К. Р. Доценко, Н. В. Луценко, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.056.53

СРАВНИТЕЛЬНО-СОПОСТАВИТЕЛЬНЫЙ АНАЛИЗ ОТЕЧЕСТВЕННЫХ СРЕДСТВ СЕТЕВОЙ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ

Аннотация. В статье проведен сравнительный анализ отечественных межсетевых экранов и криптографических шлюзов от ведущих российских производителей и сформулированы функциональные требования к современным средствам защиты информации, обеспечивающим фильтрацию, маршрутизацию, шифрование и автоматизацию управления. На основе анализа предложена универсальная архитектура замещения оборудования Cisco отечественными аналогами с учетом масштабируемости, отказоустойчивости и нормативных требований.

Ключевые слова: межсетевые экраны, криптографический шлюз, импортозамещение, автоматизация, Cisco, S-Terra, UserGate.

Введение. В условиях технологической изоляции и отказа от зарубежных поставок средств информационной безопасности (ИБ), российским организациям необходимо перейти к построению полностью отечественной сетевой инфраструктуры. Сложность заключается не только в подборе технически эквивалентных решений, но и в сохранении архитектурных принципов отказоустойчивости, масштабируемости и управляемости. Анализ научных источников [1, 2, 3, 4] показывает, что, несмотря на активное обсуждение вопросов импортозамещения и сертификации отечественных средств защиты информации (СЗИ), исследования носят обзорный характер, не затрагивая практическую реализацию, сравнение функциональных особенностей или автоматизацию управления.

В частности, в статье М.Ф. Джангирова [5] подчеркивается, что вызовы, связанные с уходом иностранных поставщиков ИБ-решений, привели к ускоренному росту отечественных разработок в сфере защиты информации. Автор отмечает, что многие организации оказались не готовы к быстрому переходу на альтернативные платформы и испытывают затруднения в выборе подходящих СЗИ, соответствующих одновременно техническим и регуляторным требованиям. Это дополнительно подчеркивает необходимость системного подхода к оценке и организации внедрения отечественных решений, основанного на сравнительном анализе и архитектурной совместимости.

На этом фоне актуальным становится комплексное исследование, ориентированное на обоснованный выбор сетевого оборудования, соответствующего нормативным требованиям и способного заменить решения Cisco без потери ключевых функций. Важным аспектом является и обеспечение гибкой интеграции с существующей IT-инфраструктурой, в том числе с системами мониторинга, каталогами пользователей и платформами автоматизации.

Проблема и цель исследования. Основной проблемой исследования стало отсутствие единого подхода к выбору отечественных СЗИ для замещения импортного оборудования в крупной корпоративной сети с распределенной архитектурой. Необходимо не просто формальное соответствие требованиям сертификации, но и поддержка механизмов гибкой маршрутизации, фильтрации, построения защищенных каналов, централизованного управления и автоматизации. В современных реалиях большое значение приобретает устойчивость решений

к нагрузке, возможность масштабирования, совместимость с DevOps-процессами и наличие открытых интерфейсов (API). Следовательно, цель настоящей работы — формулировка функциональных требований к СЗИ, сравнительный анализ доступных решений и построение архитектурного шаблона безопасной сети на основе отечественного оборудования, наиболее соответствующего для реализации защищенных сегментов различного масштаба и назначения.

Материалы и методы исследования. В качестве методологии исследования использован структурированный инженерный подход, основанный на сопоставлении функциональных и архитектурных характеристик оборудования с нормативными и эксплуатационными требованиями. Проведен анализ паспортов оборудования, технической документации, руководств по эксплуатации, а также дана сравнительная оценка практикам внедрения, описанным в публикациях и технических блогах. Дополнительно в статье были учтены результаты внутренних тестовых мероприятий, проведенных в рамках подготовки к миграции в одной из российских организаций. Особое внимание уделялось параметрам, связанным с безопасностью (сертификация, шифрование, отказоустойчивость), автоматизацией (поддержка REST API, централизованное управление) и масштабируемостью (кластеризация, производительность, доступность модельной линейки).

Результаты исследования. Формализованные функциональные требования к отечественным межсетевым экранам предполагают наличие механизмов фильтрации трафика на уровнях L3–L7, поддержки DPI, IDS/IPS, управления NAT/PAT, SSL-инспекции, интеграции с системами аутентификации и каталогами (TACACS+, RADIUS, LDAP). Современные межсетевые экраны также должны поддерживать QoS, кластеризацию, централизованное управление через WEB-интерфейс, CLI или API. Немаловажным является наличие развитой модельной линейки, способной покрыть диапазон от филиала до ЦОД. В качестве примера, UserGate предлагает модели от D200 до F8000 с производительностью от 250 Мбит/с до 40 Гбит/с, что делает его применимым на всех уровнях сети. Аналогично xFirewall (Infotecs) предлагает модели xF100–xF65000, а PT NGFW — высокопроизводительные платформы до 400 Гбит/с.

Для обоснованного выбора технических решений была проведена сравнительная оценка отечественных межсетевых экранов. Обобщенные результаты анализа представлены в табл. 1.

Таблица 1

Сравнительный анализ межсетевых экранов

Параметр	*Cisco*	*UserGate*	*VipNet xFirewall*	*PT NGFW*
1	*2*	*3*	*4*	*5*
Разработчик	Cisco Systems	UserGate	ИнфоТеКС (ViPNet)	Positive Technologies
Сертификаты	-	ФСТЭК, ФСБ	ФСТЭК, ФСБ	ФСТЭК, ФСБ
Модельная линейка	ASA 5506-X (750 Мбит/с), ASA 5516-X (1.8 Гбит/с), Firepower 1010 (850 Мбит/с), Firepower 2110 (3 Гбит/с), 4110 (20+ Гбит/с), 9300 (100+ Гбит/с)	D200 (1 Гбит/с), D500 (1 Гбит/с), E1000 (5 Гбит/с), E3000 (10 Гбит/с), F8000 (60 Гбит/с)	xF100 (1 Гбит/с), xF1000 C/D (5 Гбит/с), xF5000 (20 Гбит/с), xF65000 (65 Гбит/с)	PT NGFW 1010 (4 Гбит/с), 1050 (10 Гбит/с), 2020 (100 Гбит/с), 3040 (300 Гбит/с), 3050 (до 400 Гбит/с)

Окончание табл. 1

1	*2*	*3*	*4*	*5*
Поддержка DPI (глубокий анализ трафика)	Да	Да	Да	Да
Система IDS/IPS	Да (Snort, Firepower)	Да	Да	Да
L2/L3 VPN	Да (IPsec, DMVPN, FlexVPN)	Да (IPsec)	Да (IPlir, IPsec)	Да (IPsec)
SSL-инспекция	Да	Да	Нет	Да
WEB-фильтрация	Да	Да (по категориям и контенту)	Ограничена (список URL)	Да
Интеграция с TACACS+, RADIUS, LDAP	Да	Да (с ограничением)	Да	Да
Способы управления (CLI, WEB, API)	CLI, WEB, REST API	WEB, CLI, REST API	WEB, CLI (без REST API)	WEB, CLI, API
DMVPN	Да (DMVPN — собственная разработка)	Нет	Нет	Нет
QoS (приоритезация трафика)	Да (Modular QoS CLI, NBAR)	Да (простой приоритетный контроль)	Нет	Частично (примитивный механизм в профилях)
NAT / PAT	Да (DNAT, SNAT, Policy NAT)	Да (включая Policy NAT)	Да	Да
Защита от DDoS-атак	Да	Да (ограниченно, через фильтры)	Частично (ручная настройка ACL)	Да (интегрировано)
Кластеризация	Да (VRRP, StackWise, HA)	Да	Да	Да
Контроль приложений (Application Control)	Да (AppID, AVC, QoS)	Да	Да	Да
Анализ почтового трафика (SMTP/ IMAP/POP3)	Да (через Cisco ESA или Firepower)	Частично (в составе UTM-функций)	Нет	Да
Журналирование / Интеграция с SIEM / SNMP	Да (Syslog, SNMP, NetFlow, EEM)	Да (Syslog, SNMP, REST API)	Частично (Syslog, SNMP), неунифицированно	Да (Syslog, REST API, интеграция с SIEM, SNMP)
Особенности	Западный вендор, нет поддержки на территории РФ	Поддержка REST API, централиз. управление, нет ping tcp	Только один администратор в сессии конфигурации, нет ping tcp/capture, доступна Linux-оболочка, ограниченный функционал в WEB	Мощная архитектура, широкий функционал, но низкая активность поддержки, высокая стоимость

Сравнительный анализ межсетевых экранов выявил, что наибольшее соответствие требованиям построения защищенной, масштабируемой и управляемой сети демонстрирует решение от UserGate. Его преимущество заключается в сбалансированной архитектуре, широком модельном ряде, наличии REST API и централизованного управления, поддержке всех необходимых сетевых функций (DPI, NAT/PAT, BGP/OSPF, QoS), а также в высоком уровне интеграции с системами мониторинга посредством протокола SNMP (Zabbix и др.). Несмотря на отдельные ограничения в области диагностики (например, отсутствие ping TCP), эти аспекты компенсируются за счет развитой экосистемы управления и автоматизации. В отличие от PT NGFW, UserGate обладает более доступной поддержкой и гибкой ценовой политикой. По сравнению с xFirewall, не имеет ограничений в одновременной конфигурации, а архитектура не привязана к закрытой ViPNet-инфраструктуре. Это делает выбор UserGate оптимальным в качестве основного межсетевого экрана в отечественной архитектуре защищенной сети.

Функциональные требования к криптографическим шлюзам включают поддержку отечественных алгоритмов ГОСТ Р 34.12-2015 и ГОСТ 28147-89, протоколов IPsec/IKEv2, возможность NAT Traversal, GRE, работу в сценариях mesh и hub-and-spoke (DMVPN), поддержку BGP и маршрутизируемых туннелей. Также важны наличие REST API, взаимодействие с внешними УЦ, автоматизация управления ключами, централизованное управление и отказоустойчивость. Шлюзы должны поддерживать мониторинг туннелей, failover по интерфейсам и динамическое масштабирование.

В рамках исследования дана сравнительно-сопоставительная оценка возможностей криптографических шлюзов, представленных на российском рынке. Сводные данные приведены в табл. 2.

Таблица 2

Сравнительный анализ отечественных криптографических шлюзов

Параметр	*S-Terra*	*VipNet Coordinator HW*	*Континент АП*	*Застава*
1	*2*	*3*	*4*	*5*
Разработчик	С-Терра СиЭсПи	ИнфоТеКС	Код Безопасности	НТЦ Протей
Сертификация	ФСТЭК, ФСБ	ФСТЭК, ФСБ	ФСТЭК, ФСБ	ФСТЭК, ФСБ
Модельная линейка	Gate 100 (0.2 Гбит/с), Gate 1000 (1 Гбит/с), Gate 3000 (3 Гбит/с), Gate 7000 (10 Гбит/с), Gate 8000 (15+ Гбит/с)	HW50-4X (0.1 Гбит/с), HW100-4X (0.2 Гбит/с), HW1000 (1 Гбит/с), HW2000 (3 Гбит/с), HW5000-4X (5 Гбит/с)	АП-100 (до 1 Гбит/с), АП-300 (до 1 Гбит/с), АП-500 (до 1 Гбит/с)	Застава-Т (до 1 Гбит/с), мобильные USB
Поддерживаемые алгоритмы шифрования	ГОСТ 28147-89, ГОСТ Р 34.12-2015, IPSec, AES (128, 192, 256 бит), DES, 3DES	IPlir (проприетарный)	ГОСТ 28147–89	ГОСТ 28147-89, IPSec, AES (256, 192, 128 бит), DES, 3DES
Кластеризация / отказоустойчивость	Да	Да	Да	Ограниченно

Окончание табл. 2

1	*2*	*3*	*4*	*5*
Поддержка DMVPN/динамических туннелей	Частично (GRE + BGP)	Нет	Нет	Нет
Встроенный межсетевой экран	Да (базовая фильтрация)	Да (базовая фильтрация)	Да (базовая фильтрация)	Нет
Совместимость с маршрутизаторами	Да	Ограниченно (только ViPNet)	Да	Да
Автоматизация/интеграция с Ansible, API	Да (REST API, шаблоны)	Ограниченно (через ViPNet Центр)	Ограничено	Нет
Централизованное управление	Да (CSO)	Да (ViPNet Центр)	Да	Нет
Журналирование / SIEM	Да (Syslog, SNMP, Zabbix)	Да (через ViPNet Центр)	Да (Syslog, SNMP)	Частично
Поддержка NAT-T	Да	Да	Да	Да
Интеграция с TACACS+, RADIUS, LDAP	Да	Да (в рамках ViPNet CoCenter)	Да (в рамках управляющего центра)	Нет
Способы управления (CLI, WEB, API)	CLI, WEB, REST API (CSO)	WEB, CLI	WEB, CLI, ограниченный API	CLI (локально), WEB-конфигуратор ограничен
Особенности	Поддержка iBGP, mGRE, высокая гибкость	Закрытая архитектура, требует ViPNet-инфраструктуру	Простота развертывания, ограниченная автоматизация	Минимум функций, надежен, но без автоматизации

Наибольшую полноту реализации этих требований демонстрирует S-Terra Gate: наличие моделей от 100 до 8000, производительность до 15 Гбит/с, поддержка кластеризации, частичная поддержка DMVPN-сценариев, CSO-платформа управления и REST API. ViPNet Coordinator HW надежен и сертифицирован, но закрыт архитектурно и не поддерживает внешнюю автоматизацию. «Континент АП» и «Застава» позиционируются как решения для периферийных или удаленных точек, не предназначенные для гибких маршрутизируемых схем.

Рекомендуемая архитектура сети строится на связке UserGate + S-Terra Gate с дифференциацией по зонам: ЦОД — F8000 + Шлюз 8000, региональные площадки — E3000 + Шлюз 1000/3000, филиалы — D500 + Шлюз 100. Это позволяет покрыть все типы площадок и обеспечить сертификационное соответствие, управляемость и отказоустойчивость.

Заключение. Проведенное исследование подтвердило, что выбор отечественных СЗИ должен основываться на сопоставлении функциональных характеристик с архитектурными требованиями защищенных сетей. При этом важна не только сертификация, но и возможности централизованного управления, автоматизации, совместимость с маршрутными протоколами

и системами мониторинга. Связка UserGate и S-Terra Gate на текущий момент является универсальным решением для замещения оборудования Cisco, позволяющим сохранять управляемость, масштабируемость и гибкость. Перспективным направлением дальнейших исследований является разработка автоматизированных шаблонов конфигурации, интеграция с CI/CD-пайплайнами и развитие мультивендорной совместимости.

СПИСОК ЛИТЕРАТУРЫ

1. Безродных О. А. Использование различных межсетевых экранов нового поколения для защиты корпоративной сети от сетевых атак / О. А. Безродных // Инновации. — № 50. — С. 1693-1702.
2. Барищук А. Е. Импортозамещение шлюзов для комплексной защиты защиты от сетевых угроз (UTM/NGFW-решений) / А. Е. Барищук // Континент. — 2023. — Т. 4. — С. 278.
3. Чайка Е. М., Белов С. П. Обзор криптошлюзов для защиты информации в корпоративных сетях / Е. М. Чайка // Научный результат. Информационные технологии. — 2024. — Т. 9, № 1. — С. 3-9.
4. Тутов И. М. Анализ рынка средств криптографической защиты информации в России / И. М. Тутов // Теория и практика современной науки. — 2019. — № 1 (43). — С. 621-624.
5. Джангиров М. Ф. Импортозамещение на рынке информационной безопасности / М. Ф. Джангиров // Молодой ученый. — 2023. — № 1 (448). — С. 4-7.