АНО «НИИ СИСТЕМНОГО СИНТЕЗА», ПАСПОРТ ПРОВЕРКИ ИБ 3.0, РЕДАКЦИЯ 26 ОКТЯБРЯ 2026 ГОДА

MITR, открытые пакеты и испытатель INDRA: что измерено и как это повторить

Документ адресован специалисту по информационной безопасности. Каждое число о MITR приведено в нём с датой и местом замера, рядом стоят команды повтора и границы применимости, а того, что не измерялось, в документе нет.

1. Предмет

MITR проверяет вызов инструмента агентом, когда модель уже закончила рассуждение: имя действия, аргументы, адресата и факты из источников, назначенных организацией; текст модели и слова самого агента в расчёт не берутся. Правило, или контракт, хранится отдельным файлом. Решатель Z3 (открытая разработка Microsoft Research) в логике QF_UFLIA, то есть в бескванторной логике с неинтерпретируемыми функциями и линейной целочисленной арифметикой, доказывает, что при этих фактах действие соблюдает условие безопасности. Если доказательства нет, в режиме запрета действие останавливается.

На каждое решение пишется квитанция. Квитанции сцеплены в цепь хеш-функцией SHA-256 (SHA — Secure Hash Algorithm, стандарт хеширования), и голову цепи раз в сутки закрепляет внешний свидетель времени OpenTimestamps, поэтому правка задним числом обнаруживается при пересчёте.

Гарантия MITR — корректность: разрешённое действие соблюдает правило. Полноту правил MITR не обещает, потому что перевод нормы в правило делает человек, и квитанция называет правило, по которому принято решение.

2. Замеры MITR

- **Двадцать контрактов из двадцати** работают в режиме запрета; режим снят из окружения живого процесса службы 25 октября 2026 года.
- **Решение по правилу в прогретом процессе** занимает в медиане 1,08 миллисекунды, в 95-м процентиле 1,96 миллисекунды и в 99-м процентиле 3,61 миллисекунды. Замер 24 октября 2026 года охватил 1 000 решений на 20 контрактах, из них 500 допусков и 500 отказов, без единого ложного допуска или отказа.
- **Вызов вместе с объяснением отказа** в том же замере занимает в медиане 5,22 миллисекунды, а первое решение в только что запущенном процессе — 30,7 миллисекунды в медиане по 300 запускам.
- **Набор атак на действия** из 157 случаев, где 114 атак и 43 штатных вызова, 24 октября 2026 года прошёл без единой пропущенной атаки и без ложных отказов.
- **Три известных пробела правил** набор называет сам: перезапуск проверяющей службы допускается без одобрения, и на это время хук пропускает действия без проверки; явное возражение владельца не спрашивается на двух из трёх путей удаления события; маркер одобрения ставит рабочая станция агента вместо подписи владельца. Закрытие пробелов стоит в плане работ.
- **Цепь квитанций** ведётся с 16 сентября 2026 года и на 25 октября насчитывает 5 094 записи; она сходится от первой записи.

- **Внешний свидетель времени** закрепил эпоху 33 из 5 079 записей меткой в блоке Bitcoin 973 024, отметка — 25 октября 2026 года.
- **Повтор решений проверщиком для постороннего** совпал в 5 079 случаях из 5 079 без расхождений; повтор 25 октября 2026 года выполнил сам институт.
- **Каждый из 92 отказов** за тридцать суток до 25 октября 2026 года назвал нарушенное условие, а ошибки факта опровергнуты 94 записями в той же цепи.
- **Шесть утверждений о MITR** суточный прибор подтвердил полностью за 23 октября 2026 года; за 24 октября подтверждены пять из шести, а одно не измерено. Цель — шесть из шести четырнадцать суток подряд.
- **Автоматические тесты кода** в прогоне, завершённом 26 октября 2026 года, прошли все 6 414, отказов нет.

MITR работает непрерывно с 24 апреля 2026 года и держит действия агентов института. Замеры сняты на собственном сервере института с четырьмя ядрами серверного процессора и восемью гигабайтами памяти, а разброс под промышленной нагрузкой определяется на совместном стенде с заказчиком.

3. Открытые пакеты

Пакеты опубликованы под лицензией Apache-2.0 и проверяют вызов сопоставлением с образцом, без решателя: решатель и цепь с внешним свидетелем есть только в MITR. В публичном каталоге PyPI пакетов института нет, а под именем `mcp-sentinel` там лежит посторонний проект, поэтому пакеты ставятся только с ключом `--no-index` из скачанного каталога.

Контрольные суммы приведены в формате, который читает команда `sha256sum -c`: строки ниже сохраняются в файл рядом со скачанными пакетами и проверяются одной командой.

```
681a4db59a1a44e89a2b1386ec4b4f2e1fc23c1025c295b9ebf00fd5d20901ea  mcp_sentinel-1.1.2-py3-none-any.whl
abb88978db7b34a2f1f56e0eff42bcd1365b9cc0eb17e4a4380f7815e4f1b79e  mcp_sentinel-1.1.2.tar.gz
8d4ffe60f41ebd377c476f369655aaef5e0ac91858a3d294be37fd1e3100bc87  iss_ledger_117-1.1.1-py3-none-any.whl
6eccef523e24fa60fed29c78866ff12afbab092bd17d51642e00d34dfcea9fa5  iss_ledger_117-1.1.1.tar.gz
7ed0ae9073f512a5cfd71b62904094ca36d0ae2fdb1b4bfff5900d3e368781c3  iss_agent_kit-0.1.1-py3-none-any.whl
0314047404888c29a231fc8710874f15bc2bd75e2b89ba7c4c882da3c792116a  iss_agent_kit-0.1.1.tar.gz
1ff894574407307d33ec99115652bcaec4e53d06189178696d0db1c767a8608f  iss_verifier.py
```

Файлы лежат по адресу `https://isslab.ru/wp-content/uploads/iss-utils/`, исходные тексты — на `https://git.isslab.ru/isslab/`. Журнал `iss-ledger-117` сцеплен хеш-функцией ГОСТ Р 34.11-2012 «Стрибог-256» и проходит контрольные примеры описания этого алгоритма (RFC 6986); цепь MITR считается по SHA-256, а второй дайджест по ГОСТ для неё остаётся замыслом.

4. Испытатель INDRA

Испытатель INDRA — внутренний стенд собственной разработки для проверки веб-сервисов и программных интерфейсов (API). Протокол приёмки 25 октября 2026 года закрыл 12 критериев из 12 на размеченном наборе из 28 сценариев, где 14 уязвимых и 14 чистых: найдены все 14 уязвимостей, ложных срабатываний нет.

Автоматическая проверка охватывает семь классов: внедрение команд в запросы к базе данных (SQL), внедрение команд операционной системы, обход каталога, доступ к чужим объектам по прямой ссылке (IDOR) и обход авторизации на уровне объекта (BOLA), подделку запросов на стороне сервера (SSRF), утечку секретов и отсутствие заголовков безопасности. Истощение ресурсов проверяется только в

лабораторном режиме. Программный фильтр в пути запроса перехватил все 26 разрушительных запросов до отправки, а зондирование ограничено белым списком адресов арендатора.

Протокол приёмки остаётся документом разработчика и не заменяет сертификата Федеральной службы по техническому и экспортному контролю (далее — ФСТЭК России).

5. Как повторить

Цепь квитанций MITR

```
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   # 0 — якоря сошлись
curl -O https://asi5.ru/console/verify/gate-anchor-epoch-33.json
curl -O https://asi5.ru/console/verify/gate-anchor-epoch-33.json.ots
ots --no-bitcoin verify gate-anchor-epoch-33.json.ots          # метка календаря, без узла Bitcoin
# сверка с блоком 973 024: ots verify при доступном узле Bitcoin
```

Открытый пакет без сети

```
mkdir wheels && cd wheels
curl -O https://isslab.ru/wp-content/uploads/iss-utils/mcp_sentinel-1.1.2-py3-none-any.whl
curl -O https://isslab.ru/wp-content/uploads/iss-utils/iss_ledger_117-1.1.1-py3-none-any.whl
sha256sum *.whl   # mcp-sentinel требует журнал iss-ledger-117; суммы — в разделе 3
cd .. && python3 -m venv .venv && . .venv/bin/activate
pip install --no-index --find-links ./wheels mcp-sentinel
mcp-sentinel check --tool sql_query --args '{"query": "DROP TABLE users;"}'
# BLOCK, код выхода 2
```

6. Границы применимости

- MITR доказывает допустимость действия при переданных ему фактах, а сами факты устанавливают системы заказчика, поэтому неверное правило даёт доказанно неверный допуск.
- Агент, у которого есть собственные ключи от систем, обходит любой слой контроля. Свойство «мимо MITR не пройти» принадлежит установке: ключи держит MITR, а у агента остаётся только право запросить проверку.
- Текст модели, качество её ответа и закладки в её весах лежат вне предмета MITR.
- Сертификата соответствия у MITR нет. На значимых объектах критической информационной инфраструктуры применяется установленный порядок подтверждения соответствия программного обеспечения и аттестации системы.
- Проверки третьей стороной ещё не было: набор атак и повтор цепи прогонял сам институт, а всё, что нужно для стороннего повтора, опубликовано.

Автономная некоммерческая организация «Научно-исследовательский институт системного синтеза», ОГРН 1267700083617, ИНН 9731161602. 121352, город Москва, улица Давыдковская, дом 18, помещение VIII. Почта: info@isslab.ru, страница: isslab.ru/mitr/, редакция 26 октября 2026 года.