НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ СИСТЕМНОГО СИНТЕЗА · ПРОДУКТОВЫЙ ПАСПОРТ · 15 НОЯБРЯ 2026 ГОДА

Комплекс INDRA: проверка защищённости цифровых сотрудников и сервисов за 14 суток

Быстрое испытание корпоративных цифровых сотрудников, поисковых баз и веб-сервисов из текущего бюджета за 350 000 рублей без остановки работы и без выгрузки закрытых сведений наружу.

Что требуется от заказчика. Предприятие открывает на четырнадцать календарных суток доступ в режиме чтения к тестовой копии проверяемого цифрового сотрудника, веб-сервиса или внутреннего шлюза и оплачивает фиксированный договор **350 000 рублей** из текущего бюджета службы безопасности. Доступ на запись к живым учётным базам и платёжным ключам не запрашивается.

Что получает заказчик взамен. Заказчик получает полную проверку сервиса комплексом INDRA (от английского *Invariant, Nondestructive, Deterministic Resilience Audit* — Инвариантная неразрушающая диагностика рисков и аудит, И-Н-Д-Р-А). На четырнадцатый день передаются протокол найденных уязвимостей с квитанциями по ГОСТ Р 34.11-2012, карта соответствия приказу № 117 и готовые правила защиты для шлюза MITR без переписывания кода.

РАЗДЕЛ 01 · НАЗНАЧЕНИЕ ПРОВЕРКИ И ТРЕБОВАНИЯ ЗАКОНА

1. Какие риски цифровых сотрудников закрывает четырнадцатидневное испытание

Когда компания подключает цифровых сотрудников к почте, документообороту и учётным базам, обычные межсетевые экраны перестают видеть главную угрозу. Скрытая инструкция внутри присланного резюме, счёта или сверки способна заставить доверенную программу подменить реквизиты получателя или отправить базу клиентов постороннему адресату.

Автономная некоммерческая организация «Научно-исследовательский институт системного синтеза» (далее — Институт) проводит проверку комплексом INDRA в связке со шлюзом MITR (от английского *Mediating Invariant-Trust Resolver* — посреднический решатель инвариантного доверия). Испытание идёт в режиме зеркалирования трафика на тестовом стенде и не мешает штатной работе отделов.

Итоговый отчёт подтверждает выполнение требований приказа Федеральной службы по техническому и экспортному контролю (далее — ФСТЭК России) от 11 апреля 2025 года № 117, **вступившего в силу 1 марта 2026 года**. Документ учитывает пункты 59–62 о запрете передачи защищаемых данных внешним моделям, проект изменений № 170500 по автономным программам, рекомендации Банка России № 3-МР и статью 53.1 Гражданского кодекса Российской Федерации (далее — Гражданский кодекс).

РАЗДЕЛ 02 · ПРИБОРНЫЕ ПОКАЗАТЕЛИ ИСПЫТАТЕЛЬНОГО СТЕНДА

2. Измеренная точность комплекса INDRA и решателя MITR

Приборные показатели испытательного комплекса и проверочного шлюза измерены на внутренних эталонных стендах Института до прохождения независимой аккредитованной испытательной лаборатории. Контур исполнения разделён по принципу верифицируемой архитектуры: вне рабочего цикла решатель Z3 синтезирует и проверяет политику безопасности, а в момент вызова работает детерминированный исполнитель объёмом менее 3 000 строк кода. Математическое доказательство распространяется строго на формализованные аксиомы: смысловую верность перевода деловых и правовых норм в правила утверждает ответственный специалист заказчика по обратному переводу ограничений на русский язык.

ПРОВЕРЯЕМЫЙ УЗЕЛ	ПОДТВЕРЖДЁННЫЙ РЕЗУЛЬТАТ	ПРОТОКОЛ И ДАТА ЗАМЕРА
Эталонный стенд INDRA	**Выполнены 12 критериев из 12 на внутреннем эталонном наборе из 28 сценариев (14 уязвимых и 14 чистых): найдены все 14 уязвимостей при нуле ложных тревог**	**Внутренний эталонный полигон INDRA, замер от 25 октября 2026 года (indra.center)**
Предохранитель опасных проб	**Перехвачены до отправки все 26 разрушительных тестовых вызовов из 26; проверка ограничена белым списком адресов**	**Фильтр исходящих запросов комплекса INDRA, замер от 25 октября 2026 года**
Скорость шлюза MITR (офлайн-компилятор Z3 и компактный исполнитель)	**Прогретая медиана 1,08 миллисекунды, 95-й перцентиль 1,96 миллисекунды; 5,22 миллисекунды с объяснением причины отказа; 30,7 миллисекунды при холодном запуске на обычном процессоре**	**Прогон 1 000 решений по 20 правилам (500 допусков и 500 отказов, ноль ошибок), 24 октября 2026 года**
Отражение атак на цифровых сотрудников	**Заблокированы все 114 атак и пропущены все 43 штатные команды на внутреннем корпусе из 157 сценариев (6 414 автотестов кода)**	**Внутренний состязательный стенд MITR от 24 октября 2026 года (до внешней лаборатории)**
Неизменяемый журнал доказательств	**Цепь из 5 373 записей SHA-256 за 55 завершённых эпох (на 15 ноября 2026 года) с привязкой эпохи 33 к блоку Bitcoin 973 024 и пакет iss-ledger-117 по ГОСТ Р 34.11-2012. Для юридической значимости на критической информационной инфраструктуре дополняется меткой времени аккредитованного удостоверяющего центра и усиленной квалифицированной электронной подписью по Федеральному закону № 63-ФЗ (iss-ledger-117 не заменяет сертифицированное средство криптографической защиты информации)**	**Открытый проверщик asi5.ru/console/verify/ (mitr.asi5.ru)**

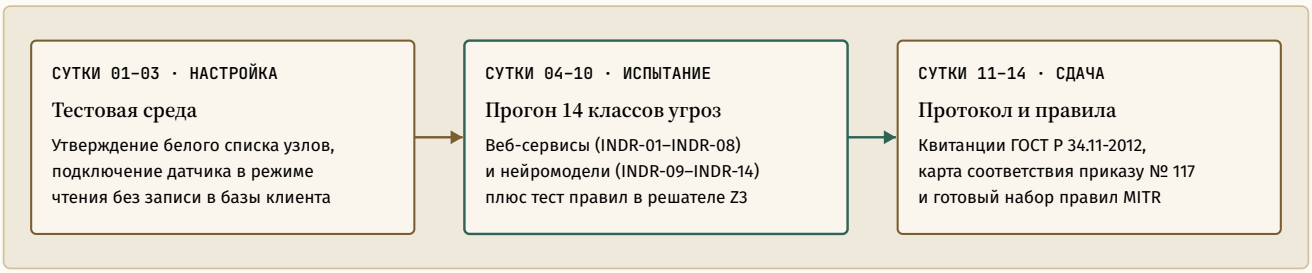


Рисунок 1. График четырнадцатидневного обследования: все проверки идут в режиме чтения на тестовых копиях без риска для рабочих серверов.

РАЗДЕЛ 03 · ЧЕТЫРНАДЦАТЬ ПРОВЕРЯЕМЫХ КЛАССОВ УГРОЗ

3. Что именно проверяет комплекс INDRA за две недели

Полевая редакция объединяет восемь классов угроз веб-сервисов и шесть классов угроз языковых моделей и цифровых сотрудников на базе лабораторного эталона из 28 сценариев (замер 25 октября 2026 года: двенадцать критериев из двенадцати). Разделение контуров строгое: генератор безопасных зондов работает в закрытом контуре комплекса, а клиент получает автономный скрипт повтора replay_verify_findings.py и открытые инструменты проверки без блокирующей привязки к поставщику.

- **Инъекции и системные команды** (INDR-01, INDR-02, INDR-05). Автоматический генератор в режиме щадящего зондирования (ACTIVE_SAFE) проверяет подстановку инструкций в запросы к базам данных, отражённый вывод страниц и передачу системных команд из параметров вызова.
- **Подмена сетевых запросов, обход каталогов и доступ к записям** (INDR-03, INDR-04, INDR-07). Стенд тестирует чтение закрытых внутренних адресов облачной среды, выход за пределы каталога файлов и доступ к чужим карточкам или договорам по прямому идентификатору записи.
- **Обход проверки подлинности и пассивный контроль нагрузки** (INDR-06, INDR-08). Комплекс выявляет пропуск отладочных заголовков и авторизации, а отсутствие ограничений частоты запросов и объёма ответа (INDR-08) диагностирует строго по пассивным заголовкам и политикам (PASSIVE_POLICY) без нагрузочного давления на рабочие серверы.
- **Прямые и скрытые подмены инструкций языковых моделей** (INDR-09, INDR-10, INDR-11). Испытание воспроизводит перехват управления цифровым сотрудником через прямой ввод или внешний документ, а также попытки раскрытия закрытых служебных инструкций ассистента.
- **Эскалация инструментов, утечка сведений и смешение баз знаний** (INDR-12, INDR-13, INDR-14). Проверка охватывает несанкционированный вызов внешних инструментов протокола контекста модели (MCP), утечку секретных ключей и персональных данных в ответах, а также смешение документов разных организаций в поиске знаний (RAG).

РАЗДЕЛ 04 · УСЛОВИЯ ДОГОВОРА И СДАВАЕМЫЕ МАТЕРИАЛЫ

4. Фиксированная смета 350 000 рублей и комплект итоговых документов

Условия договора рассчитаны на быстрое подписание внутри лимита прямых закупок руководителя службы безопасности без долгого тендера.

УСЛОВИЕ ДОГОВОРА	ЗНАЧЕНИЕ	ПРАКТИЧЕСКАЯ ПОЛЬЗА ДЛЯ ЗАКАЗЧИКА
Цена и налоги	**350 000 рублей** (при договоре с Институтом налог на добавленную стоимость не начисляется; через коммерческого оператора применяется ставка 22 процента)	Вписывается в лимит текущих расходов директора по информационной безопасности или информационным технологиям
Сроки подписания и работ	От 3 до 5 рабочих дней на подписание; 14 календарных суток на обследование	Соглашение о неразглашении по форме клиента и полная картина уязвимостей внутри одного расчётного месяца
Сдаваемый комплект	Три официальных документа и электронный архив квитанций	1) Доклад для руководства по приказу ФСТЭК России № 117 и рекомендациям Банка России № 3-МР; 2) Протокол уязвимостей с хэшами ГОСТ Р 34.11-2012; 3) Пакет готовых правил для включения шлюза MITR
Следующий шаг при необходимости	Пилот MITR Enterprise на 30 дней (900 000 рублей) либо целевая разработка от 5 000 000 рублей	По целевым договорам научных разработок (глава 38 Гражданского кодекса и Перечень № 988) расходы учитываются с коэффициентом 2 по статье 262 Налогового кодекса Российской Федерации

РАЗДЕЛ 05 · ПРЕДВАРИТЕЛЬНАЯ СВЕРКА И ПРАВОВЫЕ ГРАНИЦЫ

5. Пятиминутная проверка инструментов и оговорка об аттестации

Специалист заказчика может до заключения договора проверить целостность открытой цепи квитанций и блокировку опасного запроса на изолированной рабочей станции.

```
curl -O https://asi5.ru/console/verify/verify_chain_standalone.py.txt
mv verify_chain_standalone.py.txt verify_chain_standalone.py
curl -O https://asi5.ru/console/verify/gate_anchors-public.jsonl
python3 verify_chain_standalone.py gate_anchors-public.jsonl   # код выхода 0 — якоря цепи сошлись

pip install --no-index --find-links https://isslab.ru/wp-content/uploads/iss-utils/index.html mcp-sentinel
mcp-sentinel check --tool sql_query --args '{"query": "DROP TABLE users;"}'   # BLOCK, код выхода 2
```

- **Сохранность данных клиента.** Во время проверки комплекс INDRA не меняет записи в рабочих базах, не запрашивает платёжные ключи и не отправляет документы предприятия во внешние облака.
- **Граница с государственной аттестацией.** Протокол обследования служит инженерным документом для закрытия уязвимостей, но не заменяет аттестат соответствия значимого объекта критической инфраструктуры, выдаваемый лицензиатом ФСТЭК России.

Автономная некоммерческая организация «Научно-исследовательский институт системного синтеза», ОГРН 1267700083617, ИНН 9731161602, КПП 773101001. Адрес: 121352, город Москва, улица Давыдковская, дом 18, помещение VIII. Прямой контакт для согласования технического задания и соглашения о конфиденциальности: электронная почта af@isslab.ai, витрина https://indra.center/ru/#request-pilot. Редакция 2.0 от 15 ноября 2026 года.