Модуль зеркалирования (Replicator): отправка копий пакетов на Приёмники с сохранением временных характеристик; поддержка синхронного режима для исключения потерь при резервировании. - Модуль записи (Recorder): локальная запись PCAP/PCAPNG с ротацией; модуль извлечения медиапотоков в аудиофайлы **WAV/MP3** (транскодирование). - Модуль управления и API: CLI и REST API для конфигурации и мониторинга; **модуль управления учетными записями и ролями (RBAC)**. - Модуль наблюдаемости: метрики, логи, алерты; аудит действий пользователей. - **Модуль обеспечения отказоустойчивости (HA):** мониторинг здоровья (health-check/heartbeat), управление виртуальным адресом (VIP) или маршрутом, автоматическое переключение **основной ↔ резервный** без потери данных.

4.2. **Схема отказоустойчивости** - Режим **Active/Passive** (обязателен) с автоматическим failover по тайм-ауту здоровья; опционально Active/Active для масштабирования. - Репликация состояния очередей/журналов записи (write-ahead log) на резервный узел; при отказе основного — догон резервным без потери записанных кадров (условие: синхронная репликация включена). - Возможность использования **виртуального IP** (keepalived/VRRP) или внешнего балансировщика.

4.3. **Платформы выполнения (по выбору Заказчика):** - **Windows Server 2019+** (служба Windows Service) и/или **Linux x86_64** (Ubuntu LTS/DEB, RHEL/AlmaLinux/RPM, systemd-unit). Допускается смешанная схема основной/резервный.

4.4. **Способ поставки:** - Пакеты DEB/RPM + systemd-unit для Linux; MSI/служба для Windows (nssm/sc create не требуется, собственный сервис). - Опционально: контейнер Docker/OCI с health-check.

5. Функциональные требования

5.1. **Поддерживаемые протоколы и порты** - SIP по UDP и TCP (по умолчанию 5060/udp, 5060/tcp; диапазон настраиваемый). - SIP-TLS (по умолчанию 5061/tcp). При отсутствии ключей расшифровки — зеркалирование метаданных/заголовков без раскрытия полезной нагрузки. - RTP/RTCP: определение по полям SDP (m=audio/video, c=IN IP4/IP6, a=rtpmap и др.), динамический диапазон портов настраиваемый; извлечение аудиопотоков и сохранение в **WAV/MP3**.

5.2. **Режимы работы** - **Mirror-forward**: онлайн-копирование пакетов на список Приёмников (1..N) по UDP/GRE/RAW-сокету; поддержка нескольких профилей Приёмников. - **Local-record**: запись SIP/RTP в файлы PCAP/PCAPNG с ротацией по размеру/времени, с каталогизацией по датам. - **Dual**: одновременная запись и зеркалирование.

5.3. **Фильтрация и выбор трафика** - BPF-фильтры на входе (например: `udp port 5060 or tcp port 5060`), настраиваемые списки включений/исключений по IP/сетям/портам/префиксам. - Фильтрация по атрибутам SIP: From/To, Call-ID, User-Agent, Method (INVITE/REGISTER/SUBSCRIBE и др.). - Возможность white/black-list по доменам/REALM/Proxy-Auth.

5.4. **Корреляция SIP↔RTP** - Выделение SDP из сообщений SIP, построение «диалога» и динамическая подписка на соответствующие RTP/RTCP-потоки. - Опция «только SIP» (без RTP) и «SIP+RTP».

5.5. **Зеркалирование на Приёмники** - Поддержка 1..N Приёмников; для каждого — адрес, протокол доставки (UDP/GRE), MTU, ttl, DSCP/ToS, опция туннелирования (GRE/IP-IP). - Режим сохранения исходных адресов (RAW/TEE) либо переадресации через отправителя (нативный IP отправителя = узел ПО). - **Резервирование:** пара основных/резервных Приёмников; автоматическое переключение на резервный при недоступности основного (порог по тайм-ауту/потерям настраиваем). - **Без потери информации:** при включённом синхронном режиме — запись в локальный журнал (WAL) до подтверждения зеркалирования на активный Приёмник; при переключении — гарантированный догон на резервный.

5.6. **Запись и хранение** - Формат PCAP/PCAPNG (с возможностью «только заголовки»). - **Извлечение аудио:** демультиплексирование RTP и сохранение аудиодорожек в формат **WAV (PCM 8/16 kHz)** и/или **MP3 (битрейт настраиваемый)**. Параллельная запись PCAP и аудио допускается. - Ротация: по времени (мин/час/сутки) и/или по размеру; глубина хранения по лимиту диска и политике удаления (FIFO, по дате, по возрасту записи). - Индексация: журнал

файлов, карта сессий (Call-ID → список файлов/смещений) в SQLite/JSON-индексе; хранение метаданных вызовов (см. 5.8).

5.7. **Управление и интеграции** - **CLI**: команды запуска/остановки, загрузка/проверка конфигурации, просмотр статуса и метрик. - **REST API** (HTTP/HTTPS): чтение/запись конфигурации, метрики, поиск сессий, выгрузка срезов PCAP и аудиофайлов по фильтрам (Call-ID, время, номера), управление пользователями и ролями. - **Метрики**: Prometheus endpoint (например, `/metrics`). - **Логирование**: текст/JSON; уровни (ERROR/WARN/INFO/DEBUG); интеграция с journald и Windows Event Log. - **Аудит-лог**: изменения конфигурации, доступ по API, операции с записями (просмотр/редактирование/удаление/экспорт).

5.8. **Конфигурация** - Единый файл `config.yaml` (Linux) / `appsettings.json` или реестр (Windows) + переменные окружения. - Горячая перезагрузка (SIGHUP/API) без прерывания захвата. - Валидация конфигурации и сухой запуск (`--check`).

5.9. **Обработка шифрованного трафика** - SIP-TLS: при отсутствии ключей — зеркалируются только заголовки и метаданные (IP/порты, время, размер). При наличии ключевого материала — допустима расшифровка согласно политике Заказчика (опция). - SRTP: зеркалирование и запись возможны как «чёрного ящика» (без расшифровки) с сохранением временных меток и размеров; при наличии ключей — опциональная расшифровка/декодирование в аудио (WAV/MP3) по политике Заказчика.

5.10. **Доступность и отказоустойчивость / переключение на резерв** - Автоматическое обнаружение отказа основного узла/приёмника (health-checks, мониторинг потерь/тайм-аутов). - Автопереключение потоков на резервный узел/приёмник с сохранением целостности записи; режим **synchronous mirroring** (WAL + подтверждения) — для сценариев «без потери данных»; режим **best-effort** — при ограничениях сети. - Поддержка нескольких источников трафика (несколько интерфейсов) и нескольких пар основной/резервный. - Запуск как сервис ОС (Windows Service / systemd) с автоматическим рестартом, watchdog-проверками и зависимостями.

5.11. **Управление правами доступа (RBAC)** - Роли: `admin`, `ops`, `auditor`, `viewer` (минимум); возможность добавления кастомных ролей. - Матрица прав: - Просмотр: списки вызовов, метаданные, прослушивание аудио (по политике), экспорт. - Редактирование: конфигурация, метаданные вызовов (с протоколированием изменений). - Управление: создание/блокировка пользователей, назначение ролей, ключи API, доступ по mTLS/LDAP/AD. - Интеграция с **Active Directory/LDAP**; поддержка SSO (Kerberos/NTLM/LDAP-bind) — по согласованию. - Политики паролей/токенов: длина, срок действия, ротация, двуфакторная аутентификация (опция).

5.12. **Обработка и редактирование данных** - Редактирование метаданных вызовов (дата/время, внутренний номер вызывающего/вызываемого, теги) с ведением **журнала изменений (who/what/when)**; неизменность исходных PCAP/аудио. - Массовые операции по правилам (bulk-update) через API с валидацией. - **Автоматическая очистка** устаревших данных по политикам хранения: по возрасту, по объёму, по признаку завершённости; «корзина» с отложенным удалением.

5.13. **Метаданные и каталоги** - Фиксация для каждого вызова: дата/время начала/окончания, **внутренний номер вызывающего**, **внутренний номер вызываемого**, Call-ID, IP/порты, кодеки (из SDP), объём/длительность, хэш целостности файлов. - Соблюдение иерархии каталогов

хранения в соответствии с требованиями Заказчика (например: `YYYY/MM/DD/<internal_src>/<internal_dst>/`).

6. Нефункциональные требования

6.1. **Производительность и надёжность** - До 2 Гбит/с совокупного трафика при средней длине пакета 300 байт; потери зеркалируемых пакетов ≤ 0,5% в режиме best-effort и **0% в синхронном режиме** при корректно настроенном резервировании и пропускной способности. - До 1 000 одновременных SIP-диалогов; до 5 000 CPS для сигнализации (при «только SIP»). - **Непрерывная работа в режиме сервиса ОС** (Windows Service/systemd), автозапуск при старте ОС, восстановление после сбоев.

6.2. **Безопасность** - Ролевая модель доступа (см. 5.11), аутентификация по AD/LDAP/mTLS, HTTPS (TLS 1.2+), шифрование секретов в хранилище. - Журнал аудита всех действий; неизменяемость аудита (WORM-хранилище опционально).

6.3. **Совместимость** - Форматы аудио: **WAV, MP3**; сетевые захваты: PCAP/PCAPNG; совместимость с Wireshark/tshark, Arkime. - Интеграция с Prometheus/Grafana; экспорт в SIEM (CEF/JSON) по аудит-событиям.

6.4. **Масштабирование** - Горизонтальное (Active/Active) для распределения нагрузки по интерфейсам/потокам; центральный каталог метаданных (СУБД) — по согласованию.

7. Интерфейсы

7.1. **CLI** (примеры):

```
sipmirror run --config /etc/sipmirror/config.yaml
sipmirror status
sipmirror pcap export --call-id <CALL-ID> --from 2025-10-01T10:00:00Z --to
2025-10-01T10:05:00Z -o /tmp/call.pcap
```

7.2. **REST API** (примеры конечных точек): - `GET /api/v1/status` — состояние сервиса. - `GET /api/v1/metrics` — метрики Prometheus. - `GET /api/v1/calls?callId=...` — поиск диалогов. - `POST /api/v1/export` — формирование PCAP-среза по фильтрам. - `PUT /api/v1/config` — загрузка конфигурации, `GET /api/v1/config` — чтение.

7.3. **Формат конфигурации (пример `config.yaml` / `appsettings.json`)**

```
capture:
  interfaces: ["eth0"]
  bpf: "udp port 5060 or tcp port 5060"
  sip:
    include_methods: ["INVITE","REGISTER","SUBSCRIBE","MESSAGE"]
  rtp:
    enabled: true
    port_range: "10000-65000"
```

```
    audio:
      extract: true
      wav:
        enabled: true
        sample_rate: 8000
      mp3:
        enabled: true
        bitrate_kbps: 64
mirror:
  enabled: true
  synchronous: true  # для режима без потерь
  receivers:
    - name: primary
      mode: udp
      address: 192.0.2.10
      port: 9000
      dscp: 46
    - name: secondary
      mode: udp
      address: 198.51.100.20
      port: 9000
record:
  enabled: true
  dir: "/var/log/sipmirror"
  format: "pcapng"
  rotate:
    size_mb: 512
    interval_min: 60
    retention_days: 90
metadata:
  index: "sqlite:///var/lib/sipmirror/index.db"
  fields:
["start_time","end_time","caller_internal","callee_internal","call_id","codecs","duration_sec"
rbac:
  provider: "local" # или ldap/ad
  roles:
    - name: admin
      permissions: ["config:rw","users:rw","records:rw","export","audit:r"]
    - name: ops
      permissions: ["config:r","records:rw","export","audit:r"]
    - name: auditor
      permissions: ["records:r","audio:play","export","audit:r"]
    - name: viewer
      permissions: ["records:r","audio:play"]
cleanup:
  policies:
    - name: default_age
      type: age
      days: 90
      soft_delete_days: 14
    - name: size_cap
```

```
      type: size
      max_gb: 500
api:
  listen: ":8080"
  tls:
    enabled: false
    cert_file: "/etc/sipmirror/tls.crt"
    key_file: "/etc/sipmirror/tls.key"
logging:
  level: "info"
  json: true
service:
  mode: "systemd" # или windows-service
```

8. Документация и обучение

- Руководство пользователя (оператора) с примерами.
- Руководство администратора (установка, обновления, бэкапы, метрики, интеграции).
- Описание REST API (OpenAPI/Swagger).
- Памятка по безопасности и ограничениях при шифровании (SIP-TLS/SRTP).

9. Состав поставки

- Исполняемые файлы/пакеты ПО.
- Скрипты и юниты для systemd.
- Базовая конфигурация и шаблоны.
- Набор тестовых данных/трафика для приёмочных испытаний.
- Исходные коды и сборочный скрипт (если предусмотрено Договором).

10. Правовые требования

- Передача исключительных прав на ПО Заказчику в полном объёме, включая исходные коды, документацию и материалы, созданные в рамках работ.
- Гарантия отсутствия нарушений третьих лиц. Используемые сторонние библиотеки перечисляются с лицензиями, совместимыми с передачей прав (MIT/BSD/Apache-2.0 и т.п.).

11. Качество кода и тестирование

- Язык реализации: **по выбору Исполнителя** (рекомендуется Go/Rust). Код оформлен в соответствии со стандартами выбранного языка.
- Unit-тесты: покрытие критической логики не менее 70%.
- Интеграционные тесты: эмуляция SIP-диалогов с генераторами (sipp) и воспроизведение pcap (tcpreplay).
- Нагрузочное тестирование (см. Раздел 6.1) — отчёт с графиками.

12. Этапы и сроки (под требования Заказчика)

1. **Анализ существующих систем в Банке**: аудит текущего решения, точек зеркалирования, схемы резервирования, политик ИБ.

2. **Оценка объёмов данных и требований хранения/резервирования**: расчёт дисковых ёмкостей, битрейтов, RPO/RTO, матрица ролей.
3. **Проектирование архитектуры резервирования и хранения**: схема Active/Passive (VIP/VRRP), репликация журналов, каталог метаданных, схемы каталогов.
4. **Разработка подсистемы распределения пользовательских прав (RBAC)** и интеграции с AD/LDAP.
5. **Реализация основных модулей**:
6. Захват и зеркалирование трафика (SIP/RTP, SIP-TLS/SRTP опционально).
7. Автопереключение потоков (failover) и синхронное зеркалирование.
8. Управление правами доступа, аудит, API/CLI.
9. Редактирование метаданных и политики автоматической очистки.
10. Извлечение аудио и хранение WAV/MP3, каталогизация метаданных.
11. **Тестирование**: функциональное, нагрузочное, долговременное, ИБ-тесты, тест миграции и failover.
12. **Внедрение без простоя (zero-downtime cutover)** и **обучение персонала**. *(Календарный план — не более 20 календарных дней на миграцию архивов; детальный график — в Графике работ.)*

13. Порядок приёмки

13.1. **Функциональные испытания**: - Захват SIP (UDP/TCP), регистрация диалогов, фильтрация по методам/Call-ID — OK. - Экспорт PCAP и аудио (WAV/MP3) по Call-ID/номерам/времени — OK. - Зеркалирование на $\geq$2 Приёмника с **автопереключением** — OK. - Корреляция и зеркалирование RTP для вызовов — OK (при «SIP+RTP»). - Управление ролями/пользователями, разграничение прав — OK.

13.2. **Нагрузочные/надёжностные испытания**: - Генерация трафика до целевых параметров (Раздел 6.1); потери $\leq$ порогов; проверка режима **0% потерь** при синхронном зеркалировании. - Долговременный прогон 72 часа; отсутствие утечек; стабильность служб ОС. - Тест **failover**: имитация отказа основного — непрерывность записи и зеркалирования, отсутствие потери аудио/PCAP.

13.3. **ИБ-испытания**: - Аутентификация AD/LDAP/mTLS, роли и политики, аудит изменений и доступов, экспорт журналов в SIEM.

13.4. **Приёмка миграции архивов**: - Полный перенос исторических записей в штатную структуру каталогов и БД, контрольные суммы совпадают. - Временные рамки — $\leq$ **20 календарных дней**, без прерывания работы действующей системы (используется поэтапная репликация и переключение по методике blue-green).

13.5. **Результат**: Акт сдачи-приёмки.

14. Эксплуатационные требования

- Установка без перезагрузки ОС; обновление без потери данных; работа в режиме сервиса **Windows/Linux** (Windows Service / systemd).
- Требования к ресурсам (минимум): 2 vCPU, 4 ГБ RAM, 20 ГБ SSD (для базовой записи); масштабирование согласно нагрузке.
- Мониторинг: Prometheus (Linux) / PerfCounters + Event Log (Windows); алерты при: >80% диска, отсутствии Приёмников, росте потерь, отказе основного узла.

- Резервное копирование каталога данных (PCAP/аудио) и БД метаданных; регламенты восстановления.

15. Ограничения и допущения

- При SIP-TLS/SRTP без ключевого материала содержимое полезной нагрузки не анализируется и не декодируется.
- При зеркалировании best-effort гарантии доставки отсутствуют, если не оговорено иное (QoS/приоритет может быть настроен по DSCP).

16. Гарантийные обязательства и поддержка

- Гарантия: 12 месяцев с даты приёмки (исправление ошибок уровней Critical/High в регламентные сроки: 1/3 рабочих дня соответственно).
- Поддержка: электронная почта/трекер; SLA и расширенная поддержка — по отдельному соглашению.

17. Приложения

Приложение А. Таблица целевых параметров производительности/хранения

Параметр	Базовое значение	Примечание
Максимальная скорость зеркалирования	2 Гбит/с	На сервер 8 vCPU/16 ГБ
Максимум Приёмников	5	Одновременная отправка
Глубина хранения PCAP/Аудио	90 дней	Политики очистки 5.12
Потери пакетов	0% (sync) / ≤0,5% (best-effort)	См. 5.10

Приложение Б. Чек-лист приёмки (раздел 13)

Приложение В. OpenAPI-спецификация REST API (включая RBAC и операции с аудио/метаданными)

Приложение Г. Инструкция по безопасной эксплуатации (SIP-TLS/SRTP, AD/LDAP, аудит)

Приложение Д. План миграции и методика cutover без простоя

Все параметры, отмеченные как «опционально/пример», подлежат уточнению в процессе согласования с Заказчиком без изменения сути работ по Договору.