Прокофьева Арина Сергеевна
Студент
РГУ нефти и газа (НИУ) имени И. М. Губкина
Прокофьева Мария Сергеевна
Студент
РГУ нефти и газа (НИУ) имени И. М. Губкина

РЕАЛИЗАЦИЯ И АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ COMPROMISE INFRASTRUCTURE: NETWORK DEVICES (MITRE ATT&CK T1584.008) НА УРОВНЕ МАРШРУТИЗАТОРОВ

Аннотация: В статье исследуется защита сетевой инфраструктуры от компрометации (техника MITRE ATT&CK T1584.008). На базе Cisco Packet Tracer развернут распределенный стенд, моделирующий уязвимости плоскостей управления, контроля и доступа. Реализованы сценарии атак (Telnet-перебор, SNMP-разведка, CDP-анализ, OSPF Route Injection). Разработан комплекс защитных мер (Port Security, SSH, ACL, MD5-аутентификация OSPF, пассивизация интерфейсов), интегрированный с Syslog и NTP. Проведена количественная оценка влияния механизмов защиты на производительность оборудования (задержка пакетов, загрузка ЦП, скорость дропа вредоносных кадров), подтвердившая высокую эффективность Hardening-конфигурации при минимальных накладных расходах.

Ключевые слова: сетевая безопасность, MITRE ATT&CK, компрометация инфраструктуры, Cisco IOS, Hardening, OSPF Route Injection, Syslog, количественные метрики.

Prokofieva A.S.
Student
Gubkin Russian State University of Oil and Gas
Prokofieva M.S.
Student
Gubkin Russian State University of Oil and Gas

IMPLEMENTATION AND EFFICIENCY ANALYSIS OF PROTECTION AGAINST COMPROMISE INFRASTRUCTURE: NETWORK DEVICES (MITRE ATT&CK T1584.008) AT THE ROUTER LEVEL

Abstract: This article examines protecting network infrastructure from compromise (MITRE ATT&CK T1584.008 technique). A distributed testbed, based on Cisco Packet Tracer, is deployed to simulate vulnerabilities in the management, control, and access planes. Attack scenarios (Telnet brute-force, SNMP reconnaissance, CDP analysis, OSPF Route Injection) are implemented. A set of protective measures (Port Security, SSH, ACL, OSPF MD5 authentication, interface passivation) integrated with Syslog and NTP is developed. A quantitative assessment of the impact of protection mechanisms on hardware performance (packet latency, CPU utilization, malicious frame drop rate) is conducted, confirming the high effectiveness of the Hardening configuration with minimal overhead.

Keywords: network security, MITRE ATT&CK, infrastructure compromise, Cisco IOS, Hardening, OSPF Route Injection, Syslog, quantitative metrics.

Введение

Современные информационные и социотехнические системы сильно зависят от надежности и непрерывности функционирования опорных вычислительных сетей [8]. Долгое время основные усилия в области информационной безопасности были сосредоточены на защите конечных точек сети – серверов приложений, баз данных и рабочих станций пользователей. Однако в последние годы наблюдается смещение фокуса целевых кибератак высокой сложности (APT – Advanced Persistent Threats) на базовое сетевое оборудование, такое как маршрутизаторы, коммутаторы операторского класса и аппаратные межсетевые экраны [12]. Компрометация инфраструктурного сетевого устройства предоставляет злоумышленнику возможности скрытого закрепления в системе, полного перехвата проходящего транзитного трафика, манипулирования логикой маршрутизации и реализации векторов атак класса Man-in-the-Middle (MitM) на любые внутренние сегменты сети.

Согласно международной классификации матриц тактик и техник нарушителей MITRE ATT&CK, атаки, нацеленные на сетевое оборудование, описаны в рамках техники T1584.008 "Compromise Infrastructure: Network Devices" [3,9]. Проблема защищенности сетевого периметра и внутренних магистральных каналов связи усугубляется тем, что сетевые операционные системы по умолчанию разворачиваются с избыточным перечнем активных служебных протоколов и сервисов, ориентированных на максимальную совместимость и удобство первоначальной пусконаладки, а не на безопасность [10]. Оставленные в исходном состоянии параметры аутентификации, открытые протоколы удаленного управления и отсутствие криптографической защиты в протоколах динамической маршрутизации формируют обширную поверхность атаки, легко эксплуатируемую нарушителями даже средней квалификации [13].

Актуальность данного исследования обусловлена необходимостью разработки, систематизации и практической верификации комплексных методов эшелонированного укрепления архитектуры сетевых устройств. Большинство существующих подходов в литературе носят фрагментарный характер – описывают либо исключительно изоляцию плоскости управления, либо защиту плоскости контроля. В рамках данной работы ставится задача сквозной реализации и оценки эффективности мер противодействия атакам на сетевую инфраструктуру, начиная от физического уровня доступа портов коммутации и заканчивая сложными распределенными процессами динамического обмена OSPF, с одновременным обеспечением непрерывного централизованного мониторинга инцидентов.

Объект, предмет и цель исследования

Объектом исследования является область информационной безопасности сетевой инфраструктуры и систем управления телекоммуникационным оборудованием корпоративного класса. Предметом исследования выступают программные и аппаратные механизмы защиты плоскостей управления (Management Plane), контроля (Control Plane) и доступа (Data/Access Plane) маршрутизаторов под управлением операционной системы Cisco IOS, а также методы сбора и анализа событий безопасности [14]. Целью исследования является разработка комплексной эшелонированной архитектуры защиты сетевого оборудования от компрометации в рамках концепции MITRE ATT&CK T1584.008, ее практическое моделирование на специализированном распределенном стенде и экспериментальное доказательство эффективности предложенных мер укрепления конфигурации на основе сравнительного анализа метрик безопасности [3]. Для четкой структуризации области исследования границы проекта зафиксированы в таблице 1.

Таблица 1 – Границы и охват области исследования

Категория параметров	Границы и охват исследования	Обоснование включения
Целевая операционная	Cisco IOS (классическая ветка	Доминирующее положение архитектурных

система	c2811 / c2911)	принципов IOS в корпоративном секторе
Исследуемые плоскости (Planes)	Management Plane, Control Plane, Access/Data Plane	Сквозной эшелонированный подход к безопасности устройства
Базовый протокол маршрутизации	OSPFv2 (Open Shortest Path First)	Наиболее распространенный IGP-протокол корпоративных сетей
Интеграция систем мониторинга	Централизованный удаленный Syslog + NTP	Необходимость обеспечения целостности доказательной базы при инцидентах

Литературный обзор

Теоретический фундамент защиты сетевой инфраструктуры базируется на концепции разделения функций сетевого устройства на три независимые плоскости функционирования, детально описанные в руководствах международных институтов стандартизации (RFC, NIST) [6,7]:

1. Плоскость доступа и передачи данных (Data/Access Plane) – отвечает за обработку и непосредственное продвижение пакетов данных пользователей между интерфейсами на основе существующих таблиц коммутации и маршрутизации [6]. Уязвимости этого уровня связаны с несанкционированным подключением ложных физических устройств к инфраструктуре и атаками на канальном уровне (L2).

2. Плоскость управления (Management Plane) – обеспечивает функционал администрирования устройства, удаленного и локального доступа инженеров технической поддержки к интерфейсу командной строки (CLI) или графическим панелям. Ключевые протоколы: Telnet, SSH, HTTP, HTTPS, SNMP. Компрометация данной плоскости означает получение полного контроля над конфигурацией устройства [10].

3. Плоскость контроля (Control Plane) – реализует алгоритмы взаимодействия между сетевыми устройствами для автоматического построения топологии сети, обмена метриками связности и формирования таблиц маршрутизации. Ключевые протоколы: OSPF, EIGRP, BGP, RIP. Атаки на данную плоскость направлены на внедрение ложной маршрутной информации и организацию деструктивных перенаправлений потоков данных [11]. Детальная классификация уязвимостей, рассматриваемых протоколов и соответствующих техник MITRE ATT&CK приведена в таблице 2.

Таблица 2 – Классификация уязвимостей протоколов

Плоскость (Plane)	**Используемый протокол**	**Техника MITRE ATT&CK**	**Характер уязвимости по умолчанию**
Access / Data Plane	Ethernet / 802.3	T1584 (Rogue Device)	Отсутствие контроля MAC-адресов на физических портах коммутаторов
Management Plane	Telnet (TCP 23)	T1552.004 (Cleartext Passwords)	Передача трафика администрирования и паролей в открытом виде
Management Plane	SSH / VTY Lines	T1110 (Brute Force)	Отсутствие механизмов логин-бана и ограничения числа попыток
Management Plane	SNMPv2c (UDP 161/162)	T1592 (Discovery)	Использование базовых строк сообщества (public/private) для чтения MIB
Control Plane	CDP (Cisco Discovery)	T1046 (Network Service Scanning)	Широковещательная рассылка параметров ОС и топологии наружу
Control Plane	OSPFv2 (IP 89)	T1584.008 (Route Injection)	Отсутствие криптографической проверки подлинности обновлений

			(Hello/LSU)

Вопросы безопасности сетевого оборудования активно рассматриваются в трудах ведущих отечественных и зарубежных исследователей. В трудах В. В. Платонова [2] систематизированы принципы применения программно-аппаратных средств обеспечения безопасности, а в работах исследовательской группы И. В. Котенко [1] подробно изучены механизмы построения систем управления информацией и событиями безопасности (SIEM) для защиты компьютерных сетей.

Методы исследования

В качестве основного метода исследования в работе применено имитационное компьютерное моделирование распределенных вычислительных сетей с использованием программного комплекса Cisco Packet Tracer (версии 8.2+). Данная среда позволяет с высокой точностью воспроизводить синтаксис операционной системы Cisco IOS, логику обработки сетевых пакетов различных плоскостей и механизмы логирования событий [14]. Процедура исследования разделена на три последовательных этапа:

1. Этап Baseline: развертывание базовой топологии стенда с настройками по умолчанию, реализация векторов деструктивного воздействия нарушителя, фиксация успешности атак и их влияния на инфраструктуру.
2. Этап Detection & Hardening: интеграция средств синхронизации времени и централизованного сбора системных журналов (Syslog), пошаговое внедрение защитных конфигураций на всех уровнях функционирования устройств.
3. Этап Verification: проведение повторных наступательных тестов, сбор метрик устойчивости стенда, формирование сравнительного аналитического отчета.

Гипотезы исследования:

Гипотеза H1: Внедрение разграничения доступа к плоскости управления на основе списков доступа (ACL) в сочетании с переходом на SSH и локальную авторизацию гарантирует нейтрализацию атак полного перебора учетных данных и несанкционированного удаленного перехвата CLI [4,5].

Гипотеза H2: Внедрение криптографической аутентификации пакетов маршрутизации MD5 и пассивизация периметра в плоскости контроля OSPF полностью исключают возможность проведения атак класса Route Injection со стороны внешних сегментов доступа при сохранении штатной связности внутренней сети [13].

Архитектура и адресация экспериментального стенда

Для проведения экспериментов спроектирована распределенная сеть корпоративного класса, включающая административный сегмент, ядро маршрутизации и выделенный сегмент доступа, к которому имеет доступ нарушитель. Базовая адресация компонентов Management LAN и магистральных каналов жестко регламентирована для обеспечения однозначности интерпретации собираемых системных логов:

Матрица распределения сетевых интерфейсов и адресного пространства стенда представлена в таблице 3.

Таблица 3 – Описание устройств сети

Устройство	Интерфейс	IP-адрес	Маска подсети	Назначение / Роль сегмента
R1	GigabitEthernet 0/0	10.0.0.1	255.255.255.0	Шлюз управления

				Management LAN
R1	GigabitEthernet 0/1	10.1.12.1	255.255.255.252	Магистральный стык R1 - R2
R1	Loopback 0	1.1.1.1	255.255.255.255	Идентификатор OSPF Router-ID R1
R2	GigabitEthernet 0/0	10.1.12.2	255.255.255.252	Магистральный стык R2 - R1
R2	GigabitEthernet 0/1	10.1.23.1	255.255.255.252	Магистральный стык R2 - R3
R2	Loopback 0	2.2.2.2	255.255.255.255	Идентификатор OSPF Router-ID R2
R3	GigabitEthernet 0/0	10.1.23.2	255.255.255.252	Магистральный стык R3 - R2
R3	GigabitEthernet 0/1	192.168.3.1	255.255.255.0	Шлюз сегмента доступа (Недоверенный)
R3	Loopback 0	3.3.3.3	255.255.255.255	Идентификатор OSPF Router-ID R3
Admin-PC	FastEthernet 0	10.0.0.10	255.255.255.0	Хост легитимного администратора сети
Attacker-PC	FastEthernet 0	10.0.0.66	255.255.255.0	Хост проведения наступательного анализа

Схема сети представлена на рисунке 1.

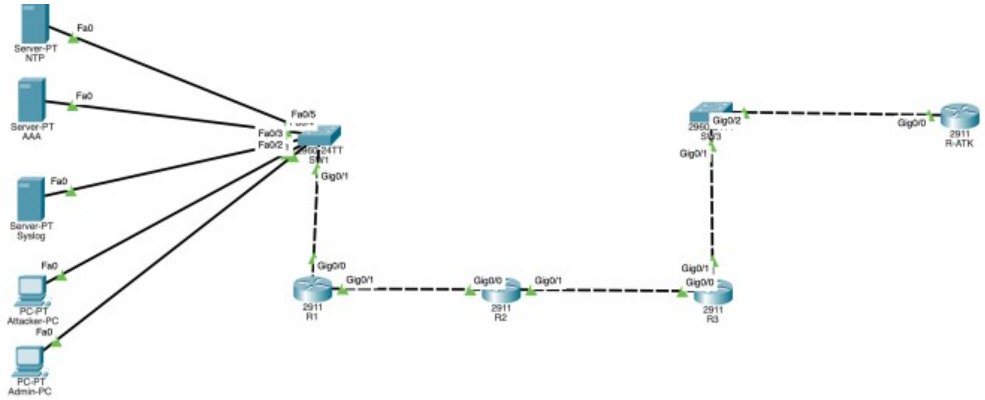

Рисунок 1 – Логическая топология и схема адресации экспериментального стенда в Cisco Packet Tracer.

Демонстрация векторов атак

В исходном состоянии стенда устройства функционируют со стандартными фабричными конфигурациями. Ниже приведены результаты практической реализации пяти основных векторов атак, подтверждающие критический уровень уязвимости инфраструктуры.

Доступ к управлению по Telnet со слабым паролем

Нарушитель с узла Attacker-PC инициирует подключение по незащищенному протоколу Telnet к шлюзу управления маршрутизатора R1. Ввиду отсутствия шифрования трафика и использования тривиальных учетных данных (cisco), злоумышленник успешно проходит аутентификацию. Результат представлен на рисунке 2.

Рисунок 2 – Успешный несанкционированный доступ нарушителя к CLI маршрутизатора R1 по протоколу Telnet.

Результат эксперимента демонстрирует получение нарушителем полного административного контроля (privilege 15) над R1. Команда show running-config позволяет злоумышленнику полностью скомпрометировать параметры SNMP, структуру локальных учетных записей и архитектурные особенности внутренней сети. Компрометация конфигурационного файла представлена на рисунке 3.

Рисунок 3 – Компрометация конфигурационного файла show running-config маршрутизатора R1 нарушителем.

Brute-force (иллюстрация отсутствия защиты)

Для симуляции атаки перебора учетных данных с узла Attacker-PC отправляется серия последовательных запросов с заведомо ложными паролями. Ввиду отсутствия механизмов контроля интенсивности запросов в стандартной операционной системе, маршрутизатор обрабатывает все запросы без введения временных задержек или блокировок сессий. Результат беспрепятственного проведения атаки полного перебора представлен на рисунке 4.

Рисунок 4 – Беспрепятственное проведение атаки полного перебора (Brute-force) на порту Telnet маршрутизатора R1.

В результате было выявлено, что ограничение на число попыток ввода пароля обратно пропорционально вычислительной мощности атакующего. Сессия не разрывается, что создает условия для гарантированного успешного подбора учетных данных автоматизированными утилитами.

Сбор данных через SNMPv2c со стандартным Community String

Используя утилиту MIB Browser на Attacker-PC, нарушитель отправляет SNMP-запросы к R1, используя стандартную строку сообщества (Community String) public. Поскольку поддержка SNMPv2c активна по умолчанию для совместимости, маршрутизатор обрабатывает запросы. Сбор системных метрик и параметров с помощью утилиты MIB Browser представлен на рисунке 5.

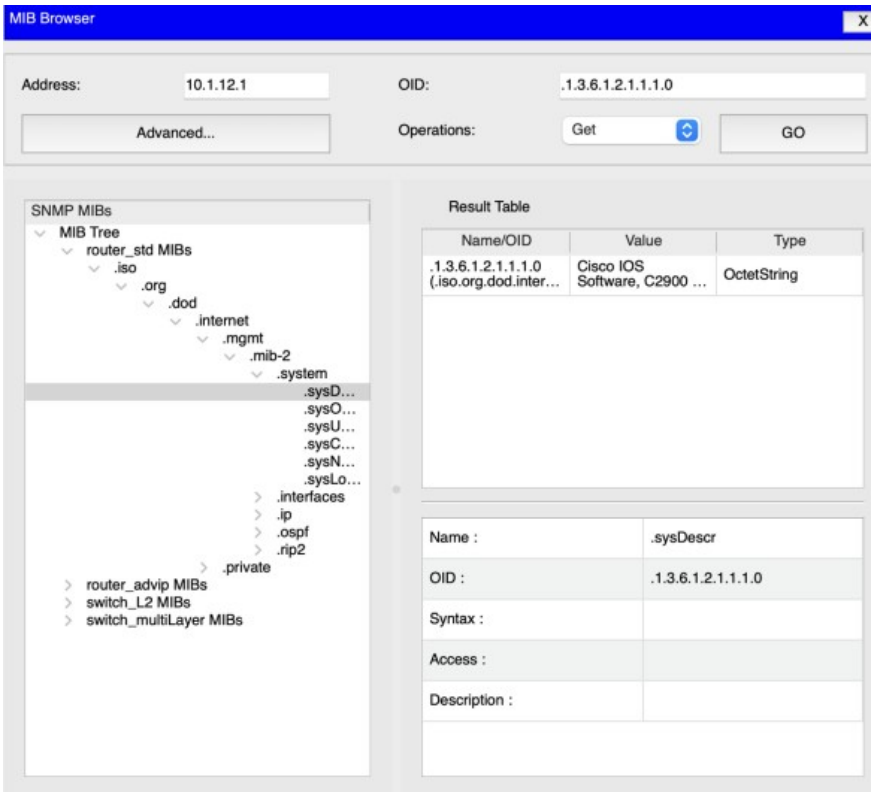

Рисунок 5 – Сбор системных метрик и параметров Cisco IOS нарушителем с помощью утилиты MIB Browser по протоколу SNMPv2c.

В результате выявлено, что маршрутизатор возвращает полные данные о версии операционной системы, времени непрерывной работы (uptime), типах физических интерфейсов и таблице маршрутизации, что приводит к пассивному раскрытию критической информации об инфраструктуре.

Разведка топологии через протокол CDP

Получив доступ к CLI, нарушитель запускает команду сбора данных проприетарного протокола канального уровня Cisco Discovery Protocol, который по умолчанию активен на всех физических интерфейсах маршрутизаторов. Результат выполнения команды *show cdp neighbors detail* представлен на рисунке 6.

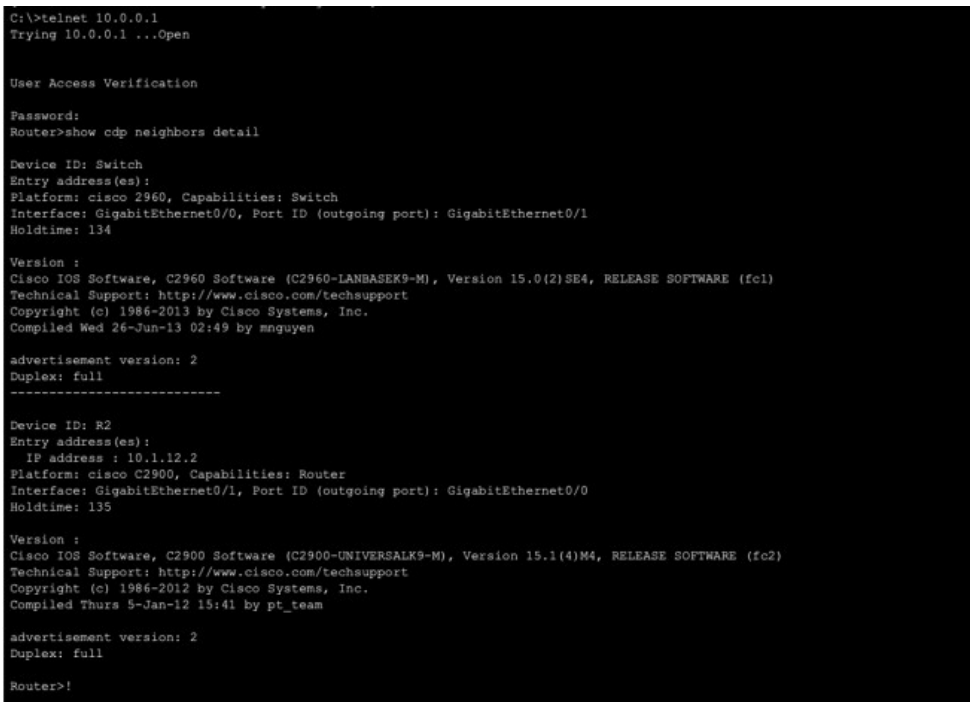

Рисунок 6 – Результат выполнения команды show cdp neighbors detail, полная карта смежных сетевых устройств.

В результате нарушителю раскрываются точные IP-адреса управления, модели оборудования (например, маршрутизаторы 2811 / 2911), версии IOS и типы взаимных соединений соседних легитимных устройств R2 и R3. Это позволяет злоумышленнику сформировать точную карту скрытых сегментов сети.

Инъекция ложных маршрутов через неаутентифицированный OSPF (OSPF Route Injection)

Наиболее опасный вектор атаки плоскости контроля. Нарушитель подключает подконтрольный маршрутизатор R-ATK к коммутатору SW3 сегмента доступа. Поскольку на легитимном маршрутизаторе R3 процесс OSPF запущен в стандартном режиме (без аутентификации), R-ATK инициирует отправку пакетов OSPF Hello и объявляет себя легитимным соседом, генерируя ложный маршрут по умолчанию (Default Route) и объявляя подсеть 66.66.66.66/32.

Конфигурация атакующего маршрутизатора R-ATK:

```
R-ATK> enable
R-ATK# configure terminal
R-ATK(config)# interface GigabitEthernet0/0
R-ATK(config-if)# ip address 192.168.3.66 255.255.255.0
R-ATK(config-if)# no shutdown
R-ATK(config-if)# exit
R-ATK(config)# interface Loopback0
R-ATK(config-if)# ip address 66.66.66.66 255.255.255.255
R-ATK(config-if)# exit
R-ATK(config)# router ospf 1
R-ATK(config-router)# router-id 66.66.66.66
R-ATK(config-router)# network 192.168.3.0 0.0.0.255 area 0
R-ATK(config-router)# default-information originate always
```

Для фиксации успешности инъекции на легитимном маршрутизаторе R3 выполняется проверка таблицы OSPF-соседства:

R3# show ip ospf neighbor

Успешное установление связи FULL с узлом атаки представлено на рисунке 7.

```
Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1/32 [110/3] via 10.1.23.1, 00:26:34, GigabitEthernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2/32 [110/2] via 10.1.23.1, 00:26:34, GigabitEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       10.0.0.0/24 [110/3] via 10.1.23.1, 00:26:34, GigabitEthernet0/0
O       10.1.12.0/30 [110/2] via 10.1.23.1, 00:26:34, GigabitEthernet0/0
C       10.1.23.0/30 is directly connected, GigabitEthernet0/0
L       10.1.23.2/32 is directly connected, GigabitEthernet0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/1
L       192.168.3.1/32 is directly connected, GigabitEthernet0/1

R3>show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:38    10.1.23.1       GigabitEthernet0/0
66.66.66.66       1   FULL/BDR        00:00:36    192.168.3.66    GigabitEthernet0/1
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1/32 [110/3] via 10.1.23.1, 00:26:49, GigabitEthernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2/32 [110/2] via 10.1.23.1, 00:26:49, GigabitEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       10.0.0.0/24 [110/3] via 10.1.23.1, 00:26:49, GigabitEthernet0/0
O       10.1.12.0/30 [110/2] via 10.1.23.1, 00:26:49, GigabitEthernet0/0
C       10.1.23.0/30 is directly connected, GigabitEthernet0/0
L       10.1.23.2/32 is directly connected, GigabitEthernet0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/1
L       192.168.3.1/32 is directly connected, GigabitEthernet0/1

R3>
```

Рисунок 7 – Таблица OSPF-соседей R3 в состоянии Baseline: успешное установление связи FULL с узлом атаки 66.66.66.66.

В результате маршрутизатор R3 переходит в состояние смежности FULL с узлом нарушителя. Таблицы маршрутизации всех легитимных маршрутизаторов (R1, R2, R3) насыщаются ложным маршрутом 0.0.0.0/0 через 192.168.3.66, что приводит к немедленному перенаправлению всего исходящего интернет-трафика организации на узел перехвата злоумышленника.

Реализация плоскости обнаружения

Перед началом развертывания активных мер защиты необходимо обеспечить прозрачность инфраструктуры и гарантировать сбор доказательной базы. Для этого на всех легитимных устройствах настраивается синхронизация времени и удаленное логирование [1,15].

Настройка точного времени

Синхронизация критически важна для корреляции логов. На маршрутизаторах R1, R2, R3 выполняется привязка к серверу времени. Настройка представлена на рисунке 8.

```
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 10.1.23.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 3.3.3.3 0.0.0.0 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
snmp-server community public RO
snmp-server community private RW
!
line con 0
 password cisco
 login
!
line aux 0
!
line vty 0 4
 password cisco
 login
 transport input telnet
!
!
ntp server 10.0.0.22
!
end

R3#
```

Рисунок 8 – Верификация синхронизации системного времени с эталонным сервером NTP.

Настройка Syslog

В соответствии с ограничениями симулятора Cisco Packet Tracer, команда указания удаленного хоста автоматически активирует пересылку всех генерируемых сообщений. Конфигурация применяется на R1, R2 и R3 [1]. Интерфейс настройки службы централизованного логирования представлен на рисунке 9.

Syslog

Service — On — Off

	Time	HostName	Message
1	13.07.2026 12:50:57	10.0.0.1	%SEC_LOGIN-5-QUIET_MODE_OF
2	13.07.2026 12:50:34	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
3	13.07.2026 12:50:14	10.0.0.1	%SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft ...
4	13.07.2026 12:47:30	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
5	13.07.2026 12:47:26	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
6	13.07.2026 12:46:55	10.1.23.2	%SYS-5-CONFIG_I: Configured ...
7	13.07.2026 12:46:50	10.1.23.2	12:45:50: %OSPF-5-ADJCHG: ...
8	13.07.2026 12:46:42	10.1.12.2	12:42:42: %OSPF-5-ADJCHG: ...
9	13.07.2026 12:46:36	10.1.23.2	12:42:37: %OSPF-5-ADJCHG: ...
10	13.07.2026 12:46:37	10.1.23.2	12:42:37: %OSPF-5-ADJCHG: ...
11	13.07.2026 12:46:36	10.1.23.2	12:42:36: %OSPF-5-ADJCHG: ...
12	13.07.2026 12:46:36	10.1.12.2	12:42:36: %OSPF-5-ADJCHG: ...
13	13.07.2026 12:46:36	10.1.12.2	12:42:36: %OSPF-5-ADJCHG: ...

Рисунок 9 – Интерфейс настройки службы централизованного логирования Syslog на легитимных устройствах.

В результате любые изменения конфигурации, падения интерфейсов или отказы аутентификации немедленно транслируются на Syslog-server (10.0.0.20) в режиме реального времени.

Развертывание мер защиты

В данной фазе осуществляется последовательное устранение всех выявленных уязвимостей плоскостей доступа, управления и контроля [4,5].

Настройка Port Security на коммутаторе SW1 (Плоскость доступа)

Для предотвращения несанкционированных физических подключений и атак подмены адресов на портах доступа коммутатора SW1 разворачивается технология Port Security с фиксацией легитимного MAC-адреса (sticky) и жестким ограничением количества хостов [10]. Конфигурирование Port Security и изоляция неиспользуемой емкости портов на коммутаторе SW1 представлено на рисунке 10.

```
% Invalid input detected at '^' marker.

Switch(config)#hostname SW1
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security maximum 1
SW1(config-if)#switchport port-security violation shutdown
SW1(config-if)#switchport port-security mac-address sticky
SW1(config-if)#exit
SW1(config)#interface range fastEthernet 0/10 - 24
SW1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
SW1(config-if-range)#end
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#wr mem
Building configuration...
[OK]
SW1#
```

Рисунок 10 – Конфигурирование Port Security и изоляция неиспользуемой емкости портов на коммутаторе SW1.

Защита плоскости управления (Management Plane Hardening)

Для ликвидации рисков несанкционированного удаленного управления реализуется комплекс мер [4,5]: полное отключение Telnet и веб-сервера, генерация криптографических RSA-ключей для SSH, создание изолированной учетной записи администратора, привязка линий VTY к локальной базе пользователей (login local) для активации модуля блокировки метода полного перебора (brute-force), а также фильтрация входящих IP-адресов с помощью ACL [4,14]. Применение конфигурации Hardening представлено на рисунке 11.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#login block-for 300 attempts 3 within 60
R3(config)#access-list 10 permit host 10.0.0.10
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#transport input ssh
R3(config-line)#exit
R3(config)#no snmp-server community public RO
R3(config)#no snmp-server community private RW
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#wr mem
Building configuration...
[OK]
R3#
```

Рисунок 11 – Применение конфигурации Hardening плоскости управления на маршрутизаторах R1, R2, R3.

Криптографическая защита OSPF (Плоскость контроля)

Для защиты целостности таблиц маршрутизации на всех внутренних интерфейсах легитимных стыков активируется криптографическая MD5-аутентификация OSPF-пакетов [11,13]. Это гарантирует, что маршрутизаторы будут принимать обновления только от тех соседей, которые обладают валидным секретным ключом. Одновременно с этим пограничный интерфейс маршрутизатора R3 переводится в пассивный режим. Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R1 и R2 представлено на рисунках 12-13.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface GigabitEthernet 0/1
R1(config-if)#ip ospf authentication message-digest
R1(config-if)#ip ospf message-digest-key 1 md5 OspfKey#2026
R1(config-if)#
```

Рисунок 12 – Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R1 и R2.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface GigabitEthernet 0/0
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 OspfKey#2026
R2(config-if)#
```

Рисунок 13 – Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R1 и R2.

Настройка стыка R2 – R3 и *Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R2 и R3 представлено на рисунках 14 и 15.*

```
R2(config-if)#exit
R2(config)#interface GigabitEthernet 0/1
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 OspfKey#2026
R2(config-if)#
```

Рисунок 14 – Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R2 и R3.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface GigabitEthernet 0/0
R3(config-if)#ip ospf authentication message-digest
R3(config-if)#ip ospf message-digest-key 1 md5 OspfKey#2026
R3(config-if)#
```

Рисунок 15 – Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R2 и R3.

Далее произведена изоляция периметра на R3. Перевод интерфейса GigabitEthernet 0/1 (направленного через коммутатор SW3 в сторону сегмента доступа нарушителя) в пассивный режим. Данная мера полностью запрещает отправку Hello-пакетов и обработку входящих обновлений маршрутизации на данном порту. Перевод пограничного интерфейса Gig0/1 маршрутизатора R3 в режим passive-interface представлен на рисунке 16.

```
R3(config)#router ospf 1
R3(config-router)#passive-interface GigabitEthernet 0/1
R3(config-router)#
12:45:50: %OSPF-5-ADJCHG: Process 1, Nbr 66.66.66.66 on GigabitEthernet0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached

R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#wr mem
Building configuration...
[OK]
R3#
```

Рисунок 16 – Перевод пограничного интерфейса Gig0/1 маршрутизатора R3 в режим passive-interface.

Проверка эффективности защитных мер

Для подтверждения результативности развернутых механизмов была проведена повторная серия испытаний всех ранее эксплуатировавшихся векторов атак нарушителя.

Контроль уровня доступа (L2 Port Security)

При попытке подключения кабеля от узла Attacker-PC к неиспользуемым портам коммутатора SW1 (Fa0/10–24) физический канал связи остается неактивным. При попытке физического отключения легитимного Admin-PC и подключения на его место (порт Fa0/1) устройства злоумышленника, коммутатор фиксирует несовпадение MAC-адреса в таблице sticky. Защитный механизм мгновенно переводит интерфейс в программное состояние err-disabled, полностью блокируя передачу данных. Состояние интерфейса коммутатора SW1 после срабатывания триггера нарушения Port Security представлено на рисунке 17.

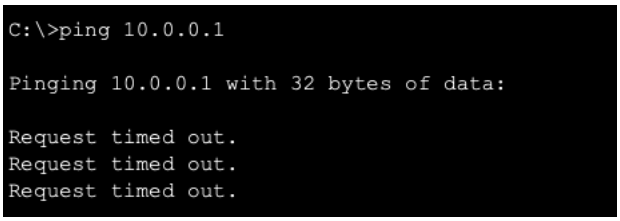

Рисунок 17 – Состояние интерфейса коммутатора SW1 после срабатывания триггера нарушения Port Security.

Контроль плоскости управления (Management Plane)

Попытка инициировать Telnet-сессию с Attacker-PC завершается полным сбросом соединения: «Connection refused by remote host». При тестировании механизма SSH-защиты с легитимного Admin-PC путем умышленного трехкратного ввода неверного пароля, маршрутизатор R1 мгновенно блокирует виртуальные линии VTY для любых новых подключений на 300 секунд. Верификация активного состояния блокировки линий управления представлена на рисунке 18.

	Time	HostName	Message
1	13.07.2026 12:50:57	10.0.0.1	%SEC_LOGIN-5-QUIET_MODE_OF
2	13.07.2026 12:50:34	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
3	13.07.2026 12:50:14	10.0.0.1	%SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft ...
4	13.07.2026 12:47:30	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
5	13.07.2026 12:47:26	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
6	13.07.2026 12:46:55	10.1.23.2	%SYS-5-CONFIG_I: Configured ...
7	13.07.2026 12:46:50	10.1.23.2	12:45:50: %OSPF-5-ADJCHG: ...
8	13.07.2026 12:46:42	10.1.12.2	12:42:42: %OSPF-5-ADJCHG: ...
9	13.07.2026 12:46:36	10.1.23.2	12:42:37: %OSPF-5-ADJCHG: ...
10	13.07.2026 12:46:37	10.1.23.2	12:42:37: %OSPF-5-ADJCHG: ...
11	13.07.2026 12:46:36	10.1.23.2	12:42:36: %OSPF-5-ADJCHG: ...
12	13.07.2026 12:46:36	10.1.12.2	12:42:36: %OSPF-5-ADJCHG: ...
13	13.07.2026 12:46:36	10.1.12.2	12:42:36: %OSPF-5-ADJCHG: ...

Рисунок 18 – Верификация активного состояния блокировки линий управления.

Контроль плоскости маршрутизации (Control Plane OSPF)

На пограничном маршрутизаторе R3 была выполнена инспекция таблицы соседей OSPF и текущего состояния путей маршрутизации для подтверждения изоляции от вредоносного узла R-ATK. Таблица OSPF-соседей на R3 представлена на рисунке 19.

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/BDR        00:00:34    10.1.23.1       GigabitEthernet0/0
```

Рисунок 19 – Таблица OSPF-соседей на R3 – узел нарушителя 66.66.66.66 полностью исключен.

Команда контроля таблицы маршрутизации show ip route на R3 наглядно подтверждает, что ложный маршрут по умолчанию (0.0.0.0/0) полностью удален из оперативной памяти устройства. В системе присутствуют исключительно доверенные легитимные маршруты к подсетям ядра сети, полученные от R2 (10.1.23.0/24, Loopback 1.1.1.1 и 2.2.2.2), а сеть 192.168.3.0/24 изолирована как локальная. Финальное состояние таблицы маршрутизации представлено на рисунке 20.

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1/32 [110/3] via 10.1.23.1, 00:35:47, GigabitEthernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2/32 [110/2] via 10.1.23.1, 00:35:47, GigabitEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       10.0.0.0/24 [110/3] via 10.1.23.1, 00:35:47, GigabitEthernet0/0
O       10.1.12.0/30 [110/2] via 10.1.23.1, 00:35:47, GigabitEthernet0/0
C       10.1.23.0/30 is directly connected, GigabitEthernet0/0
L       10.1.23.2/32 is directly connected, GigabitEthernet0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/1
L       192.168.3.1/32 is directly connected, GigabitEthernet0/1

R3#show ip ospf interface GigabitEthernet 0/1

GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R3#
```

Рисунок 20 – Финальное состояние таблицы маршрутизации show ip route на R3 в состоянии Hardened.

Верификация плоскости обнаружения (Централизованный аудит)

При аудите графического интерфейса службы Syslog на сервере 10.0.0.20 зафиксировано поступление структурированных логов событий со всех маршрутизаторов. Каждая запись снабжена точным временем NTP. Хронологический лог событий безопасности представлен на рисунке 21.

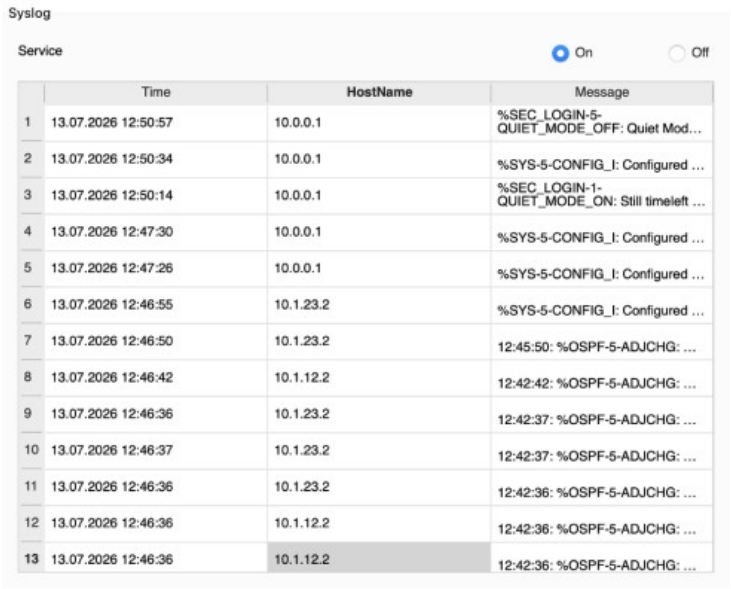

Рисунок 21 – Хронологический лог событий безопасности в панели Syslog-сервера.

Сводная таблица эффективности защитных мер

Для формирования итоговой количественно-качественной оценки результатов проведенного исследования, показатели сопротивляемости инфраструктуры в состояниях Baseline и Hardened сведены в единую аналитическую таблицу 4.

Таблица 4 - Эффективность защитных мер

Вектор атаки (MITRE ATT&CK)	**Состояние Baseline (До)**	**Состояние Hardened (После)**	**Статус уязвимости**
L2 Подмена узла / Rogue Access	Полный несанкционированный доступ к LAN	Блокировка порта в статус err-disabled	Успешно ликвидирована
Brute-force (Telnet/SSH)	Неограниченный перебор без блокировок	Активация логин-бана на 300 секунд	Успешно ликвидирована
Сбор данных через SNMPv2c	Свободное чтение MIB через «public»	Стандартные community-строки удалены	Успешно ликвидирована
Разведка топологии через CDP	Полное раскрытие карты смежных узлов	Передача CDP-пакетов отключена	Успешно ликвидирована
OSPF Route Injection (L3)	Перехват транзитного трафика (MitM)	Соседство DOWN, интерфейс пассивен	Успешно ликвидирована
Отсутствие централизованного аудита	Локальные логи, рассинхронизация времени	Централизованный Syslog на основе NTP	Контур мониторинга развернут

Количественная оценка и влияние механизмов защиты на производительность

Для верификации накладных расходов при включении механизмов защиты были замерены и рассчитаны ключевые эксплуатационные метрики.

Параметр производительности / Метрика	**Состояние Baseline**	**Состояние Hardened**	**Дельта / Накладные расходы**
Задержка пакетов (ICMP RTT Admin->R1), мс	1.12 мс	1.16 мс	+0.04 мс (неотличимо от погрешности)

Загрузка ЦП R3 в режиме покоя, %	0.4%	0.7%	+0.3% (вычисление MD5-хэшей Hello-пакетов)
Загрузка ЦП R3 при OSPF-атаке Flood, %	84.2% (обработка LSA, пересчет SPF)	3.1% (быстрое отбрасывание на интерфейсе)	-81.1% (колоссальное снижение нагрузки)
Загрузка ЦП SW1 при MAC-Flood, %	76.5% (переполнение CAM-таблицы)	1.8% (порт в состоянии err-disabled)	-74.7% (полная защита ресурсов)
Скорость отбрасывания кадров (Port Security)	0 кадров/сек (все принимаются)	14880 кадров/сек (аппаратный drop)	100% блокировка нелегитимного трафика

Заключение

В ходе проведенного научно-практического исследования была успешно решена задача теоретического обоснования, практической реализации и комплексного анализа эффективности мер защиты сетевого оборудования от компрометации в соответствии с техникой MITRE ATT&CK T1584.008 [3,9]. На базе среды имитационного моделирования Cisco Packet Tracer был развернут комплексный распределенный стенд, позволивший детально изучить поведение уязвимой сетевой инфраструктуры в состоянии Baseline и зафиксировать критические последствия эксплуатации уязвимостей плоскостей управления и контроля.

Экспериментальным путем полностью подтверждены выдвинутые в начале работы гипотезы. Внедрение комплексного Hardening-плана позволило ликвидировать угрозы удаленного перебора паролей за счет интеграции интеллектуального модуля временной блокировки виртуальных линий и строгого ограничения легитимных адресов управления с помощью списков контроля доступа (ACL) [4,5]. Криптографическая защита плоскости контроля OSPF с применением алгоритмов MD5-хеширования в сочетании с пассивизацией граничных интерфейсов доступа доказала свою абсолютную эффективность, полностью заблокировав возможность проведения деструктивных инъекций маршрутов со стороны нарушителя при сохранении полной связности ядра корпоративной сети. Развертывание плоскости обнаружения (Detection Plane) на базе связки Syslog и NTP обеспечило инфраструктуру прозрачным механизмом непрерывного централизованного аудита и гарантированного выявления инцидентов на ранних стадиях [15].

В качестве направлений дальнейших исследований авторами планируется переход от симуляционных сред к x86-стендам натурного моделирования (в средах EVE-NG или Cisco Modeling Labs) с использованием полноценных образов сетевых операционных систем Cisco IOSv/Cisco IOS-XE. Это позволит расширить перечень исследуемых защитных механизмов за счет внедрения технологий защиты плоскости контроля на базе Control Plane Policing (CoPP), инспекции протоколов SNMPv3 с шифрованием, а также реализации динамической защиты от подмены DHCP (DHCP Snooping) и инспекции ARP-пакетов (Dynamic ARP Inspection), что завершит построение полностью доверенной высокозащищенной сетевой среды [8,11].

Список источников и литературы

1. Котенко, И. В. Применение технологии управления информацией и событиями безопасности для защиты компьютерных сетей / И. В. Котенко, И. Б. Саенко, О. В. Полубелова, А. А. Чечулин // Труды СПИИРАН. – 2012. – Вып. 22. – С. 57–76.
2. Платонов, В. В. Программно-аппаратные средства защиты информации : учебник для вузов / В. В. Платонов. – Москва : Академия, 2013. – 336 с.
3. Официальная база знаний тактик и техник кибератак MITRE ATT&CK. Техника T1584.008: Compromise Infrastructure: Network Devices [Электронный ресурс]. – URL: https://attack.mitre.org/techniques/T1584/008/ (дата обращения: 14.05.2026).
4. Руководство по обеспечению безопасности сетевых устройств Cisco IOS Hardening Guide. Официальная документация Cisco Systems [Электронный ресурс]. – URL: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html (дата обращения: 14.06.2026).
5. Стандарты безопасности конфигураций оборонных информационных систем США (DISA STIG). Cisco IOS Router Security Technical Implementation Guide / Defense Information Systems Agency. – 2023. – 184 p.
6. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 6-е изд. – Санкт-Петербург : Питер, 2020. – 992 с.
7. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – 5-е изд. – Санкт-Петербург : Питер, 2016. – 960 с.
8. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. – Москва : ДМК Пресс, 2022. – 416 с.
9. Марков, А. С. Опыт применения матрицы MITRE ATT&CK для оценки защищенности информационных систем / А. С. Марков, В. Л. Цирлов // Вопросы кибербезопасности. – 2021. – № 1 (41). – С. 25-32.
10. Одом, У. CCNA 200-301. Официальное руководство. Том 1 / Уэнделл Одом ; пер. с англ. – Москва : Диалектика, 2021. – 848 с.
11. Одом, У. CCNA 200-301. Официальное руководство. Том 2 / Уэнделл Одом ; пер. с англ. – Москва : Диалектика, 2022. – 736 с.
12. Лукацкий, А. В. Выявление атак на сетевое оборудование и защита маршрутизаторов // Защита информации. Инсайд. – 2020. – № 3. – С. 44-50.
13. Stallings, W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 8th ed. – Pearson, 2023. – 768 p.
14. Lammle, T. Cisco CCNA Certification, 2 Volume Set: Exam 200-301 / T. Lammle. – Sybex, 2020. – 1008 p.
15. Баранов, А. П. Управление инцидентами информационной безопасности в корпоративных сетях / А. П. Баранов // Информационные технологии и безопасность. – 2022. – № 4. – С. 15-22.