РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ И АДМИНИСТРАТОРА

программы для ЭВМ «Версиум AI»

1. Общие сведения

1.1. Назначение документа

Настоящее руководство описывает работу с программой для ЭВМ «Версиум AI» (далее программа) через веб-интерфейс. Руководство предназначено для пользователей, администраторов и сотрудников, выполняющих функции аудита информационной безопасности. Установка программы описана в документе «Инструкция по установке», состав функций в документе «Описание функциональных характеристик».

1.2. Назначение программы

Программа является единой контролируемой точкой доступа сотрудников, приложений и AI-агентов организации к языковым моделям. Программа обнаруживает и маскирует чувствительные данные до передачи в модель, останавливает передачу запрещённой информации, фиксирует обращения к моделям и позволяет поручать AI-агентам задачи на серверах организации в рамках утверждённых рабочих процессов и выданных прав.

Программа работает в двух режимах, которые используются одновременно и имеют общие настройки.

- **Веб-платформа.** Сотрудники работают с AI-агентами в веб-чате программы.
- **Прокси для ИИ-трафика.** Приложения, сервисы и AI-агенты организации обращаются к языковым моделям через API шлюза программы по персональным токенам.

1.3. Роли

Роль	Назначение
Пользователь	Работа в чате с доступными AI-агентами, запуск сценариев и процессов, работа в пространствах, подключение личных исполнителей, выпуск личных токенов прокси, ведение личной базы знаний агентов
Администратор	Настройка провайдеров, агентов, навыков, MCP-серверов, исполнителей, процессов, расписаний, сценариев, пространств, маскирования, прокси; управление пользователями, группами, способами входа, лицензиями и пакетами конфигурации; просмотр аудита и сводной панели
ИБ-аудитор	Просмотр аудита диалогов, журнала доступа к оригиналам и журнала файлов пространств; раскрытие немаскированных значений с обязательной фиксацией факта раскрытия

Пользователю может быть назначено несколько ролей, при входе он получает объединение их полномочий. Доступ к агентам, процессам, исполнителям, сценариям и пространствам дополнительно выдаётся группам пользователей. Объект, право на который не выдано, пользователю не виден.

1.4. Требования к рабочему месту

Для работы требуется компьютер с современным веб-браузером (актуальные версии Яндекс Браузера, Chromium, Google Chrome, Mozilla Firefox, Microsoft Edge, Safari) и сетевой доступ к адресу

установки программы по протоколу HTTPS. Установка дополнительного программного обеспечения на рабочее место не требуется, кроме случаев подключения личного исполнителя (раздел 3.6) или клиентского приложения через прокси (раздел 3.7).

1.5. Термины

Термин	Значение
Провайдер	Источник языковых моделей: внешний сервис, модель организации или локальная модель в контуре заказчика
AI-агент	Профиль работы с моделью: основная модель, системная инструкция, навыки, инструменты и права их использования
Навык (скилл)	Переиспользуемый набор инструкций для агента в формате SKILL.md
MCP-сервер	Внешний поставщик инструментов для агентов по протоколу Model Context Protocol, например информационная система организации
Исполнитель	Отдельно устанавливаемая программа, которая выполняет инструменты агента (файловые операции, команды, скрипты) на сервере организации
Сценарий запуска	Сохранённая связка агента и исполнителя или рабочий процесс, который пользователь запускает с главной страницы
Пространство	Рабочая область, объединяющая чаты, файлы, базу знаний и состав агентов
Маска	Замена чувствительного значения, которую получает модель вместо оригинала
Оригинал	Исходное немаскированное значение

2. Начало работы

2.1. Вход в программу

1. Откройте в браузере адрес программы, выданный администратором, например `https://ai.company.ru`.
2. Введите логин и пароль. В зависимости от настроек организации вход выполняется по локальной учётной записи, по учётной записи Active Directory или через корпоративный сервис единого входа (кнопка входа через OpenID Connect).
3. Если администратор установил признак смены пароля, задайте новый пароль при первом входе.

При вводе неверных данных выводится сообщение об ошибке. Если вход запрещён настройками сопоставления ролей, обратитесь к администратору.

2.2. Интерфейс программы

Экран программы состоит из бокового меню слева и рабочей области справа. В верхней части рабочей области выводится строка навигации.

В нижней части бокового меню расположены переключатель **«Работа»** / **«Администрирование»** (второй пункт доступен только администратору и ИБ-аудитору) и карточка

текущего пользователя с его ролью. Через карточку пользователя открываются личные настройки (язык интерфейса, часовой пояс, смена пароля) и выполняется выход из программы. Боковое меню сворачивается кнопкой рядом с логотипом.

Меню раздела «Работа» содержит пункты «Сценарии», «Все чаты», «Мои исполнители», «LLM-прокси», «LLM-вики», а также поиск и список пространств пользователя.

Меню раздела «Администрирование» сгруппировано по блокам «Настройка ИИ» (провайдеры, агенты, управление LLM-прокси, скрипты, процессы, исполнители, MCP-серверы, скиллы), «Безопасность» (словари, маскирование), «Аудит» (аудит диалогов, журнал доступа, файлы пространств) и «Управление» (дашборд, пользователи, группы пользователей, настройки авторизации, политика LLM-вики, пакеты конфигурации, сценарии запуска, пространства, планировщик, лицензии). Состав меню зависит от ролей пользователя.

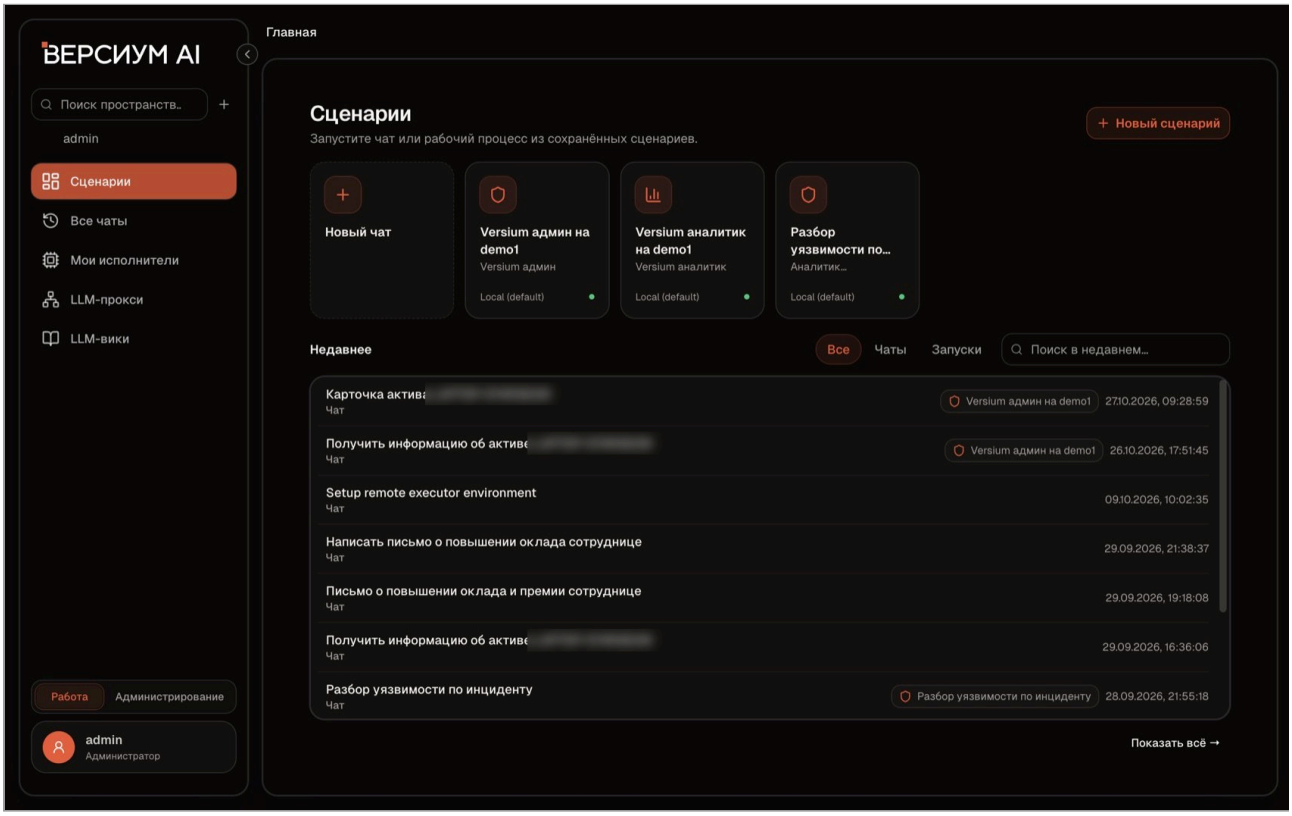


Рисунок 1. Главная страница «Сценарии»

3. Работа пользователя

3.1. Главная страница и сценарии

Главная страница «Сценарии» открывается после входа. В верхней части страницы выводятся плитки сценариев запуска, доступных пользователю. На плитке указаны название сценария, AI-агент и исполнитель, а цветной индикатор показывает, доступен ли исполнитель.

- Нажмите плитку сценария, чтобы открыть новый чат с заданным агентом и исполнителем или запустить рабочий процесс.
- Нажмите плитку **«Новый чат»**, чтобы выбрать агента и исполнителя вручную.
- Кнопка **«Новый сценарий»** создаёт личный сценарий (если это разрешено администратором).

Ниже расположен блок **«Недавнее»** с последними чатами и запусками процессов. Переключатели «Все», «Чаты», «Запуски» и строка поиска позволяют отфильтровать список, ссылка «Показать всё» открывает полную историю.

3.2. Работа в чате с AI-агентом

1. Откройте чат через сценарий или плитку «Новый чат».
2. Введите сообщение в поле внизу экрана и нажмите кнопку отправки или клавишу Enter. Сочетание Shift+Enter переносит строку.
3. Чтобы сослаться на файл или папку рабочей области исполнителя, введите символ `@` и выберите объект из списка.
4. Ответ агента выводится по мере формирования. Ответ можно остановить и при необходимости отправить сообщение повторно.

В заголовке чата отображаются имя агента, исполнитель и его состояние, а также заполнение контекста модели. При приближении к пределу контекста история беседы уплотняется автоматически.

В ходе работы агент показывает выполняемые шаги, вызываемые инструменты и список задач с отметками выполнения. Если право агента на инструмент требует подтверждения, программа выводит запрос. Пользователь разрешает вызов однократно или до конца сеанса либо отклоняет его. Если агенту не хватает сведений, он задаёт уточняющий вопрос с вариантами ответа, пользователь может выбрать вариант или ввести свой.

Изображения прикрепляются к сообщению, только если это разрешено политикой провайдера. Если сообщение содержит информацию, запрещённую к передаче, оно не отправляется в модель и пользователь получает сообщение о причине блокировки.

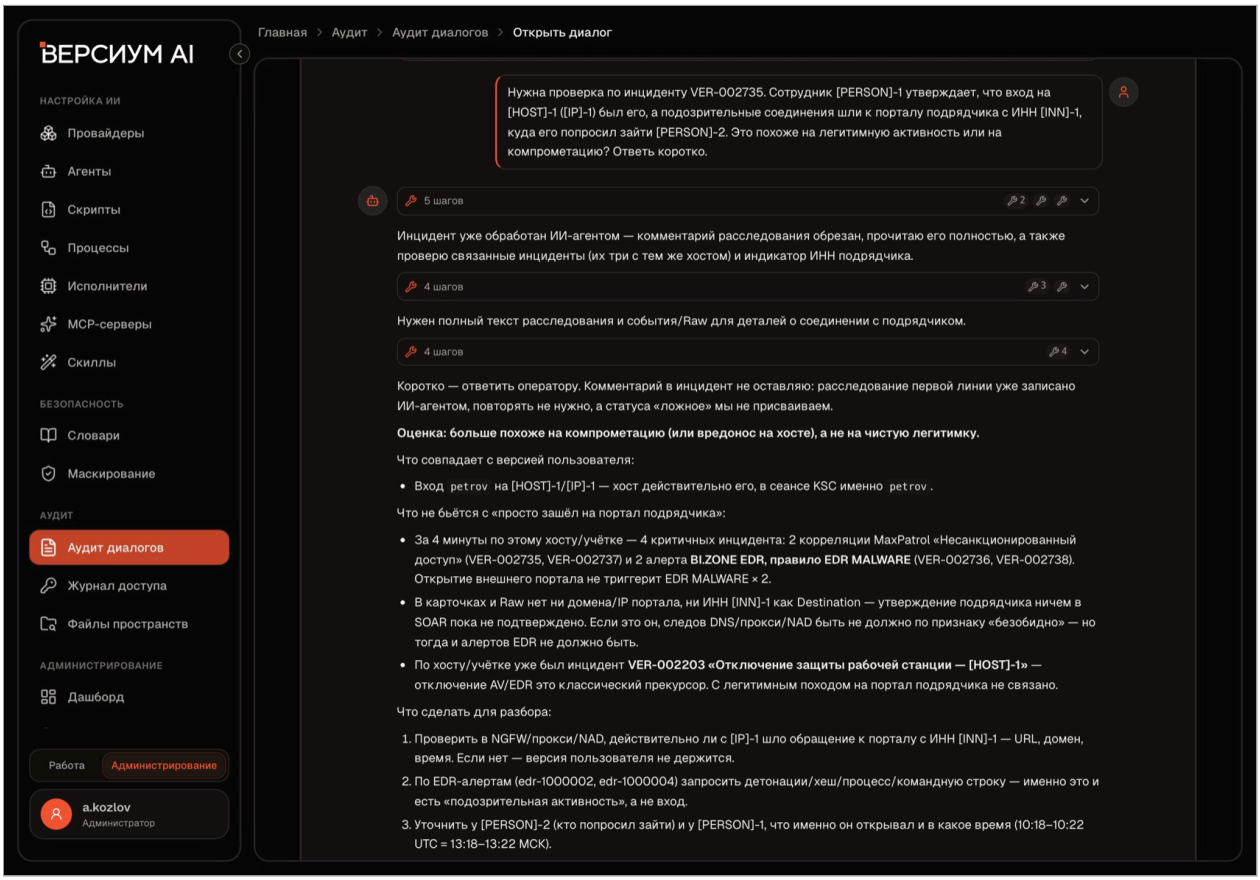


Рисунок 2. Чат с AI-агентом и маскирование данных

Защита данных в чате. Пользователь работает с настоящими данными. Перед передачей в модель программа заменяет чувствительные значения масками, а в ответе модели восстанавливает оригиналы. Внутри одного диалога одно и то же значение получает одну и ту же маску. Какие данные маскируются, определяет администратор (раздел 4.10).

3.3. Все чаты

Раздел **«Все чаты»** содержит полную историю чатов пользователя с поиском, фильтрами и сортировкой. Для каждого чата указаны название, сценарий, агент, исполнитель, объём использованных токенов, дата создания и последней активности. Кнопка «Открыть чат» продолжает беседу.

3.4. Пространства

Пространство объединяет чаты, файлы, базу знаний и состав агентов для команды или задачи. Каждому пользователю создаётся личное пространство, общие пространства создаёт администратор и выдаёт к ним доступ группам. Список пространств выводится в боковом меню, для поиска используется строка «Поиск пространств», кнопка «+» создаёт новое пространство (если это разрешено).

В пространстве доступны его чаты, файлы и агенты, допущенные в пространство. Чаты выполняются на домашнем исполнителе пространства. Операции с файлами пространства фиксируются в журнале.

3.5. LLM-вики

LLM-вики является личной базой знаний, которую агенты ведут между чатами пользователя. Для начала работы нажмите **«Включить LLM-вики»**. Агенты дополняют вики по ходу работы и используют накопленные сведения в следующих беседах. Доступ к функции определяется политикой администратора.

3.6. Мои исполнители

Раздел позволяет подключить собственный компьютер пользователя как личный исполнитель для личных сценариев.

1. Нажмите **«Подключить исполнитель»**, укажите имя и, при необходимости, описание.
2. Нажмите **«Скачать исполнитель»** и загрузите дистрибутив для своей операционной системы.
3. Запустите исполнитель с одноразовым токеном подключения, который программа покажет после создания. Токен показывается один раз, сохраните его до запуска.
4. Исполнитель подключится к программе исходящим соединением и получит статус «Онлайн». Входящий порт на компьютере не требуется.

3.7. LLM-прокси

Раздел позволяет подключить клиентское приложение (например, AI-ассистента разработчика) к языковым моделям через шлюз программы.

1. Нажмите **«Новый токен»**.
2. Выберите провайдер-шлюз и режим. В режиме **«Ключ компании»** запросы выполняются с ключом организации, хранящимся в шлюзе, и направляются на выбранный маршрут. В режиме **«Свой ключ»** (если право выдано администратором) используется собственный ключ пользователя, который проходит через шлюз без сохранения.
3. Выберите маршрут (модель или агента), задайте имя токена и срок действия в днях (не более 90 или иного значения, установленного администратором).
4. Нажмите **«Создать токен»**. Программа покажет токен и готовые настройки подключения клиентского приложения. Токен показывается один раз.

Список **«Мои токены»** содержит выпущенные токены, срок их действия и позволяет отозвать токен. Программа напоминает об истечении срока. Запросы через прокси маскируются, проверяются

политиками и фиксируются в журнале аудита так же, как сообщения в чате.

3.8. Запуск сценария из платформы Versium

При совместном использовании с платформой Versium сценарий программы открывается из карточки объекта платформы кнопкой **«Запрос к ИИ»**. Программа создаёт новый чат и автоматически отправляет первое сообщение, собранное из шаблона сценария и параметров ссылки, например номера инцидента. Чат выполняется от имени вошедшего пользователя, с его правами, лимитами и аудитом.

4. Администрирование

Функции раздела доступны пользователям с ролью «Администратор». Для перехода переключите боковое меню в режим «Администрирование». Изменения в формах сохраняются кнопками «Сохранить», «Добавить» или «Создать», кнопка «Отмена» или закрытие окна отменяет изменения. Удаление объектов выполняется кнопкой «Удалить» с подтверждением.

4.1. Провайдеры и модели

Раздел **«Провайдеры»** содержит список подключённых провайдеров языковых моделей.

1. Нажмите **«Добавить провайдера»**.
2. Укажите имя провайдера, тип (например, OpenAI-совместимый HTTP-интерфейс или аудируемый шлюз), базовый URL и ключ доступа.
3. Задайте политику **«Картинки в чате»** («Запрещено», с предупреждением или фиксацией в аудите, «Разрешено»). К изображениям маскирование не применяется, поэтому по умолчанию их передача запрещена.
4. Нажмите **«Добавить провайдера»**.

Кнопка **«Модели»** на карточке провайдера открывает перечень моделей провайдера, в котором задаются модели и их цены для учёта стоимости. Для провайдеров типа «аудируемый шлюз» на карточке отображаются политика двоичного содержимого и политика серверных инструментов провайдера.

Ключ доступа хранится в шлюзе в зашифрованном виде и в интерфейсе не показывается. Для замены ключа введите новое значение, пустое поле сохраняет ранее введённый ключ. Агенты и приложения обращаются к модели по её имени в программе, поэтому замена провайдера или модели не требует изменения приложений.

4.2. AI-агенты

Раздел **«Агенты»** содержит профили AI-агентов. Новый агент создаётся кнопкой **«Добавить агента»**, существующий изменяется кнопкой «Редактировать» на карточке. Окно редактирования содержит четыре вкладки.

Профиль. Имя агента, описание, системная инструкция (системный промпт) и основная модель.

Инструменты и разрешения. Для каждого инструмента задаётся режим использования.

Режим	Действие
Разрешено	Агент вызывает инструмент без подтверждения
Подтверждать каждый раз	Перед каждым вызовом пользователь подтверждает действие
Подтвердить один раз на сессию	Подтверждение запрашивается один раз за сеанс

Режим	Действие
Запрещено	Агент видит инструмент, но вызвать его не может
Скрыто	Инструмент агенту не виден

На вкладке настраиваются файловые операции на исполнителе (чтение, запись, правка, поиск, удаление), инструменты каждого MCP-сервера (режим по умолчанию для сервера и исключения для отдельных инструментов) и перечень навыков, которые агент может вызвать. Навыки и инструменты, не выданные агенту явно, по умолчанию скрыты. Собственные (нативные) инструменты провайдера модели запрещены безусловно.

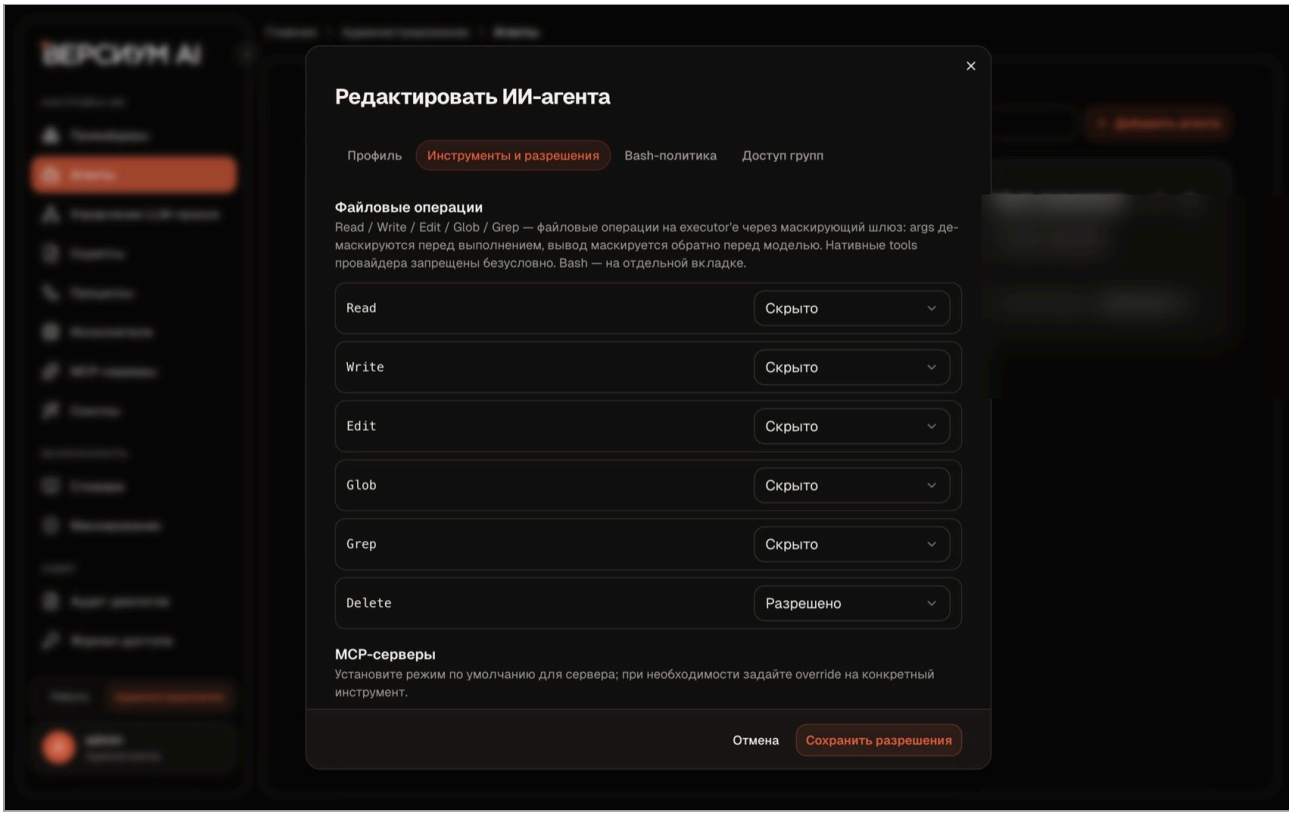


Рисунок 3. Права агента на инструменты

Bash-политика. Общий режим выполнения команд, правила для отдельных команд (побеждает наиболее точное совпадение), дополнительные разрешённые пути и переключатели для потенциально опасных конструкций командной оболочки: выход за пределы рабочей папки, подстановка команд, `eval` и `source`, запуск интерпретатора с флагом `-c`, передача вывода в оболочку, удалённое выполнение через `ssh`, `find -exec` и `xargs`. По умолчанию такие конструкции запрещены. Внутри пространств дополнительные пути не действуют.

Доступ групп. Группы пользователей, которым доступен агент. Участники групп видят агента в списке выбора в чате.

Изменения на вкладках сохраняются кнопками «Обновить агента» или «Сохранить разрешения».

4.3. Скиллы

Раздел **«Скиллы»** содержит навыки агентов. Навык загружается кнопкой **«Добавить скилл»** одним из способов: файл SKILL.md, zip-архив с одним или несколькими навыками либо вставленный текст. Имя навыка берётся из описания в файле или задаётся вручную в формате kebab-case. Агент получает навык только после выдачи на вкладке «Инструменты и разрешения» профиля агента.

4.4. MCP-серверы

Раздел **«MCP-серверы»** содержит подключённые поставщики инструментов.

1. Нажмите **«Добавить MCP-сервер»**.
2. Укажите имя, описание, область действия (системный сервер или сервер на конкретном исполнителе) и URL.
3. Выберите способ авторизации (без авторизации, токен, API-ключ с именем HTTP-заголовка, логин и пароль, OAuth2 Client Credentials) и введите секрет.
4. Нажмите **«Создать»**.

Программа автоматически получает перечень инструментов сервера. На карточке отображаются состояние подключения («Онлайн» или «Ошибка»), время последнего опроса, текст последней ошибки и число инструментов. Кнопка «Показать инструменты» выводит инструменты с описаниями и входными схемами, кнопка «Обновить инструменты» повторяет опрос.

Флажок «Не проверять сертификат сервера» допускается только для тестовых стендов. Для серверов с сертификатом внутреннего удостоверяющего центра добавьте корневой сертификат в настройках авторизации (раздел 4.15).

В программу встроен управляющий MCP-сервер, через который администратор может настраивать программу из чата (MCP-серверы, агенты и их права, провайдеры, маскирование, расписания). Он доступен только администраторам.

4.5. Исполнители

Раздел **«Исполнители»** содержит удалённые исполнители организации.

1. Нажмите **«Добавить исполнителя»**, укажите имя и описание, нажмите «Создать». Программа выдаст одноразовый токен подключения.
2. Нажмите **«Скачать исполнитель»** и загрузите дистрибутив для Linux или Windows.
3. Установите исполнитель на целевом сервере и запустите его с токеном подключения.

На карточке исполнителя отображаются состояние, имя хоста, операционная система, версия, рабочая папка и время последней активности. Исполнитель работает в пределах рабочей папки, права на исполнитель выдаются группам.

4.6. Скрипты и рабочие процессы

Раздел **«Скрипты»** содержит каталог скриптов для процессов. При добавлении указываются название, описание, путь к скрипту на исполнителе и аргументы.

Раздел **«Процессы»** содержит рабочие процессы. Кнопка **«Добавить процесс»** открывает визуальный редактор. Процесс собирается на холсте перетаскиванием узлов из панели слева: начало, AI-агенты, скрипты, параллельное выполнение, ожидание параллельных шагов, цикл. Узлы соединяются переходами, следующий шаг выбирается по коду результата предыдущего. Для цикла задаётся ограничение числа итераций и условие досрочного выхода.

- **«Валидация»** проверяет структуру процесса.
- **«Сохранить процесс»** сохраняет изменения.
- **«Запустить»** выполняет процесс с начальным вводом. В ходе запуска отображаются состояние узлов и попытки, упавший шаг интерактивного запуска можно повторить.

Агент в процессе выполняет только утверждённые шаги. Исполнитель процесса выбирается в верхней части редактора.



Рисунок 4. Визуальный редактор рабочего процесса

4.7. Планировщик

Раздел **«Планировщик»** запускает рабочие процессы по расписанию.

1. Нажмите **«Новое расписание»**.
2. Задайте cron-выражение. Программа покажет ближайшие запуски в часовом поясе UTC и в локальном времени.
3. Укажите название, описание, часовой пояс и процесс.
4. При необходимости переопределите исполнитель и задайте политики: наверстывание пропущенных запусков, поведение при наложении на активный запуск, максимальная длительность запуска, разрешение интерактивности для фоновых запусков.
5. Включите расписание и сохраните его.

В списке расписаний отображаются cron-выражение, следующий запуск, результат последнего запуска и признак включения. Процесс можно запустить вне расписания.

4.8. Сценарии запуска

Раздел **«Сценарии запуска»** содержит общие и групповые сценарии, которые пользователи видят плитками на главной странице. Кнопка **«Создать сценарий»** открывает форму.

Поле	Значение
Название, иконка, описание	Отображаются на плитке
Тип	Чат или рабочий процесс
Видимость	Личная, для групп, для всей организации
Пространство	Пространство, в котором создаются чаты сценария
Агент, исполнитель	Агент и исполнитель для чата (конкретный или удалённый)

Поле	Значение
Шаблон первого сообщения	Текст, который отправляется автоматически. Вставки вида `{IncidentId}` заполняются из ссылки
Ключ ссылки	Идентификатор для открытия сценария из внешней системы (строчные латинские буквы, цифры и дефис). Оставьте пустым, если сценарий не открывают по ссылке

Значения параметров ссылки ограничены буквами, цифрами и знаками `. _ : -`, что исключает передачу произвольного текста через ссылку.

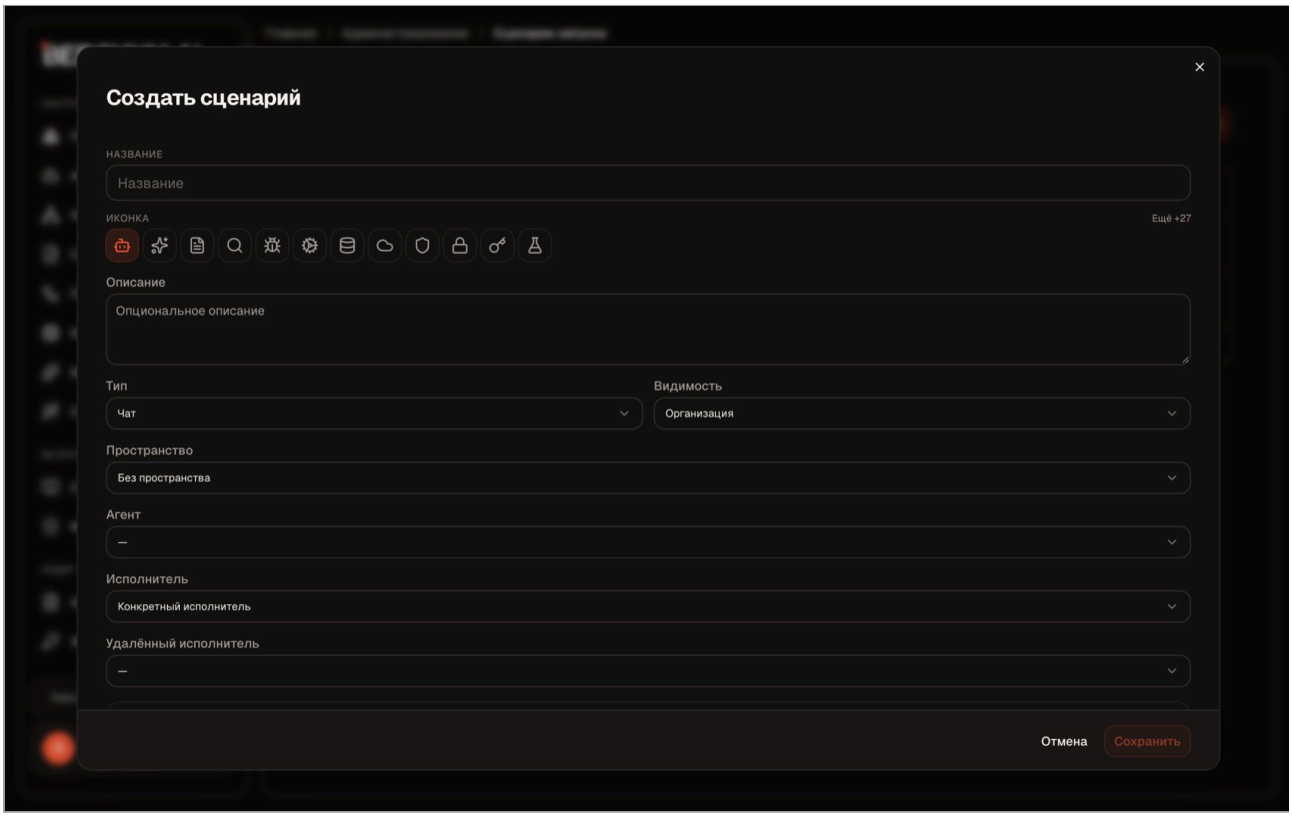


Рисунок 5. Создание сценария запуска

4.9. Пространства

Раздел **«Пространства»** содержит все пространства с видимостью, домашним исполнителем, числом агентов, групп и чатов и состоянием. Кнопка **«Новое пространство»** открывает форму, в которой задаются название, слаг (формируется из названия), описание, иконка, видимость, домашний исполнитель, допустимые агенты, агент по умолчанию и группы с доступом. Пространство можно перевести в архив. Агента, которому разрешён выход за пределы рабочей папки, привязать к пространству нельзя.

4.10. Маскирование и словари

Раздел **«Маскирование»** содержит механизмы обнаружения и замены чувствительных данных. Кнопка **«Новый механизм»** открывает форму.

Поле	Значение
Название, описание	Наименование правила

Поле	Значение
Тип обнаружения	Регулярное выражение, список слов (словарь), шаблон (адрес электронной почты, телефон, URL, IP-адрес, банковская карта), диапазон чисел, алгоритм Луна, распознавание именованных сущностей с помощью языковой модели
Параметры обнаружения	Шаблон регулярного выражения и учёт регистра, перечень слов, границы диапазона в зависимости от типа
Тип замены	Константа с уникальной нумерацией (например, `[REDACTED]-1`) или правдоподобное значение из словаря замен
Восстанавливать в прокси	Восстановление оригинала в ответах прокси. Для секретов (паролей, ключей) флажок следует выключить
Тип токена прокси	Обязателен для маскирования в прокси. Для правил, действующих только в чатах, поле оставляется пустым

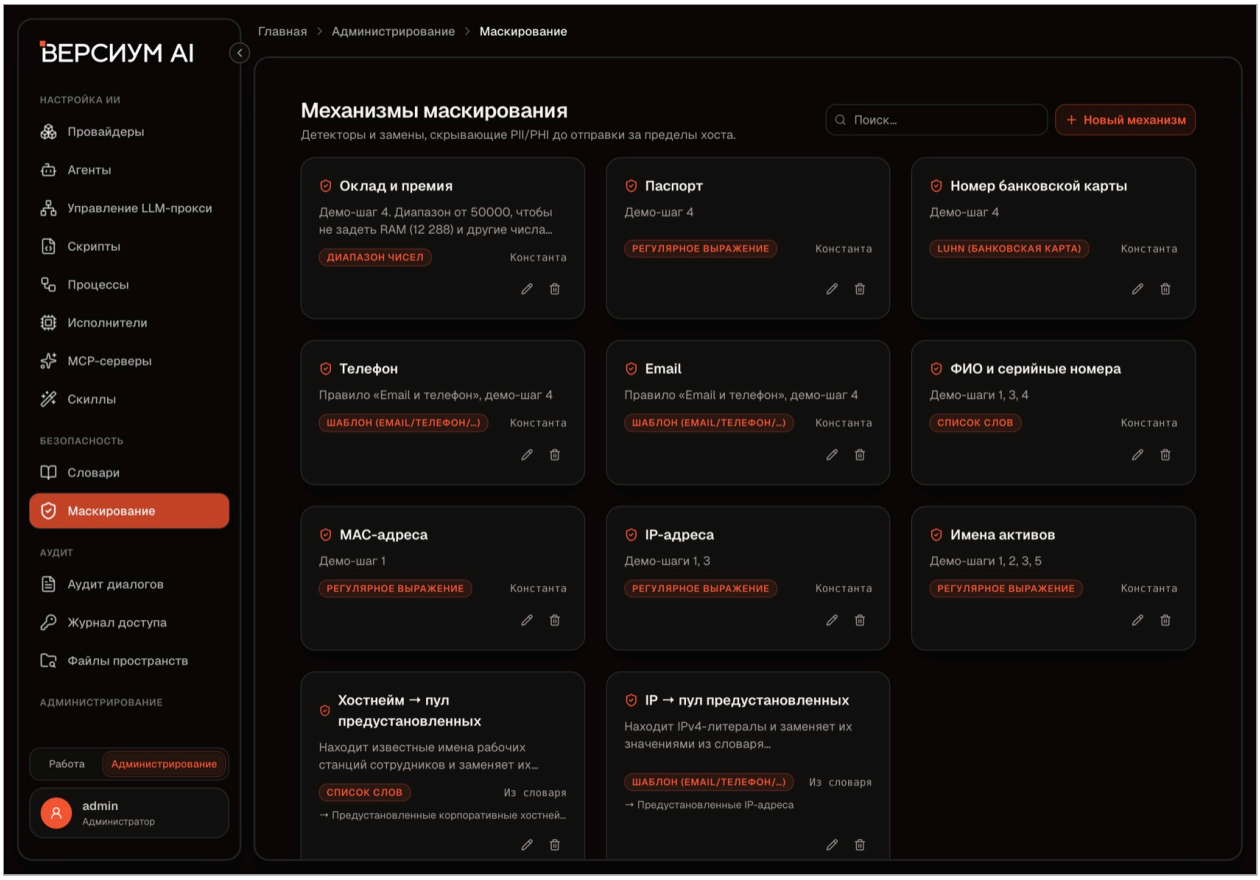


Рисунок 6. Механизмы маскирования

Раздел **«Словари»** содержит словари замен, то есть списки правдоподобных значений (например, условных имён хостов или IP-адресов), которые подставляются вместо оригиналов. Словарь создаётся кнопкой **«Новый словарь»** и наполняется вручную или с помощью AI-агента с предварительным просмотром.

Набор и порядок механизмов маскирования назначаются каждому провайдеру отдельно. Например, для локальной модели в контуре организации маскирование может быть ослаблено, а для внешнего провайдера применяться в полном объёме. Если правила изменены, в разделе «Управление LLM-прокси» доступна команда «Перемаскировать историю».

4.11. Блокировка передачи данных

Программа останавливает запрос, если он содержит информацию, запрещённую к передаче, и сообщает причину пользователю или приложению. Администратор настраивает блокировку следующими средствами.

- Политика изображений и двоичного содержимого для каждого провайдера (раздел 4.1).
- Политика серверных инструментов провайдера для прокси: блокировать, только фиксировать в аудите, разрешать.
- Режимы «Запрещено» и «Скрыто» для инструментов агентов и Bash-политика (раздел 4.2). Команды, не прошедшие политику, не выполняются.

4.12. Управление LLM-прокси

Раздел **«Управление LLM-прокси»** содержит вкладки.

- **Маршруты моделей.** Имя маршрута, провайдер-шлюз, модель, протокол, малая модель для служебных запросов, пресет клиентского приложения, группы с доступом, признак включения.
- **Маршруты агентов.** Маршрут к AI-агенту программы через прокси. Доступ определяется правами агента (раздел 4.2).
- **Право «Свой ключ».** Группы, которым разрешено использовать собственный ключ провайдера.
- **Токены.** Выпуск токена для пользователя или технической учётной записи и список всех токенов с возможностью отзыва.
- **Настройки.** Срок хранения записей, бюджет времени на маскирование, минимальная длина известного оригинала, максимальный срок токена и срок напоминания об истечении, имена инструментов командной оболочки, разрешение самостоятельной выдачи токенов пользователями, отклонение подписочных токенов в режиме «Свой ключ», команда «Перемаскировать историю».

4.13. Политика LLM-вики

Раздел определяет, кому доступна личная база знаний агентов. Режимы доступа «Разрешено всем», «Всем, кроме списка», «Никому, кроме списка». Изменение сохраняется кнопкой «Сохранить».

4.14. Пользователи, группы и лимиты

Раздел **«Пользователи»** содержит учётные записи с логином, именем, ролями, источником (локальная запись, Active Directory, OIDC) и признаком активности.

1. Нажмите **«Создать пользователя»**.
2. Укажите логин, источник, имя и фамилию.
3. Для локальной записи задайте пароль и, при необходимости, признак смены пароля при следующем входе.
4. Назначьте хотя бы одну роль («Администратор», «ИБ-аудитор», «Пользователь») и группы.
5. Нажмите «Сохранить».

В списке пользователей доступны отключение учётной записи, смена пароля и назначение личных лимитов.

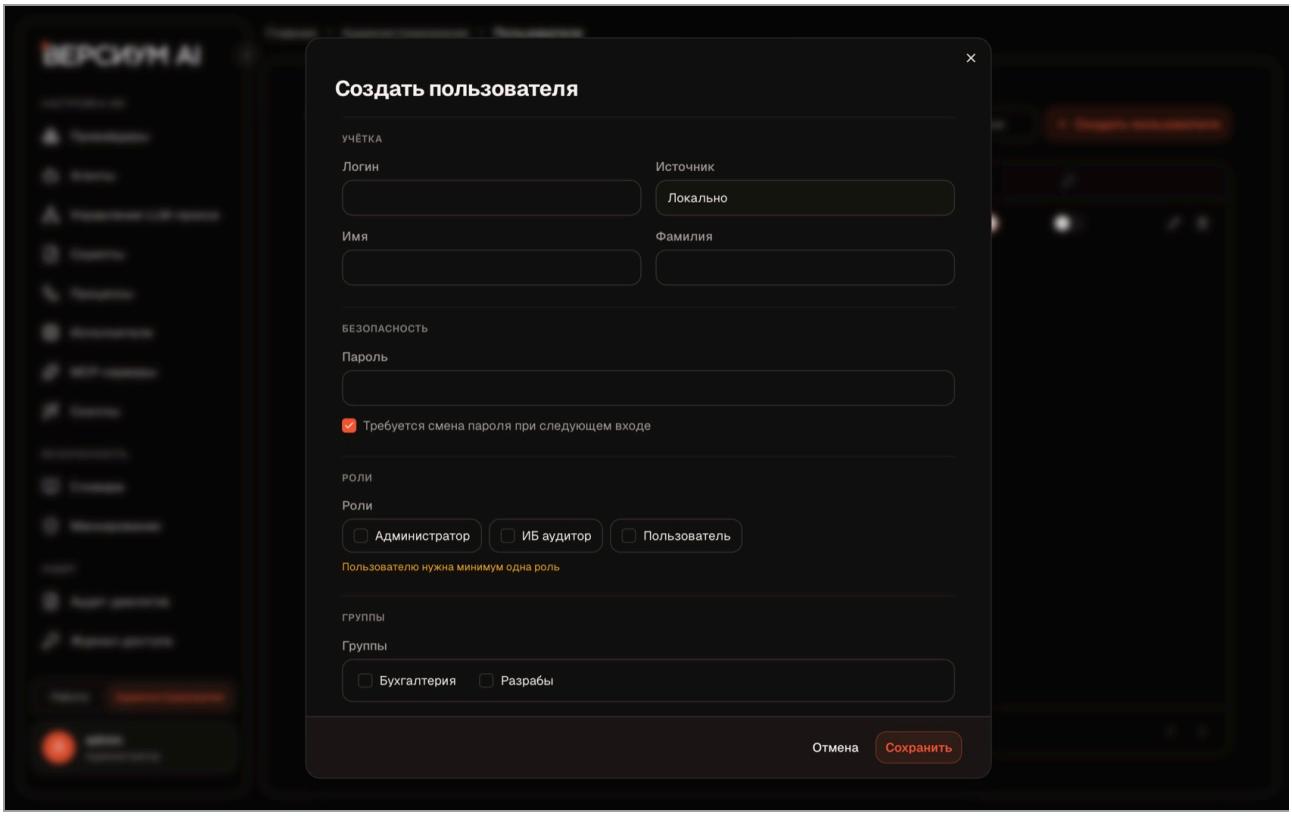


Рисунок 7. Создание пользователя

Раздел **«Группы пользователей»** содержит группы, которые являются единицей выдачи прав на агентов, исполнителей, процессы, сценарии и пространства. Группа создаётся кнопкой **«Создать группу»**, состав изменяется кнопкой «Управление членством». Для группы задаются лимиты числа сообщений за 5 часов и за неделю (на участника и на общий пул группы) и недельный потолок расходов. Стоимость рассчитывается по ценам, заданным для моделей.

Для интеграций с внешними системами создаются технические учётные записи с ролью, ограниченной задачей интеграции.

4.15. Настройки авторизации

Раздел содержит три вкладки.

Active Directory. Включение входа через AD, сервер, порт, использование LDAPS, формат UPN пользователя, атрибут групп, сервисная учётная запись (обычно не нужна), база и фильтр поиска, роль по умолчанию. Значение роли по умолчанию «Нет» запрещает вход пользователям, не попавшим ни под одно сопоставление, и рекомендуется как безопасное. Кнопка **«Проверить подключение»** получает корневой сертификат с контроллера домена и показывает отпечаток для сверки. Этот же сертификат используется для исходящих HTTPS-соединений программы во внутренней сети, например к MCP-серверам. Флажок «Игнорировать ошибки сертификата» допускается только для тестов.

OIDC. Включение входа через OpenID Connect, текст кнопки входа, URL провайдера, Client ID, Client secret, запрашиваемые scopes и имя claim с ролями или группами.

Сопоставление ролей. Соответствие групп AD и значений claim OIDC ролям программы. При каждом входе пользователь получает объединение всех подходящих ролей.

4.16. Дашборд

Раздел **«Дашборд»** показывает сводные показатели за 24 часа, 7 или 30 дней.

- Расходы, число запросов и токенов, доля успешных запросов, длительность обработки, число активных пользователей.
- Инвентарь: число провайдеров, моделей, агентов, навыков, MCP-серверов, исполнителей, скриптов, процессов, пользователей, групп и словарей.
- Графики расходов и токенов по дням, трафика по источникам, запросов по моделям, топ по расходам, длительность хода.
- Операции: запуски процессов и срабатывания планировщика.
- Инфраструктура: исполнители и MCP-серверы в сети.
- Контроль: раскрытия масок и созданные маски, расход лимитов групп.

Включение автообновления обновляет показатели без перезагрузки страницы.

4.17. Пакеты конфигурации

Раздел позволяет переносить настройки между установками программы.

- **Экспорт.** Укажите идентификатор пакета, выберите виды объектов (провайдеры, модели, агенты, навыки, MCP-серверы, скрипты, процессы, словари и механизмы маскирования, привязки маскирования к провайдерам, роли, группы, сопоставления ролей, исполнители, настройки AD и OIDC) и нажмите «Экспортировать». При включении секретов архив защищается паролем.
- **Импорт.** Загрузите архив, при необходимости введите пароль и нажмите «Предпросмотр». Программа покажет изменения до их применения.
- **Установленные.** Перечень установленных пакетов.
- **Обновления вендора.** Доступные обновления пакетов правообладателя.

4.18. Лицензии

Раздел **«Лицензии»** показывает статус лицензии (состояние, адрес установки, заказчик, дату истечения и результат самопроверки) и список загруженных файлов лицензий.

1. Перетащите файл `.lic` в область загрузки или выберите его.
2. Нажмите **«Загрузить»**.

Электронная подпись и принадлежность ключа продукту проверяются локально, без обращения к внешним серверам. Программа предупреждает о скором истечении срока. Лицензия ограничивает количество пользователей, количество MCP-серверов и срок действия. При отсутствии действующей лицензии доступны только вход и раздел «Лицензии».

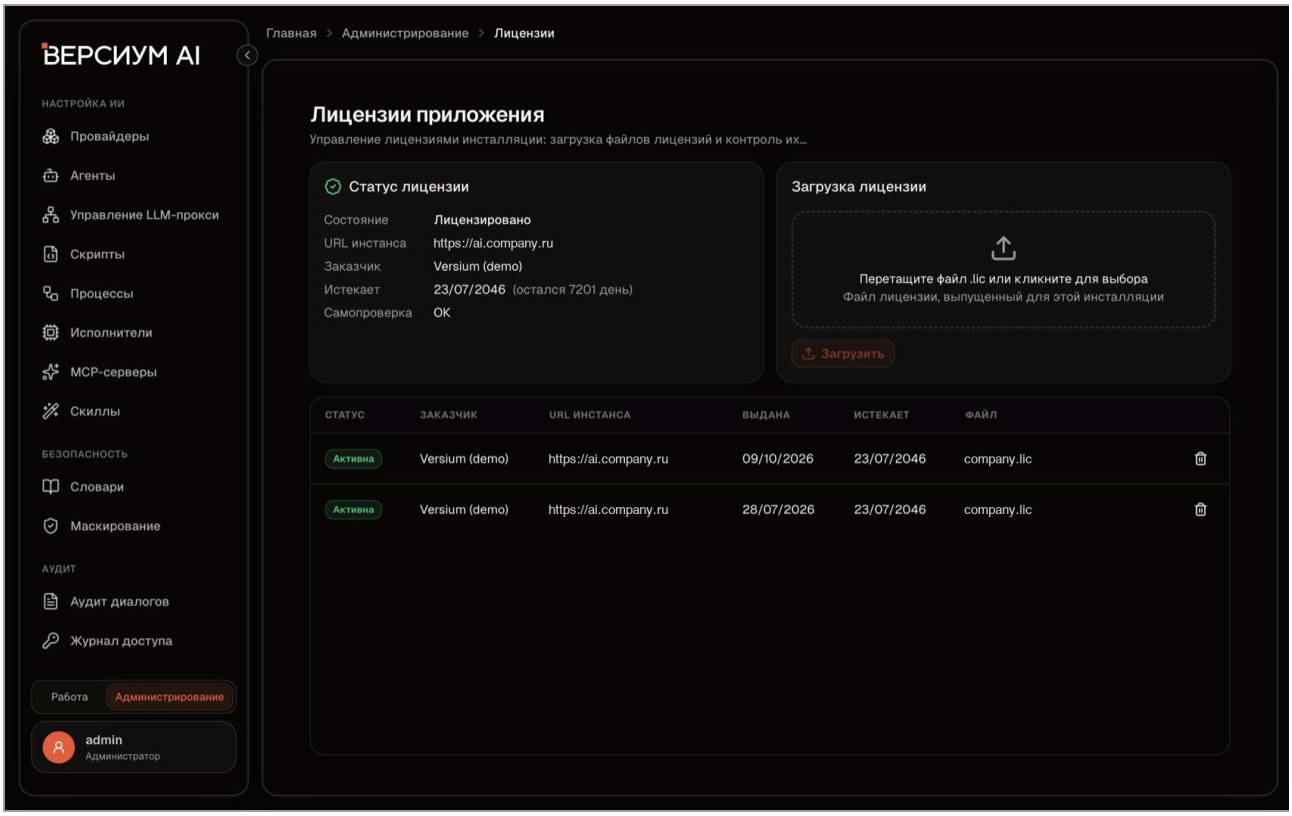


Рисунок 8. Управление лицензиями

5. Работа ИБ-аудитора

Функции раздела доступны ролям «ИБ-аудитор» и «Администратор».

5.1. Аудит диалогов

Раздел **«Аудит диалогов»** содержит все обращения к моделям: чаты, шаги рабочих процессов, запросы через прокси и служебные запросы. Для каждой записи указаны время, источник, название, агент, модель, токены, стоимость, длительность и статус. Записи фильтруются и сортируются.

При открытии записи доступны вкладки «Чат» и «Разбор». По умолчанию показывается запрос в том виде, в котором он ушёл в модель (с масками), и перечень замаскированных сущностей. Кнопка **«Показать оригиналы»** после явного подтверждения раскрывает исходные значения и восстановленный ответ. Каждое раскрытие фиксируется в журнале доступа.

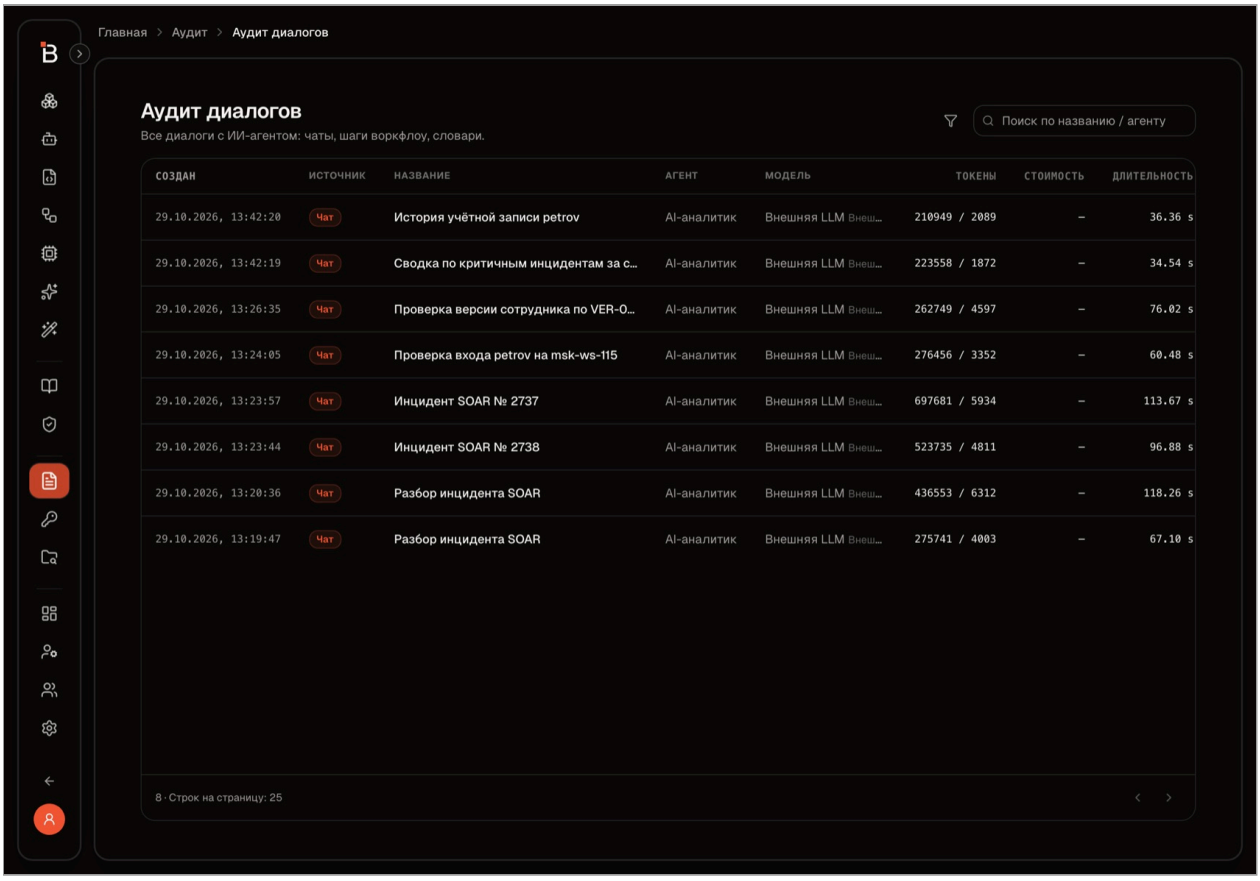


Рисунок 9. Аудит диалогов

5.2. Журнал доступа к оригиналам

Раздел **«Журнал доступа»** показывает, кто и когда раскрывал немаскированные оригиналы: пользователь, действие, диалог, агент, время. Ссылка «Открыть диалог» переходит к записи аудита. Записи журнала изменить или удалить через интерфейс нельзя.

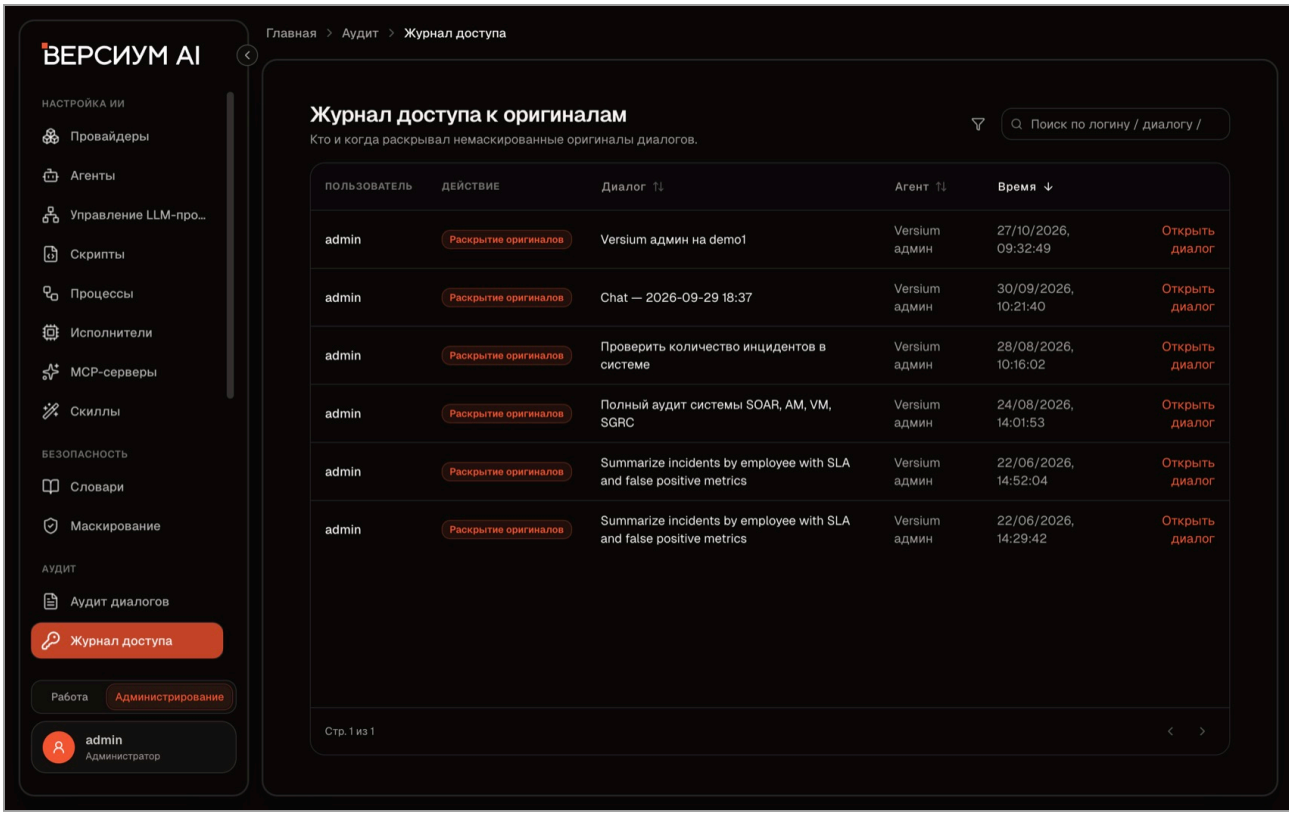


Рисунок 10. Журнал доступа к оригиналам

5.3. Журнал файлов пространств

Раздел **«Файлы пространств»** фиксирует операции пользователей с файлами пространств: время, пользователь, пространство, действие, путь, результат и объём.

6. Типовые задачи

Задача	Порядок действий
Дать сотруднику доступ к агенту	Создать или найти пользователя (4.14), включить его в группу, выдать группе доступ к агенту на вкладке «Доступ групп» (4.2) и, при необходимости, к сценарию (4.8)
Подключить новую модель	Добавить провайдера и модели (4.1), назначить механизмы маскирования провайдеру (4.10), выбрать модель в профиле агента или маршруте прокси (4.2, 4.12)
Подключить информационную систему	Добавить MCP-сервер (4.4), проверить перечень инструментов, задать режимы инструментов в профиле агента (4.2)
Защитить новый вид данных	Создать механизм маскирования (4.10), при необходимости словарь замен, проверить маскирование в тестовом чате и в аудите диалогов (5.1)
Автоматизировать регулярную задачу	Добавить скрипты (4.6), собрать и проверить процесс, создать расписание (4.7)

Задача	Порядок действий
Подключить приложение через прокси	Создать маршрут модели (4.12), выпустить токен пользователю или технической учётной записи, передать настройки подключения владельцу приложения
Перенести настройки на другую установку	Экспортировать пакет конфигурации и импортировать его с предварительным просмотром (4.17)

7. Сообщения и типовые проблемы

Ситуация	Причина и действия
Не удаётся войти	Неверный логин или пароль, учётная запись отключена или вход запрещён сопоставлением ролей. Обратитесь к администратору
В списке нет нужного агента или сценария	Группе пользователя не выдан доступ. Администратору выдать доступ на вкладке «Доступ групп» или в настройках сценария
Исполнитель в состоянии «Офлайн»	Служба исполнителя остановлена или нет исходящего соединения с программой. Проверить работу исполнителя и сетевой доступ
MCP-сервер в состоянии «Ошибка»	Неверный адрес или секрет авторизации, недоверенный сертификат. Проверить параметры сервера и корневой сертификат (4.4, 4.15)
Сообщение заблокировано	Сообщение содержит запрещённую информацию или изображение при запрещающей политике. Удалить данные из сообщения или обратиться к администратору
Превышен лимит сообщений или расходов	Исчерпан лимит пользователя или группы. Дождаться обновления периода или обратиться к администратору
Токен прокси отклонён	Истёк срок или токен отозван, используется не тот режим. Выпустить новый токен (3.7)
Доступен только раздел «Лицензии»	Нет действующей лицензии. Загрузить файл лицензии (4.18)

8. Техническая поддержка

Обращения в техническую поддержку принимаются по электронной почте info@versium.ru и по иным каналам, указанным в договоре (лицензионном соглашении). В обращении укажите версию программы, описание проблемы, время её возникновения и, при наличии, снимки экрана без чувствительных данных.