

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

AI-Driven Intelligent Security

Интеллектуальное решение на базе ИИ для тестирования и валидации безопасности ядра сети 5G (5GC)

I. Ключевые преимущества: ИИ-нативная архитектура, замкнутый интеллектуальный цикл и глубокая валидация

Решение формирует передовую ИИ-нативную систему автоматизированной валидации безопасности ядра сети 5G. Большие языковые модели (LLM) глубоко анализируют семантику протоколов 3GPP и обеспечивают автоматизацию всего процесса - от поиска уязвимостей, создания тестовых сценариев и настройки среды до захвата трафика и интеллектуального анализа. Замкнутый цикл значительно повышает эффективность обнаружения уязвимостей и глубину проверки, сокращая традиционный ручной цикл тестирования с нескольких недель до нескольких часов.

II. Основные функции

Функция	Описание
Интеллектуальное создание и проверка уязвимостей	LLM с обучением без примеров автоматически создаёт семантически корректные, но аномальные на границах тестовые сценарии, включая некорректные передачи обслуживания и сигнальные штормы, а затем проверяет их эффективность с помощью средств инструментального тестирования.
Глубокий анализ протокольных аномалий	Двойные механизмы ИИ и правил анализируют рсар-файлы и точно выявляют нарушения протоколов, выходы из конечных автоматов, подмену параметров, скрытые цепочки атак и другие аномалии при доле ложных срабатываний менее 5%.
Многомерное моделирование атак	Поддерживает интерфейсы NAS, PFCP, SBI и HTTP/2 и моделирует более 20 типов атак, характерных для 5GC: незаконный доступ, внедрение сигнализации, DDoS, повышение привилегий API и другие.
Замкнутый цикл валидации и рекомендации по устранению	Автоматически формирует отчёты об уязвимостях, схемы цепочек атак, пакеты доказательств рсар и рекомендации по устранению с указанием пунктов 3GPP и обеспечивает интеграцию с процессами DevSecOps.

2.1. Описание ключевого процесса

2.1.1. Схема выполнения задачи

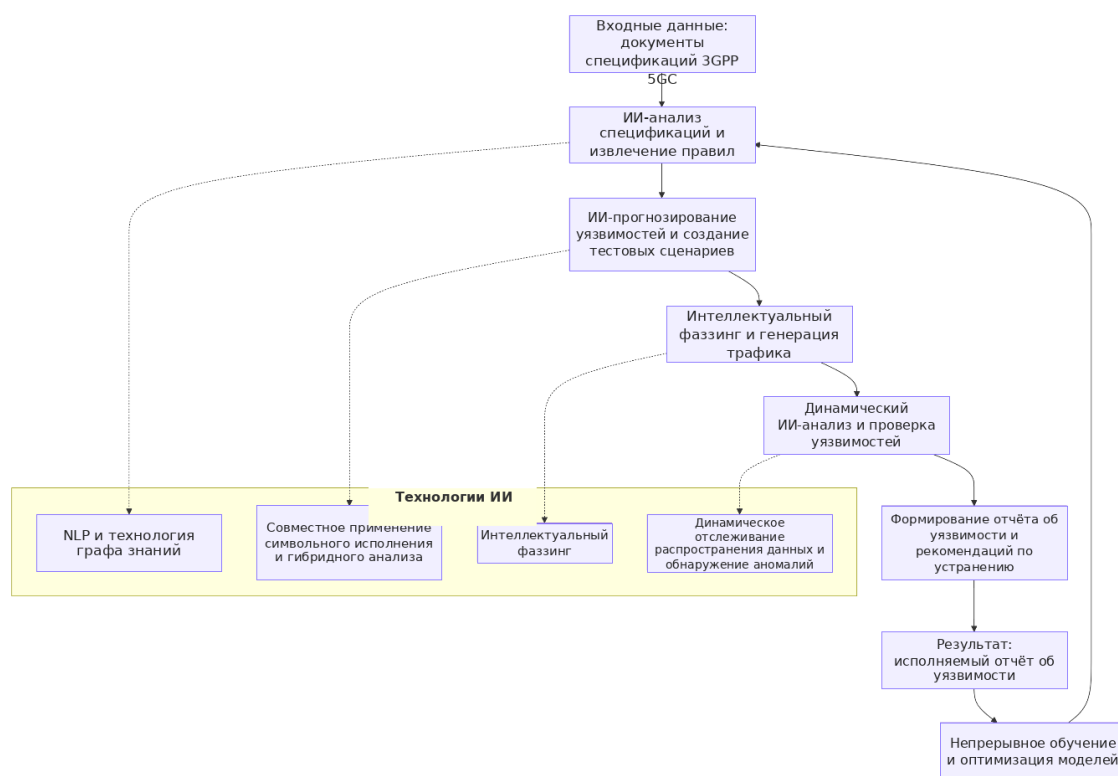


Рисунок 1. Замкнутый процесс интеллектуального тестирования и валидации безопасности 5G

2.1.2. Анализ протоколов и извлечение правил на базе ИИ

Подробности: этап формирует базу знаний системы. Традиционный подход требует от специалистов по безопасности вручную изучать десятки тысяч страниц документов 3GPP, включая TS 23.501, 23.502 и 29.501, что занимает много времени и приводит к пропускам. Решение использует NLP и графы знаний для автоматического «чтения» и понимания сложных стандартов:

- **Извлечение сущностей и связей:** модели NLP, включая дообученные BERT и LLM, выявляют ключевые сущности: типы сообщений Registration Request, информационные элементы SUCI и 5G-GUTI, этапы процедур, состояния REGISTERED, а также ограничения и зависимости.
- **Построение графа знаний:** извлечённые сущности и связи формируются в граф знаний протоколов 5G. Узлы представляют сетевые элементы, сообщения, параметры или состояния, а рёбра - связи между ними, например «отправляет», «содержит» или «зависит от».
- **Автоматическое извлечение правил:** из графа формируются машиноисполняемые правила тестирования безопасности, например: «AMF должен проверить SUCI до назначения 5G-GUTI».

Значение:

- **Автоматизация:** освобождает специалистов от трудоёмкого изучения документации и резко повышает эффективность.
- **Полнота и точность:** ИИ последовательно обрабатывает все детали протоколов и превосходит ручной анализ по охвату.
- **Машиночитаемый результат:** создаёт структурированную вычислимую базу знаний для автоматизированного тестирования.

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

2.1.3. Прогнозирование уязвимостей и создание тестовых сценариев на базе ИИ

Подробности: используя граф знаний протоколов, ИИ имитирует мышление злоумышленника, прогнозирует риски и создаёт тестовые сценарии:

- **Прогнозирование уязвимостей:** исторические данные CVE объединяются с графом знаний для выявления потенциально опасных мест, например незащищённых параметров состояния или состояний гонки.
- **Интеллектуальное создание сценариев:** символьное исполнение и гибридный анализ исследуют логические пути, а интеллектуальный фаззинг создаёт семантически корректные, но логически аномальные тесты. Пример - правильно сформированный запрос PDU-сеанса, отправленный в неверный момент. Результат передаётся средствам инструментального тестирования протоколов в формате JSON.

Значение:

- **Проактивная защита:** выявляет неизвестные уязвимости нулевого дня, отсутствующие в существующих базах.
- **Высокая результативность:** целевые тестовые сценарии уменьшают шум и превосходят случайное тестирование.
- **Глубокое покрытие:** достигает сложных состояний и взаимодействий протоколов, недоступных при ручном тестировании.

2.1.4. Интеллектуальный фаззинг и проверка уязвимостей

Подробности: созданные тестовые сценарии проверяются с помощью программируемых протоколов или средств инструментального тестирования 5GC:

- **Создание экземпляра сценария:** абстрактный сценарий преобразуется в конкретную процедуру 5G, например регистрацию или передачу обслуживания.
- **Динамическое отслеживание распространения данных:** целевые системы, включая AMF и SMF, контролируются на предмет аномалий, вызванных тестовыми данными.
- **Обратная связь в реальном времени:** стратегия фаззинга корректируется по данным о сбоях и журналах, автоматизируя цикл «создать - проверить - оптимизировать».

Значение:

- **Подтверждение концепции:** преобразует потенциальные уязвимости в практические доказательства.
- **Точная локализация:** определяет конкретные ошибки кода или логики с помощью отслеживания распространения данных.
- **Автоматизация замкнутого цикла:** исключает ручное вмешательство.

2.1.5. Анализ и формирование отчётов на базе ИИ

Подробности: по журналам тестирования и рсар-файлам формируются отчёты, удобные как для специалистов, так и для машинной обработки:

- **Структурированные отчёты:** содержат последовательности сигнализации, схемы Mermaid, анализ отказов, первопричины и выводы.
- **Интеллектуальные исправления:** предлагают практические рекомендации со ссылками на пункты 3GPP и примерами кода или конфигурации.
- **Непрерывное обучение:** обратная связь уточняет модели ИИ и обеспечивает их саморазвитие.

Значение:

- **Ускорение устранения:** понятное описание проблемы сокращает среднее время восстановления (MTTR).

- **Готовность к аудиту:** полная цепочка доказательств обеспечивает соответствие проверкам, включая MLPS 2.0 в Китае.
- **Сохранение знаний:** закрепляет накопленную экспертизу по безопасности внутри платформы.

III. Ключевые возможности

- **Автоматическое обнаружение уязвимостей:** круглосуточное сканирование узлов 5GC, включая AMF, SMF и UDM, для выявления уязвимостей нулевого дня и ошибок конфигурации.
- **Оценка базового уровня безопасности:** проверка соответствия ETSI, NIST и 3GPP до развёртывания.
- **Расследование атак:** восстановление маршрутов атак по рабочему трафику с сопоставлением MITRE ATT&CK и индикаторами компрометации (IOC).
- **Учения красной и синей команд:** настраиваемые сценарии атак для обучения безопасности и оценки реагирования.

IV. Ценность для заказчика

Проблема заказчика	Преимущество решения
Низкая эффективность тестирования и высокие трудозатраты	Повышение эффективности в 10 раз и сокращение затрат на 70%
Реактивное устранение уязвимостей	Проактивное выявление уязвимостей нулевого дня; MTTD менее 1 часа
Большое количество ложных срабатываний и сложная проверка	ИИ и правила обеспечивают точность более 95%; повторное воспроизведение одним нажатием
Отсутствие доказательств для аудита соответствия	Автоматическое формирование доказательств ISO 27001, NIST CSF и MLPS 2.0
Недостаточное покрытие из-за сложности 5GC	Покрытие более 98% благодаря семантическим граничным сценариям

V. Технические особенности

- **Механизм семантического анализа протоколов:** LLM-анализатор 3GPP извлекает конечные автоматы и ограничения сообщений для формирования аномальных сценариев, например неаутентифицированных запросов PDU.
- **Двойной анализ ИИ и правил:** обнаружение аномалий на базе ИИ сочетается с проверками правил 3GPP, снижая количество ложных срабатываний, например при проверке SUPI узлом AMF.
- **Саморазвивающиеся тестовые сценарии:** обучение с подкреплением оптимизирует стратегии по частоте обнаружения, делая тестирование эффективнее со временем.
- **Тестирование с цифровым двойником:** атаки моделируются в изолированных средах 5GC без риска для продуктивной сети.

VI. Заключение

По мере перехода 5G к облачной архитектуре, сервисной модели и открытым интерфейсам традиционное тестирование безопасности перестаёт справляться со сложностью протоколов и скрытыми атаками. Решение, в котором ИИ выступает «мозгом», автоматизация - «руками», а валидация замкнутого цикла - «глазами», формирует систему интеллектуальной проверки безопасности нового поколения. Она помогает операторам, поставщикам и предприятиям обеспечить раннее выявление уязвимостей, практическое устранение рисков, подтверждаемое соответствие требованиям и проактивную защиту.

