ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.492.4

DOI: 10.21822/2073-6185-2024-51-4-154-163 Обзорная статья/ Review article

Российские средства межсетевого экранирования для защищенных систем

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

Резюме. Цель. Цель работы заключается в сравнительном анализе российского рынка средств межсетевого экранирования для защищенных систем. Резкое увеличение спроса на продукцию отечественных производителей связано с необходимостью отказа от использования зарубежной продукции в сфере информационной безопасности и перехода на средства защиты информации, произведенные в России. **Метод.** В качестве методов исследования используются: систематизация, описание и анализ. В работе анализ функционала будет проведен в отношении следующих решений: изделие «Универсальный шлюз безопасности «UserGate», комплекс безопасности «Континент 4», программно-аппаратный комплекс «ViPNet xFirewall 5», программный комплекс «Межсетевой экран с системой обнаружения вторжений Ideco UTM». **Результат.** В качестве параметров для сравнения средств межсетевого экранирования были выбраны: функциональность межсетевых экранов как сетевого оборудования, как средства защиты, возможности кластеризации, соответствие требованиям ФСТЭК. Проведенный анализ средств межсетевого экранирования показал, что российский рынок предлагает пользователям достойные аналоги зарубежных продуктов. Однако у рассматриваемых решений отсутствуют некоторые функциональные возможности, что, в свою очередь, указывает на недостаточную зрелость отечественного рынка межсетевых экранов. **Вывод.** Принятие решения о выборе должно быть продиктовано требованиями конкретной организации, исходя из запросов потребителя на функциональность или стабильность работы файрвола.

Ключевые слова: информационная безопасность, средства защиты информации, межсетевой экран, файрвол, импортозамещение, ФСТЭК

Для цитирования: А.М. Садыков, Р.Р. Ямалетдинов, Д.И. Сабирова. Российские средства межсетевого экранирования для защищенных систем. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(4):154-163. DOI:10.21822/2073-6185-2024-51-4-154-163

Russian firewall screening tools for secured systems

A.M. Sadykov [1], R.R. Yamaletdinov [2], D.I. Sabirova[1]
[1]Kazan National Research Technological University,
[1]68 Karl Marks St., Kazan 420015, Russia,
[2]LLC «Iciel System Technologies»,
[2]34 Sibirsky Trakt St. build. 1, Kazan 420029, Russia

Abstract. Objective. The purpose of the work is to make the comparative analysis of the firewall tools for secure systems on the Russian market. The sharp increase in demand for products from domestic developers is associated with the need to abandon the use of foreign information security tools and transition to Russian analogues. **Method**. Systematization, description and analysis are used as research methods. In this work functional analysis will be carried out in relation to the following solutions: «Universal security gateway «UserGate», security complex «Continent 4», hardware and software complex «ViPNet xFirewall 5», «Firewall with Ideco

UTM intrusion detection system». **Result.** For comparison of firewall tools the following parameters were chosen: functionality of firewalls as network equipment, as means of protection, possibility of clustering, compliance with FSTEC requirements. The analysis of firewall tools showed that the Russian market offers to users worthy analogues of foreign products. However in this solutions some functionality is missing, which indicates the insufficient maturity of the domestic market of firewalls. **Conclusion.** The choice decision should be dictated by the requirements of a particular organization, based on consumer requests for the functionality or stability of the firewall.

Keywords: information security, information security tools, firewall, import substitution, FSTEC

For citation: 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; 51(4):154-163. DOI:10.21822/2073-6185-2024-51-4-154-163.

Введение. Защита сетевого периметра - одна из самых актуальных задач по обеспечению информационной безопасности любой компании, у которой есть доступные из интернета ресурсы. В соответствии со статистикой ГК «Солар», построенной на основании информации об инцидентах в ИБ, выявленных Solar JSOC, в 1-м квартале 2023 года число кибератак увеличилось на 43 %, при этом доля сетевых атак выросла с 7 % до 8 % [1].

1 мая 2022 года был издан Указ Президента Российской Федерации № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», который устанавливает, что «с 1 января 2025 года субъектам критической информационной инфраструктуры Российской Федерации запрещается использовать иностранное программное обеспечение, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними» [2].

Данный нормативно-правовой акт указывает на необходимость отказа от использования зарубежной продукции в сфере информационной безопасности и перехода на отечественные средства защиты информации. Это требование привело к резкому увеличению спроса на продукцию отечественных производителей, в частности на средства межсетевого экранирования. Отечественные разработчики были вынуждены в срочном порядке и в очень краткий срок начать разработку собственных продуктов, имеющих функционал и производительность максимально приближенные к лучшим иностранным аналогам.

Таким образом, в связи с бурным развитием российского рынка средств межсетевого экранирования, и активным ростом целенаправленных киберугроз, вопросы импортозамещения и обеспечения сетевой безопасности информационных систем приобретают особую важность.

Постановка задачи. На основе требований регулятора в области технической защиты информации и определенных наиболее важных критериев провести анализ предлагаемых отечественным рынком средств межсетевого экранирования для использования в защищенных автоматизированных системах.

Согласно Требованиям к межсетевым экранам, утвержденные приказом ФСТЭК России от 9 февраля 2016 г. N 9, межсетевой экран (МЭ) представляет собой «программное или программно-техническое средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через них информационных потоков и используемым в целях обеспечения защиты некриптографическими методами, информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа» [3].

Методы исследования. Как правило МЭ устанавливают на границе информационной системы или между границами сегментов. Такая практика полезна тем, что проходящий поток данных фильтруется, и обрабатывается не только при пересечении внешнего периметра, но и при хождении в локальной вычислительной сети.

В соответствии с отчетом «Magic Quadrant for Network Firewalls» 2022 года выделяются следующие лидеры на иностранном рынке: Palo Alto Networks, Fortinet, Check Point Software technologies [4]. Они обладают максимальными функциональными возможностями и производительностью, что позволяет использовать их в крупном и малом бизнесе. Изучив данные решения, можно выделить наиболее важные критерии выбора средства межсетевого экранирования:

- функциональность как сетевого устройства – средство межсетевого экранирования встраивается в сетевую инфраструктуру, следовательно, оно должно иметь возможность размещения в роли роутера, коммутатора или моста;

- функциональность как средства защиты информации – МЭ должен обеспечивать защиту на высоком уровне от атак, вирусов и других уязвимостей, передаваемых сетевым путем;

- возможность кластеризации –важнейшая функция сетевого оборудования, обеспечивающее инфраструктуре практически мгновенное автоматическое реагирование на отказ элемента системы.

Можно выделить следующие параметры функциональности на уровне сетевого оборудования:

- маршрутизация. Как правило, средство межсетевого экранирования устанавливают между сегментами инфраструктуры, будь то логическая или физическая граница, сети на разных портах устройства фигурируют различные, следовательно, файрвол должен уметь направлять трафик в правильную сеть, руководствуясь маршрутами;

- NAT (Network Address Translation). Сетевой функционал NAT был создан для группировки ip-адресов в один в пользу экономии сетевого пространства. Но данное свойство – скрывать внутренние ip-адреса за внешним, служит и для обеспечения безопасности устройств. Тем самым, злоумышленник, находящийся во внешней сети и зная внешний адрес компании, не знает внутренних адресов ресурсов организации [5];

- поддержка распространенных протоколов динамической маршрутизации. Важность данной функции обусловлена тем, что крупные компании выстраивают маршруты внутри своей сети с помощью протоколов динамической маршрутизации, следовательно, устройство фильтрации трафика, тоже должно уметь передавать свои маршруты. Помимо этого, существуют продукты, для правильной работы которых, необходимо пользоваться динамическим протоколом маршрутизации, например, КриптоПро NGate, в котором осуществляется балансировка VPN сессий с помощью протокола OSPF;

- агрегация. Как правило, средство межсетевого экранирования имеет небольшое количество физических сетевых портов. Для корректного разделения сетевой инфраструктуры на сегменты, на портах создают виртуальные интерфейсы – bond, превращая один физический порт в несколько логических. Так же, бонд позволяет совмещать логически несколько физических портов, обеспечивая большую пропускную способность и дополнительную отказоустойчивость продукта;

- контроль пропускной способности. Немаловажной функцией является контроль пропускной способности зон. Это помогает правильно регулировать сетевой ресурс, избегая его переполнения и нарушения доступности информации;

- производительность. Любая вычислительная система имеет свой предел нагрузки. В сетевом оборудовании важно, чтобы производительность была достаточной для работы оборудования во время пиковой загруженности, иначе устройство может отказать. К производительности можно отнести максимальную скорость физических портов, объем дискового пространства и оперативной памяти, а также вычислительную мощность процес-

сора. Можно выделить следующие параметры функционала средства межсетевого экранирования как средства защиты информации:

- фильтрация на основе отслеживания состояния соединений – позволяет отслеживать не отдельные передающиеся пакеты, а полноценное устанавливаемое соединение;
- VPN (Virtual Private Network) позволяет объединить локальные вычислительные сети, их сегменты или отдельные компьютеры предприятия в единую защищенную виртуальную сеть на базе общедоступных каналов передачи данных;
- IPS (Intrusion Prevention System). «Система предотвращения вторжений» позволяет выявлять и блокировать соединения по которому передаются эксплойты, и прочие уязвимости. IPS должен уметь определять вторжения на базе: сигнатур уязвимостей, статических аномалий, анализа протоколов и созданных вручную сигнатур.

Средство межсетевого экранирования должно иметь возможность периодического обновления сигнатур уязвимостей, управления политиками IPS, сбора дампа трафика при срабатывании политики IPS, категорирования действий IPS по разным профилям;

- защита от DoS – возможность защиты веб-серверов, конечных точек и самого средства межсетевого экранирования от распределенных атак типа «отказ в обслуживании»;
- контроль приложений – МЭ должен уметь классифицировать и контролировать не просто соединения, а соединения, направленные в сторону определенного приложения, например, «YouTube»;
- антивирус – наличие встроенного антивируса, для потоковой проверки передаваемых файлов и скриптов до их попадания конечному пользователю;
- веб-фильтрация – возможность фильтрации не только по ip-адресам, но и по веб-адресам сайтов;
- email фильтрация – позволяет МЭ анализировать электронную почту, проходящую через него, перенаправлять ее, отправлять содержимое для проверки на угрозы, а также фильтровать в зависимости от сконфигурированных параметров. Дает возможность настройки защиты сервисов электронной почты от спама, путем анализа содержимого писем и их источников;
- эмуляция подозрительных файлов – возможность безопасного запуска подозрительных файлов, на встроенной виртуальной системе, или в облаке для наблюдения за последствиями запуска файла;
- https инспекция – функционал позволяет фильтровать зашифрованные сетевые пакеты, путем проведения атаки «man-on-the-middle», когда сертификаты клиента и сервера подменяются на сертификаты МЭ. Данный функционал ограничен некоторым объемом расшифрованных данных пакета. Но с помощью функции глубокого анализа «DPI» - deep packet inspection, МЭ способен расшифровывать весь пакет, во вред производительности;
- user-based политики – должна иметься возможность построения политик доступа на основе пользователей, зарегистрированных в системе с помощью LDAP или гостевого портала;
- возможность создания правил с учетом даты и времени – возможность интегрировать в правила дату и время для более гибкой настройки политики безопасности;
- интеграция с серверами LDAP – наличие возможности синхронизации учетных записей с сервера LDAP, для централизованного управления доступом на основе прав пользователя;
- гостевой портал – наличие возможности настройки доступа для внедоменных пользователей, или гостей, не состоящих в группах LDAP;
- DNS Proxy – функционал позволяет перехватывать DNS запросы пользователей и изменять или перенаправлять их в зависимости от заданных администратором правил;
- централизованное управление – централизованное управление позволяет редактировать политики безопасности на множестве подчиненных устройствах межсетевого

экранирования с одного сервера, это минимизирует человеческий фактор при редактировании политик для группы машин. Так же, централизованное управление, позволяет установить уже созданную политику на новый брандмауэр, установленный в рамках расширения или замены предыдущего;

- передача на выделенный log сервер – наличие возможности передачи журналов действия на выделенный сервер журналирования, для экономии пространства на устройстве, и централизованного доступа к логам систем;

- различные роли доступа администраторов – МЭ должен обладать возможностью создания внутренних учетных записей с доступом только для чтения, или с доступом к ограниченному функционалу устройства;

- мультифакторная аутентификация – должна быть возможность интеграции с сервисами мультифакторной аутентификации для реализации многослойной, а значит более эффективной защиты аккаунта от несанкционированного доступа;

- логирование действий администратора – должна быть встроена система журналирования изменений устройства, для расследования инцидентов, связанных с ним;

- возможность передачи журналов в SIEM (Security information and event management) – наличие возможности автоматической передачи журналов в SIEM систему, для оперативного реагирования на инциденты, а также поиска и устранения уязвимостей;

- оповещения администраторов об инцидентах – возможность оповещения администраторов системы об изменениях, смене статуса оборудования и прочего;

- управление точками восстановления наличие возможности создавать точку восстановления МЭ, для возвращения к предыдущей конфигурации при неудачных обновлениях и прочих изменениях конфигурации.

Можно выделить следующие параметры функциональности по кластеризации:

- поддержка кластера отказоустойчивости. High-availability кластер – кластер отказоустойчивости, зачастую подразумевающий одновременно один активный узел. Другие элементы кластера находятся в режиме ожидания, пока активная нода не проявит признаки отказа. В момент аварии обрабатываемые данные передаются по выделенному каналу синхронизации на пассивный член кластера, и он переключается в активный, перехватывая всю работу на себя;

- кластер балансировки нагрузки. Load balancing кластер – кластер, в котором каждый элемент находится в активном состоянии и обрабатывает информацию. Входящий трафик равномерно распределяется между узлами кластера, обеспечивая увеличение максимально возможной нагрузки на оборудование.

Российский рынок средств межсетевого экранирования только в начале своего развития и в настоящее время представлен пока не очень большим количеством продуктов. Однако, крупные производители в области информационной безопасности анонсируют, что активно ведут разработку МЭ нового поколения. Вследствие чего ближайшее время количество предложений на рынке увеличится и их качество улучшится из-за выросшей конкуренции.

В работе анализ функционала будет проведен в отношении следующих отечественных решений:

1. Изделие «Универсальный шлюз безопасности «UserGate» [6].
2. Комплекс безопасности «Континент 4» [7].
3. Программно-аппаратный комплекс «ViPNet xFirewall 5» [8].
4. Программный комплекс «Межсетевой экран с системой обнаружения вторжений Ideco UTM» [9].

Сравнение средств межсетевого экранирования по параметрам, характеризующим функциональность межсетевых экранов как сетевого оборудования, как средства защиты и вариантам кластеризации [6-14] представлено в табл. 1.

Таблица 1. Сравнение средств межсетевого экранирования, представленных на российском рынке
Table 1. Comparison of the firewall tools available on the Russian market

Параметр/ Parameter	**Межсетевой экран/ Firewall**			
	Usergate	**Континент/ Continent 4**	**xFirewall 5**	**Ideco UTM 14**
Функциональность межсетевых экранов как сетевого оборудования/ Functionality of firewalls as network equipment				
Маршрутизация	Маршрутизация на уровне ОС Unix	Маршрутизация на уровне ОС Unix	Маршрутизация на уровне ОС Unix	Маршрутизация на уровне ОС Unix
NAT	Имеется NAT как DNAT и SNAT	Имеется NAT как DNAT и SNAT	Имеется NAT как DNAT и SNAT	Имеется NAT как DNAT и SNAT
Поддержка распространенных протоколов динамической маршрутизации	OSPF, BGP, RIP	OSPF, BGP	OSPF, RIP	OSPF, BGP, RIP
Агрегация	Имеется	Имеется	Имеется	Отсутствует
Контроль пропускной способности	Правила управления пропускной способностью позволяют ограничить канал для определенных пользователей, хостов, сервисов, приложений.	Имеется возможность создавать правила приоретизации и маркировки трафика, указывать полосы пропускания для каждого приоритета и трафика в целом	Имеется возможность создавать правила приоретизации и маркировки трафика, указывать полосы пропускания для каждого приоритета и трафика в целом	Имеется возможность балансировки трафика в Мбит/с между внешними интерфейсами
Производительность ак сетевое оборудование	До 10Гбит/с	До 10Гбит/с	До 10Гбит/с	До 10Гбит/с
Производительность с активным файерволом	До 60 Гбит/с	До 80 Гбит/с	До 19 Гбит/с	До 76,3
Производительность со всеми включенными функциями	до 8 Гбит/с	До 7 Гбит/с	До 669 Мбит/с	До 3,7 Гбит/с
Максимальное кол-во сессий	48000000	10 000 000	9900000	5 000 000
Функциональность межсетевых экранов как средства защиты информации/ Functionality of firewalls as a means of information protection				
Фильтрация на основе отслеживания состояния соединений	Имеется	Имеется	Имеется	Имеется
IPS на основе сигнатур	Имеется	Имеется	Имеется	Имеется
IPS на основе статических аномалий	Имеется	Имеется	Имеется	Отсутствует
IPS по анализу состояний протоколов	Отсутствует	Отсутствует	Отсутствует	Отсутствует
VPN	В сертифицированной версии отсутствует. В несертифицированной поддерживаются протоколы L2TP, IPSec с Cisco. Поддерживает два типа VPN-сетей: Remote Access VPN и Site-to-Site VPN	Собственный стек протоколов. Симметричное шифрование в соответствии с ГОСТ 28147-89 Поддерживает Site-to-Site VPN. Клиент-серверные решения имеются в виде отдельных продуктов: Континент TLS и Континент АП	Только для канала управления. Для остального трафика отсутствует функционал СКЗИ. VPN реализуется с помощью ViPNet. Coordinator	Поддерживаются протоколы PPTP, PPPoE, IKEv2/IPSec, SSTP, L2TP/IPSec Доступно VPN подключение на основе собственного клиента. Поддерживает два типа VPN-сетей: Remote Access VPN и Site-to-Site VPN. В сертифицированной версии VPN отсутствует.
Создание собственных сигнатур	Гибкая настройка правил обнаружения, есть возможность загрузить свои базы сигнатур и настроить их обновление	Имеется	Имеется	Отсутствует
Возможность категорировать действия IPS по разным профилям	Имеется	Отсутствует	Отсутствует	Отсутствует
Защита от DoS	Имеется	Имеется	Имеется	Имеется
Контроль веб-приложений	Для самых популярных соцсетей. Имеется возможность ограничивать отдельные действия в соцсетях	Для Facebook, LinkedIn, Instagram, Twitter	Для самых популярных соцсетей	Имеется возможность заблокировать доступ к ресурсам из нескольких десятков категорий, в т.ч., к социальным сетям.
Антивирус	Потоковый антивирус Usergate. Выявлением сигнатур занимаются эксперты Центра мониторинга и реагирования UserGate (MRC-UG).	Отсутствует	Антивирусная защита с помощью Антивируса Касперского для Proxy Server	Антивирус Касперского. В сертифицированной версии отсутствует
Веб-фильтрация	Блокировка посещения потенциально опасных ресурсов, а также, когда это необходимо, сайтов, не связанных с работой	Блокировка посещения потенциально опасных ресурсов и сайтов из списка. Механизм работает как прокси, и устанавливает	Блокировка посещения потенциально опасных ресурсов, а также, когда это необходимо, сайтов, не связанных с работой	Блокировка определенных приложений, а также блокировка с помощью контент-фильтра

		соединение с веб-ресурсом от своего имени.		
Email фильтрация	Поддерживается работа с протоколами POP3 и SMTP. Позволяет проверять почтовый трафик антиспамом Usergate, проверять SMTP-трафик с помощью технологии DNSBL.	Поддерживается работа с протоколами IMAP, POP3 и SMTP	Фильтрация почты производится Антивирусом Касперского для Proxy Server	Поддерживается работа с протоколами IMAP, POP3 и SMTP
Встроенная или облачная эмуляция подозрительных файлов	Отсутствует	Отсутствует	Отсутствует	Отсутствует
https инспекция	Можно настроить инспектирование https только для определенных категорий трафика	Имеется	Имеется	Имеется
User-based политики	Имеется	Имеется	Имеется только по отношению к пользователям с LDAP сервера	Имеется
Возможность создания правил с учетом даты и времени	Имеется	Имеется	Имеется	Имеется
Интеграция с серверами LDAP	Имеется	Имеется	Имеется	Имеется
Гостевой портал	Имеется	Отсутствует	Отсутствует	Имеется
DNS Proxy	Имеется	Имеется	Имеется	Имеется
Централизованное управление	Имеется	Имеется	Имеется	Имеется Отсутствует в сертифицированной версии
Передача на выделенный log сервер	Имеется	Имеется	Имеется	Имеется
Различные роли доступа администраторов	Возможность создания учетных записей администраторов с различными правами на просмотр и изменение разделов конфигурации.	4 встроенные роли, возможность создания пользовательских, назначения нескольких ролей одному администратору	2 встроенные роли - пользователь и Администратор. Наличие нескольких вариантов УЗ Администратора (администратор всей сети ViPNet, администратор группы узлов, локальный администратор узла)	Две встроенные роли: Администратор и ReadOnly
Логирование действий администратора	Имеется	Имеется	Имеется	Только журнал авторизации пользователей
Возможность передачи журналов в SIEM	Имеется SNMP	Имеется SNMP	Имеется SNMP	Имеется SNMP
Мультифакторная аутентификация	Штатными средствами можно использовать TOTP как второй фактор, есть возможность подключать технологических партнеров из открытой экосистемы UserGate (Multifactor или Аладдин)	Отсутствует	Отсутствует	Двухфакторная аутентификация через сервис SMS Aero. Отсутствует в сертифицированной версии
Оповещения администраторов об инцидентах	SMTP, отправка сообщений по электронной почте	SMTP, отправка сообщений по электронной почте. SMPP, отправка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки	Отсутствует	Оповещения через Telegram-bot
Управление точками восстановления	Только экспорт настроек	Экспорт политики безопасности	Экспорт справочников, лицензий и настроек	Создание встроенной резервной копии с возможностью выгрузки на FTP сервер
Варианты кластеризации/Clustering options				
Кластер отказоустойчивости	Объединение до 4 узлов	Имеется	Имеется, без синхронизации активных соединений	Имеется, без синхронизации активных соединений
Кластер балансировки нагрузки	Объединение до 4 узлов	Отсутствует	Отсутствует	Отсутствует

Как видно из табл. 1 некоторые функциональные возможности отсутствуют у рассматриваемых решений, что говорит о недостаточной зрелости отечественного рынка МЭ.

Требования к МЭ, утвержденные приказом ФСТЭК России от 9 февраля 2016 г. N 9, выделяют шесть классов защиты и их необходимость использования в информационных системах различных типов и классов, а также регламентируют 5 типов МЭ [3, 11]. Требования к МЭ для каждого типа и класса определены в соответствующих методиче-

ских документах, которые содержат профили защиты, утверждённых 12 сентября 2016 г. ФСТЭК России [11]. Спецификация профилей защиты представлена в табл. 2.

Таблица 2. Спецификация профилей защиты межсетевых экранов
Table 2. Specification of firewall protection profiles

Тип межсетевого экрана/ Firewall type	Класс защиты/ Protection class					
	6	5	4	3	2	1
«А»	ИТ.МЭ.А6.ПЗ	ИТ.МЭ.А5.ПЗ	ИТ.МЭ.А4.ПЗ	ИТ.МЭ.А3.ПЗ	ИТ.МЭ.А2.ПЗ	ИТ.МЭ.А1.ПЗ
«Б»	ИТ.МЭ. Б6.ПЗ	ИТ.МЭ. Б5.ПЗ	ИТ.МЭ. Б4.ПЗ	ИТ.МЭ. Б3.ПЗ	ИТ.МЭ. Б2.ПЗ	ИТ.МЭ. Б1.ПЗ
«В»	ИТ.МЭ.В6.ПЗ	ИТ.МЭ.В5.ПЗ	ИТ.МЭ.В4.ПЗ	ИТ.МЭ.В3.ПЗ	ИТ.МЭ.В2.ПЗ	ИТ.МЭ.В1.ПЗ
«Г»	ИТ.МЭ. Г6.ПЗ	ИТ.МЭ. Г5.ПЗ	ИТ.МЭ. Г4.ПЗ	-	-	-
«Д»	ИТ.МЭ.Д6.ПЗ	ИТ.МЭ.Д6.ПЗ	ИТ.МЭ.Д6.ПЗ	-	-	-

В табл. 3 содержится информация о наличии у рассматриваемых средств межсетевого экранирования сертификатов ФСТЭК России, отмечены сведения о соответствии требованиям российского законодательства [15, 16].

Таблица 3. Сведения о сертификации
Table 3. Certification Information

Наименование/ Title	Сертификат/ Certificate	Соответствие требованиям документов/ Compliance with document requirements
Изделие «Универсальный шлюз безопасности «UserGate»	Сертификат ФСТЭК России №3905, действует до 26.03.2026	Требования доверия (4), Требования к МЭ, Профиль защиты МЭ (ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ (ИТ.МЭ.Б4.ПЗ), Профиль защиты МЭ (ИТ.МЭ.Д4.ПЗ), Требования к СОВ, Профили защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ)
Комплекс безопасности «Континент». Версия 4.	Сертификат ФСТЭК России №4496, действует до 14.12.2026	Требования доверия (4), Требования к МЭ, Профиль защиты МЭ (ИТ.МЭ.А4.ПЗ), Требования к СОВ, Профили защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ)
Программно-аппаратный комплекс ViPNet xFirewall 5	Сертификат ФСТЭК России №4501, действует до 28.12.2026	Требования доверия (4), Требования к МЭ, Профиль защиты МЭ (ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ (ИТ.МЭ.Б4.ПЗ), Требования к СОВ, Профили защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ), ЗБ
Программный комплекс Межсетевой экран с системой обнаружения вторжений Ideco UTM	Сертификат ФСТЭК России №4503, действует до 28.12.2026	Требования доверия (4), Требования к МЭ, Профиль защиты МЭ (ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ (ИТ.МЭ.Б4.ПЗ), Требования к СОВ, Профили защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ)

Все рассматриваемые средства межсетевого экранирования можно использовать в государственных информационных системах I класса защищенности, в автоматизированных системах управления производственными и технологическими процессами I класса защищенности, в информационных системах персональных данных I уровня защищенности персональных данных, в информационных системах общего пользования II класса.

Обсуждение результатов. Результаты проведенного исследования показывают, что на сегодняшний день самым функциональным отечественным средством межсетевого экранирования является UserGate. Он обладает почти всем востребованным функционалом, и в настоящее время, является наиболее приближенным к решениям мирового уровня. К основным недостаткам данного продукта можно отнести нестабильность работы. Администратор может столкнуться с проблемами, начиная от полного выхода оборудования из строя, заканчивая периодическими простоями сетевой инфраструктуры [6, 10].

Решение «Континент 4» является продуктом ООО «Код Безопасности» – одного из главных производителей средств защиты информации на отечественном рынке. К достоинствам данного МЭ можно отнести покрытие большего требуемого функционала, а также достаточно стабильную работу, но фактическая производительность «Континента 4» является низкой [7, 11].

На основании проведенного сравнительного анализа самым стабильным из рассматриваемых вариантов можно считать VipNet xFirewall 5. Однако данное средство межсетевого экранирования, несмотря на свои преимущества, является самым нефункцио-

нальным и наименее производительным. Основным недостатком является невозможность его развертывания без покупки и лицензирования дополнительного средства криптографической защиты информации – VipNet Coordinator [8, 12].

Ideco UTM имеет простой и понятный веб-интерфейс управления, что сильно выделяет его среди конкурентов, однако обладает слабым функционалом: например, в нем плохо проработан CLI интерфейс командной строки, а сертифицированная версия совсем ограничена в возможностях. Тем не менее Ideco UTM показывает достаточно стабильную работу [9, 13].

Вывод. Проведенный сравнительных анализ средств межсетевого экранирования показал, что российский рынок предлагает пользователям достойные аналоги зарубежных продуктов. Однако у рассмотренных решений отсутствуют некоторые функциональные возможности, что говорит о недостаточной зрелости отечественного рынка МЭ. Принятие решения о выборе должно быть продиктовано требованиями конкретной организации, исходя из запросов потребителя на функциональность или стабильность работы файрвола. На основании проведенного исследования было выявлено, что наиболее функциональными средствами межсетевого экранирования можно считать UserGate и «Континент 4». Удовлетворить потребность пользователя в стабильной и бесперебойной работе с большей вероятностью удастся продукту VipNet xFirewall 5 и МЭ Ideco UTM.

Библиографический список:

1. Обзор рынка NGFW — 2023 // Анализ рынка информационной безопасности в России [Электронный ресурс]. - URL: https://www.anti-malware.ru/analytics/Market_Analysis/NGFW-2023 (дата обращения: 21.03.2024).
2. 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).
3. Информационное сообщение ФСТЭК «Об утверждении требований к межсетевым экранам» от 28 апреля 2016 г. N 240/24/1986 (последняя редакция) [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-28-aprelya-2016-g-n-240-24-1986 (дата обращения: 21.03.2024).
4. Recognized in 2022 Gartner Magic Quadrant for Network Firewalls for the 13th time [Электронный ресурс]. – URL: https://www.fortinet.com/solutions/gartner-network-firewalls (дата обращения: 21.03.2024).
5. От частного к общему: разбираемся в принципах работы Network Address Translation (NAT) [Электронный ресурс]. – URL: https://habr.com/ru/companies/otus/articles/779970/ (дата обращения: 21.03.2024).
6. Официальный сайт UserGate [Электронный ресурс]. URL: https://www.usergate.com/ru (дата обращения: 21.03.2024).
7. Официальный сайт код безопасности Континент 4 [Электронный ресурс]. – URL: https://www.securitycode.ru/products/kontinent-4/ (дата обращения: 21.03.2024).
8. Официальный сайт VipNet xFirewall 5 [Электронный ресурс]. – URL: //infotecs.ru/product/vipnet-xfirewall-5.html#docs (дата обращения: 21.03.2024).
9. Официальный сайт Ideco UTM [Электронный ресурс].URL: https://ideco.ru/ (дата обращения: 21.03.2024).
10. UserGate Руководство администратора [Электронный ресурс]. – URL: https://docs.usergate.com/dokumentaciya-120/ (дата обращения: 21.03.2024).
11. Код безопасности Континент 4 Руководство администратора [Электронный ресурс]. – URL: https://www.securitycode.ru/products/kontinent-4/?tab=support (дата обращения: 21.03.2024).
12. VipNet xFirewall 5 Руководство администратора [Электронный ресурс]. – URL: https://infotecs.ru/downloads/documents/vipnet-xfirewall-5/ (дата обращения: 21.03.2024);
13. Ideco UTM 14 Руководство администратора [Электронный ресурс]. – URL: https://docs.ideco.dev/v/v14 (дата обращения: 21.03.2024).
14. Православные NGFW [Электронный ресурс]. – URL: https://habr.com/ru/companies/icl_services/articles/701424/ (дата обращения: 21.03.2024).
15. Государственный реестр сертифицированных средств защиты информации [Электронный ресурс]. – URL: https://reestr.fstec.ru/reg3 (дата обращения: 21.03.2024).

16. Информационное сообщение ФСТЭК «Об утверждении методических документов, содержащих профили защиты межсетевых экранов» от 12 сентября 2016 г. N 240/24/4278 (последняя редакция) [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-12-sentyabrya-2016-g-n-240-24-4278 (дата обращения: 21.03.2024).

References:

1. NGFW market review - 2023 // Analysis of the information security market in Russia [Electronic resource]. URL: https://www.anti-malware.ru/analytics/Market_Analysis/NGFW-2023 (date of access: 03/21/2024). (In Russ).
2. 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(date of access: 03/21/2024). (In Russ).
3. Information message of FSTEC «On approval of requirements for firewalls» dated April 28, 2016 N 240/24/1986 (latest edition) [Electronic resource]. URL: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-28-aprelya-2016-g-n-240-24-1986 (date of access: 03/21/2024). (In Russ).
4. Recognized in 2022 Gartner Magic Quadrant for Network Firewalls for the 13th time [Electronic resource]. URL: https://www.fortinet.com/solutions/gartner-network-firewalls (date of access: 03/21/2024).
5. From specific to general: understanding the principles of Network Address Translation (NAT) [Electronic resource].URL: https://habr.com/ru/companies/otus/articles/779970/(date of access: 03/21/2024). (In Russ).
6. Official website of UserGate [Electronic resource]. URL: https://www.usergate.com/ru (date of access: 03/21/2024). (In Russ).
7. Official website security code Continent 4 [Electronic resource]. URL: https://www.securitycode.ru/products/kontinent-4/ (date of access: 03/21/2024). (In Russ).
8. Официальный сайт VipNet xFirewall 5 [Electronic resource]. URL: https: //infotecs.ru/product/vipnet-xfirewall-5.html#docs (date of access: 03/21/2024). (In Russ).
9. Ideco UTM official website[Electronic resource].URL:https://ideco.ru/(date of access: 03/21/2024).(In Russ).
10. UserGate Administrator's Guide [Electronic resource]. URL: https://docs.usergate.com/dokumentaciya-120/ (date of access: 03/21/2024). (In Russ).
11. Security code Continent 4 Administrator's Guide [Electronic resource]. URL: https://www.securitycode.ru/products/kontinent-4/?tab=support (date of access: 03/21/2024). (In Russ).
12. VipNet xFirewall 5 Administrator Guide [Electronic resource]. URL: https://infotecs.ru/downloads/documents/vipnet-xfirewall-5/ (date of access: 03/21/2024). (In Russ).
13. Ideco UTM 14 Administrator Guide [Electronic resource]. URL: https://docs.ideco.dev/v/v14 (date of access: 03/21/2024). (In Russ).
14. Orthodox NGFW [Electronic resource]. URL: https://habr.com/ru/companies/icl_services/articles/701424/ (date of access: 03/21/2024). (In Russ).
15. State Register of Certified Information Security Tools [Electronic resource]. URL: https://reestr.fstec.ru/reg3 (date of access: 03/21/2024). (In Russ).
16. Information message of FSTEC “On approval of methodological documents containing firewall protection profiles” dated September 12, 2016 N 240/24/4278 (latest edition) [Electronic resource]. URL: https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-12-sentyabrya-2016-g-n-240-24-4278 (date of access: 03/21/2024). (In Russ).

Сведения об авторах:

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

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

Сабирова Динара Илнуровна, кандидат химических наук, доцент кафедры «Информационная безопасность»; dinka-sab@mail.ru. ORCID 0009-0007-5066-5907

Information about authors:

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

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

Dinara I. Sabirova, Cand. Sci. (Eng), Assoc. Prof., dinka-sab@mail.ru, ORCID 0009-0007-5066-5907.

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/ Received 12.06.2024.

Одобрена после рецензирования/ Reviced 12.07.2024.

Принята в печать/ Accepted for publication 10.10.2024.