БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2026. – № 2 (121). – 91–106

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2026-2-91-106

РАЗРАБОТКА МЕТОДИКИ ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЯ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ*

К.А. БИРЮКОВ[1], А.В. ИВАНОВ[2]

[1] *РФ, 630047, г. Новосибирск, ул. Окружная, 29В, ООО «Предприятие “ЭЛТЕКС”», руководитель группы лицензирования сервисного центра ESR. E-mail: kirill.biryukov@eltex-co.ru*
[2] *РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент, заведующий кафедрой защиты информации. E-mail: andrej.ivanov@corp.nstu.ru*

В настоящей статье рассматривается разработка универсальной комплексной методики тестирования систем обнаружения и предотвращения вторжений для объективной оценки их эффективности в условиях роста сложности сетевых атак. Существующие подходы часто зависят от конкретного производителя, что затрудняет независимый сравнительный анализ. Методика основана на модульном подходе и реализуется на тестовом стенде с непосредственным включением системы на пути сетевого трафика. В рамках исследования сформулированы требования к методике, включая универсальность, воспроизводимость, простоту применения и прозрачность анализа результатов. В ходе функциональных тестов проверяется блокировка атак в реальном времени, корректность журналирования, обработка правил для различных протоколов, контентная фильтрация и поведение системы в режиме отказа. В статье предложена структура оценки, соответствующая рекомендациям стандартов ISO/IEC 27034-1 и NIST SP 800-94. Разработанное решение позволяет проводить независимый сравнительный анализ средств защиты независимо от вендора и сокращать затраты на тестирование, обеспечивает воспроизводимость тестов и повышает обоснованность выбора средств защиты для критической инфраструктуры.

Ключевые слова: система обнаружения вторжений, система предотвращения вторжений, методика тестирования, inline-режим, сигнатуры, фильтрация трафика

* Статья получена 12 мая 2026 г.

ВВЕДЕНИЕ

В условиях цифровой трансформации критической инфраструктуры системы обнаружения и предотвращения вторжений (Intrusion Detection and Prevention Systems, далее IDS/IPS) становятся неотъемлемым компонентом эшелонированной защиты, обеспечивая мониторинг и блокировку вредоносной активности [1]. Однако надежность периметра безопасности напрямую зависит от корректности конфигурации и действительной эффективности применяемых средств защиты.

Для подтверждения соответствия заявленных функций систем IDS/IPS их производители требуют проведения объективной оценки их характеристик [2]. Несмотря на наличие международных стандартов, практическая реализация тестирования часто сталкивается с ограничениями, связанными с отсутствием универсальных верификационных процедур. Большинство существующих подходов к оценке ориентированы на специфические программно-аппаратные комплексы, что затрудняет проведение независимого сравнительного анализа. Возникающее противоречие между необходимостью полноценного функционального и точечного тестирования имеющихся методик обусловливает актуальность разработки единого подхода к тестированию.

ПОСТАНОВКА ЗАДАЧИ

- Рассмотреть существующие методики тестирования систем IDS/IPS и выявить их слабые стороны.
- Сформировать критерии, которым должна соответствовать разрабатываемая методика тестирования.
- На основе критериев разработать методику тестирования систем IDS/IPS.

1. ПРОБЛЕМЫ СУЩЕСТВУЮЩИХ МЕТОДИК ТЕСТИРОВАНИЯ

В методиках тестирования систем IDS/IPS наблюдается следующая тенденция: процедуры оценки детально проработаны, но привязаны к конкретному продукту, так как большинство методик написаны непосредственно производителем этих систем и ориентированы на демонстрацию функционала конкретно их продукта [3]. Это не позволяет использовать данные методики в рамках тестирования различных продуктов класса IDS/IPS систем во время сравнительных тестов для выявления наиболее подходящего экземпляра под конкретные задачи.

Целью работы является разработка универсальной комплексной методики тестирования IDS/IPS, обеспечивающей объективную оценку эффективности средств защиты с возможностью полного понимания, контроля и воспроизведения тестов без необходимости обладания углубленными навыками работы с системами. Использование предложенного подхода позволит сократить затраты на тестирование, повысить объективность оценки и обеспечить более обоснованный выбор средств защиты для конкретных условий эксплуатации.

2. РАЗРАБОТКА МЕТОДИКИ ТЕСТИРОВАНИЯ

2.1. ТРЕБОВАНИЯ К МЕТОДИКЕ ТЕСТИРОВАНИЯ

Методика функционального тестирования должна соответствовать следующим критериям.

- Применимость к любой системе IDS/IPS независимо от производителя и ее типа (аппаратная/программная) [4].
- Стабильность воспроизведения тестов.
- Простота проведения тестов:
  - отсутствие необходимости использования сложного или платного программного обеспечения, предназначенного для тестирования [5];
  - легко воспроизводимые шаги методики тестирования и анализа результата для человека, не погруженного в специфику IDS/IPS систем.
- Описание назначения каждого тест-кейса, т. е. какой функционал проверяет конкретный тест-кейс и для чего этот функционал необходим в системе IDS/IPS.

В соответствии с указанными критериями была составлена методика тестирования системы IDS/IPS, включающая в себя тесты, отвечающие заданным критериям.

2.2. СХЕМА СТЕНДА ТЕСТИРОВАНИЯ

Для возможности проведения тестирования необходимо построить тестовый стенд.

Тестовый стенд для тестирования систем обнаружения и предотвращения вторжений реализует двунаправленную архитектуру с размещением IDS/IPS системы в режиме inline между внешним и внутренним сетевыми сегментами [6]. Inline-режим – это режим функционирования системы IPS, при котором

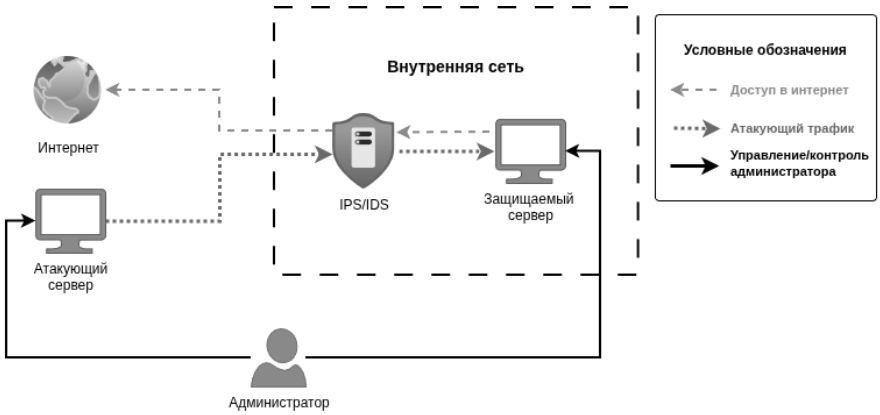

Схема стенда тестирования

Diagram of the test stand

устройство размещается непосредственно на пути сетевого трафика между внешней и защищаемой внутренней сетью, обеспечивая последовательную обработку всех проходящих пакетов [7]. Такая конфигурация соответствует рекомендациям NIST SP 800-94 и обеспечивает обязательную маршрутизацию всего трафика через систему, что критически важно для корректной оценки предотвращающих функций [8]. Стенд включает атакующую станцию с инструментами генерации эксплойтов и аномального трафика, защищаемый сервер с отключенными встроенными средствами защиты и доступом в интернет.

2.3. ПРОВЕРКА БЛОКИРОВАНИЯ АТАК В РЕЖИМЕ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Цель теста: подтвердить возможность системы IPS блокировать атаки в режиме реального времени [9].

Конфигурация стенда: IPS в режиме inline.

Конфигурация защищаемого сервера: сервисы с известными уязвимостями, для которых существуют готовые сигнатуры.

Конфигурация атакующей станции: утилита Metasploit Framework для эксплуатации уязвимостей, утилита iperf3 для генерации легитимного трафика в режиме фонового потока.

Методика тестирования: в рамках подготовки тестовой среды необходимо настроить IPS в inline-режиме с политикой блокирования для выбран-

ных сигнатур атак [10]; с помощью утилиты Metasploit выполнить последовательную генерацию атак с атакующей станции на защищаемый сервер [11], а также выполнить чередование атак с легитимным трафиком для проверки отсутствия влияния на легальный трафик.

Анализ результатов: сопоставить записи журнала IDS с фактическим состоянием защищаемого сервера, удостовериться в отсутствии вредоносной нагрузки при наличии события блокировки.

Ожидаемый результат: система должна выполнить полную блокировку атакующего трафика с генерацией события предотвращения в журнале и отсутствием признаков успешной эксплуатации уязвимости на защищаемом сервере [12].

Критерии успеха: полное блокирование всех проведенных атак при сохранении целостности легитимного трафика.

Критерии неуспеха: успешная эксплуатация уязвимости при наличии записи о блокировке в журнале (несоответствие лога реальному поведению) или блокирование легитимного трафика.

2.4. ПРОВЕРКА КОРРЕКТНОСТИ ЖУРНАЛИРОВАНИЯ И СООТВЕТСТВИЯ ЗАПИСЕЙ РЕАЛЬНЫМ СОБЫТИЯМ

Цель теста: подтвердить полноту, точность и целостность данных, фиксируемых системой в журналах событий.

Конфигурация стенда: развертывание IDS/IPS в режиме inline с настроенным полным журналированием событий в системе IDS.

Конфигурация защищаемого сервера: отключенные встроенные механизмы защиты хоста, настроенный сетевой интерфейс во внутреннем сегменте защищаемой сети.

Конфигурация атакующей станции: настроенный сетевой интерфейс во внешнем сегменте сети, утилита Scapy для генерации аномального трафика, утилита iperf3 для генерации легитимного трафика в режиме фонового потока.

Методика тестирования: развернуть IDS/IPS в режиме inline с настроенным полным журналированием событий; выполнить последовательную генерацию атак типа icmp-flood с помощью Scapy с одновременной генерацией легитимного фонового трафика через iperf3; провести атаку типа syn-flood путем генерации TCP-пакетов с флагом SYN через Scapy с интенсивностью, превышающей пороговое значение системы (например, 1500 соединений в секунду), с одновременной передачей легитимных установок соединений для проверки дифференциации атакующего и легитимного трафика [13]; дополнительно выполнить атаку типа UDP-flood с генерацией пакетов с произволь-

ными портами назначения через Scapy для имитации спуфинга и использованием iperf3 в режиме генерации UDP-трафика с пропускной способностью, превышающей лимит системы.

Анализ результатов: сравнить данные журнала событий с фактическими действиями, совершенными в ходе теста, а именно: временные метки событий, IP-адрес источника и цели, его порт, тип протокола, количество обработанных пакетов, действие системы обнаружения и предотвращения вторжений (блокировка, ограничение, журналирование).

Ожидаемый результат: система обеспечивает журналирование всех событий в соответствии с ее фактическими действиями.

Критерии успеха

- Разница во времени между реальным событием и тем, как оно записано, меньше одной секунды.
- Заявленное действие системы соответствует ее фактическому поведению.
- Отсутствуют ложные срабатывания на легитимном трафике.

Критерии неуспеха

- Разница во времени между реальным событием и тем, как оно записано, более одной секунды для более чем 5 % трафика.
- Заявленное действия системы не соответствует ее фактическому поведению.
- В журнале присутствуют ложные срабатывания на легитимном трафике (например, заявленная блокировка при прохождении пакетов).

2.5. ПРОВЕРКА СРАБАТЫВАНИЯ ПРАВИЛ ПО КОНКРЕТНЫМ ПРОТОКОЛАМ

Цель теста: проверить корректную отработку правила системы IDS/IPS по конкретным сетевым протоколам [14].

Конфигурация стенда: развертывание системы IPS в режиме с конфигурацией правил для протоколов TCP, UDP, ICMP, IP, HTTP.

Конфигурация защищаемого сервера: отключенные встроенные механизмы защиты хоста, настроенный сетевой интерфейс во внутреннем сегменте защищаемой сети.

Конфигурация атакующей станции: утилита Scapy для генерации трафика в формате конкретного протокола.

Методика тестирования: выполняем последовательную генерацию трафика по протоколам TCP, UDP, ICMP, IP, HTTP с помощью утилиты Scapy.

Анализ результатов: каждый тип протокола должен вызвать срабатывание правила, относящегося конкретно к его типу.

Ожидаемый результат: система должна обеспечить корректное детектирование и отработку правил для каждого протокола без взаимного влияния.

Критерии успеха

- Полное детектирование целевых аномалий для каждого протокола с корректной привязкой к соответствующему правилу.
- Отсутствие ложных срабатываний правил на легитимном трафике других протоколов.

Критерии неуспеха

- Отсутствие детектирования более чем 1 % аномальных пакетов для любого протокола.
- Ложное срабатывание правила для протокола, отличного от целевого.
- Расхождение между заявленным действием правила и фактическим поведением трафика (например, заявленная блокировка при прохождении пакетов).

2.6. ПРОВЕРКА НАСТРОЙКИ КАТЕГОРИЙ КОНТЕНТНОЙ ФИЛЬТРАЦИИ

Цель теста: подтвердить корректность и возможность фильтрации трафика по конкретным категориям контента [15].

Конфигурация стенда: развертывание системы IPS в режиме inline с установленными категориями для контентной фильтрации (например, Gambling, Social-media, Games).

Конфигурация защищаемого сервера: браузер или утилита wget для отправки запросов на ресурсы из сконфигурированных категорий.

Методика тестирования: выполнить генерацию трафика путем последовательной отправки запросов на сайты из категорий gambling, social-media и games, а также на любой другой сайт, не входящий в список настроенных категорий.

Анализ результатов: проверить срабатывание соответствующего правила на каждую категорию и удостовериться в отсутствии ложных срабатываний при отправке запросов на сайты, не входящие в список настроенных категорий.

Ожидаемый результат: система должна обеспечить корректную фильтрацию трафика согласно настроенным категориям контентной фильтрации.

Критерии успеха

- Полная сработка правил при попытках доступа к ресурсам, попадающим под настроенные категории.
- Отсутствие ложных срабатываний правил на легитимном трафике.

Критерии неуспеха

- Отсутствие детектирования более чем 1 % пакетов, подходящих под трафик указанных категорий.
- Ложное срабатывание правила для легитимного трафика при доступе к ресурсу, однозначно не относящемуся к указанной категории.

2.7. ВЕРИФИКАЦИЯ РЕЖИМА ОТКАЗА В БЕЗОПАСНОЕ СОСТОЯНИЕ (FAIL-CLOSE)

Цель теста: проверить корректную реализацию принципа «отказ в безопасное состояние» (fail-safe/fail-secure), при котором система IPS в условиях неготовности (отсутствие сигнатур, сбои обновления) [16] блокирует весь входящий трафик, предотвращая потенциальную эксплуатацию уязвимостей в период незащищенного состояния.

Конфигурация стенда: развертывание системы IPS в режиме inline в конфигурации режима отказа fail-close.

Конфигурация защищаемого хоста: наличие утилиты ping для генерации ICMP трафика.

Методика тестирования: необходимо прервать возможность обновления сигнатур путем отключения связи с сервером; удалить локально сохраненные сигнатуры; выполнить генерацию легитимного ICMP трафика с помощью утилиты ping; сравнить количество отправленных и полученных пакетов; вернуть связь системы IDS/IPS с сервером сигнатур и выполнить повторную генерацию аналогичного ICMP трафика; вновь сравнить количество отправленных и полученных пакетов.

Анализ результатов: при невозможности доступа к серверу сигнатур и отсутствии их в локальном кеше блокируется весь трафик. При подключении системы к серверу сигнатур и получении с него правил легитимный трафик свободно проходит через систему IPS/IDS.

Ожидаемый результат: при отсутствии сигнатур система блокирует прохождение всего трафика.

Критерии успеха

- Полное блокирование легитимного трафика при нулевом количестве загруженных сигнатур.
- Отсутствие потерь легитимного трафика после успешной загрузки сигнатур при отсутствии активных атак.

Критерии неуспеха

- Пропускание любого трафика при отсутствии загруженных сигнатур.
- Блокирование легитимного трафика после успешной загрузки сигнатур при отсутствии активных атак.

- Отсутствие системных событий, фиксирующих переходы между состояниями загрузки сигнатур.

2.8. ПРОВЕРКА ДОСТОВЕРНОСТИ ОПЕРАТИВНОЙ СТАТИСТИКИ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Цель теста: проверить возможность просмотра оперативной информации по сконфигурированным правилам и сигнатурам, а также корректность состояния счетчиков их срабатываний.

Конфигурация стенда: развертывание системы IPS в режиме inline с настроенными категориями и URL контентной фильтрации, скачанными и примененными сигнатурами. Для всех настроек установлены различные виды действия системы (оповещение, блокировка, пропуск).

Конфигурация защищаемого хоста: браузер или утилита wget для отправки запросов на ресурсы из списка сконфигурированных URL, утилита Scapy для генерации аномального трафика.

Методика тестирования: зафиксировать показатели статистики до загрузки базы сигнатур (количество правил, сигнатур, политик) и активировать загрузку сигнатур с мониторингом процесса через средство просмотра оперативной информации; выполнить генерацию трафика, подходящего под сигнатуры различных действий, а также генерацию легитимного трафика.

Анализ результатов: сопоставить количество срабатываний в интерфейсе статистики с фактическим количеством событий в трафике; проверить отсутствие инкрементации счетчиков ложных срабатываний при обработке легитимного трафика; проверить корректность агрегации данных (суммарное количество срабатываний по политике должно равняться сумме срабатываний всех входящих в нее правил); убедиться, что отображаемые метрики точно отражают текущее состояние системы и ее действий.

Ожидаемый результат: отображаемые метрики точно отражают текущее состояние системы и ее действий.

Критерии успеха

- Средняя задержка обновления оперативной статистики менее двух секунд при нагрузке до 90 % от номинальной пропускной способности системы.
- Полное соответствие агрегированных данных на уровне политик сумме данных по входящим в них правилам.
- Отсутствие ложной инкрементации счетчиков при обработке легитимного трафика.

Критерии неуспеха

- Относительная погрешность количественных метрик более 1 % для любого из проверяемых параметров.

- Отсутствие обновления статистики более 60 секунд после завершения операции загрузки сигнатур или после серии срабатываний.
- Несоответствие между заявленным количеством сработавших правил и фактическими действиями системы (например, блокирование трафика без инкрементации счётчика).
- Нарушение иерархической целостности данных (сумма срабатываний дочерних правил не равна количеству срабатываний родительской политики) для более чем 5 % проверенных политик.

3. СРАВНЕНИЕ РАЗРАБОТАННОЙ МЕТОДИКИ ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЯ С СУЩЕСТВУЮЩИМИ АНАЛОГАМИ

Для объективной оценки преимуществ и практической ценности разработанной методики функционального тестирования был проведен сравнительный анализ с существующими подходами к тестированию средств защиты информации. В качестве объектов сравнения выбраны методологии тестирования ведущих российских вендоров (Jet, Solar, Континент) [17–19], что обеспечивает репрезентативность выборки и позволяет выявить ключевые отличия предложенного подхода.

Разработанная методология функционального тестирования систем обнаружения и предотвращения вторжений представляет собой структурированный комплекс тест-кейсов, обеспечивающий проверку ключевых функциональных свойств средств защиты в соответствии с принципами объективности и воспроизводимости, рекомендованными в работах Национального института стандартов и технологий (NIST). Методика реализует системный подход к оценке, охватывающий критические аспекты функционирования IDS/IPS: эффективность предотвращения атак в реальном времени, достоверность журналирования, корректность обработки протокольно-специфичных правил и надежность механизмов отказоустойчивости.

Структурной основой методики выступает модульная организация тестовых сценариев, каждый из которых проверяет отдельный функциональный блок системы защиты IDS/IPS. Тестовый модуль верификации блокирования атак в режиме предотвращения обеспечивает оценку способности системы к детектированию и прерыванию эксплуатации уязвимостей на уровне прикладных протоколов. Эта методика позволяет выполнить проверку работы журнала событий для подтверждения соответствий записей реальному поведению системы. Такая проверка обеспечивает соответствие методики функционального тестирования стандарту ISO/IEC 27034-1.

Сравнительный анализ функциональных методик тестирования IDS/IPS

A comparative analysis of functional testing methods for IDS/IPS

Критерий сравнения	Авторская методика	Методика Jet	Методика Solar	Методика «Континент 4» (TS Solution)
Универсальность / независимость от вендора	Да	Частично	Нет	Нет
Воспроизводимость тестов	Да	Да	Частично	Нет
Использование только бесплатного / открытого ПО	Да	Нет	Нет	Да
Четкие критерии успеха и провала для каждого теста	Да	Частично	Частично	Нет
Соответствие международным стандартам	Да	Частично	Нет	Нет
Тестирование режима Fail-Close	Да	Нет	Нет	Нет
Проверка достоверности оперативной статистики	Да	Нет	Нет	Нет
Описание назначения каждого тест-кейса	Да	Частично	Частично	Нет

Важным отличием авторской методики является наличие проверки режима отказа. Такой сценарий проверяет работу системы при отсутствии сигнатур, что позволяет оценить поведение системы в нештатной ситуации при технических сбоях.

ЗАКЛЮЧЕНИЕ

Таким образом, разработанная методика функционального тестирования позволяет выполнять оценку функциональности систем обнаружения и предотвращения вторжений независимо от их производителя с возможностью воспроизведения тестовых сценариев, используя только открытые и бесплатные инструменты. Благодаря своей структуре методика может быть применена как для комплексной проверки функциональности систем IDS/IPS, так и для частичной проверки конкретных возможностей, что обеспечивает ее значительное преимущество относительно других методик функционального тестирования систем обнаружения и предотвращения вторжений.

СПИСОК ЛИТЕРАТУРЫ

1. *Mehta H., Nizama A., Subhashini K.* Comprehensive review of network intrusion detection and prevention systems // International Journal of Latest Technology in Engineering Management and Applied Science. – 2025. – Vol. 14 (6). – P. 804–807. – DOI: 10.51583/IJLTEMAS.2025.140600087.

2. *Bhadti A., Barthakur P.* A survey on next generation intrusion detection systems empowering advanced threat detection with generative AI // International Journal of Advanced Research in Computer and Communication Engineering. – 2024. – Vol. 13 (6). – DOI: 10.17148/IJARCCE.2024.13633.

3. ISO/IEC 27034-1:2011. Information technology – Security techniques – Application security – Part 1: Overview and concepts. – URL: https://www.iso.org/standard/44378.html (accessed: 03.02.2026).

4. *Tori A.R., Hasan K.F.* An evaluation framework for network IDS/IPS datasets: leveraging MITRE ATT&CK and industry relevance metrics // arXiv preprint. – 2025. – DOI: 10.48550/arXiv.2511.12743.

5. *Kott A.* Autonomous intelligent cyber-defense agent: Introduction and overview // Advances in Information Security. Vol. 87. – Cham: Springer, 2023. – DOI: 10.1007/978-3-031-29269-9_1.

6. PP-Module for intrusion prevention systems (IPS). Version: 1.0. – NIAP, 2021. – URL: https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/MOD_IPS_v1.0.pdf (accessed: 15.02.2026).

7. *Beale J.*, et al. Snort intrusion detection and prevention toolkit. – Syngress, 2021.

8. *Scarfone K.A., Mell P.M.* Guide to intrusion detection and prevention systems (IDPS). – URL: https://csrc.nist.gov/pubs/sp/800/94/r1/ipd (accessed: 22.02.2026).

9. *Vishrutha V., Nagaraja G.S.* Real-time intrusion detection system using scapy with hybrid machine and deep learning models and smart email alerting // SSRN Electronic Journal. – 2025. – URL: https://ssrn.com/abstract=5349776 (accessed: 07.02.2026).

10. *Alqahtani H., Kumar G.* A deep learning-based intrusion detection system for in-vehicle networks with knowledge graph and statistical methods // International Journal of Machine Learning and Cybernetics. – 2024. – Vol. 16 (5–6). – P. 3539–3555. – DOI: 10.1007/s13042-024-02465-0.

11. *Tandon A., Pandey S.* A study on penetration testing using metasploit framework // International Journal of Research and Review in Applied Science, Humanities, and Technology. – 2025. – Spec. iss. – P. 83–87. – DOI: 10.71143/y4sten11.

12. *Bejtlich R.* The practice of network security monitoring. – Starch Press, 2022.

13. *Manzuik S., Gold A., Gatford C.* Network security assessment: From vulnerability to patch. – Syngress, 2006. – 372 p.

14. Fortinet. Intrusion prevention system (IPS) // Fortinet Documentation Library. – URL: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/48143/intrusion-prevention-system-ips (accessed: 07.02.2026).

15. *Sun Q.* Intrusion detection in high-performance computing. – 2024. – URL: https://hps.vi4io.org/_media/teaching/autumn_term_2023/stud/hpcsa_sun_qumeng.pdf (accessed: 05.02.2026).

16. *Аникин А.Д., Бирюков К.А., Архипова А.Б.* Анализ протоколов безопасности на базе системы распространения лицензируемого контента // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 26–35. – DOI: 10.17212/2782-2230-2023-1-26-35.

17. РТ-Солар. Solar Next Generation Firewall. Методика тестирования. Версия 1.2. – М.: ООО «РТ-Солар», 2024. – 24 с. – URL: https://rt-solar.ru/upload/docs/solar-ngfw--metodika-testirovaniya-v1.2.pdf (дата обращения: 26.03.2026).

18. Отчет о тестировании функций безопасности NGFW «Континент 4» / С.Х. Аббас, В.А. Насер, А.А. Кадим; TS Solution. – М.: ООО «Код Безопасности», 2024. – 16 с. – URL: https://www.securitycode.ru/upload/blog/Отчет%20о%20тестировании%20функций%20безопасности%20NGFW_Континент%204.pdf (дата обращения: 26.03.2026).

19. Методика функционального тестирования устройств класса NGFW/UTM: версия 2.0. – М.: Инфосистемы Джет, 2024. – 25 с. – URL: https://ngfw.jet.su/metodika_funkczionalnogo_testirovaniya_2_0.pdf (дата обращения: 26.03.2026).

Бирюков Кирилл Андреевич, руководитель группы лицензирования сервисного центра ESR компании «Элтекс». Область научных интересов: информационная безопасность, компьютерные сети. E-mail: kirill.biryukov@eltex-co.ru

Иванов Андрей Валерьевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации Новосибирского государственного технического университета. Область научных интересов: информационная безопасность, кибербезопасность. E-mail: andrej.ivanov@corp.nstu.ru

DOI: 10.17212/2782-2230-2026-2-91-106

Development of a methodology for functional testing of intrusion detection and prevention systems*

K.A. Biryukov[1], A.V. Ivanov[2]

[1] *Eltex, 29V, Okruzhnaya Street, Novosibirsk, Russian Federation, 630073, Russian Federation, head of the licensing group of the service center ESR. E-mail: kirill.biryukov@eltex-co.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, PhD in Technology, head of the Information Security Department. E-mail: andrej.ivanov@corp.nstu.ru.*

This article discusses the development of a universal, comprehensive testing methodology for intrusion detection and prevention systems, designed to objectively evaluate their effectiveness in the face of increasingly complex network attacks. Existing approaches are often vendor-specific, which hinders independent comparative analysis. The methodology is based on a modular approach and is implemented on a test bench with the system directly integrated into the network traffic path. The study formulates requirements for the methodology, including universality, reproducibility, ease of use, and transparency of results analysis. Functional tests verify real-time attack blocking, logging accuracy, rule processing for various protocols, content filtering, and system behavior in failure mode. The article proposes an evaluation framework consistent with the recommendations of ISO/IEC 27034-1 and NIST SP 800-94. The developed solution enables independent, vendor-neutral comparative analysis of security measures, reduces testing costs, ensures test reproducibility, and enhances the soundness of security measure selection for critical infrastructure.

Keywords: intrusion detection system, intrusion prevention system, testing methodology, inline mode, signatures, traffic filtering

REFERENCES

1. Mehta H., Nizama A., Subhashini K. Comprehensive review of network intrusion detection and prevention systems. *International Journal of Latest Tech-*

* *Received 12 May 2026.*

nology in Engineering Management and Applied Science, 2025, vol. 14 (6), pp. 804–807. DOI: 10.51583/IJLTEMAS.2025.140600087.

2. Bhadti A., Barthakur P. A survey on next generation intrusion detection systems empowering advanced threat detection with generative AI. *International Journal of Advanced Research in Computer and Communication Engineering*, 2024, vol. 13 (6). DOI: 10.17148/IJARCCE.2024.13633.

3. ISO/IEC 27034-1:2011. *Information technology – Security techniques – Application security* – Part 1: *Overview and concepts*. Available at: https://www.iso.org/standard/44378.html (accessed 12.02.2026).

4. Tori A.R., Hasan K.F. An evaluation framework for network IDS/IPS datasets: leveraging MITRE ATT&CK and industry relevance metrics. *arXiv preprint*, 2025. DOI: 10.48550/arXiv.2511.12743.

5. Kott A. Autonomous intelligent cyber-defense agent: Introduction and overview. *Advances in Information Security*. Vol. 87. Cham, Springer, 2023. DOI: 10.1007/978-3-031-29269-9_1.

6. *PP-Module for intrusion prevention systems (IPS)*. Version: 1.0. NIAP, 2021. Available at: https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/MOD_IPS_v1.0.pdf (accessed 15.02.2026).

7. Beale J., et al. *Snort intrusion detection and prevention toolkit*. Syngress, 2021.

8. Scarfone K.A., Mell P.M. *Guide to intrusion detection and prevention systems (IDPS)*. Available at: https://csrc.nist.gov/pubs/sp/800/94/r1/ipd (accessed 22.02.2026).

9. Vishrutha V., Nagaraja G.S. Real-time intrusion detection system using scapy with hybrid machine and deep learning models and smart email alerting. *SSRN Electronic Journal*, 2025. Available at: https://ssrn.com/abstract=5349776 (accessed 07.02.2026).

10. Alqahtani H., Kumar G. A deep learning-based intrusion detection system for in-vehicle networks with knowledge graph and statistical methods. *International Journal of Machine Learning and Cybernetics*, 2024, vol. 16 (5–6), pp. 3539–3555. DOI: 10.1007/s13042-024-02465-0.

11. Tandon A., Pandey S. A study on penetration testing using metasploit framework. *International Journal of Research and Review in Applied Science, Humanities, and Technology*. 2025, Spec. iss., pp. 83–87. DOI: 10.71143/y4sten11.

12. Bejtlich R. *The practice of network security monitoring*. Starch Press, 2022.

13. Manzuik S., Gold A., Gatford C. *Network security assessment: From vulnerability to patch*. Syngress, 2006. 372 p.

14. Fortinet. Intrusion prevention system (IPS). *Fortinet Documentation Library*. Available at: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/48143/intrusion-prevention-system-ips (accessed 07.02.2026).

15. Sun Q. *Intrusion detection in high-performance computing*. 2024. Available at: https://hps.vi4io.org/_media/teaching/autumn_term_2023/stud/hpcsa_sun_qumeng.pdf (accessed 05.02.2026).

16. Anikin A.D., Biryukov K.A., Arkhipova A.B. Analiz protokolov bezopasnosti na baze sistemy rasprostraneniya litsenziruemogo kontenta [Analysis of security protocols based on the licensed content distribution system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 26–35. DOI: 10.17212/2782-2230-2023-1-26-35.

17. RT-Solar. *Solar Next Generation Firewall. Metodika testirovaniya*. Versiya 1.2 [NGFW Solar Testing Methodology. Version 1.2]. Moscow, RT-Solar LLC, 2024. 24 p. Available at: https://rt-solar.ru/upload/docs/solar-ngfw--metodika-testirovaniya-v1.2.pdf (accessed 26.03.2026).

18. Abbas S.Kh., Naser V.A., Kadim A.A. *Otchet o testirovanii funktsii bezopasnosti NGFW «Kontinent 4»* [Security function testing report for NGFW "Continent 4"]. TS Solution. Moscow, Security Code LLC Publ., 2024. 16 p. Available at: https://www.securitycode.ru/upload/blog/Отчет%20о%20тестировании%20функций%20безопасности%20NGFW_Континент%204.pdf (accessed 26.03.2026).

19. Jet Security Team. *Metodika funktsional'nogo testirovaniya ustroistv klassa NGFW/UTM*: versiya 2.0 [Functional testing methodology for NGFW/UTM devices. Version 2.0]. Moscow, 2024. 25 p. Available at: https://ngfw.jet.su/metodika_funkczionalnogo_testirovaniya_2_0.pdf (accessed 26.03.2026).

Для цитирования:

Бирюков К.А., Иванов А.В. Разработка методики функционального тестирования систем обнаружения и предотвращения вторжений // Безопасность цифровых технологий. – 2026. – № 2 (121). – С. 91–106. – DOI: 10.17212/2782-2230-2026-2-91-106.

For citation:

Biryukov K.A., Ivanov A.V. Razrabotka metodiki funktsional'nogo testirovaniya sistem obnaruzheniya i predotvrashcheniya vtorzhenii [Development of a methodology for functional testing of intrusion detection and prevention systems]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2026, no. 2 (121), pp. 91–106. DOI: 10.17212/2782-2230-2026-2-91-106.