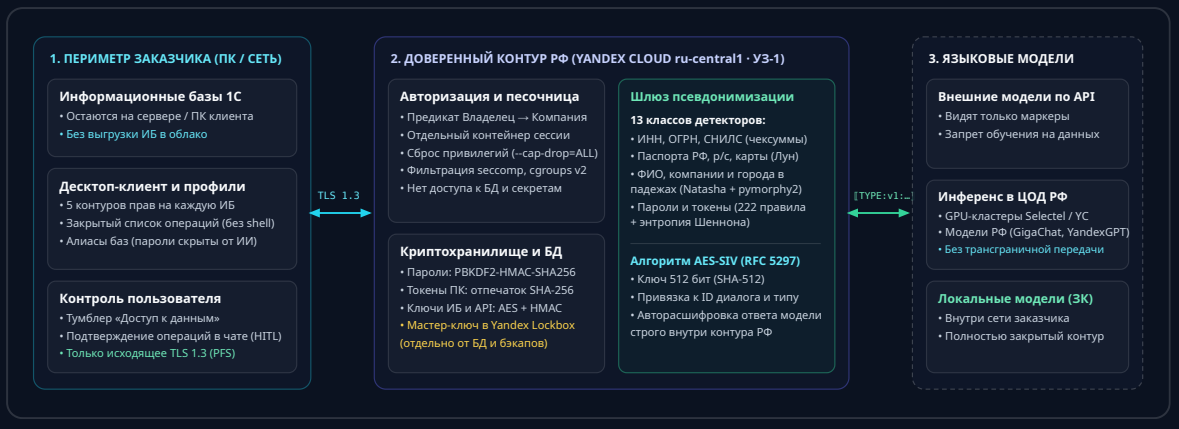
Архитектура информационной безопасности и защиты персональных данных

Техническое описание сетевой топологии, разграничения прав доступа к информационным базам 1С, криптографического хранения учётных данных и обратимой псевдонимизации чувствительных данных на границе языковых моделей.

---

1. Топология контура и схема потоков данных

Архитектура разделена на три изолированных сегмента. Входящие сетевые соединения в периметр заказчика отсутствуют; ключи шифрования БД и ключи детокенизации ПДн никогда не покидают доверенный российский контур.



Только исходящие соединения
Клиент на ПК сам устанавливает сессию по `TLS 1.3` с прямой секретностью (ECDHE + AES-GCM). Открывать порты в межсетевом экране не требуется.

Никаких произвольных команд
На рабочей станции нет свободного терминала: агент может вызывать только закрытый список операций профиля в пределах рабочей папки.

Обезличивание до выхода из РФ
ФИО, организации, реквизиты и пароли шифруются в токены `AES-SIV` до отправки запроса в модель и расшифровываются обратно только внутри РФ.

2. Разграничение прав по базам 1С и политика «Доступ к данным»

2.1. Двухуровневая блокировка чтения данных ИБ

По умолчанию агент работает только с метаданными, модулями и формами конфигурации. Запросы к записям базы данных блокируются на двух уровнях:

- **На уровне корпоративного аккаунта (`onec_data_access_allowed`):** владелец аккаунта может отключить доступ к данным для всей команды или отдельных участников.
- **На уровне сообщения сессии (`data_access_enabled`):** без явно включённого пользователем тумблера «Доступ к данным» сервер отклоняет вызов до обращения к ПК.

2.2. Скрытие строк соединения и паролей за алиасами

Агент никогда не получает адрес сервера 1С, путь к файловой базе, логин или пароль. В контекст передаётся только короткий псевдоним (например, `erp_prod`), а зашифрованные учётные данные подставляются локальным исполнителем в момент запуска платформы 1С.

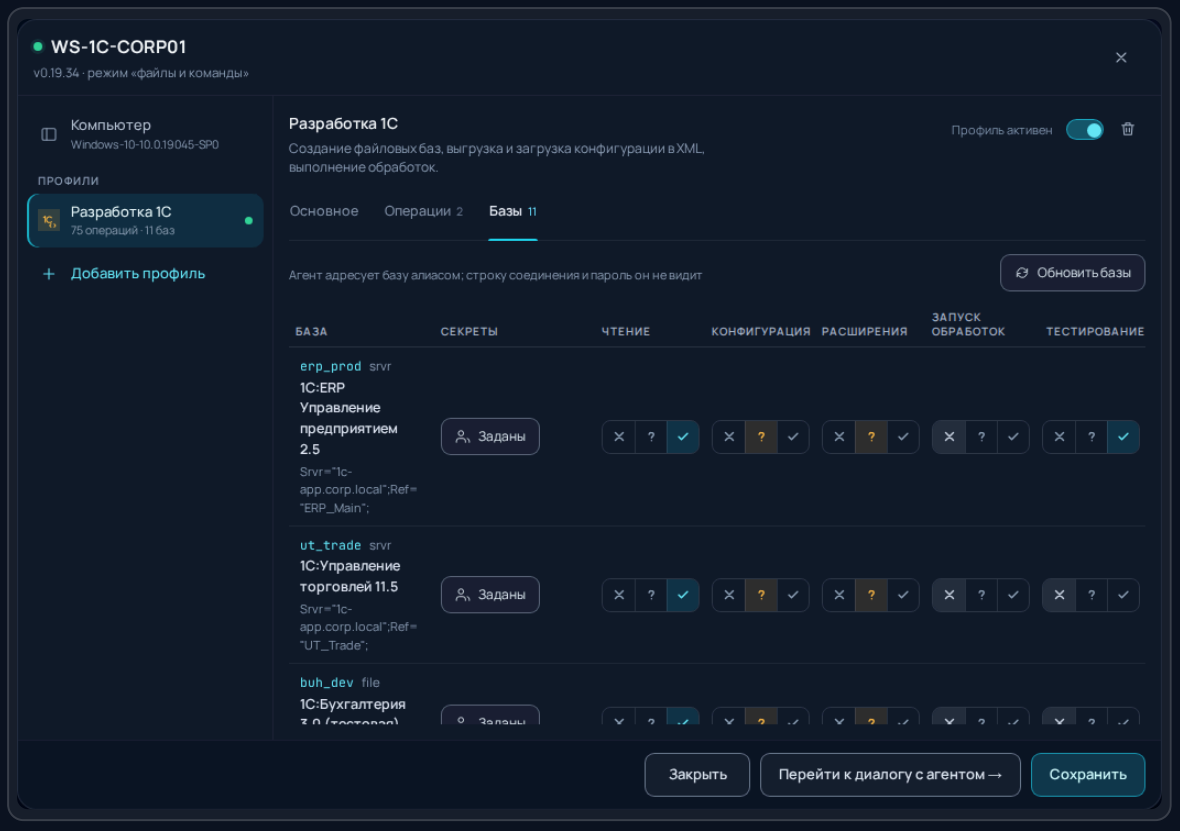


Рис. 1. Настройка профиля «Разработка 1С» в личном кабинете: алиасы баз, статус зашифрованных секретов и 5 независимых контуров разрешений (× запрещено / ? спросить / ✓ разрешено).

Контур права	Код	Контролируемые операции на рабочей станции	Режим по умолчанию
Чтение	`read`	Выгрузка метаданных в XML, чтение структуры и выполнение запросов (при включённом «Доступе к данным»)	Разрешено
Конфигурация	`config`	Загрузка изменений в основную конфигурацию ИБ и обновление конфигурации базы данных	Спросить в чате (HITL)
Расширения	`extension`	Сборка, загрузка и применение расширений конфигурации (`.cfe`) без снятия ИБ с поддержки	Спросить в чате (HITL)
Запуск обработок	`run`	Компиляция и открытие внешних обработок (`.epf`) и отчётов СКД (`.erf`) в сеансе 1С	Спросить в чате (HITL)
Тестирование	`testing`	Управляемый прогон пользовательских сценариев и проверка управляемых форм в клиенте тестирования 1С	Только для тест-баз

3. Криптографическая защита секретов и шлюз псевдонимизации ПДн

3.1. Протокол токенизации AES-SIV (RFC 5297)

• **Деривация ключа (512 бит):** `SHA-512` от ключевого материала контура.

• **Ассоциированные данные (AD):** вектор `[идентификатор_сессии, тип_сущности, v1]`.

• **Свойства:** внутри одной сессии одинаковые ФИО или ИНН дают идентичный токен ⟦`ТИП:v1:…`⟧, сохраняя связность таблиц и логики для модели. В другой сессии токен криптографически иной и не подлежит расшифровке.

3.2. Защита паролей и ключей при хранении в БД

• **Пароли пользователей:** необратимое хеширование `PBKDF2-HMAC-SHA256` с индивидуальной солью.

• **Токены компьютеров:** хранится только отпечаток `SHA-256`; сверка выполняется за константное время (`hmac.compare_digest`).

• **Пароли баз 1С и ключи интеграций:** шифрование на уровне поля БД (`AES + HMAC`); мастер-ключ хранится в **Yandex Lockbox** отдельно от БД и резервных копий.

3.3. Реестр детекторов чувствительных данных и секретов (13 классов)

Категория данных	Код детектора	Формат маркера	Механизм распознавания и верификации
ФИО и имена в падежах	`fio_nlp_ru / fio_ru`	⟦`PERSON:v1:…`⟧	Нейросеть Natasha NER + морфологический фильтр частей речи pymorphy2 + регулярные грамматики ФИО и инициалов
Компании и банки	`company_ru / org_nlp_ru`	⟦`ORGANIZATION:v1:…`⟧	ОПФ РФ (ООО, АО, ПАО, ЗАО, ИП) в кавычках + нейросетевое выделение брендов и банков без кавычек
Города и локации	`loc_nlp_ru`	⟦`LOCATION:v1:…`⟧	Нейросетевое выделение топонимов в косвенных падежах с отсечением глаголов и служебных слов
ИНН (10 и 12 цифр)	`inn`	⟦`INN_ORG / PERSON`⟧	Математическая проверка контрольных разрядов ФНС и фильтрация совпадений с дробными суммами
ОГРН и ОГРНИП	`ogrn`	⟦`OGRN / OGRN_IP`⟧	Верификация 13- и 15-значных номеров по контрольному числу (модуль 11 / 13)
СНИЛС	`snils`	⟦`SNILS:v1:…`⟧	Весовая проверка контрольной суммы СФР (ПФР) по модулю 101
Паспорт РФ	`passport_ru`	⟦`RU_PASSPORT:v1:…`⟧	Контекстный поиск серии (4 цифры), номера (6 цифр) и кода подразделения в паспортном окружении
Карты и расчётные счета	`bank_card / account`	⟦`BANK_CARD / ACCOUNT`⟧	Проверка 16-значных карт по алгоритму Луна; 20-значные расчётные и корр. счета РФ (407.., 408.., 301..)
Телефоны РФ и Email	`phone / email`	⟦`PHONE / EMAIL`⟧	Валидация российской телефонной нумерации и проверка почтовых адресов по стандарту RFC 5322
Пароли, ключи и токены	`secrets`	⟦`SECRET:v1:…`⟧	222 сигнатурных правила + расчёт информационной энтропии Шеннона (пароли в URI БД, API-ключи, JWT, приватные ключи)

4. Эшелонированная защита от атак на ИИ, контейнерная изоляция и 152-ФЗ

4.1. Матрица инженерных контрмер против специфических уязвимостей ИИ-агентов

Вектор атаки / класс угрозы	Механизм нейтрализации в Aether Lab	Системный / криптографический примитив
Косвенная промпт-инъекция и атака «запутанного посредника»	Перехват всех изменяющих вызовов детерминированным контроллером графа до фактического выполнения операции	`Аппаратная пауза графа под подтверждение (HITL) · валидация JSON-схемы аргументов`
Утечка ПДн, коммерческой тайны и паролей во внешнюю модель	Двунаправленная псевдонимизация на границе контура РФ до формирования сетевого пакета к провайдеру ИИ	`AES-SIV (RFC 5297) · привязка к сессии · морфологический NER + энтропия Шеннона`
Избыточные полномочия агента и выход за пределы рабочей папки	Отказ от свободной командной строки на ПК в пользу закрытого реестра операций профиля и канонизации путей	`Закрытый реестр операций профиля · канонизация путей (защита от «../») · 5 контуров ИБ`
Побег из контейнера и горизонтальное перемещение в облаке	Выполнение кода сессии в одноразовом непривилегированном контейнере с усечёнными системными вызовами ядра	`Сброс привилегий (--cap-drop=ALL) · запрет повышения прав · seccomp · квоты cgroups v2`
Межтенантная утечка данных и атаки по времени ответа	Принудительная фильтрация всех запросов к БД и векторным индексам по предикату компании; сверка ключей за константное время	`Строгий предикат изоляции организаций · hmac.compare_digest · SHA-256`
Лавинообразное зацикливание вызовов и исчерпание квот	Автоматическое размыкание рекурсивных циклов агента, скользящие лимиты частоты запросов и контроль бюджета	`Детектор зацикливания вызовов · скользящее окно ограничения частоты · контроль квот`

4.2. Выполнение требований 152-ФЗ, ФСТЭК и ГОСТ

• **Локализация (ч. 5 ст. 18 152-ФЗ):** СУБД PostgreSQL, векторные индексы Qdrant, кэши Redis и хранилище S3 физически расположены в РФ — ЦОД Yandex Cloud (Москва, `ru-central1`).

• **Аттестация площадки:** 1-й уровень защищённости ПДн (**УЗ-1** по ПП РФ № 1119 и приказу ФСТЭК № 21), ГОСТ Р 57580.1-2017, ISO/IEC 27001/27017/27018, PCI DSS.

• **Правовое основание:** договор с юрлицом РФ по ЭДО, NDA и поручение оператора на обработку ПДн (ч. 3 ст. 6 152-ФЗ).

• **Криптографическая санация (ст. 21 152-ФЗ):** каскадное удаление данных из таблиц, индексов, кэшей и резервных копий с оформлением акта.

4.3. Варианты развёртывания и российского GPU-инференса

• **1. Облако РФ + выделенный инференс в РФ (Selectel / Yandex Cloud):** работа платформы в ЦОД РФ (УЗ-1) с маршрутизацией запросов на выделенные GPU-кластеры в российских дата-центрах (Selectel, Yandex Cloud) и поддержкой реестровых моделей РФ (GigaChat, YandexGPT) — 0 % трансграничного трафика.

• **2. Выделенный сервер (Dedicated):** отдельный виртуальный сервер, изолированная СУБД и файловое хранилище под одного заказчика, сетевой туннель `IPsec / WireGuard` и подключение корпоративных шлюзов.

• **3. Автономный контур (на серверах заказчика):** полная установка платформы во внутреннем периметре предприятия с подключением к локальным корпоративным моделям ИИ без внешнего трафика.
