УДК 004.056.5

С.В. Корякин, srgkoryakin1@gmail.com
Институт машиноведения, автоматики и геомеханики НАН КР
Институт информационных технологий КГТУ им. И.Раззакова
Д.А. Ибраимов, dastanbrmv@gmail.com
Институт информационных технологий КГТУ им. И.Раззакова

АНАЛИТИЧЕСКИЙ ОБЗОР МЕТОДОВ ПОСТРОЕНИЯ ПОДСИСТЕМ АППАРАТНЫХ ФАЕРВОЛОВ ДЛЯ SOC

В статье представлен аналитический обзор современных решений аппаратных фаерволов, применяемых в составе подсистем кибербезопасности для Центров мониторинга безопасности (SOC). Рассмотрены архитектура, функциональные особенности и сравнительные характеристики наиболее популярных решений: Cisco ASA, Fortinet FortiGate, MikroTik RouterBOARD и Raspberry Pi 4. Особое внимание уделено вопросам стоимости, энергоэффективности, гибкости настройки и лицензирования. Выделены преимущества использования приведенных решений для малых корпоративных сетей. Проводится также анализ для подтверждения использования определенного решения в условиях ограниченного бюджета и приоритетной необходимости кастомизации и экономии ресурсов.

Ключевые слова: SOC, информационная безопасность, аппаратный фаервол, SOC, Raspberry Pi, FortiGate, Cisco ASA, MikroTik, защита сети, киберугрозы, межсетевой экран.

Введение

Согласно данным Positive Technologies, в 2024 году количество сетевых атак на страны СНГ увеличилось в 2,6 раза по сравнению с предыдущим годом, а в Кыргызстане в третьем квартале 2024 года их число возросло на 15% относительно аналогичного периода 2023 года. Особенно уязвимыми являются государственные учреждения, производственные предприятия и профессиональные сервисы. Многие продукты для защиты от атак стоят недёшево, однако не все предприятия могут позволить себе данные решения. В данной статье будет рассматриваться универсальное решение для защиты корпоративной сети организаций, преимущества использования и сравнение с аналогичными устройствами защиты.

В 2024 году общее количество DDoS-атак увеличилось на 53% по сравнению с предыдущим годом, при этом рекордная атака достигла мощности 1,14 Тбит/с, что на 65% больше предыдущего рекорда. В финансовом секторе за третий квартал 2024 года банки предотвратили 16,1 миллиона кибератак на счета клиентов, что в три раза больше по сравнению с аналогичным периодом прошлого года. В Кыргызстане в 2024 году зафиксирован трехкратный рост количества атак на государственные ресурсы. Эти данные свидетельствуют о нарастающей угрозе сетевых атак, требующей усиления мер кибербезопасности на всех уровнях.[1] Кыргызстан занимает второе место среди стран СНГ по количеству атак на государственные учреждения и третье место по атакам на телекоммуникационный сектор. Республика упоминается в 22% объявлений, связанных с кибербезопасностью.

Наибольшему числу атак подвергаются:

- 18% — государственные учреждения
- 11% — промышленный сектор
- 10% — телекоммуникации

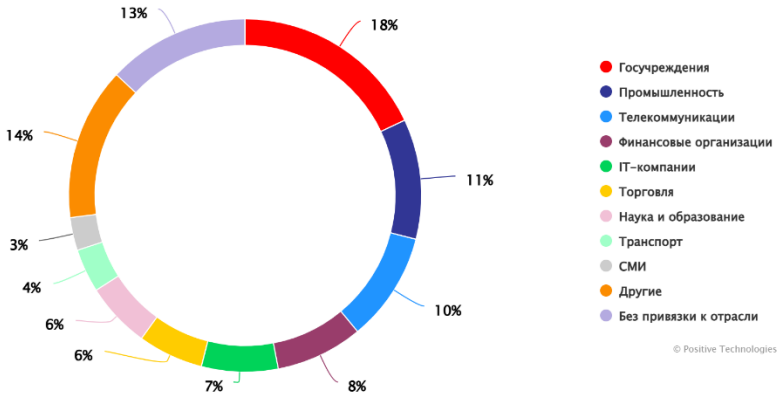

Рисунок 1 — Категории жертв среди организаций

Основными методами кибератак в Кыргызстане, как и во всем СНГ и в остальном мире, являются использование вредоносного ПО и социальная инженерия. В то же время доля DDoS-атак на организации в СНГ существенно выше общемирового показателя — 18% в СНГ против 8% в мире.

Методы защиты корпоративных сетей. С развитием технологий и удешевлением производства современные предприятия и организации всё чаще сталкиваются с необходимостью повышения уровня сетевой безопасности. Рост объемов данных, увеличение числа подключенных устройств и усложнение кибератак делают традиционные программные методы защиты недостаточными. Аппаратные фаерволы становятся важным элементом защиты, обеспечивая высокую производительность, устойчивость к нагрузкам и надежную фильтрацию трафика на аппаратном уровне. Их использование позволяет эффективно предотвращать угрозы, минимизировать задержки в передаче данных и обеспечивать гибкость в настройке политики безопасности, что делает их оптимальным решением для защиты корпоративных сетей и критически важных систем.[2]

Наиболее распространенные аппаратные файрволы. Рынок сетевой безопасности предлагает широкий спектр аппаратных межсетевых экранов – от домашних роутеров с базовым файерволом до мощных корпоративных комплексов. Рассмотрим несколько популярных современных решений и их особенности:

- **Cisco Secure Firewall (ASA/Firepower).** Cisco предлагает линейку **Next-Generation Firewall** под общим названием **Secure Firewall**. Эти решения объединяют в себе классический межсетевой экран с продвинутыми функциями фильтрации приложений и угроз. Например, Cisco NGFW контролирует использование приложений, предотвращает вторжения нового поколения и блокирует продвинутое вредоносное ПО. Отличительной чертой является богатый интерфейс управления и знакомый многим администраторам синтаксис CLI Cisco, упрощающий миграцию и поддержку.[3]
- **Fortinet FortiGate.** FortiGate – NGFW нового поколения, сочетающий в одном устройстве сразу несколько средств защиты. Помимо стандартного файрвола, FortiGate выполняет роль системы предотвращения вторжений, веб-фильтра и даже анализатора зашифрованного трафика. Это комплексное решение обеспечивает многослойную защиту: фильтрацию трафика, мониторинг приложений, блокировку атак и вредоносного контента. Аппаратные устройства FortiGate оснащены

несколькими сетевыми процессорами (для обработки трафика) и контент-процессорами (для анализа данных на лету). Пользователи отмечают интуитивно понятный интерфейс и богатую документацию по настройке.[4]

- **MikroTik RouterBOARD.** Это пример того, как удешевление аппаратных компонентов позволило выпустить бюджетные устройства с функциями файрвола. Маршрутизаторы MikroTik под управлением RouterOS поддерживают фильтрацию трафика на основе правил **iptables** (аналогично Linux). Их возможностей достаточно для малого офиса или филиала. Главное преимущество – низкая цена при приемлемом наборе функций безопасности.[5]
- **Raspberry Pi 4 в роли фаервола.** На практике Raspberry Pi 4 способен маршрутизировать трафик на скорости, близкой к 1 Гбит/с: в тестовом стенде с двумя сетевыми интерфейсами Pi 4 достиг пропускной способности порядка 949 Мбит/с при передаче через NAT. Появляется возможность реализовать межсетевой экран на недорогом оборудовании с открытым ПО. Raspberry Pi 4 предоставляет базовую аппаратную основу (CPU 1.5 ГГц, 4–8 ГБ ОЗУ, 1×GigE + USB NIC) достаточную для реализации функций фаервола и маршрутизатора в корпоративных сетях малого и частично среднего масштаба.[6]

Архитектура и принцип работы:

- **Cisco ASA** – классический аппаратный фаервол с проприетарной ОС ASA OS, обеспечивающий stateful inspection, VPN (IPsec, AnyConnect) и возможности NGFW при использовании FirePOWER. Отличается высокой надёжностью, поддержкой отказоустойчивых кластеров (HA) и глубокой интеграцией с экосистемой Cisco. Требует дорогих лицензий ($500–5000+ в год на IPS, AMP, URL-фильтрацию).
- **Fortinet FortiGate** – NGFW (Next-Generation Firewall) с аппаратными ускорителями обработки трафика (ASIC), даёт высокую производительность (от 5 Гбит/с). Предлагает интегрированные функции IPS, антивируса, VPN, контент-фильтрации, но многие возможности доступны только с платной подпиской ($500–3000+ в год).
- **MikroTik RouterBOARD** – RouterOS, поддерживает firewall, NAT, VPN (IPsec, OpenVPN), QoS и базовые функции DPI (Layer 7 фильтрация). Отличается низкой стоимостью ($50–200+ за устройство), отсутствием платных лицензий и широкими возможностями настройки. IPS/IDS, антивирусом и требует дополнительных решений для UTM-защиты.
- **Raspberry Pi 4** (Linux Firewall) – представляет собой универсальный одноплатный компьютер, на котором выполняется ОС Linux. В роли фаервола он использует iptables, firewalld, nftables, а также поддерживает VPN (WireGuard, OpenVPN) и IDS/IPS (Snort, Suricata). Основное преимущество – нулевая стоимость ПО и минимальные аппаратные затраты (~$100–150), что делает его доступным решением для малого бизнеса, удалённых офисов и образовательных учреждений. Ограничен по производительности (до 1 Гбит/с NAT, сотни Мбит/с через VPN) и требует ручной настройки. Гибкость и кастомизация открытого кода является преимуществом.

В таблице 1 представлено сравнение аппаратных решений.

Таблица 1 — Сравнение аппаратных решений

Решение	**Принцип работы**	**Преимущества**	**Недостатки**	**Актуальность**
Cisco ASA	Appliance от Cisco с	Устойчив к высоким	Очень высокая	Постепенно

(аппаратный фаервол)	проприетарной ASA OS. Stateful firewall + VPN; возможно дополнение модулем FirePOWER для NGFW. Специализированный HW с ускорением пакетов и шифрования	нагрузкам; Полностью сертифицирован; Официальная техподдержка	стоимость; Ограниченная гибкость функционала; Сложность лицензирования	классические ASA уступают место более новым NGFW (Cisco Firepower) и облачным решениям. Актуален для предприятий, уже инвестировавших в инфраструктуру Cisco
Fortinet FortiGate (NGFW)	Аппаратный межсетевой экран нового поколения. FortiOS с интегрированными IPS/AV/фильтрацией	Функционал «всё в одном»: помимо firewall и VPN включены системы противодействия угрозам	Высокая стоимость; Закрытость: платформа проприетарная, меньше возможностей кастомизации; Необходимость квалификации в специфике FortiOS для тонкой настройки	Часто выбирается как более простая в управлении альтернатива Cisco
MikroTik RouterBOARD (RouterOS)	Аппаратный маршрутизатор с ОС RouterOS. Реализует классический stateful firewall, NAT, routing, VPN	Гибкость настройки: RouterOS позволяет детально настраивать маршрутизацию, firewall, QoS; Сообщество и обучение: много инженеров знает RouterOS	Ограниченные возможности UTM: нет встроенного продвинутого анализа трафика; Отсутствие официальной техподдержки сопоставимой с крупными вендорами	Очень популярен в малом и среднем бизнесе, у интернет-провайдеров, в системах видеонаблюдения и т.п.
Raspberry Pi 4 + Linux (iptables)	Программный фаервол на базе общего ОС Linux. Пакетная фильтрация (stateful) через netfilter; гибкая настройка NAT, маршрутизации и VPN силами ПО	Низкая цена оборудования; Гибкость и кастомизация: открытое ПО, возможность установки любых сервисов; Низкое энергопотребление, малые габариты; Активное сообщество, быстрота обновлений безопасности (благодаря Linux)	Без дополнительных усилий нет «из коробки» DPI/IPS/UTM-функций, требующих отдельного ПО	Актуален для случаев, когда бюджет минимален или нужна нестандартная гибкая конфигурация

В таблице 2 представлен анализ стоимости программного обеспечения**.**

Таблица 2 — Сравнение стоимости ПО

Решение	**ПО**	**VPN**	**IDS/IPS**	**Доп. сервисы**	**Стоимость лицензии**
Cisco ASA	Cisco ASA OS	IPsec,	FirePOWER	AMP, URL-	$500–$5000+ в

	(входит в стоимость устройства)	AnyConnect VPN – требуются лицензии	IPS – лицензия $500–$2000+ в год	фильтрация – лицензии $1000+ в год	год за подписки
Fortinet Fortigate	FortiOS (входит в стоимость устройства)	IPsec, SSL VPN – бесплатно в базовой версии	IPS/IDS – требует подписки FortiGuard	Полный пакет UTM (антивирус, URL-фильтр, IPS) – подписка $500–$3000 в год	$500–$3000+ в год
Mikrotik	RouterOS (включено в цену устройства)	IPsec, L2TP, OpenVPN – бесплатно	Базовая фильтрация L7, но нет полноценного IDS/IPS	Нет встроенного антивируса, URL-фильтрации – требует сторонних решений	$0 (но функционал UTM ограничен)
Raspberry Pi 4	Linux (iptables, firewalld, nftables) – бесплатно	WireGuard, OpenVPN, StrongSwan – бесплатно	Snort, Suricata – бесплатно	Pi-hole (фильтрация DNS), Squid (прокси), Zabbix (мониторинг) – всё бесплатно	$0 (всё open-source)

Аппаратная архитектура. Возможности Raspberry Pi 4: он может оснащаться 2 ГБ, 4 ГБ или 8 ГБ оперативной памяти LPDDR4, что достаточно для задач маршрутизации и фильтрации трафика. У Raspberry Pi 4 есть один встроенный гигабитный Ethernet-порт и модули беспроводной связи Wi-Fi 802.11ac и Bluetooth 5.0. Кроме того, на плате имеются два порта USB 3.0 и два USB 2.0, которые можно использовать, например, для подключения дополнительных сетевых адаптеров. Необходимость второго сетевого интерфейса: для работы Raspberry Pi как полноценного межсетевого экрана (фаервола) рекомендуется иметь два сетевых интерфейса – один для внешней сети (WAN), второй для внутренней локальной сети (LAN). У Raspberry Pi 4 всего один Ethernet-порт, поэтому для создания второго интерфейса обычно подключают USB–Ethernet адаптер через быстрый порт USB 3.0. Такое решение поддерживает пропускную способность порядка 300–350 Мбит/с через USB-адаптер.Этого достаточно для типового интернет-канала (например, 100 Мбит/с Pi 4 обрабатывает «безупречно»). Однако достижение полной скорости 1 Гбит/с затруднительно – производительность Raspberry Pi 4 может стать бутылочным горлышком. На практике пропускная способность фаервола на Pi 4 обычно не превышает нескольких сотен мегабит.

На рисунке 2 представлено конструктивное решение платы Raspberry Pi 4.

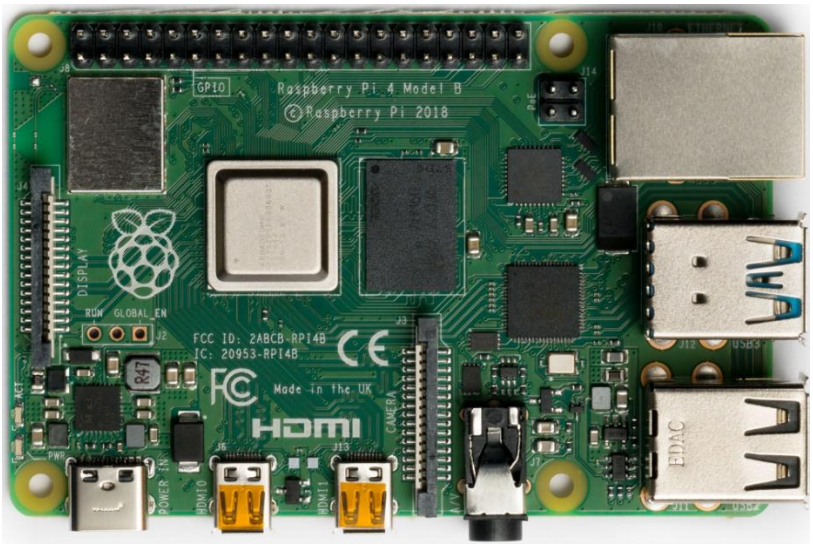

Рисунок 2—Плата Raspberry Pi 4

Ограничения и потенциальные проблемы. Несмотря на мощный процессор, Raspberry Pi 4 не обладает специализированными сетевыми сопроцессорами, которые есть у профессиональных маршрутизаторов и фаерволов. Это значит, что обработка большого объема трафика и сложных правил фильтрации ляжет на CPU, что при высокой нагрузке может привести к росту задержек или перегреву. Для стабильной работы в корпоративном режиме рекомендуется обеспечить хорошее охлаждение (радиаторы, вентилятор или корпус с пассивным охлаждением) – при длительной нагрузке Pi 4 может нагреваться до ~80°C и снижать частоту процессора. Еще один аспект – надежность хранилища: Raspberry Pi обычно загружается с microSD-карты, которая при интенсивной записи логов может изнашиваться. Решение – использовать высококачественную SD-карту или подключить SSD-накопитель через USB 3.0. Также желательно подключить Pi 4 к бесперебойнику, чтобы избежать сбоев питания.

Программная архитектура. Для работы Raspberry Pi 4 в роли аппаратного фаервола с возможностью организации VPN-доступа и защиты от brute-force атак достаточно минимального, но эффективного набора программного обеспечения: **iptables, OpenVPN** и **Fail2Ban**. Эти инструменты позволяют построить надежную и гибкую систему безопасности при минимальных ресурсах и без дополнительных затрат.

Операционная система и подготовка. Наиболее подходящей ОС является **Ubuntu Server LTS** или **Raspberry Pi OS Lite**, обеспечивающие стабильную работу, поддержку необходимых утилит и обновлений безопасности. После записи образа ОС на карту памяти (например, с помощью Raspberry Pi Imager) необходимо выполнить:

- Первичную настройку SSH-доступа;
- Установку iptables и необходимых модулей ядра (iptables-persistent для сохранения правил);
- Настройку статического IP и сетевых интерфейсов (WAN и LAN, при необходимости через USB-Ethernet адаптер).

***Iptables*: фильтрация и маршрутизация.** *Iptables* — основа безопасности Raspberry Pi. С помощью набора правил можно реализовать:

- **Сетевой экран** (фильтрация по IP, порту, протоколу);
- **NAT и форвардинг** трафика между интерфейсами;

- **Ограничение доступа к SSH и VPN** по IP и портам;
- **Защиту от сканирования портов и SYN-флудов**.[7]

OpenVPN: безопасный удаленный доступ. OpenVPN предоставляет защищенный доступ к локальной сети через шифрованный туннель. Его преимущества:

- Надежность и шифрование (TLS + AES);
- Широкая поддержка клиентов (Windows, Linux, Android, iOS);
- Простая интеграция *с iptables* и маршрутизацией.[8]

Конфигурация сервера включает генерацию PKI, настройку интерфейса *tun0* и определение диапазона IP-адресов. Важно продумать меры по защите ключей и конфигураций.

Fail2Ban: защита от перебора паролей. Fail2Ban отслеживает логи (например, */var/log/auth.log*) и автоматически блокирует IP-адреса при множественных неудачных попытках входа. Это особенно актуально для SSH и OpenVPN.[9]

На рисунке 3 представлена схема программной архитектуры Raspberry Pi 4.

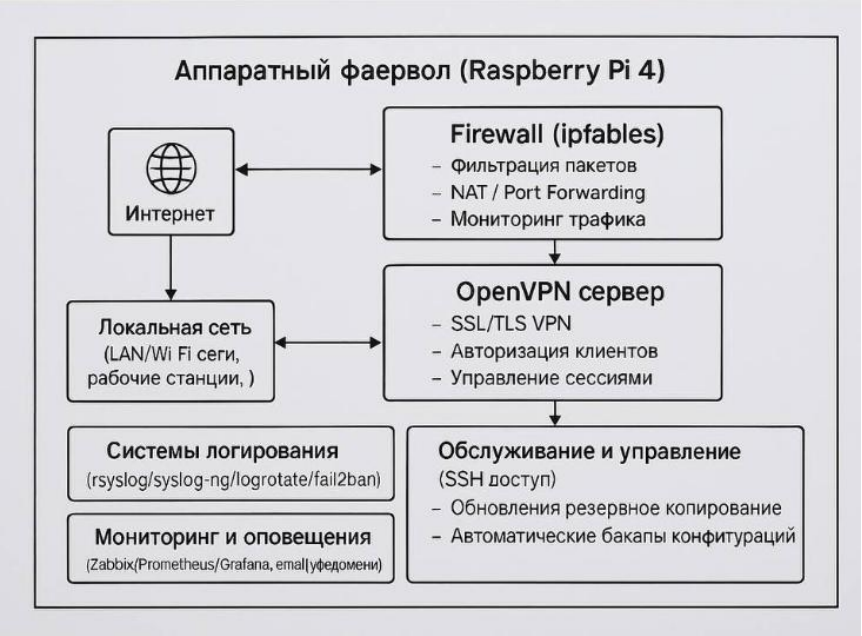

Рисунок 3 — Схема программной архитектуры Raspberry Pi 4

График стоимости устройств. На этом графике показана разница в стоимости между промышленными решениями (Cisco ASA, Fortinet FortiGate) и более доступными — MikroTik и Raspberry Pi 4. Raspberry Pi 4 выделяется как самое бюджетное решение, стоимость которого в 10–20 раз ниже, чем у коммерческих NGFW. Это делает его особенно привлекательным для малых организаций и образовательных учреждений.[10]

На рисунке 4 представлен график сравнения стоимости ПО и лицензий различных видов устройств.

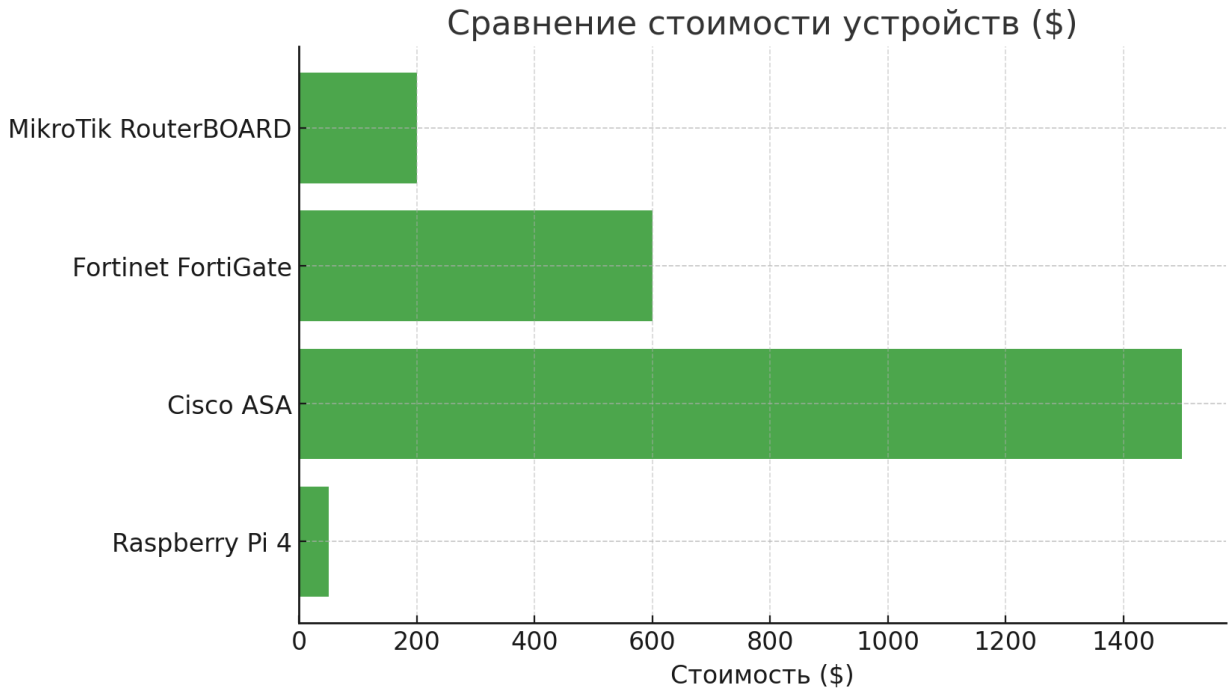

Рисунок 4 — График сравнения стоимости ПО и лицензий

Этот график иллюстрирует, сколько необходимо тратить ежегодно на лицензии и подписки. Raspberry Pi 4 не требует платных подписок вообще — всё программное обеспечение, включая VPN и IDS/IPS, является open-source. В то время как Cisco ASA и Fortinet FortiGate могут потребовать от $500 до $5000 в год на лицензии IPS, URL-фильтрацию и техподдержку.[11] На рисунке 5 представлен график сравнения стоимости технической поддержки.

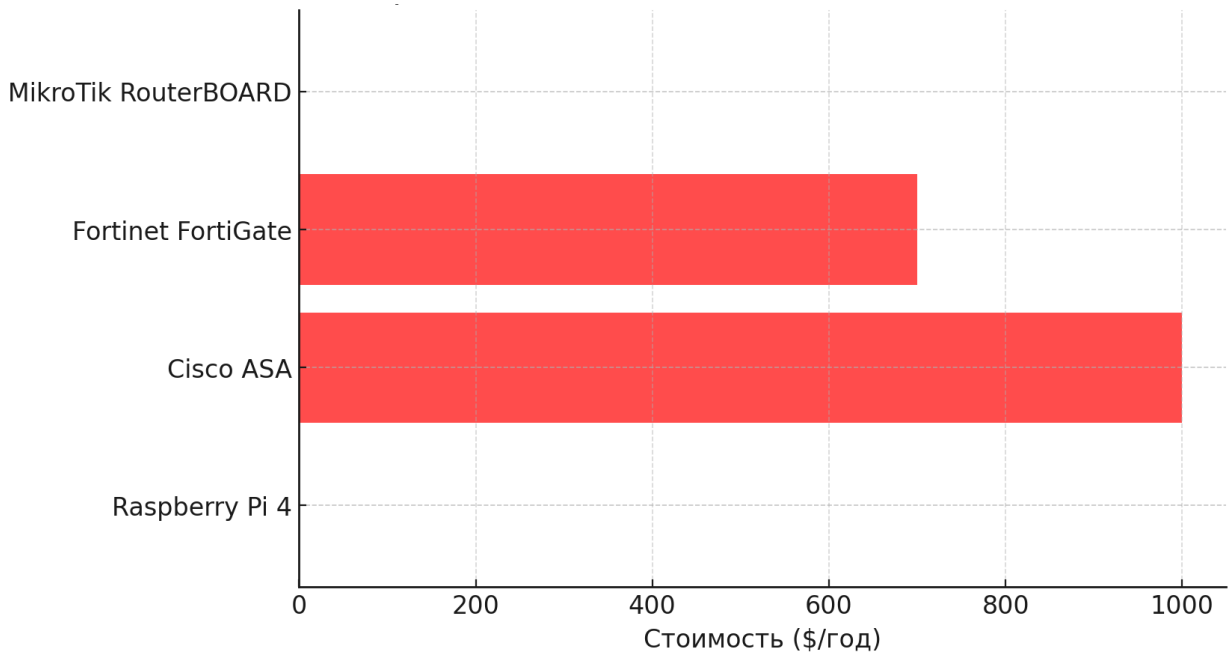

Рисунок 5 — График сравнения технической поддержки

Потребление энергии — важный фактор при постоянной работе устройств. Raspberry Pi 4 демонстрирует минимальное энергопотребление (всего 5–7 Вт), что делает

его в 3–6 раз более энергоэффективным по сравнению с Cisco или Fortinet. Это также означает экономию на электроэнергии в долгосрочной перспективе.[12] На рисунке 5 представлен график сравнения энергопотребления устройств.

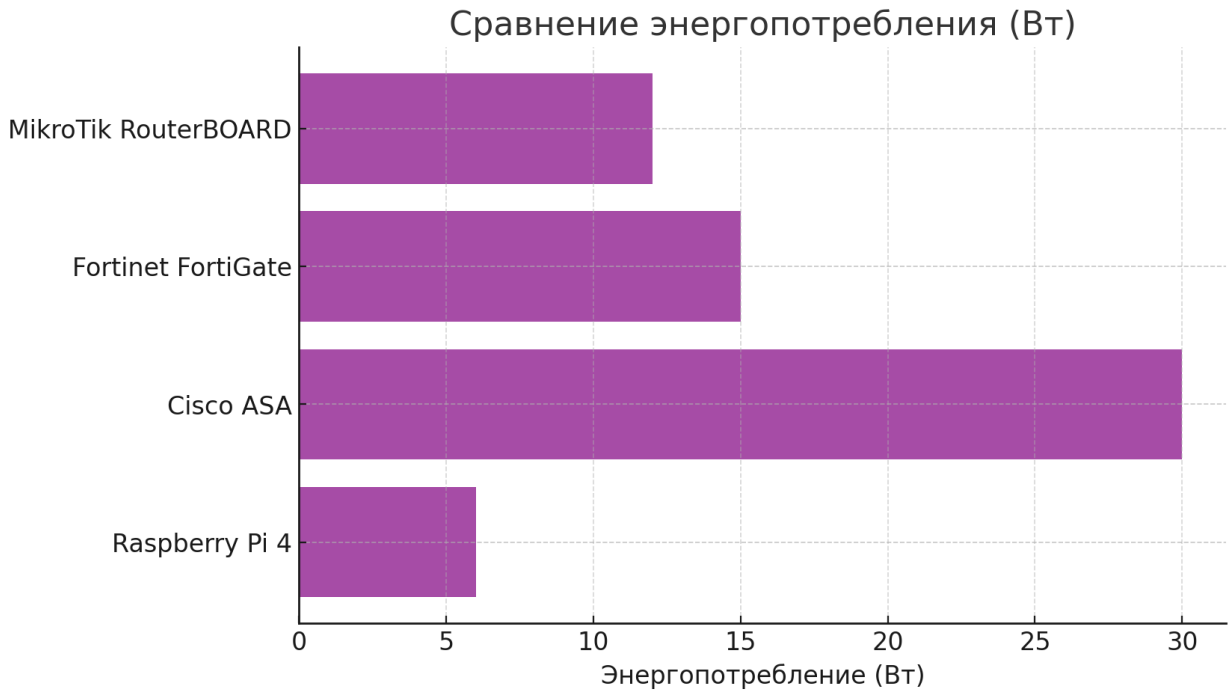

Рисунок 6 — График энергопотребления устройств

На рисунке 7 показана возможность глубокой настройки, гибкость конфигурации и открытость платформы. Raspberry Pi 4 и MikroTik занимают лидирующие позиции за счёт гибкой настройки, особенно если использовать iptables и open-source ПО. Cisco ASA и FortiGate, несмотря на широкую функциональность, ограничены проприетарными интерфейсами и жёсткой моделью лицензирования.[13]

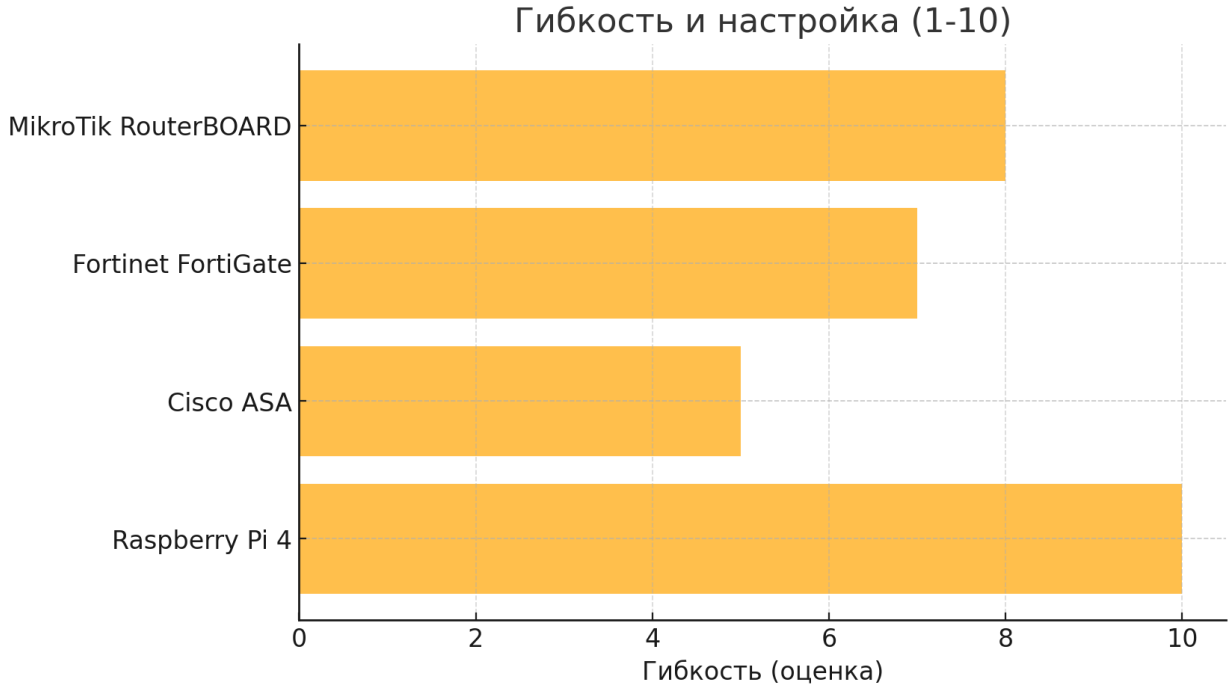

Рисунок 7 – Функциональная возможность глубокой настройки устройств

Следует отметить, что одной из важнейших характеристик является показатель пиковой производительности в идеальных условиях. Cisco ASA и FortiGate обеспечивают до 10–20 Гбит/с благодаря специализированным процессорам. Raspberry Pi 4 ограничен примерно 1 Гбит/с (и это в лучшем случае), особенно если использовать USB-Ethernet. На практике — 300–700 Мбит/с. Тем не менее этого достаточно для малого бизнеса, удалённого офиса или лабораторных задач.[13] На рисунке 8 представлен график сравнения максимальной пропускной способности устройств.

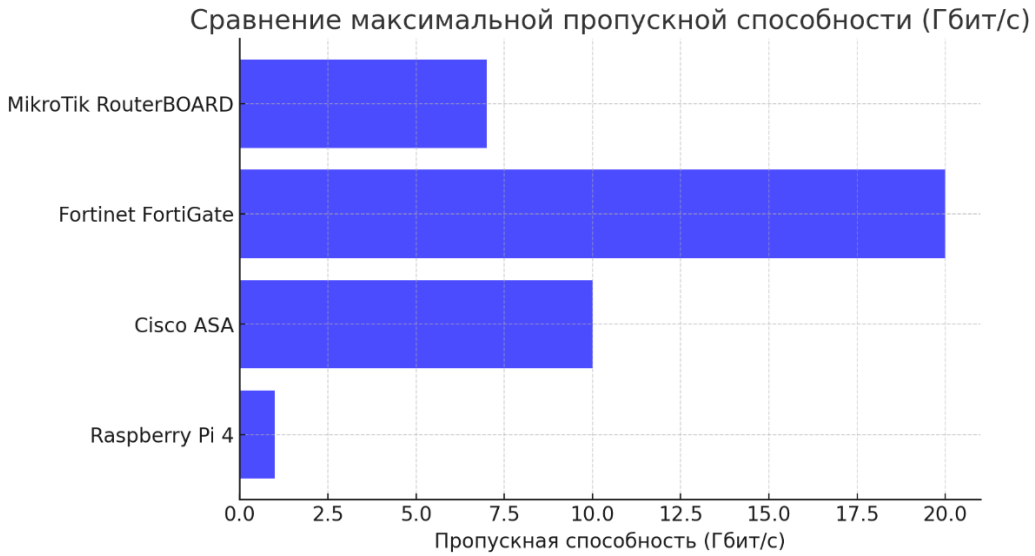

Рисунок 8— График сравнения максимальной пропускной способности

Заключение. На основе проведенного анализа аппаратных фаерволов Raspberry Pi 4, Cisco ASA, Fortinet FortiGate и MikroTik RouterBOARD можно сделать обоснованный вывод о том, что Raspberry Pi 4 является наиболее целесообразным выбором в корпоративной среде, если приоритетом являются минимальная стоимость, гибкость и энергоэффективность. В ходе сравнений были рассмотрены ключевые показатели, такие как стоимость устройства и лицензий, энергопотребление, гибкость и настройка, производительность и масштабируемость, а также функциональные возможности каждого решения.

Следует отметить, что такой показатель, как экономическая эффективность, одно из важнейших преимуществ Raspberry Pi 4. Стоимость самого устройства составляет всего $50–$100, что в 10–20 раз дешевле коммерческих фаерволов, таких как Cisco ASA и Fortinet FortiGate, цены которых могут достигать $1000–$5000 даже для базовых моделей. Кроме того, Raspberry Pi 4 не требует лицензионных платежей, в отличие от Cisco ASA и FortiGate, которые требуют дорогостоящих подписок на IPS, антивирус, контент-фильтрацию и техподдержку. Используемые в Raspberry Pi 4 программные решения, такие как iptables, WireGuard, OpenVPN, Snort и Suricata, являются бесплатными и с открытым исходным кодом, что полностью исключает необходимость дополнительных затрат. В то же время коммерческие решения, такие как Cisco ASA и Fortinet FortiGate, требуют регулярных выплат за обновления сигнатур угроз, поддержку и доступ к дополнительным функциям, что может обходиться в сотни или даже тысячи долларов ежегодно.

Кроме того, одним из наиболее важных факторов является энергоэффективность. Поскольку Raspberry Pi 4 потребляет всего 5–7 Вт, что значительно меньше, чем у аналогичных коммерческих решений. Например, Cisco ASA потребляет около 30 Вт, а

Fortinet FortiGate – 15–20 Вт, что делает Raspberry Pi 4 в 3–5 раз более экономичным с точки зрения энергопотребления. В условиях постоянной работы это приводит к значительной экономии электроэнергии, что особенно важно для организаций, развертывающих несколько точек защиты сети. Более того, низкое энергопотребление позволяет использовать Raspberry Pi 4 в сценариях, где доступны ограниченные источники питания, например, в удаленных офисах, мобильных сетях или лабораторных средах.

Еще одно ключевое преимущество Raspberry Pi 4 – гибкость и возможность кастомизации. В отличие от проприетарных решений, ограниченных возможностями конкретного вендора, Raspberry Pi 4 позволяет использовать любое программное обеспечение: от стандартного Linux-файервола на основе iptables/nftables до специализированных дистрибутивов, таких как pfSense, OpenWRT, IPFire. Это позволяет гибко адаптировать устройство под любые задачи: настройка маршрутизации, VPN, NAT, DPI, IDS/IPS, контент-фильтрация, QoS, а также интеграция с SIEM-системами для мониторинга безопасности. В отличие от коммерческих решений, Raspberry Pi 4 не ограничен жёсткими политиками лицензирования и может быть модифицирован под любые требования.

Таким образом, с точки зрения производительности, Raspberry Pi 4, конечно, уступает коммерческим решениям. Его пропускная способность ограничена 1 Гбит/с, в то время как Fortinet FortiGate и Cisco ASA могут достигать 10–20 Гбит/с благодаря специализированным аппаратным ускорителям обработки трафика. Однако для малых офисов, удаленных филиалов, образовательных учреждений и домашних лабораторий производительности Raspberry Pi 4 вполне достаточно. Кроме того, если не используются сложные функции, такие как глубокая инспекция пакетов (DPI) или антивирусный анализ трафика в реальном времени, разницы в скорости работы с коммерческими решениями практически не будет.

Ключевым аспектом предлагаемого решения является масштабируемость и надёжность. Поскольку коммерческие решения, такие как Cisco ASA и FortiGate, рассчитаны на обслуживание сотен тысяч соединений одновременно, в то время как Raspberry Pi 4 может поддерживать десятки тысяч соединений (до 50 000 в зависимости от конфигурации). Это означает, что Raspberry Pi 4 идеален для небольших сетей, но в крупных корпоративных инфраструктурах может оказаться недостаточно мощным. Тем не менее за счёт открытого ПО и гибкости его можно использовать как вспомогательное устройство – например, в качестве VPN-шлюза, резервного фаервола, контент-фильтра или honeypot-системы для анализа атак.

Именно поэтому выбор Raspberry Pi 4 как аппаратного фаервола обоснован в сценариях, где ключевыми критериями являются минимальные затраты, энергосбережение и гибкость настройки. В случае, если организация не готова тратить тысячи долларов на коммерческие решения, не нуждается в высокопроизводительном NGFW (Next-Generation Firewall) и имеет базовые компетенции в администрировании Linux, Raspberry Pi 4, данное решение становится оптимальным выбором для обеспечения поставленных задач ИБ, которое позволяет развернуть мощное и полностью кастомизируемое решение для защиты сети при минимальных инвестициях и с возможностью дальнейшего масштабирования.

Литература

1. Актуальные киберугрозы в странах СНГ, 2023–2024 [Электронный ресурс] // Positive Technologies. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/, свободный.
2. DDoS-атак стало больше в 2,6 раза во второй половине 2024 года [Электронный ресурс] // ComNews. – 17.02.2025. – Режим доступа: https://www.comnews.ru/content/237793/2025-02-17/2025-w08/1008/ddos-atak-stalo-bolshe-26-raza-vo-vtoroy-polovine-2024-g, свободный.
3. Cisco ASA with FirePOWER Services Series [Электронный ресурс] // Cisco. – Режим доступа: https://www.cisco.com/c/en/us/support/security/asa-firepower-services/series.html, свободный.
4. Fortinet named a Leader in The Forrester Wave: Enterprise Firewall Solutions, Q4 2024 [Электронный ресурс] // Fortinet. – Режим доступа: https://www.fortinet.com/blog/business-and-technology/fortinet-named-leader-in-the-forrester-wave-enterprise-firewall-solutions-q4-2024-report, свободный.
5. MikroTik hEX router [Электронный ресурс] // MikroTik. – Режим доступа: https://mikrotik.com/product/hex_2024, свободный.
6. How to protect your network with a Raspberry Pi firewall [Электронный ресурс] // XDA Developers. – Режим доступа: https://www.xda-developers.com/protect-network-with-raspberry-pi-firewall/, свободный.
7. OpenVPN [Электронный ресурс]. – Режим доступа: https://openvpn.net/, свободный.
8. Netfilter Project [Электронный ресурс]. – Режим доступа: https://netfilter.org/, свободный.
9. Fail2Ban [Электронный ресурс] // Офиц. вики Fail2Ban. – Режим доступа: https://www.fail2ban.org/wiki/index.php/Main_Page, свободный.
10. Cisco ASA 5500 Series Next-Generation Firewalls – Data Sheet [Электронный ресурс] // Cisco. – Режим доступа: https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html, свободный.
11. FortiGate 60F – Technical Data Sheet [Электронный ресурс] // Fortinet. – Режим доступа: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-60f.pdf, свободный.
12. Raspberry Pi 4 as a Gigabit Router [Электронный ресурс] // Jeff Geerling's Blog. – 2020. – Режим доступа: https://www.jeffgeerling.com/blog/2020/raspberry-pi-4-gigabit-router-open-source, свободный.
13. MikroTik Performance Tests [Электронный ресурс] // MikroTik Wiki. – Режим доступа: https://wiki.mikrotik.com/wiki/Performance_tests, свободный.