ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.492.4
CC BY 4.0
DOI: 10.21822/2073-6185-2025-52-2-150-158 Оригинальная статья/ Original article

Методика нагрузочного тестирования средств межсетевого экранирования

А.М. Садыков[1], Р.Р. Ямалетдинов[2]
[1]Казанский национальный исследовательский технологический университет,
[1] 420015 г. Казань, ул. Карла Маркса, 68, Россия,
[2] ООО «АйСиЭлСТ»,
[2] 420029, Казань, ул. Сибирский тракт, д. 34 к.1, Россия

Резюме. Цель. Цель работы заключается в разработке методики нагрузочного тестирования отечественных межсетевых экранов для оценки их реальной пропускной способности и устойчивости под нагрузкой. Это необходимо для проверки соответствия заявленныхпроизводителем характеристик предлагаемых средств межсетевого экранирования для использования в конкретных защищенных автоматизированных системах. **Метод.** Метод исследования - эмпирический. Предложен и описан испытательный стенд с генератором трафика Cisco TRex, который эмулирует нагрузку. Созданы шаблоны трафика для имитации различных сетевых условий. Методика тестирование включает три режима: маршрутизация без фильтрации, полная блокировка трафика и фильтрация на уровне приложений. Нагрузка постепенно увеличивается до выявления предельных значений стабильной работы. **Результат.** Для проведения нагрузочного тестирования средств межсетевого экранирования разработана методика проведения испытаний. Определены количественные показатели производительности межсетевого экрана в разных режимах. **Вывод.** Предлагаемая методика предназначена для объективной оценки производительности межсетевых экранов. Она позволяет выбирать оптимальные решения по защите информации, выявлять критические сценарии и предотвращать использование недостаточно производительных решений.

Ключевые слова: информационная безопасность, защита информации, межсетевой экран, методика тестирования, трафик, пропускная способность

Для цитирования: А.М. Садыков, Р.Р. Ямалетдинов. Методика нагрузочного тестирования средств межсетевого экранирования. Вестник Дагестанского государственного технического университета. Технические науки. 2025;52(2):150-158.DOI:2025;52(2): 150-158. DOI:10.21822/2073-6185-2025-52-2-150-158

Methodology of load testing of firewalling tools

A.M. Sadykov[1], R.R. Yamaletdinov[2]
[1]Kazan National Research Technological University,
[1]68 Karl Marx St., Kazan 420015, Russia,
[2]«ICIEL System Technologies»,
[2]34 build 1, Sibirsky Trakt, Kazan, 420029, Russia

Abstract. Objective. The purpose of the work is to develop a methodology for load testing domestic firewalls to assess their real throughput and stability under load. This is necessary to verify the compliance of the characteristics of the proposed firewalls declared by the manufacturer for use in specific protected automated systems. **Method.** The research method is empirical. A test bench with a Cisco TRex traffic generator that emulates the load is proposed. Traffic patterns are created to simulate various network conditions. The testing methodology includes three modes: routing without filtering, complete traffic blocking, and filtering at the application level. The load is gradually increased until the limit values of stable operation are identified. **Result.** A testing methodology was developed to conduct load testing of firewalls. Quantitative indicators of firewall

performance in different modes were determined. **Conclusion.**The proposed methodology is intended for an objective assessment of firewall performance. It allows choosing optimal solutions for information protection, identifying critical scenarios and preventing the use of insufficiently productive solutions.

Keywords: information security, information protection, firewall, testing methodology, traffic, throughput

For citation: A.M. Sadykov, R.R. Yamaletdinov. Methodology of load testing of firewalling tools. Herald of Daghestan State Technical University. Technical Sciences. 2025; 52(2): 150-158. (In Russ) DOI:10.21822/2073-6185-2025-52-2-150-158

Введение. Межсетевой экран (МЭ) играет ключевую роль в обеспечении информационной безопасности, выступая в качестве программного или программно-технического средства контроля и фильтрации информационных потоков согласно заданным правилам. Он предназначен для защиты данных некриптографическими методами, в том числе информации ограниченного доступа.

Установка МЭ на границе информационной системы или между ее сегментами позволяет эффективно фильтровать трафик, снижая риски утечек и несанкционированного проникновения как извне, так и внутри локальной сети.

Постановка задачи. Целью исследования является разработка новой методики тестирования отечественных межсетевых экранов, описание ее ключевых особенностей и основных этапов работы, а также обоснование ее необходимости.

Эффективность функционирования межсетевого экрана непосредственно влияет на общий уровень защищённости информационной инфраструктуры. Правильно подобранное и протестированное решение обеспечивает оперативную реакцию на угрозы, оптимальные показатели пропускной способности и совместимость с остальными средствами защиты.

Нагрузочное тестирование выступает критически важным этапом оценки, так как без объективных измерений производительности и устойчивости существует риск выбора неподходящего решения, в результате чего повышается вероятность успешной реализации атак. В рамках таких проверок выявляют реальные возможности МЭ по фильтрации и переработке трафика при высокой нагрузке, оценивают соответствие заявленным характеристикам и проверяют способность устройства сохранять эффективность при изменяющихся условиях эксплуатации.

Так, например, для комплексных решений класса NGFW (Next-Generation Firewall), в которых одновременно функционируют файрвол, система предотвращения вторжений (IPS) и механизм глубокой инспекции пакетов (DPI), производительность анализируется для каждого из компонентов отдельно, что помогает детально оценить потенциал системы в целом.

Современные инструменты, такие как CiscoTRex, позволяют эмулировать реальные сценарии и задавать различные профили трафика, обеспечивая точную оценку производительности [1]. При этом учитываются такие параметры, как предельная пропускная способность, число новых и одновременных соединений, а также поведение системы при увеличении объёмов трафика [2, 3].

Оценка межсетевых экранов может включать различные аспекты и методики. Стандартизированные подходы дают возможность унифицировать результаты тестирования и сопоставлять их с решениями конкурентов. Регулярная проверка МЭ позволяет не только подтвердить соответствие заявленным характеристикам, но и своевременно выявить уязвимости, оценить их критичность посредством рекомендаций стандарта CommonVulnerabilityScoringSystem (CVSS), а также определить удобство и надёжность использования. Таким образом, комплексное тестирование межсетевых экранов выступает в качестве обязательного этапа при выборе и внедрении средств защиты в корпоративную среду.

Исследованию МЭ и их тестированию, в том числе с использованием различных методик посвящен ряд работ [5-12]. Тестирование пропускной способности и устойчивости подразумевает нагружение МЭ трафиком различной интенсивности и структуры, измерение задержек, потерь пакетов, времени реакции на изменения нагрузки. Подход описан в современных методиках от ГК «Солар» [2], а также в рекомендациях от ведущих вендоров, регулярно обновляемых в 2023–2024 гг.[4].

Согласно Указа Президента РФ от 1 мая 2022 г. N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации зарубежного производства [5]. Исходя из этого, в сфере информационной безопасности осуществляется переход на отечественные продукты, поэтому возникает необходимость анализа предлагаемых отечественным рынком средств межсетевого экранирования для использования в защищенных автоматизированных системах.

Компания «АйСиЭлСТ» реализует комплексные проекты в области системной интеграции и информационной безопасности, в том числе построение систем защиты информации объектов критической информационной инфраструктуры. При этом информация о МЭ, доступная непосредственно от производителя, чаще всего представляет собой рекламу, преувеличивающую достоинства и скрывающую недостатки. Для осознанного выбора желательно получить четкое и достоверное описание качественных характеристик продукта, его надежности и уязвимых мест [6]. Одним из этапов такого исследования является нагрузочное тестирование.

Методы исследования. В настоящее время большинство методик тестирования МЭ созданы для зарубежных решений и не учитывают специфику отечественных решений. Это приводит к тому, что оценка их эффективности и безопасности может быть неполной или некорректной.

В связи с этим возникает необходимость в разработке и внедрении в практику специализированной методики, адаптированной под особенности отечественных МЭ с целью тестирования ряда продуктов и проверки их на соответствие заявленным производителями характеристикам.

Для проведения нагрузочного тестирования средств межсетевого экранирования была разработана методика проведения испытаний. Так как, число правил безопасности на межсетевом экране прямо влияют на его производительность, а при эксплуатации firefall политики выстраиваются гибким образом, в методике рассматривается производительность при отработке лишь 1-2 правил - как эталон производительности.

Цель данной методики - вычислить фактическую производительность средства межсетевого экранирования путем генерации нагрузки и эмулирования потока трафика на него. Этапы тестирования, согласно методике, описаны далее.

При проведении тестирования используется ПО «Генератор траффика CiscoTRex», являющееся программным генератором трафика с открытым исходным кодом. Он позволяет воспроизводить разные типы трафика и анализировать данные при их получении [2].

Для тестирования продукта его необходимо соединить с сервером TRex согласно схеме, представленной на рис. 1.

На рис. 1 видно, что TRex выступает в роли как клиента, так и сервера, тем самым эмулируя прохождение трафика через межсетевой экран в другой сегмент сети.

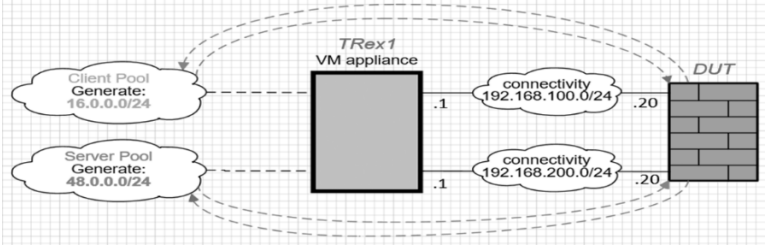

Рис. 1 - Схема подключения оборудования на стенде
Fig. 1 - Wiring diagram of the equipment on the stand

Это подтверждает схема, представленная на рис.2.

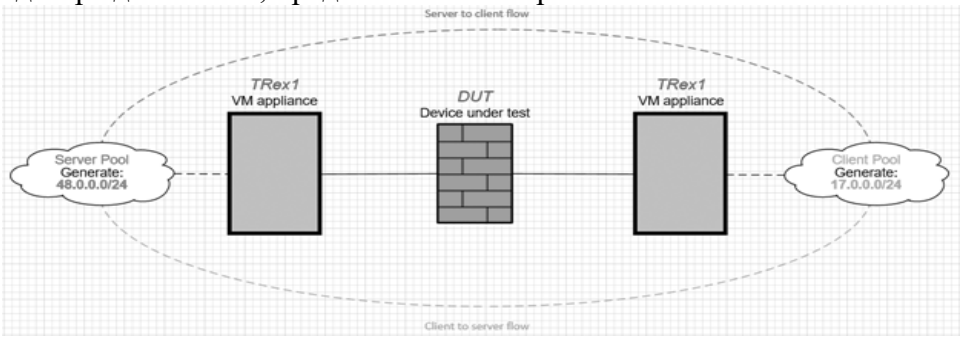

Рис. 2 - Схема потоков трафика в стенде
Fig. 2 - Schematic of traffic flows in the booth

Начальная установка - на тестируемом устройстве необходимо настроить сетевую связность для прохождения пакетов, генерируемых устройством с ПО TRex.

Учитывая архитектурные особенности межсетевого экрана, в разделе политик безопасности необходимо создать первую по списку политику, разрешающую весь сетевой трафик «permitanyany». Также включить логирование трафика для отслеживания правильности обработки и возможности своевременного реагирования на инциденты.

На генераторе трафика TRex необходимо создать шаблоны из существующих в базовой инсталляции «.pcap» файлов. Параметры шаблонов представлены в табл. 1 и 2.

Таблица 1. Шаблон №1 «template_test_1.py»
Table 1. Template #1«template_test_1.py»

Наименование файла .pcap File name	**Описание содержимого трафика Description of traffic content**	**Количество подключений в секунду Number of connections per second**
dns_0.pcap	протокол dns, payload 77/93 байт – запрос/ответ	50
delay_10_http_browsing_0.pcap	протокол http, payload 1518 байт	100

Таблица2. Шаблон №2 «template_test_2.py»
Table 2. Template #2 «template_test_2.py»

Наименование файла .pcap File name	**Описание содержимого трафика Description of traffic content**	**Количество подключений в секунду Number of connections per second**
delay_10_smtp_0.pcap	протокол SMTP, payload 64-1518байт	20
delay_10_citrix_0.pcap	протокол TCP в который вложен трафик приложения, payload 64-1517 байт	30

Процентное соотношение типов трафика в шаблонах, число подключений в секунду для каждого типа трафика — «.pcap» файла, выбирается исходя из представления о содержимом трафика в сети индивидуально. Это соотношение в идеальных условиях измерений подбирается максимально приближенными к реальным по числу TCP и UDP соединений и размеру пакетов. После создания шаблонов запустить генерацию трафика на TRex с использованием шаблона template_test_1.py для проверки работоспособности стенда. Проверить полученные значения, свидетельствующие о корректном беспрепятственном прохождении трафика на основе статистики TRex и соответствующих логах прохождения трафика на межсетевом экране.

1 этап — Измерение пропускной способности сетевого трафика. Целью этапа является определение сетевой пропускной способности и сравнение ее с заявленными характеристиками производителя. Для этого необходимо провести последовательные замеры значений с помощью генерации трафика, подготовленного шаблонами, зафиксировать результаты и найти максимальное значение пропускной способности.

Для измерения пропускной способности трафика в режиме, когда межсетевой экран работает как маршрутизатор — устройство 3 уровня модели OSI, с единственной политикой, разрешающей любой трафик, необходимо убедиться в соответствующих настройках.

Для измерения можно использовать как все подготовленные шаблоны — производить замеры, как и по одному шаблону с фиксацией результатов, затем по следующему, и так далее, так и частью шаблонов, либо один из них, например, template_test_1.py.

Шаг 1. Опираясь на заявленные характеристики производителя, выбрать некоторое начальное количество трафика. Например, при условии, что тестируется межсетевой экран с интерфейсом, поддерживающим максимальную скорость 1 Гбит/сек, и заявленной производителем пропускной способностью в 900 Мбит/сек в режиме Firewall – выбрать 800 Мбит/сек, для последующей масштабируемости нагрузки стендирования. Приравнять начальное значение b—bandwidth— «Пропускная способность» 800 Мбит/сек.

Шаг 2. Ориентируясь на b подготовить шаблон таким образом, чтобы суммарный объем трафика составил значение приблизительно равное b. Достигается это изменением в шаблоне значения мультипликатора cps — connectionspersecond — «Соединения в секунду» для каждого типа трафика (рис.3).

```
return ASTFProfile(default_ip_gen=ip_gen,
                   cap_list=[
                             ASTFCapInfo(file="/opt/trex/v3.00/avl/dns_0.pcap", cps=1000.0),
                             ASTFCapInfo(file="/opt/trex/v3.00/avl/delay_10_http_browsing_0.pcap", cps=2000.0)
                            ])
```

Рис. 3 - Значение мультипликатора cps для dns_0.pcap
Fig. 3 - Value of cps multiplier for dns_0.pcap

Шаг 3. Произвести первый замер с подготовленным шаблоном, после чего записать результаты статистики с TRex в табличном виде. Далее повторить шаги с 1 по 3, увеличивая b при каждой итерации на 5% в соответствии с формулой 1.

$$bn = 1{,}05 \times b(n-1), \quad (1)$$

где bn– значение пропускной способности при n-ом замере, Мбит/сек;$bn-1$— значение пропускной способности при (n-1)-ом замере, Мбит/сек.

Замеры повторять до тех пор, пока не будут зафиксированы потери, превышающие 2% пакетов в статистике, выдаваемой TRex. После нахождения значения bn выполнить ряд замеров с шагом 1% в сторону уменьшения в соответствии с формулой 2.

$$bcn = 0{,}99 \times bc(n-1), \quad (2)$$

где bcn— значение пропускной способности при n-ом замере, Мбит/сек;$bcn-1$— значение пропускной способности при (n-1)-ом замере, Мбит/сек.

Замеры повторять до тех пор, пока в статистике TRex потери пакетов не опустятся ниже уровня в 2%. Таким образом будет найдено максимальное значение пропускной способности, при котором на интересуемом нас профиле трафика межсетевой экран выдает максимальные значения производительности —$bmax$ в качестве устройства 3 уровня модели OSI без проверок, инспекций и политик безопасности.

2 этап — Измерение производительности в режиме Firewall. Целью этапа является определение производительности межсетевого экрана при настроенной политике «denyanyany» и сравнение с заявленными характеристиками производителя. Для этого необходимо провести последовательные замеры значений с помощью генерации трафика подготовленными шаблонами и зафиксировать результат, найти максимальное значение трафика, при котором межсетевой экран продолжит корректно отрабатывать — блокировать весь генерируемый трафик, логируя и оставаясь доступным для управления.

Для измерения производительности межсетевого экрана в режиме блокировки всего трафика необходимо настроить запрещающую весь сетевой трафик политику «denyanyany» и либо сделать ее единственной в списке политик, либо переместить вверх.

Шаг 1. В качестве первого замера использовать значения для шаблонов, которые были использованы при последнем замере из предыдущего этапа — значения cps выставленные в шаблонах при нахождении $bmax$.

Если на данном шаге весь трафик был корректно заблокирован межсетевым экраном, лог об этом был соответствующим образом сгенерирован и межсетевой экран не потерял управление — оставался доступным для управления во время проведения замера, то дальнейшие шаги не выполняются, так как найдено искомое значение. При этом значение f равняется максимальной пропускной способности межсетевого экрана и является искомым значением $fmax$— максимальная производительность firewall в режиме блокировки всего трафика.

Шаг 2. Если на предыдущем шаге рассматриваемые показатели не были достигнуты - доступность для управления, корректное логирование, блокирование всего проходящего через межсетевой экран трафика, перейти к следующему измерению уменьшая значение f на 10% пропорционально уменьшая cps для pcap в используемом шаблоне в соответствии с формулой 3.

$$fn = 0{,}9 \times f(n-1), \quad (3)$$

где fn– значение производительности firewall в режиме блокировки всего трафика при n-ом замере, Гбит/сек;$f(n-1)$– значение производительности firewall в режиме блокировки всего трафика при (n-1)-ом замере, Гбит/сек.

Замеры повторять до тех пор, пока не будут зафиксированы отслеживаемые показатели: доступность для управления, корректное логирование, блокирование всего проходящего через межсетевой экран трафика. Как только будет найдено значение fn при котором все показатели стабильны, приступить к замерам в сторону увеличения на 1% в соответствии с формулой 4.

$$fcn = 1{,}01 \times fc(n-1), \quad (4)$$

где fcn– значение производительности firewall в режиме блокировки всего трафика при n-ом замере, Мбит/сек;$fc(n-1)$– значение производительности firewall в режиме блокировки всего трафика при (n-1)-ом замере, Мбит/сек.

Таким образом будет найдено максимальное значение трафика, при котором межсетевой экран способен его корректно блокировать. Замеры повторять до тех пор, пока отслеживаемые показатели не начнут деградировать. Последний замер, при котором показатели были корректны и будет искомым значением $fmax$, являющимся максимальной производительностью межсетевого экрана в режиме блокирования всего трафика.

3 этап — Измерение производительности Firewall с использованием «Application Control». Целью этапа является определение производительности межсетевого экрана при настроенных политиках блокировки приложений «denyapplication (smtp, citrix)» и сравнение с заявленными характеристиками производителя. Для этого необходимо провести последовательные замеры значений с помощью генерации трафика подготовленными шаблонами, зафиксировать результаты, найти максимальное значения трафика, при котором межсетевой экран продолжит корректно отрабатывать – блокировать весь генерируемый трафик приложений, логируя, оставаясь доступным для управления.

Во время тестирования будет осуществляться блокировка трафика приложений smtp и citrix. При этом трафик приложения smtp – SimpleMail Transfer Protocol – является стандартизированным протоколом и имеет свой номер и может быть идентифицирован по флагам в заголовках пакета. Трафик приложения citrix должен распознаваться по сигнатурам на основе payload, так как не имеет своих идентификаторов в заголовках сетевых пакетов. Для измерения производительности межсетевого экрана в режиме Firewall с использованием «Application Control» необходимо настроить запрещающую политику «denysmtp, citrix» и либо сделать ее единственной в списке политик, либо переместить вверх. После нее необходимо добавить разрешающую политику «permitanyany» — в случае если тестируемое устройство не распознает трафик приложений, он будет пропущен.

Шаг 1. В качестве первого замера выбрать значение, соответствующее $fmax$с его параметрами шаблона. Произвести замер, записать полученные результаты в табличном виде.

Если на данном шаге весь трафик был корректно заблокирован межсетевым экраном, лог об этом был соответствующим образом сгенерирован и межсетевой экран не потерял управление - оставался доступным для управления во время проведения замера, то дальнейшие шаги не выполняются, так как найдено искомое значение. При этом значение App – «firewallwithappcontrol» равняется максимальной пропускной способностью межсетевого экрана в режиме блокирования по трафику приложений и является искомым значением $Appmax$— максимальной производительностью firewall с использованием «Application Control».

Шаг 2. В случае если на предыдущем шаге рассматриваемые показатели не были достигнуты — доступность для управления, корректное логирование, блокирование всего трафика приложений, проходящего через межсетевой экран, перейти к следующему измерению уменьшая значение App на 10% пропорционально уменьшая cps для pcap в используемом шаблоне в соответствии с формулой 5.

$$Appn = 0{,}9 \times App(n - 10, \quad (5)$$

где $Appn$ – значение производительности в режиме Firewall с использованием «ApplicationControl» при n-ом замере, Мбит/сек;$App(n-1)$– значение производительности в режиме Firewall с использованием «ApplicationControl» при (n-1)-ом замере, Мбит/сек.

Замеры повторять до тех пор, пока не будут зафиксированы отслеживаемые показатели. Как только будет найдено значение $Appn$ при котором все показатели стабильны, приступить к замерам в сторону увеличения на 1% в соответствии с формулой 6.

$$Appcn = 1{,}01 \times Appc(n-1), \quad (6)$$

где $Appcn$ – значение производительности в режиме Firewall с использованием «ApplicationControl» при n-ом замере, Мбит/ск; $Appc(n-1)$ – значение производительности в режиме Firewall с использованием «ApplicationControl» при (n-1)-ом замере, Мбит/с.

Замеры повторять до тех пор, пока отслеживаемые показатели не начнут деградировать. Последний замер, при котором показатели были корректны и будет искомым значением $Appmax$, являющимся максимальной производительностью межсетевого экрана в режиме Firewall когда блокирование трафика происходит на основе распознавания приложений.

Обсуждение результатов. В данной работе была предложена и рассмотрена методика нагрузочного тестирования средств межсетевого экранирования.

На основе проведенного анализа выявлено, что межсетевые экраны играют ключевую роль в обеспечении информационной безопасности, фильтруя и контролируя сетевые потоки данных. Однако эффективность их работы во многом зависит от соответствия заявленным характеристикам и способности справляться с реальными нагрузками, возникающими в процессе эксплуатации. Разработанная методика позволяет:

- определить пределы производительности межсетевого экрана;
- проверить корректность обработки различных типов трафика;
- выявить критические сценарии, в которых система может давать сбой;
- оценить соответствие заявленным характеристикам производителя.

Использование инструментов, таких как CiscoTRex, и разработка индивидуальных тестовых шаблонов позволяет воспроизвести реальную нагрузку, что особенно важно для анализа работы NGFW-решений.

С помощью данной методики будет проведено исследование средств межсетевого экранированиядля защищенных систем, представленных на российском рынке анализ, которых был проведен [13].

Вывод. Предложенная методика нагрузочного тестирования предназначена для проведения оценки соответствия заявленных производителем межсетевых экранов характеристик с полученными в ходе исследований и на основе данных результатов создавать наиболее подходящие решения по информационной безопасности для конкретных организаций.

Библиографический список:

1. TRexDocumentation [Электронный ресурс]. –Режим доступа: https://trex-tgn.cisco.com/trex/doc/ (дата обращения: 10.12.2024).
2. Тестирование межсетевых экранов [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/products/solar_ngfw/blog/3959/ (дата обращения: 10.12.2024)
3. Online инструменты для простейшего Pentest-а [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/tssolution/articles/323896/ (дата обращения: 10.12.2024).
4. Тестирование межсетевых экранов нового поколения: опыт с Solar NGFW [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/practice/methods/Solar-NGFW (дата обращения: 10.12.2024).
5. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 01.05.2022 № 250 (последняя редакция) [Электронный ресурс]. - URL: http://publication.pravo.gov.ru/Document/View/0001202205010023 (дата обращения: 21.03.2024).
6. Взгляд экспертов на российский рынок межсетевых экранов нового поколения (NGFW) [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/NGFW-market-overview-AMLive (дата обращения: 10.12.2024)
7. А.Г. Богораз, О.Ю. Пескова. Методика тестирования и оценки межсетевых экранов // Известия ЮФУ. Технические науки. 2013. № 12 (149). URL: https://cyberleninka.ru/article/n/metodika-testirovaniya-i-otsenki-mezhsetevyh-ekranov (дата обращения: 13.02.2025).
8. Е.А. Васильева, Н.В. Медведев. Методика тестирования межсетевых экранов / Безопасность информационных технологий. – 2008. – Т. 15, № 1. – С. 21-25.
9. А.С. Марков, В.Л. Цирлов, А.В. Барабанов Разработка методики испытаний межсетевых экранов по требованиям безопасности информации. // Вопросы защиты информации, 2011. № 3. С.19-24.
10. В.В. Галимский. Методика нагрузочного тестирования межсетевых экранов / В.В. Галимский, Ю.Е. Подгурский // Неделя науки СПбПУ: Материалы научного форума с международным участием. Институт прикладной математики и механики, Санкт-Петербург, 30 ноября – 05 2015 года / – Санкт-Петербург: Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого", 2015. – С. 174-176.
11. Д.А. Свечников. Методика тестирования межсетевых экранов по требованиям безопасности информации / Д.А. Свечников, Д.С. Царев // Информационные системы и технологии. – 2011. – № 3(65). – С. 136-140.
12. А.Г. Богораз. Методика тестирования межсетевых экранов / А.Г. Богораз // Информационное противодействие угрозам терроризма. – 2014. – № 22. – С. 89-92.
13. В.Ф. Ахмадиева. Разработка методики тестирования межсетевых экранов по требованиям безопасности информации, сравнительный анализ методик "Positive technology" и "Digital security" / В.Ф. Ахмадиева, В.Ф. Ахмадиева // Инновационное развитие современной науки: новые подходы и актуальные исследования : сборник материалов Международной научно-практической конференции, Москва, 30 ноября 2023 года. – Москва: Алеф, 2023. – С. 165-169. – doi: 10.26118/5957.2023.71.49.002.
14. А.М. Садыков, Р.Р. Ямалетдинов, Д.И. Сабирова. Российские средства межсетевого экранирования для защищенных систем // Вестник Дагестанского государственного технического университета. 2024. № 4 (51). С. 154-163. doi: 10.21822/2073-6185-2024-51-4-154-163

References:

1. Cisco. TRexOfficia lDocumentation. Access: https://trex-tgn.cisco.com/ (reference date: 10.12.2024). (In Russ.).
2. GK «Solar». Metodika testirovanija Solar NGFW. URL: https://rt-solar.ru/products/solar_ngfw/blog/3959/ (reference date: 10.12.2024) (In Russ.).
3. Habr. Testirovanie proizvoditel'nosti sistem IB. URL: https://habr.com/ru/companies/tssolution/articles/323896/ (reference date: 10.12.2024). (In Russ.).
4. Anti-Malware.ru. Metodiki testirovanija mezhsetevyh jekranov. URL: https://www.anti-malware.ru/practice/methods/Solar-NGFW (reference date: 10.12.2024). (In Russ.).
5. On additional measures to ensure information security of the Russian Federation: Decree of the President of the Russian Federation dated 05/01/2022 No. 250 (latest edition) [Electronic resource]. URL: http://publication.pravo.gov.ru/Document/View/0001202205010023 (reference date: 10.12.2024). (In Russ).
6. Vzgljad expertov na rossijskij rynok megsetevyh ekranov novogo pokoleneja (NGFW) URL: https://www.anti-malware.ru/analytics/Market_Analysis/NGFW-market-overview-AMLive (reference date: 10.12.2024). (In Russ.).
7. Bogoras A.G.,Peskova O.Yu. Methodology for testing and assessment of firewalls.*Izvestiya SFedU. Engineering Sciences.* 2013. №12 (149): 148-156.(In Russ.).
8. Vasileva E.A., Medvedev N.V. Methodology for testing of firewalls. IT Security. 2008. № 1(15): 21-25.(In Russ.).

9. Markov A.S., Tsirlov V.L., Barabanov A.V. Development of technique for firewalls security testing. *Information security questions*. 2011;3:19-24. (In Russ.).
10. Podgursky Yu.E. Firewall load testing methodology. Science week SPbPU. *Proceedings of the scientific forum with international participation. Institute of Applied Mathematics and Mechanics*. Saint Petersburg: Publishing House of Polytechnical University; 2015:174-176. (In Russ.).
11. Svechnikov D.A.,Tsarev D.S. Firewalls testing technique as information security requires. *Information systems and technologies.*2011;3(65):136-140. (In Russ.).
12. Bogoraz A.G.Testing methodology firewall. *Information counteraction to terrorism threats*. 2014;22:89-92. (In Russ.).
13. Ahmadiyeva V.FAkhmadieva V.F.Development of a methodology for testing inter-internetic displays on information security requirements, a comparative analysis of "POSITIVE TECHNOLOGY" and "DIGITAL SECURITY" methods.*Innovative development of modern science: new approaches and current research: collection of materials of the International scientific and practical conference*. Moscow: LLC "ALEF publishing house" 2023: 165-169. – doi: 10.26118/5957.2023.71.49.002. (In Russ.).
14. A.M. Sadykov, R.R. Yamaletdinov, D.I. Sabirova. Russian firewall screening tools for secured systems. *Herald of daghestan state technical university. technical sciences.* 2024;4(51):154-163. doi: 10.21822/2073-6185-2024-51-4-154-163. (In Russ.)

Сведения об авторах:

Александр Мунирович Садыков, кандидат технических наук, доцент, кафедра «Информационная безопасность», alex.sadykov@mail.ru. ORCID 0009-0005-8893-7846.

Роман Русланович Ямалетдинов, старший системный инженер; yamaletdinov.r2000@gmail.com.

Information about authors:

Alexander M. Sadykov, Cand. Sci. (Eng), Assoc. Prof., Department of Information Securityalex.sadykov@mail.ru, ORCID 0009-0005-8893-7846.

Roman R. Yamaletdinov, Senior Systems Engineer, yamaletdinov.r2000@gmail.com.

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 06.03.2025.

Одобрена после рецензирования / Reviced 26.04.2025.

Принята в печать /Accepted for publication 17.05.2025.