СЛУЖЕБНОЕ ЗАДАНИЕ № 1 НА РАЗРАБОТКУ
ПО «DeteAct Avatar»

г. Москва 12.01.2026 г.

1. Общество с ограниченной ответственностью «Непрерывные технологии» ОГРН 1197746340330 (далее **«Общество»**) в лице Генерального директора Ганиева Омара Аркадьевича поручает работникам Общества, указанным ниже в настоящем Служебном задании, в пределах их трудовых обязанностей осуществить разработку ПО «DeteAct Avatar», описание и требования которого содержится в Приложении № 1 к настоящему Служебному заданию (далее **«РИД»**).

2. Разработка РИД в соответствии с настоящим Служебным заданием поручается следующим работникам Общества:

№ п/п	ФИО	Должность
1.	Дробачевский Ян Борисович	Старший программист

3. Подписывая настоящее Служебное задание, работник подтверждает, что:

   - Он ознакомлен с настоящим Служебным заданием.
   - Разработка РИД входит в его трудовые обязанности.
   - Исключительное право на РИД будет принадлежать работодателю единолично.
   - Выплата вознаграждения работнику не предусматривается.

Генеральный директор Ганиев О.А.

Со Служебным заданием ознакомлен и согласен:

№ п/п	ФИО	Должность	Подпись
1.	Дробачевский Ян Борисович	Старший программист	

Приложение № 1 к
Служебному заданию № 1на разработку
ПО «DeteAct Avatar»
от 12.01.2026 г.

ОПИСАНИЕ И ОСНОВНЫЕ ТРЕБОВАНИЯ К РИД

1. Общие характеристики

ПО должно представлять собой систему автономного тестирования на проникновение, выполняющую анализ защищённости информационных систем без участия человека при помощи ИИ-агентов на базе больших языковых моделей.

ПО должно поддерживать работу с различными агентскими системами (harness) и различными поставщиками больших языковых моделей, включая публичные облачные сервисы и модели, развёрнутые локально. Проверки должны выполняться в изолированной среде со специализированным набором инструментов анализа защищённости.

2. Функциональные характеристики

Автономное тестирование на проникновение веб-приложений, мобильных приложений и сетевой инфраструктуры при помощи ИИ-агентов;

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: валидация, перепроверка, уточнение и дедупликация находок;

Ведение 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;

Разграничение доступа на основе ролей, двухфакторная аутентификация, учёт расхода вычислительных ресурсов, интеграция с внешними системами через REST API.

3. Календарный план

Недели 1–4: исследование существующих решений и возможностей больших языковых моделей в задачах анализа защищённости.

Недели 5–8: разработка архитектуры оркестратора ИИ-агентов, планирование.

Недели 9–14: разработка прототипа оркестратора и изолированной среды выполнения проверок.

Недели 15–18: разработка веб-интерфейса, реестра проектов и находок.

Недели 19–24: реализация режимов тестирования и верификации находок, формирования отчётности, интеграций с внешними системами и разграничения доступа.