Сеидов М. С-А.
Студент
3 курс, факультет «Комплексной безопасности топливно-энергетического комплекса»
РГУ нефти и газа (НИУ) имени И.М. Губкина
Россия, г. Москва

Ясевич Б. О.
Студент
3 курс, факультет «Комплексной безопасности топливно-энергетического комплекса»
РГУ нефти и газа (НИУ) имени И.М. Губкина
Россия, г. Москва

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ CIS BENCHMARK ДЛЯ МЕЖСЕТЕВЫХ ЭКРАНОВ НА БАЗЕ ОС АЛЬТ В КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЕ

ВВЕДЕНИЕ

Корпоративные сети все чаще включают несколько зон доверия, удаленное администрирование и постоянный обмен данными между внутренними и внешними сегментами, поэтому межсетевой экран становится ключевым элементом управляемой политики безопасности [1]. Современные исследования показывают, что эффективность межсетевого экранирования зависит не только от выбора средства защиты, но и от формализованной проверки его конфигурации, поскольку ошибки правил, избыточно открытые сервисы и недостаточное журналирование снижают устойчивость инфраструктуры к сетевым атакам [2, 3]. В этих условиях CIS Benchmarks целесообразно рассматривать как основу для построения эталонной модели безопасной настройки систем и сетевых устройств.

Цель работы заключается в оценке эффективности применения эталонной модели безопасной конфигурации, сформированной на основе CIS Benchmarks для межсетевых экранов различных вендоров, к программному

межсетевому экрану на базе ОС Альт. Для достижения поставленной цели необходимо выполнить следующие задачи:

1) Выделить типовые требования CIS Benchmarks к защищенной конфигурации межсетевых экранов;

2) Сформировать обобщенную эталонную модель оценки конфигурации межсетевого экрана;

3) Определить применимость данной модели к программному межсетевому экрану на базе ОС Альт;

4) Показать практическую реализацию ключевых требований средствами firewalld и nftables;

5) Оценить полноту реализации требований и выявить ограничения выбранного подхода.

Объектом исследования является программный межсетевой экран на базе ОС Альт, функционирующий в модели корпоративной инфраструктуры с несколькими изолированными сетевыми сегментами и использующий firewalld с nftables для реализации политики фильтрации. Предметом исследования является применимость требований CIS Benchmarks для промышленных и программных межсетевых экранов к конфигурации данного межсетевого экрана.

В работе использованы методы сравнительного анализа CIS Benchmarks для промышленных и программных межсетевых экранов, декомпозиции требований по функциональному назначению, сопоставления требований с возможностями ОС Альт, firewalld и nftables, а также лабораторного эксперимента на виртуальном стенде с четырьмя сетевыми сегментами.

Научная новизна работы заключается в том, что CIS Benchmarks для промышленных межсетевых экранов рассматриваются не как набор вендорно-зависимых инструкций, а как источник повторяющихся требований к защищенной конфигурации, которые могут быть преобразованы в универсальную контрольную модель. В отличие от прямого переноса

рекомендаций CIS на Linux-систему, в работе выполняется декомпозиция требований по функциональному назначению.

Практическая значимость работы заключается в возможности использования предложенной эталонной модели как контрольной матрицы при настройке и проверке программных межсетевых экранов на базе ОС Альт. Полученные результаты могут быть применены при построении импортозамещающих корпоративных инфраструктур, где требуется обоснованная и воспроизводимая настройка политики межсетевого экранирования средствами отечественной операционной платформы.

В качестве платформы исследования выбрана ОС Альт как отечественный дистрибутив, применимый в импортозамещающих инфраструктурах и представленный в российской программной экосистеме. Значимость выбора усиливается наличием серверных редакций ОС Альт в реестре российского программного обеспечения и сертифицированной редакции «Альт СП», а также поддержкой стандартных Linux-механизмов межсетевого экранирования firewalld и nftables.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И ФОРМИРОВАНИЕ ЭТАЛОННОЙ МОДЕЛИ

Межсетевой экран в корпоративной инфраструктуре следует рассматривать не только как средство разрешения или блокирования отдельных сетевых соединений, а как элемент реализации политики безопасности между сегментами с различным уровнем доверия. В соответствии ГОСТ Р ИСО/МЭК 27033-1-2011 межсетевой экран рассматривается как барьер безопасности, размещаемый между различными сетевыми средами и обеспечивающий пропуск только авторизованного трафика, соответствующего локальной политике безопасности [4]. В NIST SP 800-41 Rev. 1 «Guidelines on Firewalls and Firewall Policy» межсетевые экраны определяются как устройства или программные средства, управляющие потоками трафика между сетями или узлами с различными состояниями защищенности, при этом особое внимание уделяется не только выбору

технологии, но и разработке, тестированию, внедрению и сопровождению политики межсетевого экранирования [5].

Для российской нормативной базы вопросы межсетевого экранирования, журналирования и контроля конфигурации связаны с требованиями к защите государственных информационных систем и значимых объектов критической информационной инфраструктуры. Приказ ФСТЭК России от 25.12.2017 № 239 обосновывает необходимость контролируемой настройки средств защиты в инфраструктурах повышенной значимости [6], методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» закрепляет меры управления доступом, регистрации событий безопасности и контроля защищенности [7], а ГОСТ Р 59548-2022 задает требования к регистрируемой информации по событиям безопасности [8].

Современная корпоративная сеть редко представляет собой единый защищенный периметр, поскольку в ее состав входят внутренние сегменты, удаленный доступ, серверные зоны, облачные ресурсы и инфраструктура администрирования. В архитектуре нулевого доверия, описанной NIST, подчеркивается снижение роли физического или логического местоположения узла как самостоятельного основания для доверия. Поэтому межсетевой экран должен обеспечивать не только защиту внешней границы, но и контроль взаимодействия между внутренними сетевыми средами, ограничение административного доступа и поддержку принципа минимально необходимого сетевого обмена.

Научные публикации последних лет подтверждают, что эффективность межсетевого экранирования определяется не фактом наличия средства защиты, а качеством его конфигурации и возможностью объективной проверки результата. Исследования рассматривают испытания межсетевых экранов, анализ отечественных средств межсетевого экранирования, тестирование сертифицированных решений, формализацию сетевой сегментации и выявление аномалий в политиках firewall [2, 3, 9–11]. Общим

выводом этих работ является необходимость представления политики межсетевого экрана в проверяемой форме, поскольку рост числа правил и сегментов повышает вероятность конфликтов, избыточных разрешений, теневых правил и ошибок администрирования.

Для построения эталонной модели оценки важно учитывать, что политика межсетевого экранирования должна быть выражена через совокупность устойчивых требований, не зависящих от конкретного производителя. К таким требованиям относятся разделение сетей на зоны безопасности, запрет неразрешенного трафика по умолчанию, явное описание допустимых сервисов, защита плоскости управления, ограничение доступа к административным интерфейсам, журналирование разрешенных и запрещенных событий, контроль изменений конфигурации и возможность восстановления настроек [10].

В качестве основы для формирования эталонной модели целесообразно рассматривать не единичный CIS Benchmark, а совокупность рекомендаций, относящихся к классу Network Devices и специализированным межсетевым экранам. В рамках исследования анализируются CIS Benchmarks для Palo Alto Firewall, Fortinet FortiGate, Cisco ASA и Cisco Firepower Threat Defense, Check Point Firewall, Sophos Firewall, pfSense Firewall и OPNsense. Выбор указанных документов обусловлен тремя критериями. Во-первых, все они относятся к специализированным средствам межсетевого экранирования или сетевым устройствам с выраженной firewall-функциональностью. Во-вторых, совокупность выбранных продуктов охватывает как коммерческие промышленные NGFW-платформы, так и программные межсетевые экраны, что снижает зависимость эталонной модели от архитектуры одного производителя. В-третьих, в этих документах повторяются сопоставимые группы требований: защита интерфейсов управления, ограничение административного доступа, разграничение сетевых сред, запрет неразрешенного трафика, контроль правил, журналирование и управление конфигурацией. Включение pfSense Firewall и OPNsense дополнительно

позволяет проверить, что выделяемые требования характерны не только для аппаратно-программных промышленных решений, но и для программных firewall-платформ.

Сопоставление выбранных CIS Benchmarks показывает, что при различии архитектуры конкретных продуктов в них повторяются общие требования к защищенной конфигурации межсетевого экрана: защита плоскости управления, ограничение административного доступа, использование защищенных протоколов администрирования, разграничение сетевых сред, запрет неразрешенного трафика, отказ от чрезмерно широких правил, журналирование событий и контроль конфигурации.

На основании сопоставления выделяются пять групп требований, пригодных для построения эталонной модели оценки межсетевого экрана на базе ОС Альт. К ним относятся защита плоскости управления через ограничение административного доступа и отключение небезопасных протоколов, сегментация сети с привязкой интерфейсов и источников трафика к отдельным зонам, политика фильтрации с запретом неразрешенного трафика и явным описанием допустимых сервисов, регистрация событий с журналированием разрешенных и заблокированных соединений, а также управляемость конфигурации, включающая резервное копирование, контроль изменений и возможность восстановления параметров межсетевого экрана.

В исследовании межсетевой экран рассматривается как программная реализация на базе ОС Альт, однако фактическая фильтрация трафика опирается на стандартные механизмы сетевого стека Linux. На уровне ядра эту функцию выполняет подсистема Netfilter, а современным средством управления правилами является nftables, использующее таблицы, цепочки и правила для обработки входящего, исходящего и транзитного трафика [12]. Документация Netfilter определяет nftables как замену iptables, ip6tables, arptables и ebtables, что подтверждает его применимость в качестве низкоуровневого механизма реализации правил фильтрации, формируемых firewalld в экспериментальном стенде [13].

Прямая настройка nftables требует детального описания таблиц, цепочек, правил и порядка их обработки, поэтому в корпоративной среде целесообразно использовать firewalld как более управляемый уровень администрирования. Firewalld предоставляет модель зон, сервисов, источников трафика и постоянной конфигурации, а также выступает контроллером для nftables, позволяя изменять правила без перезапуска службы межсетевого экрана [14, 15].

Сопоставление требований CIS Benchmarks с возможностями ОС Альт позволяет перейти от вендорно-зависимых рекомендаций к эталонной модели оценки, в которой учитываются не команды конкретных платформ Palo Alto, FortiGate, Cisco ASA, Check Point или Sophos, а содержательная цель каждого требования. В работе под эталонной моделью понимается исследовательская контрольная модель, сформированная путем обобщения повторяющихся требований CIS Benchmarks и используемая как набор проверяемых требований к защищенной конфигурации программного межсетевого экрана. Термин «зона безопасности» используется как логическая сетевая среда с определенным уровнем доверия и как объект firewalld, к которому привязываются интерфейсы, источники трафика, сервисы и правила обработки пакетов. Результаты сопоставления представлены в таблице 1.

Таблица 1 - Сопоставление требований

Группа требований	**Проявление в CIS Benchmarks**	**Адаптация к ОС Альт**
Защита плоскости управления	Ограничение доступа к управлению, запрет небезопасных протоколов	Отдельная management-зона, SSH только из доверенной подсети
Разделение зон безопасности	Зоны, интерфейсы, межзонные правила, local-in policies	Зоны external, users, servers, management с привязкой интерфейсов
Запрет по умолчанию	Блокирование неописанного трафика, отказ от широких правил	Target DROP, удаление лишних сервисов, явные разрешения
Межзонное взаимодействие	Разрешение только заданных потоков между зонами	Политики firewalld и расширенные правила для нужных направлений

Журналирование событий	Логирование правил, событий управления и передачи во внешние системы	LogDenied, журналы firewalld/nftables, syslog или rsyslog
Системные параметры	Настройка времени, учетных записей, тайм-аутов и параметров управления	sysctl, auditd, systemd-журналы, настройки SSH и учетных записей
Контроль конфигурации	Резервное копирование, аудит состояния, контроль изменений	Permanent-конфигурация, экспорт правил, хранение в репозитории

Таким образом, CIS Benchmarks для сетевых устройств позволяют выделить повторяющиеся принципы защищенной конфигурации. Эти принципы используются как эталонная модель оценки межсетевого экрана на базе ОС Альт, а практическая часть показывает, какие из них реализуются средствами firewalld и nftables, а какие требуют дополнительных механизмов операционной системы или специализированных firewall-платформ.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ И ОЦЕНКА ЭФФЕКТИВНОСТИ

При выборе способа реализации эталонной модели на ОС Альт сопоставлены три подхода:

– прямое использование nftables;

– применение готовых профилей безопасности ОС;

– настройка firewalld с nftables в качестве механизма исполнения правил.

Прямое управление nftables обеспечивает максимальную гибкость, но усложняет сопровождение и хуже соответствует зональной логике CIS Benchmarks. Готовые профили безопасности усиливают параметры ОС, учетные записи, службы и журналирование, однако не формируют полноценную политику межсетевого взаимодействия между сетевыми средами. Поэтому в качестве основного подхода выбран firewalld, поскольку он предоставляет модель зон, сервисов и политик, сохраняя применение правил через nftables.

Экспериментальный стенд представляет собой модель корпоративной сети, разделенной на несколько изолированных IP-сегментов, взаимодействие

между которыми осуществляется через центральный межсетевой экран (рисунок 1).

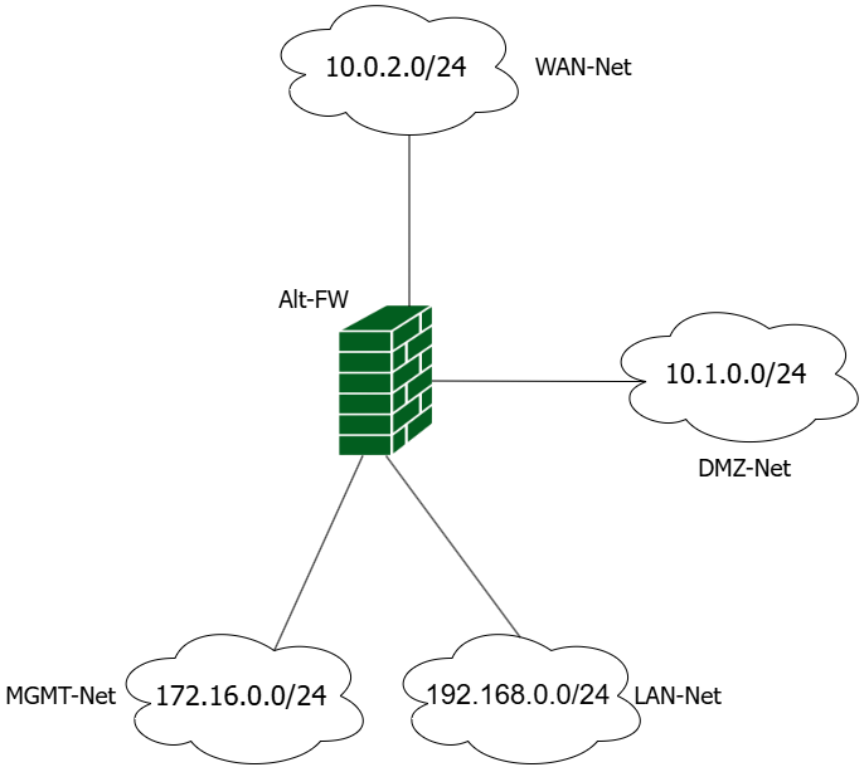

Рисунок 1 – Схема экспериментального стенда

В качестве межсетевого экрана используется узел на базе ОС Альт, характеристики которого представлены в таблице 2.

Таблица 2 – Характеристика виртуальной машины

Характеристика	**Значение**
Используемый дистрибутив	ОС Альт Сервер 11.0
Версия ядра Linux	6.12.27-6.12-alt1syste
Количество виртуальных CPU	4
Количество оперативной памяти, Гб	4
Количество сетевых адаптеров	4
Тип адаптера	Intel PRO/1000 MT Desktop (82540EM)
Объем виртуального диска, Гб	50
Версия firewalld	2.4.1
Версия nftables	1.1.3

В состав стенда входят четыре сетевых сегмента 10.0.2.0/24, 10.1.0.0/24, 172.16.0.0/24 и 192.168.0.0/24 (рисунок 1). Каждый сегмент рассматривается как отдельная зона безопасности, для которой задаются собственные правила

доступа, допустимые сервисы и ограничения на обмен трафиком с другими зонами. Центральный межсетевой экран обеспечивает контролируемое взаимодействие между подсетями, применяет правила фильтрации, ограничивает административный доступ и обеспечивает журналирование событий безопасности.

Первым требованием эталонной модели является защита плоскости управления, поскольку административный доступ напрямую влияет на конфигурацию межсетевого экрана. В стенде это требование реализуется выделением зоны corp_management для сегмента 172.16.0.0/24, привязкой к ней административного интерфейса и разрешением SSH только в данной зоне. На рисунке 2 показаны команды firewalld, создающие зону управления, задающие политику DROP, выполняющие привязку интерфейса и передающие итоговые правила в nftables для применения на уровне ядра.

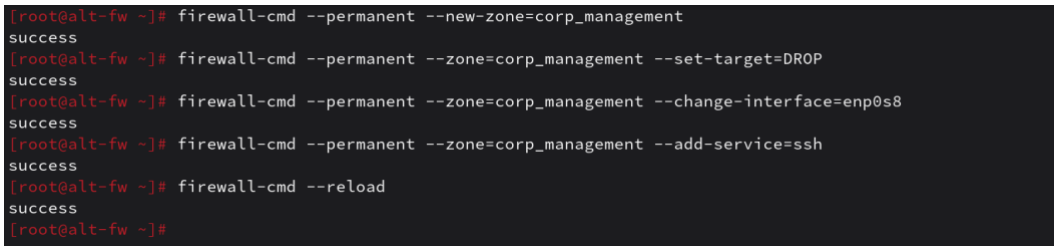

Рисунок 2 - Создание и настройка зоны управления

Следующим требованием является разделение инфраструктуры на зоны безопасности, при котором каждая IP-подсеть стенда получает собственные правила обработки трафика. В рассматриваемой схеме сегмент 10.0.2.0/24 соответствует зоне corp_external, 10.1.0.0/24 – зоне corp_servers, 172.16.0.0/24 – зоне corp_management, а 192.168.0.0/24 – зоне corp_users. Практическая настройка, показанная на рисунке 3, включает создание зон firewalld, установку ограничительной политики по умолчанию и привязку интерфейсов межсетевого экрана к соответствующим зонам.

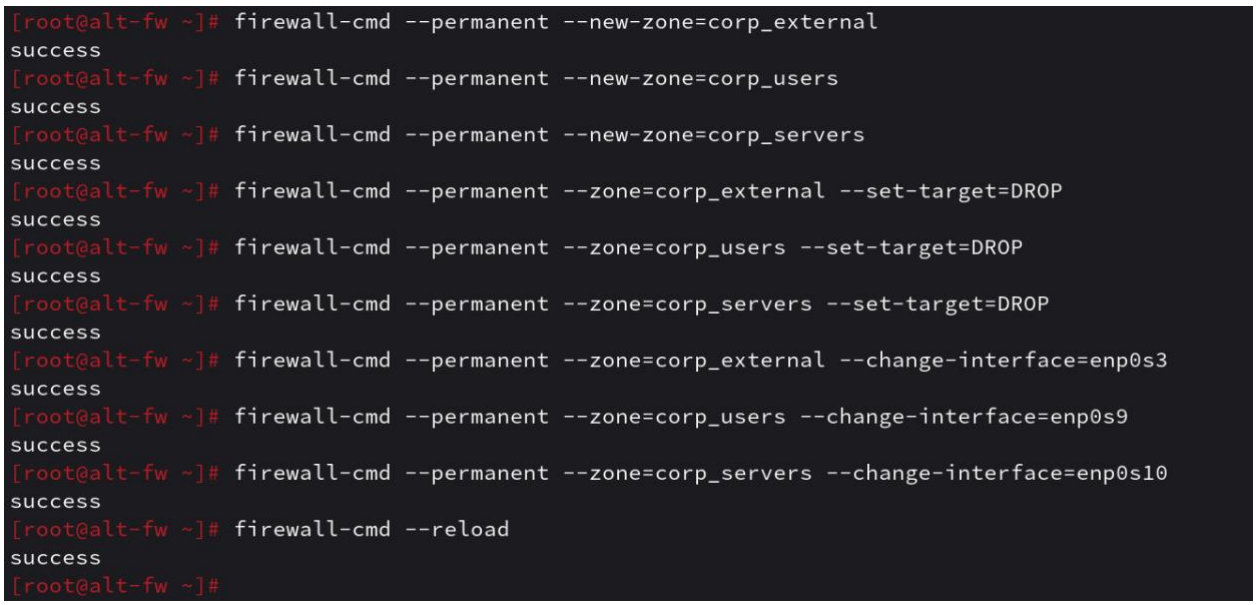

Рисунок 3 - Настройки зон безопасности

Следующим требованием является контроль межзонного взаимодействия, при котором межсетевой экран определяет не только принадлежность трафика к зоне, но и допустимые направления обмена. В стенде для политики pol_users_to_external разрешается доступ из пользовательской зоны corp_users во внешнюю зону corp_external только по сервисам HTTP, HTTPS и DNS, что показано на рисунке 4.

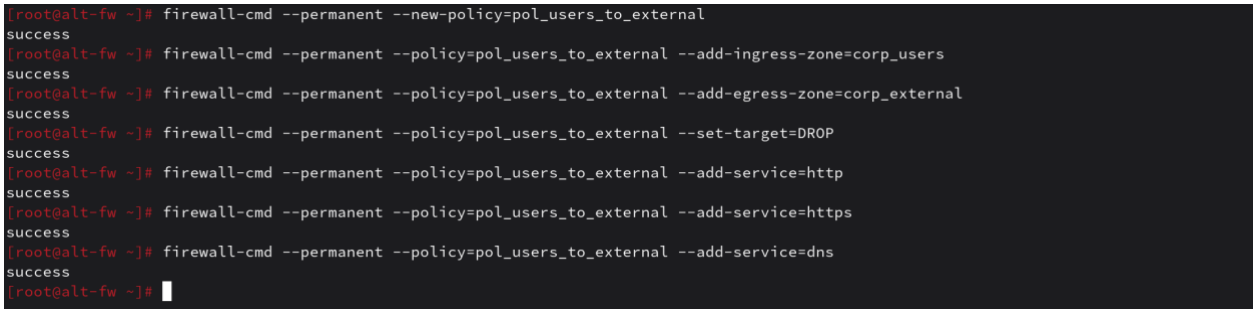

Рисунок 4 - Настройка зонального взаимодействия

Следующим требованием является журналирование событий межсетевого экрана, необходимое для фиксации обращений, не соответствующих заданной политике безопасности. В стенде это показано на политике pol_users_to_external. Для заблокированного трафика добавляется расширенное правило firewalld с журналированием и последующим отбрасыванием пакета. Префикс FW_DROP_USERS_EXT позволяет выделять события данного направления межзонного обмена среди остальных сообщений ядра и firewalld, что отражено на рисунке 5.

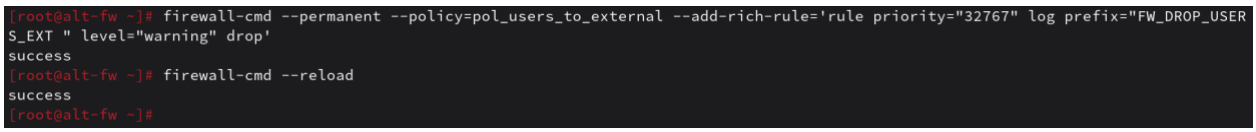

Рисунок 5 – Настройка журналирования заблокированного трафика для политики pol_users_to_external

Безопасность системных параметров относится к уровню операционной системы и не реализуется непосредственно средствами firewalld. Firewalld управляет зонами, сервисами и политиками, передавая правила в nftables, тогда как параметры сетевого стека Linux настраиваются через механизмы ядра и sysctl. Для межсетевого экрана на базе ОС Альт к таким параметрам относятся включение маршрутизации между интерфейсами, отключение source routing и ICMP redirect, фильтрация обратного пути, регистрация пакетов с некорректными адресами и ограничение реакции на широковещательные ICMP-запросы.

Управляемость конфигурации предполагает сохранение настроек межсетевого экрана в виде, пригодном для проверки, восстановления и повторного развертывания. На ОС Альт это реализуется через постоянную конфигурацию firewalld, задаваемую параметром --permanent и применяемую командой firewall-cmd --reload, а также через экспорт зон, политик и результирующих правил nftables в файлы эксплуатационной документации или систему контроля версий.

Проведенная адаптация эталонной модели показала, что требования CIS Benchmarks для промышленных межсетевых экранов могут быть частично перенесены на программный межсетевой экран на базе ОС Альт при условии их интерпретации не как вендорных команд настройки, а как функциональных требований к защищенной конфигурации. Наиболее полно средствами firewalld с backend nftables реализуются те элементы модели, которые связаны с зонированием сети, ограничением административного доступа, политикой запрета по умолчанию и контролем межзонного обмена. Обобщенная оценка применимости требований представлена в таблице 3.

Для снижения субъективности оценки используются формальные критерии. Требование считается реализованным полностью, если оно выполняется штатными средствами firewalld и nftables, имеет прямое конфигурационное выражение и проверяется командами состояния или тестовым сетевым взаимодействием. Частичная реализация фиксируется, если firewalld обеспечивает только базовый уровень, а полное выполнение требует дополнительных средств, например централизованного хранения журналов, корреляции событий или контроля изменений. Категория «реализуется средствами ОС» применяется к требованиям, настраиваемым вне firewalld через параметры ядра, системные службы, учетные записи или механизмы аудита.

Таблица 3 - Оценка применимости требований

Требование эталонной модели	**Реализация на ОС Альт**	**Итоговая оценка**
Защита плоскости управления	Выделение зоны управления, разрешение SSH только из доверенного сегмента	Реализуется полностью
Разделение зон безопасности	Создание зон для внешнего, пользовательского, серверного и административного сегментов	Реализуется полностью
Политика запрета по умолчанию	Установка target DROP для зон и разрешение только необходимых сервисов	Реализуется полностью
Контроль межзонного взаимодействия	Использование firewalld policies для описания разрешенных направлений обмена	Реализуется полностью
Журналирование событий	Локальная фиксация заблокированного трафика и событий firewalld	Реализуется частично
Безопасность системных параметров	Настройка параметров ядра через sysctl, вне firewalld	Реализуется средствами ОС
Воспроизводимость и контроль изменений	Использование permanent-конфигурации, экспорт правил firewalld и nftables	Реализуется частично

Таким образом, из 7 требований эталонной модели 4 требования реализованы полностью, 2 – частично, 1 требование реализуется средствами ОС.

ЗАКЛЮЧЕНИЕ

В ходе исследования была рассмотрена возможность применения эталонной модели защищенной конфигурации, сформированной на основе CIS

Benchmarks для промышленных межсетевых экранов, к программному межсетевому экрану на базе ОС Альт. Практическая часть показала, что firewalld с backend nftables позволяет реализовать значительную часть данной модели штатными средствами ОС Альт. Наиболее полно реализуются зонирование сети, ограничение административного доступа, явное разрешение сервисов и управление межзонными потоками. Методика может быть использована организациями, внедряющими отечественные серверные операционные системы и программные межсетевые экраны в корпоративных, государственных и импортозамещающих инфраструктурах, где требуется проверяемая настройка политики межсетевого экранирования. Следует учитывать ограничения проведенного исследования. Экспериментальная проверка выполнялась в виртуальном стенде, поэтому полученные результаты отражают корректность настройки и применимость модели в лабораторных условиях, а не поведение межсетевого экрана под промышленной нагрузкой. Используемый трафик имел синтетический характер, реальные атаки, эксплуатация уязвимостей и длительное нагрузочное тестирование не проводились. В связи с этим результаты следует рассматривать как подтверждение реализуемости и проверяемости CIS-ориентированной модели на базе ОС Альт, а не как полную оценку устойчивости решения к реальным кибератакам.

Список использованных источников:

1. Kerman A. et al. Implementing a zero trust architecture //National Institute of Standards and Technology. – 2020. – Т. 2020. – С. 17-17.

2. Садыков Александр Мунирович, Ямалетдинов Роман Русланович, Сабирова Динара Илнуровна Российские средства межсетевого экранирования для защищенных систем // Вестник ДГТУ. Технические науки. 2024. №4. URL: https://cyberleninka.ru/article/n/rossiyskie-sredstva-mezhsetevogo-ekranirovaniya-dlya-zaschischennyh-sistem (дата обращения: 12.05.2026).

3. Добрушин Михаил Михайлович, Фролов Владислав Алексеевич, Хагуров Дмитрий Евгеньевич, Горшков Алексей Николаевич МЕТОДИКА

ПРОВЕДЕНИЯ ИСПЫТАНИЙ ПО ОПРЕДЕЛЕНИЮ СПОСОБНОСТИ МЕЖСЕТЕВОГО ЭКРАНА МИНИМИЗИРОВАТЬ УЩЕРБ ОТ КОМПЬЮТЕРНЫХ АТАК // Известия ТулГУ. Технические науки. 2024. №9. URL: https://cyberleninka.ru/article/n/metodika-provedeniya-ispytaniy-po-opredeleniyu-sposobnosti-mezhsetevogo-ekrana-minimizirovat-uscherb-ot-kompyuternyh-atak (дата обращения: 12.05.2026).

4. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. М.: Стандартинформ, 2012.

5. Scarfone K., Hoffman P. Guidelines on Firewalls and Firewall Policy: NIST Special Publication 800-41 Revision 1. Gaithersburg: National Institute of Standards and Technology, 2009. DOI: 10.6028/NIST.SP.800-41r1.

6. Приказ ФСТЭК России от 25 декабря 2017 г. № 239. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. М.: ФСТЭК России, 2017.

7. Методический документ. Меры защиты информации в государственных информационных системах: утв. ФСТЭК России 11 февраля 2014 г. М.: ФСТЭК России, 2014.

8. ГОСТ Р 59548-2022. Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации. М.: Российский институт стандартизации, 2022.

9. Любименко Дмитрий Анатольевич Разработка методики тестирования на уязвимости сертифицированного межсетевого экрана для защиты объектов критической информационной инфраструктуры // I-methods. 2024. №1. URL: https://cyberleninka.ru/article/n/razrabotka-metodiki-testirovaniya-na-uyazvimosti-sertifitsirovannogo-mezhsetevogo-ekrana-dlya-zaschity-obektov-kriticheskoy (дата обращения: 12.05.2026).

10. Mhaskar N., Alabbad M., Khedri R. A formal approach to network segmentation //Computers & Security. – 2021. – Т. 103. – С. 102162.

11. Togay C. et al. A firewall policy anomaly detection framework for reliable network security //IEEE Transactions on Reliability. – 2021. – Т. 71. – №. 1. – С. 339-347.

12. Go H., Kim T. Linux Firewall Analysis Based on Nftables //IEMEK Journal of Embedded Systems and Applications. – 2025. – Т. 20. – №. 4. – С. 217-228.

13. Netfilter Project. The netfilter.org nftables project [Электронный ресурс]. 2026. URL: https://www.netfilter.org/projects/nftables/index.html (дата обращения 13.05.2026).

14. Atanasov I. From firewall to ai: Strengthening linux server security //Science, Engineering and Education. – 2024. – Т. 9. – №. 1. – С. 3-12.

15. Firewalld project. Firewalld Documentation [Электронный ресурс]. 2026. URL: https://firewalld.org/documentation/ (дата обращения 13.05.2026).

16. Уймин, А. Г. Цифровые двойники сетевых инфраструктур: точность, методы и практические решения / А. Г. Уймин // Радиотехнические и телекоммуникационные системы. – 2023. – № 3(51). – С. 44-52. – DOI 10.24412/2221-2574-2023-3-44-52. – EDN QUSITK.

17. Федеральный закон от 26 июля 2017 г. № 187-ФЗ. О безопасности критической информационной инфраструктуры Российской Федерации // Собрание законодательства Российской Федерации. 2017. № 31, ст. 4736.