

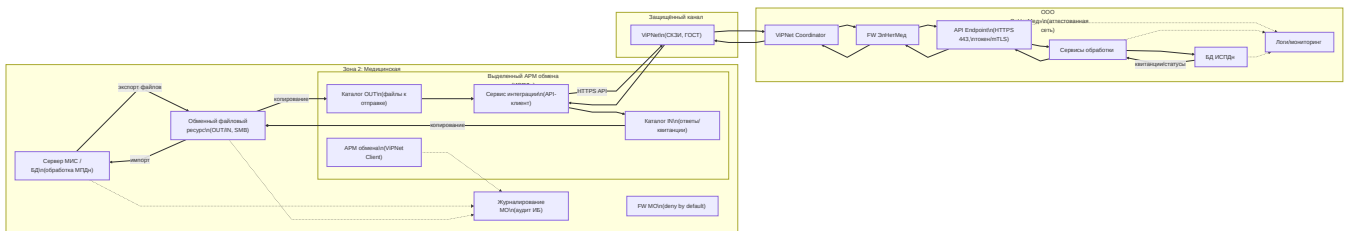


Схема сети

(файлы внутри МО → API через ViPNet наружу)

- Файловый обмен **МИС** ↔ **АРМ обмена** путём экспорта и импорта пакетов данных через контролируемый обменный ресурс с разграничением доступа и аудитом операций
- API-взаимодействие **АРМ обмена** ↔ **ООО «ЭлНетМед»**:
 - протокол **HTTPS (TCP/443)**
 - прикладная аутентификация: **токен и/или сертификат (mTLS)**
- Передача API-трафика осуществляется **исключительно внутри ViPNet**

1) Логическая схема (финальная)



2) Описание

Внутренний обмен между медицинской информационной системой и выделенным автоматизированным рабочим местом обмена осуществляется в файловом виде путём экспорта и импорта пакетов данных через контролируемый обменный ресурс с разграничением доступа и аудитом операций.

Передача данных в ООО «ЭлНетМед» выполняется выделенным АРМ обмена посредством прикладного программного интерфейса (API) по протоколу HTTPS с использованием защищённого канала связи ViPNet (сертифицированное СКЗИ).

Прикладная аутентификация осуществляется с использованием механизмов, предусмотренных API (токены и/или сертификаты). Обработка и хранение данных на стороне ООО «ЭлНетМед» выполняются в аттестованной информационной системе персональных данных.

3) Таблица потоков данных (универсальная)

№	Источник	Приёмник	Тип	Канал	Защита
1	МИС	Обменный ресурс МО	Файлы	локально	ACL, аудит
2	Обменный ресурс	АРМ обмена	Файлы	локально	ACL
3	АРМ обмена	API ЭлНетМед	API	HTTPS 443 внутри ViPNet	СКЗИ + TLS

№	Источник	Приёмник	Тип	Канал	Защита
4	API ЭлНетМед	АРМ обмена	API	HTTPS 443 внутри ViPNet	СКЗИ + TLS
5	АРМ обмена	МИС	Файлы	локально	ACL, аудит

4) Что обязательно должно быть реализовано (минимум для защиты)

На АРМ обмена

- ✓ ViPNet клиент
- ✓ API-клиент (сервис или приложение)
- ✓ Каталоги OUT / IN
- ✓ Антивирус
- ✓ Аудит файловых операций
- ✓ Ограничение сетевых подключений (только API)

В сети

- ✓ FW: разрешён **только 443/tcp** к узлам ЭлНетМед
- ✓ Нет прямого выхода МИС во внешние сети
- ✓ ViPNet — единственный путь передачи наружу

5) Почему эта схема обеспечивает требования информационной безопасности

- ✓ **МИС изолирована** от внешних сетей
- ✓ Есть **выделенный АРМ обмена**
- ✓ Есть **СКЗИ по ГОСТ**
- ✓ Прикладной уровень (API) тоже защищён
- ✓ Есть аудит и разграничение доступа