ООО «Непрерывные Технологии»
ИНН 9715347215, КПП 771501001
E-mail: info@deteact.com
Тел.: +7-499-444-12-46

Программное обеспечение для электронно-вычислительных машин «DeteAct Avatar»

Функциональные характеристики программного обеспечения

Количество страниц: 15

DeteAct, 2026

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин (сокращение)	Краткое определение
ПО	Программное обеспечение
ЭВМ	Электронная вычислительная машина
АРМ	Автоматизированное рабочее место
ПК	Персональный компьютер
ИИ	Искусственный интеллект
LLM (большая языковая модель)	Модель машинного обучения, обученная на больших объёмах текстовых данных и способная порождать текст и программный код
ИИ-агент	Программный компонент на базе большой языковой модели, самостоятельно планирующий и выполняющий последовательность действий для достижения поставленной цели
Пентест (тестирование на проникновение)	Контролируемая имитация действий нарушителя, выполняемая для выявления уязвимостей информационной системы
Находка (уязвимость)	Обнаруженный в ходе тестирования недостаток защищённости, зафиксированный в системе с описанием, доказательством и рекомендацией по устранению
Проект	Единица организации работ в ПО, объединяющая задания, находки и

	отчётные материалы по одному объекту тестирования
Задание (задача)	Запущенный в ПО процесс тестирования или обработки находок с заданными параметрами
Запуск агента	Отдельное выполнение ИИ-агента в изолированном контейнере в рамках задания
Область тестирования	Перечень узлов, доменных имён и сетевых сервисов, разрешённых к тестированию
CVSS	Common Vulnerability Scoring System — открытый стандарт количественной оценки критичности уязвимостей
PoC	Proof of Concept — подтверждение эксплуатируемости уязвимости
API	Application Programming Interface — программный интерфейс взаимодействия с внешними системами
2FA	Двухфакторная аутентификация с использованием одноразовых кодов

2. ВВЕДЕНИЕ

Данный документ включает в себя информацию об основных функциональных характеристиках системы автономного тестирования на проникновение «DeteAct Avatar» (далее — ПО «DeteAct Avatar»). Данное ПО позволяет проводить автоматизированный анализ защищённости и тестирование на проникновение информационных систем без участия человека при помощи ИИ-агентов. Правообладателем ПО «DeteAct Avatar» является ООО «Непрерывные Технологии». ПО «DeteAct Avatar» поставлено на бухгалтерский учет согласно Акту о приеме объекта нематериальных активов №2 от 08.07.2026 г, Приказу о вводе в эксплуатацию нематериальных активов №2 от 08.07.2026 г., Карточки учета НМА №002 от 08.07.2026 г.

Основные возможности при использовании ПО «DeteAct Avatar»:

- автономное тестирование на проникновение веб-приложений, мобильных приложений и сетевой инфраструктуры при помощи ИИ-агентов на базе больших языковых моделей;
- автоматический сбор информации об области тестирования, планирование этапов работ, генерация гипотез об уязвимостях и кода для их проверки;
- выполнение проверок в изолированных контейнерах со специализированным набором инструментов анализа защищённости;
- автоматическая верификация обнаруженных недостатков (безопасная и агрессивная валидация, перепроверка, уточнение, дедупликация), снижающая долю ложных срабатываний;
- ведение единого реестра проектов и находок с уровнями риска, статусами обработки и историей изменений;
- формирование отчёта о тестировании на проникновение и резюме для руководства в формате PDF по настраиваемым шаблонам;
- диалоговый режим (чат) по результатам тестирования, позволяющий получать пояснения и рекомендации по обнаруженным уязвимостям;

– мультиязычность: формирование описаний уязвимостей, рекомендаций и отчётных документов на выбранном языке, а также перевод ранее полученных результатов с одного языка на другой без повторного тестирования;
– интеграция с внешними системами через программный интерфейс (REST API) и обмен данными с платформой управления внешней атакующей поверхностью;
– разграничение доступа на основе ролей, двухфакторная аутентификация, учёт расхода вычислительных ресурсов и оценка стоимости запусков;
– осуществление технической и консультативной поддержки специалистами ООО «Непрерывные Технологии».

Для доступа к интерфейсу ПО «DeteAct Avatar» пользователю требуется автоматизированное рабочее место (АРМ), включающее:

– электронное вычислительное устройство (ПК, ноутбук или иное оборудование);
– подключение к сети Интернет;
– установленный веб-браузер, соответствующий актуальным требованиям.

Данная конфигурация обеспечивает корректное функционирование ПО и выполнение поставленных задач.

Поддерживаются следующие операционные системы автоматизированного рабочего места:

– Astra Linux Special Edition 1.7 и выше;
– РЕД ОС 7.3 и выше;
– ОС «Альт Рабочая станция» 10 и выше;
– РОСА «Хром» / РОСА «Кобальт» 12 и выше;
– Microsoft Windows 10 и выше, macOS 12 и выше.

ПО «DeteAct Avatar» реализовано в виде веб-приложения и не содержит компонентов, устанавливаемых на рабочее место пользователя, поэтому не зависит от операционной системы АРМ. Работа подтверждена, в частности, на отечественных операционных системах, включённых в единый реестр российских программ для ЭВМ и баз данных, при использовании входящих в их состав веб-браузеров.

3. ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Основные разделы интерфейса ПО «DeteAct Avatar»:

– проекты;

– задачи;

– действия;

– API-ключи;

– настройки;

– профиль.

3.1 Основные характеристики раздела «Проекты»

Раздел является стартовой страницей ПО и содержит перечень проектов пользователя с количеством находок в разбивке по уровням риска, количеством заданий и датой создания. При взаимодействии с разделом «Проекты» пользователю предоставляются следующие функциональные возможности:

– просмотр списка доступных проектов и сводной статистики по ним;

– создание нового проекта и удаление существующего;

– переход к перечню заданий и к сводке проекта;

– редактирование параметров проекта: наименование, наименование компании, имя тестировщика, версия отчёта, гриф конфиденциальности, даты начала и окончания тестирования, язык отчёта и описание;

– привязка ранее выполненных заданий к проекту и запуск нового задания;

– формирование резюме для руководства и итогового отчёта;

– ведение диалога (чата) по находкам проекта.

3.2 Основные характеристики раздела «Находки»

Раздел входит в состав сводки проекта и содержит подробные сведения об уязвимостях, обнаруженных в ходе тестирования. При взаимодействии с разделом пользователю предоставляются следующие функциональные возможности:

– просмотр таблицы обнаруженных уязвимостей и выполнение поиска по ней;

– фильтрация находок по уровню риска и по статусу обработки;

– группировка находок по наименованию;
– получение детальной информации о выбранной находке: описание, уровень риска, оценка CVSS, адрес объекта, подтверждение эксплуатируемости (PoC) и рекомендация по устранению;
– изменение статуса одной или нескольких находок, редактирование и удаление находок;
– просмотр истории изменений находки с возможностью восстановления прежних значений;
– запуск проверок находок средствами ИИ-агента: проверка, перепроверка, уточнение и дедупликация;
– переход к журналу запуска агента, в ходе которого была обнаружена находка;
– экспорт результатов в файл формата PDF или JSONL.

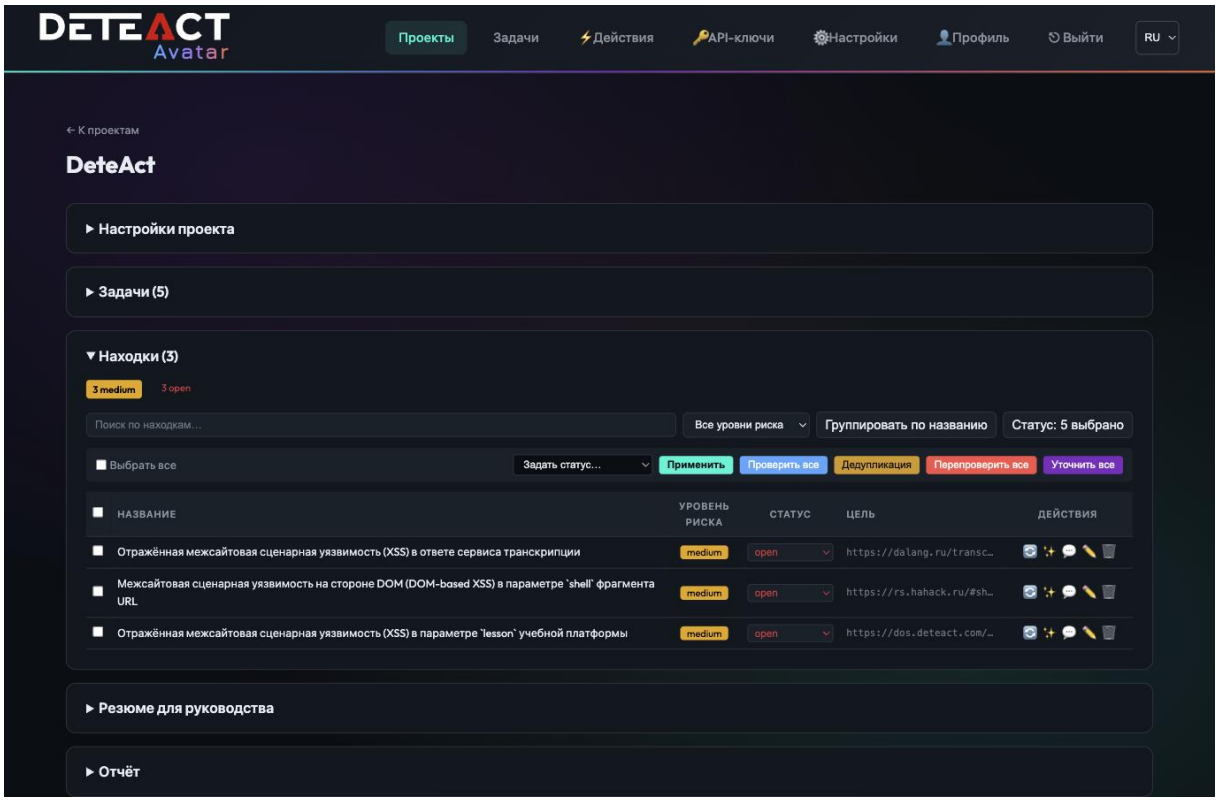

Рисунок 1. Перечень находок проекта

3.3 Основные характеристики раздела «Задачи»

При взаимодействии с разделом «Задачи» пользователю предоставляются следующие функциональные возможности:

– просмотр перечня выполненных и выполняющихся заданий с указанием даты, окружения, режима, статуса и прогресса выполнения;
– фильтрация заданий по проекту и поиск по наименованию, а также поиск по журналам выполнения с использованием регулярных выражений;
– просмотр объёма обработанных данных и оценки стоимости выполнения задания;
– получение подробных сведений о выбранном задании, включая параметры запуска и область тестирования;
– просмотр перечня запусков ИИ-агента и полного журнала работы каждого запуска;
– остановка выполняющегося задания и повторный запуск завершённого;
– перемещение заданий между проектами.

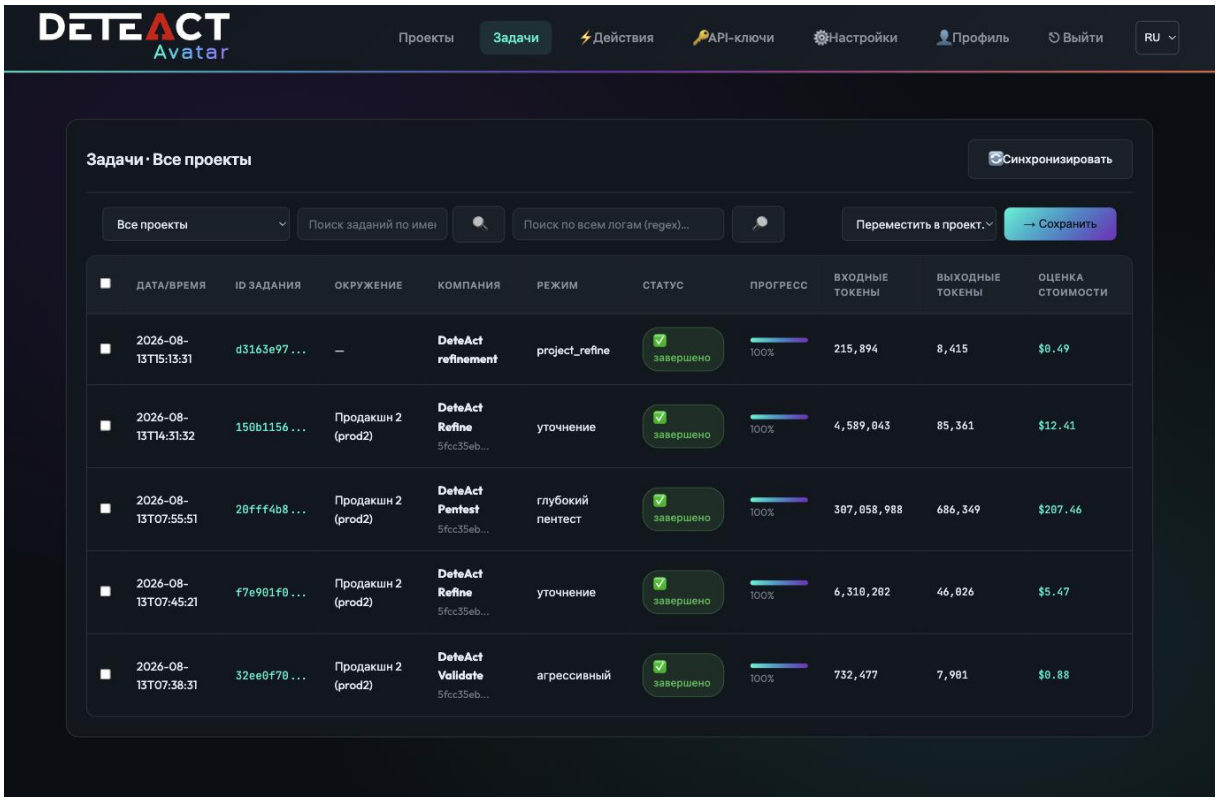

Рисунок 2. Перечень заданий

3.4 Основные характеристики раздела «Действия»

Раздел предназначен для запуска заданий на тестирование. При взаимодействии с разделом пользователю предоставляются следующие функциональные возможности:

– выбор проекта, режима тестирования, окружения и языка формируемого отчёта;
– выбор вычислительного узла, ИИ-агента, поставщика и модели, выполняющей тестирование;
– настройка параметров выполнения: число гарантированных и предельно допустимых запусков, минимальный размер результата, режим группировки целей;
– задание области тестирования и загрузка вспомогательных файлов, включая исходный код и документацию;
– включение режимов тестирования с доступом к исходному коду и с аутентификацией;
– редактирование задания для ИИ-агента и сохранение его в виде профиля для повторного использования;
– выполнение пробного прогона без изменения данных во внешних системах.

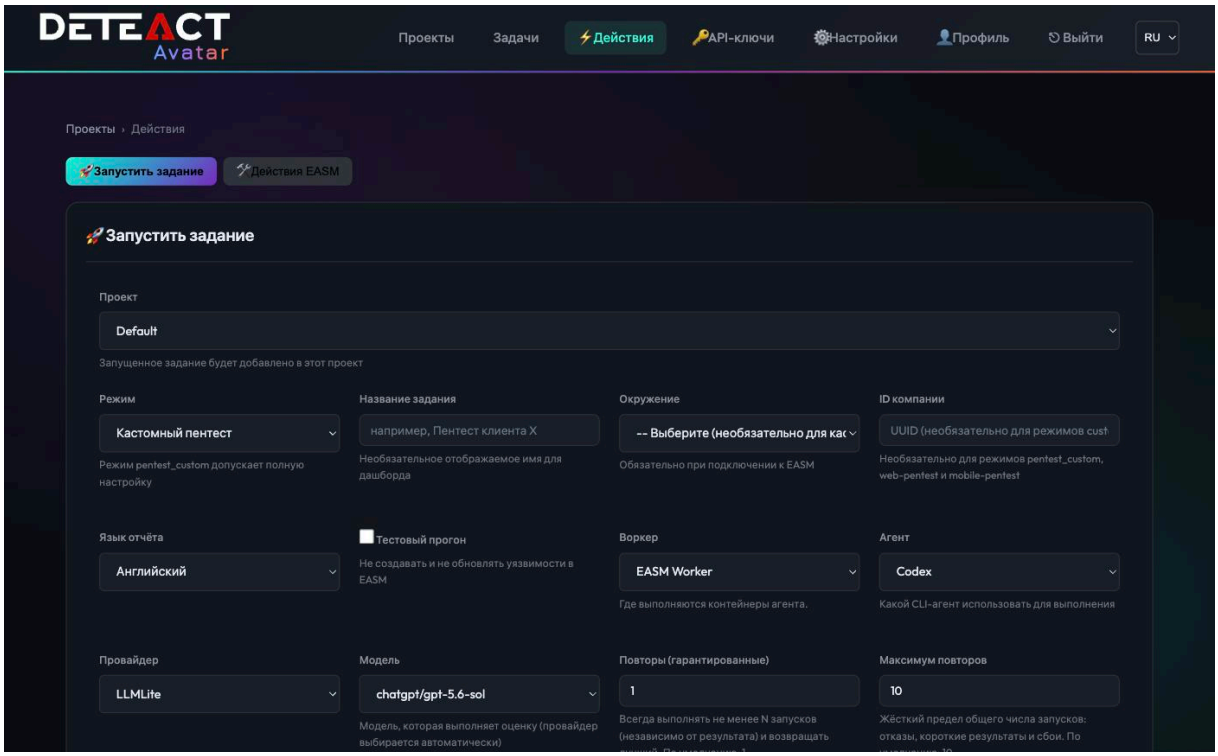

Рисунок 3. Форма запуска задания

3.5 Основные характеристики раздела «API-ключи»

В данном разделе пользователь может создать ключ для интеграции ПО с другими системами, просмотреть перечень созданных ключей и отозвать ключ. Полное значение ключа отображается однократно — в момент создания.

3.6 Основные характеристики раздела «Настройки»

Раздел доступен пользователям с ролью «Администратор» и содержит подразделы «Пользователи», «Провайдеры», «Воркеры», «Окружения», «Промпты», «Общие» и «Оформление». В разделе выполняется создание и редактирование учётных записей с назначением ролей, проектов и лимитов на запуски, подключение поставщиков больших языковых моделей и настройка их тарифов, подключение вычислительных узлов, настройка окружений и интеграций, редактирование шаблонов заданий для ИИ-агентов, выбор доступных языков интерфейса и настройка фирменного оформления отчётов.

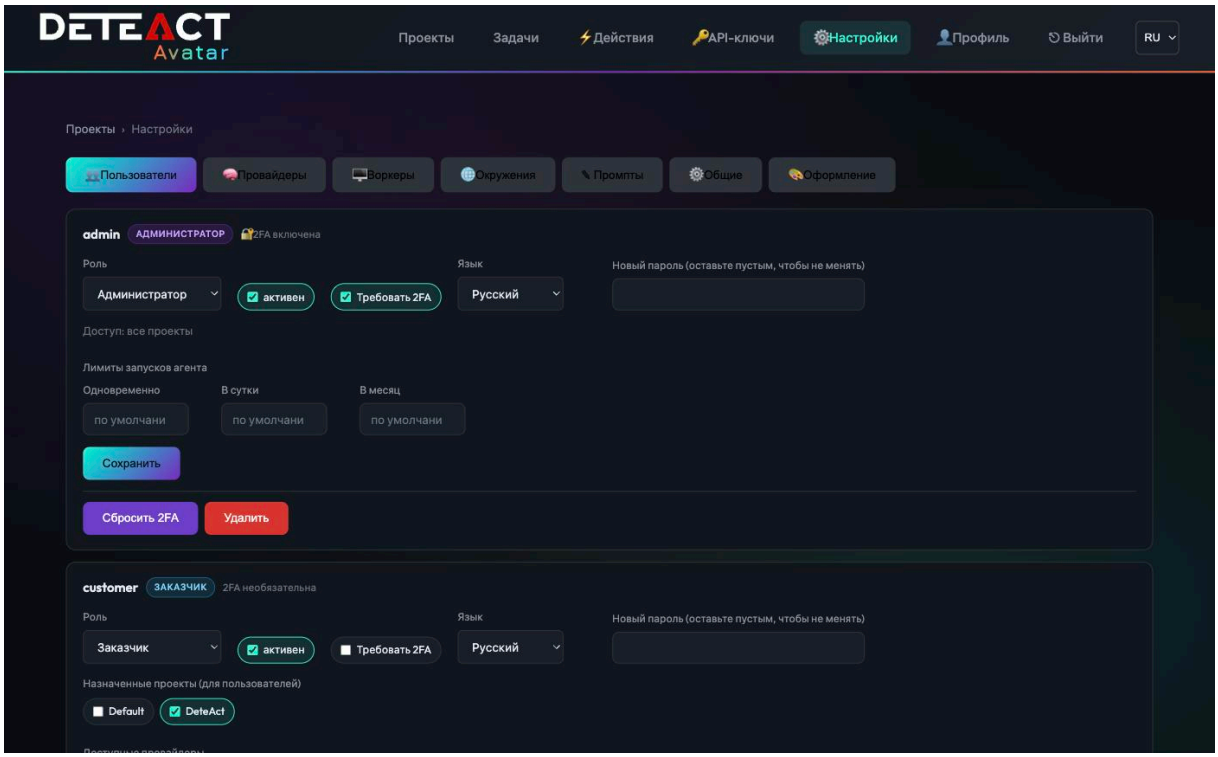

Рисунок 4. Управление учётными записями

3.7 Основные характеристики раздела «Профиль»

В данном разделе пользователь может выбрать язык интерфейса, изменить текущий пароль на новый и повторно настроить двухфакторную аутентификацию.

4. РЕЖИМЫ АВТОНОМНОГО ТЕСТИРОВАНИЯ

ПО «DeteAct Avatar» поддерживает следующие режимы выполнения заданий:

- Кастомный пентест — тестирование с полностью настраиваемым заданием для ИИ-агента: область тестирования и инструкции задаются оператором вручную;
- Глубокий пентест — углублённое тестирование узлов, полученных из системы управления внешней атакующей поверхностью, с параллельным запуском нескольких агентов;
- Веб-пентест — тестирование веб-приложений с учётом переданного контекста (исходный код, документация API, учётные данные);
- Мобильный пентест — анализ мобильных приложений по загруженным в ПО файлам сборок;
- Безопасная валидация — проверка ранее обнаруженных уязвимостей без потенциально опасных для объекта воздействий;
- Опасная валидация — проверка уязвимостей с применением активных воздействий, подтверждающих эксплуатируемость;
- Уточнение — доработка описаний, доказательств и рекомендаций по уже подтверждённым находкам;
- Перепроверка — повторная проверка находок, ранее отмеченных как устранённые;
- Дедупликация — автоматическое выявление и объединение повторяющихся находок.

5. ЯЗЫКОВЫЕ ВОЗМОЖНОСТИ

ПО «DeteAct Avatar» является мультиязычным как на уровне интерфейса, так и на уровне содержимого формируемых материалов.

- интерфейс ПО переведён на русский и английский языки; язык выбирается пользователем в разделе «Профиль», язык по умолчанию для новых учётных записей задаётся администратором;
- язык результатов тестирования задаётся при запуске задания и в настройках проекта: наименования уязвимостей, описания, подтверждения эксплуатируемости и рекомендации по устранению формируются ИИ-агентом сразу на выбранном языке;
- ранее полученные результаты могут быть переведены на другой язык без повторного тестирования — для этого достаточно изменить язык проекта и выполнить операцию уточнения находок;
- итоговый отчёт о тестировании и резюме для руководства формируются на языке, заданном для проекта;
- перечень языков не ограничен архитектурно: он определяется возможностями применяемых больших языковых моделей, что позволяет расширять состав поддерживаемых языков без доработки программного обеспечения.

При переводе результатов технические артефакты — команды, отправленные запросы и полученный от объекта тестирования вывод — сохраняются в исходном виде, что обеспечивает воспроизводимость проверок независимо от выбранного языка изложения.

6. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Доступ к функционалу ПО «DeteAct Avatar» предоставляется на основании предварительной регистрации пользователя, осуществляемой администратором после оформления необходимых юридических соглашений. После активации учетной записи вход в систему осуществляется через веб-браузер по уникальному URL-адресу, предоставляемому аккаунт-менеджером.

Информационная система функционирует в онлайн-режиме и не требует установки дополнительного программного обеспечения на рабочее место пользователя. Все действия выполняются в пользовательском интерфейсе путем взаимодействия с элементами навигации. Работа ПО «DeteAct Avatar» возможна исключительно при наличии стабильного подключения к сети Интернет.

Процесс завершения сеанса осуществляется автоматически: достаточно выйти из учетной записи или закрыть все вкладки и окна браузера, в которых открыт интерфейс сервиса.