ISSN 3033-9359
Выпуск 2 (006), 2025

НАУЧНЫЙ ЖУРНАЛ ПРОФЕССИОНАЛИТЕТ

Москва

ПРОФЕССИОНАЛИТЕТ

№ 2 (006), 2025

Научный журнал

Основан в 2023 году

Зарегистрирован федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций

Номер свидетельства ЭЛ № ФС 77-84640

Дата регистрации 01.02.2023

Учредитель:

Уймин А.Г.

Адрес редакции:

Адрес редакции: 115432, г. Москва, ул. 5-я Кожуховская, д. 18, корп. 1, пом. 12.

PROFESSIONALITET

No.2 (006), 2025

Scientific Journal

Founded in 2023

Registered with the Federal Service for Supervision of Communications, Information Technology and Mass Media

Certificate of Registration: EL No. FS 77-84640

Registration Date: 01.02.2023

Founder:

Uymin A.G.

Editorial Office:

Editorial Office Address: Premises 12, 18, Building 1, 5th Kozhukhovskaya St., Moscow, 115432, Russia.

СОДЕРЖАНИЕ

CONTENTS

Рубрика 1. Информатика и информационные процессы

УДК *004.728.4*

М. А. Ольшевская[1]

[1] *ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация*

ПРОВЕРКА РАСШИРЕНИЙ OSPFv3 RFC 8362 ДЛЯ СОВРЕМЕННЫХ СЕТЕЙ НА ОСНОВЕ ECOROUTER, RFC 2328

Аннотация*: В статье представлены результаты экспериментального исследования реализации протокола OSPFv3 в отечественной маршрутизирующей платформе EcoRouterOS Rose версии 3.2.6.2.22240-develop-f748b4f-2025.01.14 на предмет соответствия расширениям стандарта RFC 8362 «OSPFv3 Link State Advertisement Extensibility». Развёрнут изолированный лабораторный стенд из трёх виртуальных маршрутизаторов в треугольной топологии Area 0 в среде эмуляции Proxmox. Проведена валидация соответствия базовым требованиям RFC 2328 и RFC 5340, статистический анализ времени выполнения SPF, а также анализ типов LSA и захвата OSPFv3-трафика в Wireshark. Установлено, что EcoRouterOS Rose полностью соответствует базовым стандартам OSPF, однако не реализует расширения RFC 8362: флаг E-bit не устанавливается, расширенные типы LSA отсутствуют, TLV-формат не реализован. Полученные результаты показывают ограниченную готовность исследованной версии платформы к развёртыванию в сетях, требующих поддержки Segment Routing over IPv6, Flexible Algorithm и Performance-Based Routing. При интерпретации результатов сопоставлялись интервалы Hello/Dead, состав LSDB, флаги Options и время выполнения SPF, что позволило отделить базовую совместимость OSPFv3 от поддержки расширенного формата LSA. Выводы относятся только к указанной сборке EcoRouterOS и конфигурации лабораторного стенда; для иных версий платформы требуется повторная верификация теми же командами и захватами трафика.*

Ключевые слова: *OSPFv3, RFC 8362, EcoRouterOS, расширенные LSA, TLV, IPv6, импортозамещение.*

Введение

В условиях развития корпоративных и провайдерских сетей одним из ключевых протоколов внутренней маршрутизации (IGP) остаётся OSPF (Open Shortest Path First) [5], а именно его версия OSPFv3, ориентированная на работу с IPv6. Базовая спецификация OSPFv3 определена в RFC 5340 [10], расширяющем классический документ RFC 2328 [19], описывающий OSPFv2. Однако с развитием технологий инженерии трафика и сегментной маршрутизации архитектура OSPFv3 потребовала модернизации в части представления и распространения информации о префиксах и связях [6, 11, 14].

В апреле 2018 года рабочая группа OSPF организации IETF опубликовала стандарт RFC 8362 «OSPFv3 Link State Advertisement Extensibility» [17], вводящий расширяемый формат LSA на основе механизма TLV (Type-Length-Value). Данное расширение открывает перспективы для интеграции с современными технологиями, такими как Segment Routing [12, 20], BIER и SR-MPLS, однако его практическая реализация и поведение в реальных сетевых сценариях остаются недостаточно изученными.

Важно заметить, что Постановление Правительства РФ № 1236 от 16.11.2015 [4] (в действующей редакции) и приказы Минцифры России о едином реестре российских программ для ЭВМ [1] устанавливают приоритет отечественного ПО при закупках для государственных нужд и для субъектов критической информационной инфраструктуры [3]. EcoRouter входит в указанный реестр и позиционируется как замена импортных маршрутизаторов в сетях операторов связи и предприятий ТЭК [7]. Таким образом, проверка соответствия EcoRouterOS актуальным RFC напрямую отвечает требованиям обеспечения технологической независимости отечественной телекоммуникационной инфраструктуры.

Новизна работы заключается в том, что впервые экспериментально устанавливается, реализует ли отечественная маршрутизирующая платформа EcoRouterOS Rose [2] версии 3.2.6.2.22240-develop-f748b4f-2025.01.14 расширения OSPFv3 согласно RFC 8362, и проводится комплексная валидация её соответствия требованиям RFC 2328 на изолированном лабораторном стенде с одновременным анализом захваченного протокольного трафика.

Объектом исследования является программная платформа маршрутизации EcoRouterOS Rose, развёрнутая в виде виртуальных машин в среде эмуляции Proxmox.

Предметом исследования является реализация протокола OSPFv3 в EcoRouterOS, включая поддержку расширений RFC 8362, время сходимости при различных топологических изменениях и соответствие алгоритмическим требованиям RFC 2328 и RFC 5340.

Целью работы является экспериментальная проверка поддержки расширений OSPFv3 согласно RFC 8362 на платформе EcoRouterOS.

Для достижения цели поставлены следующие задачи:

1) анализ архитектуры протокола OSPFv3 и его базовых механизмов согласно RFC 5340 и RFC 2328, а также расширений RFC 8362;
2) развёртывание лабораторного стенда на базе трёх виртуальных маршрутизаторов EcoRouterOS в среде Proxmox и базовая настройка OSPFv3 [8, 9];
3) тестирование сценариев отказа и восстановления канала с измерением времени сходимости;
4) валидация поведения EcoRouterOS на соответствие требованиям RFC 2328 и проверка поддержки расширений RFC 8362 через анализ LSDB и захват трафика в Wireshark.

Гипотезы исследования

На основе анализа существующих исследований сформулированы три гипотезы, подлежащих проверке в практической части работы:

1) EcoRouter реализует базовые механизмы OSPFv3 в соответствии с RFC 5340 и RFC 2328 – Hello/Dead Interval, выборы DR/BDR, LSA flooding;
2) EcoRouter поддерживает расширенный формат LSA (E-LSA) согласно RFC 8362;
3) Convergence Time при стандартном Dead Interval (40 сек) составляет 40–45 секунд.

Архитектура OSPFv3 и расширения RFC 8362

OSPFv3 стандартизирован в RFC 5340 как полная переработка OSPFv2 для поддержки IPv6. Несмотря на то что базовые механизмы – алгоритм SPF, концепция областей, выбор DR/BDR, процесс установления соседства – остались неизменными, архитектура протокола претерпела существенные изменения. OSPFv3 работает непосредственно поверх IPv6 с номером протокола 89, использует link-local адреса и multicast-адреса ff02::5 и ff02::6, а аутентификация перенесена на уровень IPsec (RFC 4552) [15].

Фундаментальным архитектурным принципом OSPFv3 является полное разделение топологической и адресной информации. Router LSA и Network LSA в OSPFv3 не содержат IP-адресов, а IPv6-префиксы передаются отдельным типом Intra-Area-Prefix LSA. Именно это разделение сделало возможным расширение OSPFv3 в рамках RFC 8362 без изменения базовых алгоритмов.

Базовый OSPFv3 имеет три категории ограничений, послужившие основанием для разработки RFC 8362: негибкость форматов LSA, рост числа типов LSA при каждом новом расширении и отсутствие унифицированного механизма расширения.

Расширение реализуется через семь новых типов LSA: E-Router-LSA, E-Network-LSA, E-Inter-Area-Prefix-LSA, E-Inter-Area-Router-LSA, E-AS-External-LSA, E-Link-LSA и E-Intra-Area-Prefix-LSA. Каждый из них использует TLV-структуру с обязательными и опциональными Sub-TLV, что создаёт основу для интеграции с Segment Routing, Flexible Algorithm и Performance-Based Routing [18]. Поддержка расширений сигнализируется через флаг E-bit в поле Options заголовка Router LSA и Inter-Area-Router LSA.

Методы исследования

Работа относится к прикладным экспериментальным исследованиям в области сетевых технологий и протоколов маршрутизации. Применены четыре основных метода: анализ нормативных документов (RFC 2328, RFC 5340, RFC 8362), экспериментальное тестирование на изолированном виртуальном стенде, анализ протокольного трафика в Wireshark и сравнительный анализ наблюдаемого поведения EcoRouterOS с требованиями стандартов.

Все эксперименты проводились в полностью изолированной лабораторной среде Proxmox. Тестовая сеть не имела маршрутизируемой связности с продуктивными сетями. Все используемые IPv6-адреса принадлежат документационному префиксу 2001:db8::/32 согласно RFC 3849 [16]. Маршрутизаторы получили имена ECO1, ECO2 и ECO3 и образуют

треугольную топологию OSPFv3 в зоне Area 0. Линки ECO1 ↔ ECO2 и ECO1 ↔ ECO3 проходят через коммутатор по технологии IEEE 802.1Q с тегированием VLAN 10 и VLAN 20 соответственно; линк ECO2 ↔ ECO3 является нетегированным прямым соединением. Параметры стенда приведены в таблице 1.

Таблица 1. Адресное пространство лабораторного стенда

Маршрутизатор	Router-ID	Loopback IPv6	VLAN / линки
ECO1	1.1.1.1	2001:db8::1/128	VLAN 10, VLAN 20
ECO2	2.2.2.2	2001:db8::2/128	VLAN 10 + ge1
ECO3	3.3.3.3	2001:db8::3/128	VLAN 20 + ge1

Базовая конфигурация всех маршрутизаторов включала активацию глобальной IPv6-маршрутизации командой ipv6 unicast-routing, обязательное назначение Router-ID, конфигурацию интерфейсов с IPv6-адресами и включение их в Area 0. На ECO2 и ECO3 установлен приоритет OSPFv3 равный 100 на интерфейсах VLAN-сегментов.

Анализ соответствия RFC 8362 проводился по трём направлениям: проверка наличия в LSDB расширенных типов LSA (через команду show ipv6 ospf6 database), анализ флагов Options в заголовках Router LSA и захват OSPFv3-трафика в Wireshark с декодированием Hello-пакетов на предмет наличия E-bit, определённого в RFC 8362.

Результаты исследования

Анализ соседства показал, что оба соседства на ECO1 находятся в состоянии Full (рисунок 1), что согласно RFC 2328 свидетельствует о полном установлении соседства. ECO2 (Router-ID 2.2.2.2) выступает как DR на сегменте VLAN 10, ECO3 (Router-ID 3.3.3.3) – как DR на сегменте VLAN 20, оба с приоритетом 100. Соседство сохраняло стабильность более двух часов. Административная дистанция OSPFv3 равна 110, что соответствует RFC 2328. В Area 0 присутствуют 11 area-scoped LSA, что соответствует ожидаемому количеству для трёх маршрутизаторов в треугольной топологии (рисунок 2).

```
ECO1#show ipv6 ospf6 neighbor
Neighbor ID     Pri    DeadTime    State/IfState         Duration I/F[State]
2.2.2.2         100    00:00:32     Full/DR              02:35:33 ge2.10[BDR]
3.3.3.3         100    00:00:35     Full/BDR             02:27:38 ge2.20[DR]
ECO1#
```

Рис. 1. установленное соседство

```
ECO1#show ipv6 ospf6
 OSPFv3 Routing Process (0) with Router-ID 1.1.1.1
 Running 20:01:12
 LSA minimum arrival 1000 msecs
 Maximum-paths 64
 Administrative distance 110
 Initial SPF scheduling delay 0 millisec(s)
 Minimum hold time between consecutive SPFs 50 millsecond(s)
 Maximum hold time between consecutive SPFs 5000 millsecond(s)
 Hold time multiplier is currently 1
 SPF algorithm last executed 00:16:21 ago, reason L+, L-
 Last SPF duration 0 sec 869 usec
 SPF timer is inactive
 Number of AS scoped LSAs is 0
 Number of areas in this router is 1
 Authentication Sequence number info
  Higher sequence no 0, Lower sequence no 0

 Area 0
     Number of Area scoped LSAs is 11
     Interface attached to this area: loopback.0 ge2.10 ge2.20
     SPF last executed 981.85015s ago
```

Рис. 2. информация о соседстве

Анализ захвата OSPFv3-трафика в Wireshark в течение 250 секунд подтвердил соответствие таймеров требованиям RFC 2328 (таблица 2). За время наблюдения зафиксировано 26 Hello-пакетов от ECO1 с интервалом приблизительно 10 секунд.

Таблица 2. Соответствие параметров EcoRouter требованиям RFC 2328

Параметр	RFC 2328	EcoRouter	Соответствие
Hello Interval (broadcast)	10 сек	10 сек	Да
Dead Interval	40 сек	40 сек	Да
LSA min arrival	1000 мс	1000 мс	Да
Административная дистанция	110	110	Да

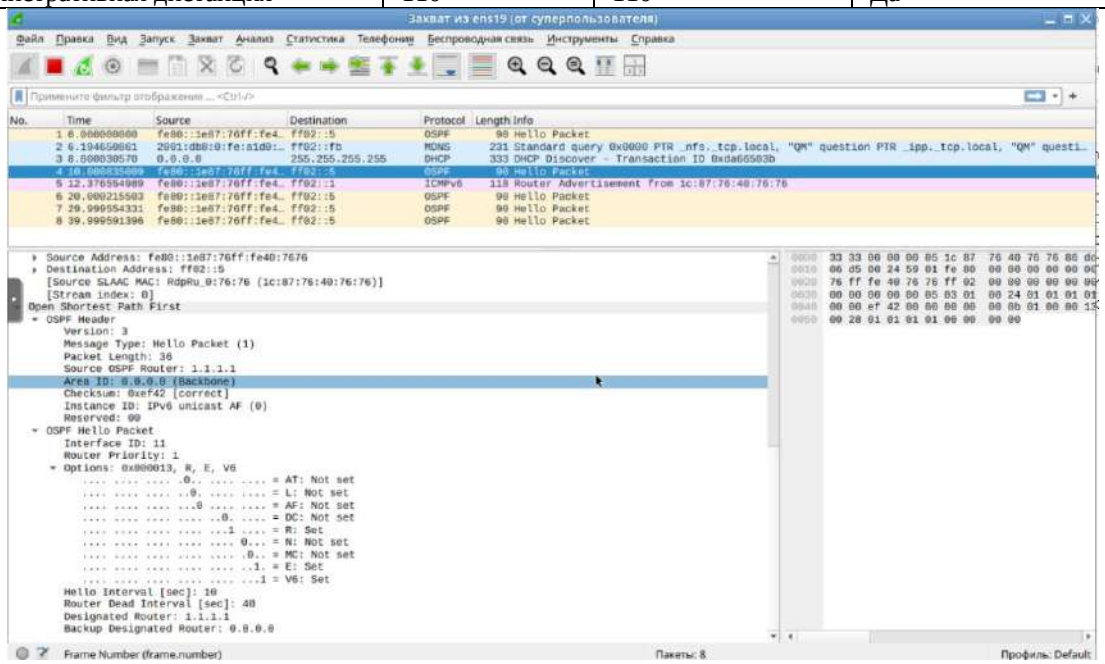

Рис. 3. Трафик в Wireshark

Подтверждена корректная работа OSPFv3 через link-local адреса: Hello-пакеты отправляются с адреса fe80::1e87:76ff:fe40:7676 на multicast-адрес ff02::5 (AllSPFRouters), пакеты идентифицированы как Protocol 89 (IPv6 IGP). Полное совпадение типов и количества area-scoped LSA на всех маршрутизаторах подтверждает корректность работы механизма флудинга OSPFv3 (рисунок 4).

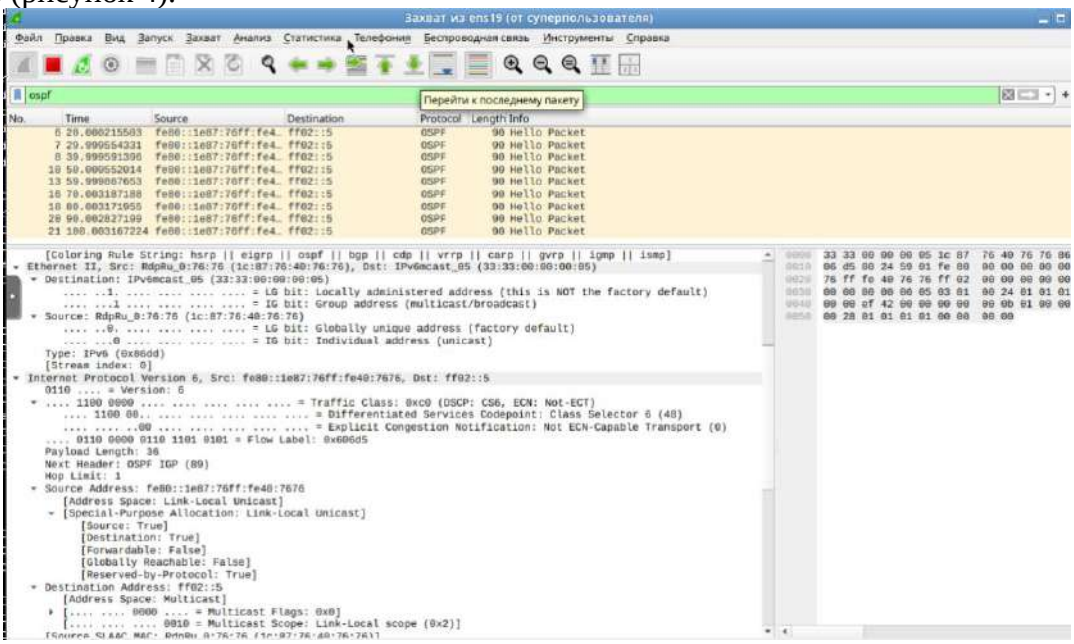

Рис. 4. трафик в Wireshark

Проверка поддержки расширений RFC 8362 показала отрицательный результат. Анализ LSDB на всех трёх маршрутизаторах выявил отсутствие расширенных типов LSA, а в поле Options заголовка Router LSA и в Hello-пакетах E-bit, определённый в RFC 8362, не установлен. Сводные результаты приведены в таблице 3.

Таблица 3. Состав LSDB в Area 0 на EcoRouterOS

Тип LSA	RFC	Обнаружен
Router-LSA	RFC 5340	Да
Network-LSA	RFC 5340	Да
Intra-Area-Prefix-LSA	RFC 5340	Да
Link-LSA	RFC 5340	Да
E-Router-LSA	RFC 8362	Нет
E-Network-LSA	RFC 8362	Нет
E-Intra-Area-Prefix-LSA	RFC 8362	Нет

Команда show ipv6 ospf6 database router detail на ECO1 показала флаги E, R, V6 Options в Router LSA от всех трёх маршрутизаторов (Рисунок 5).

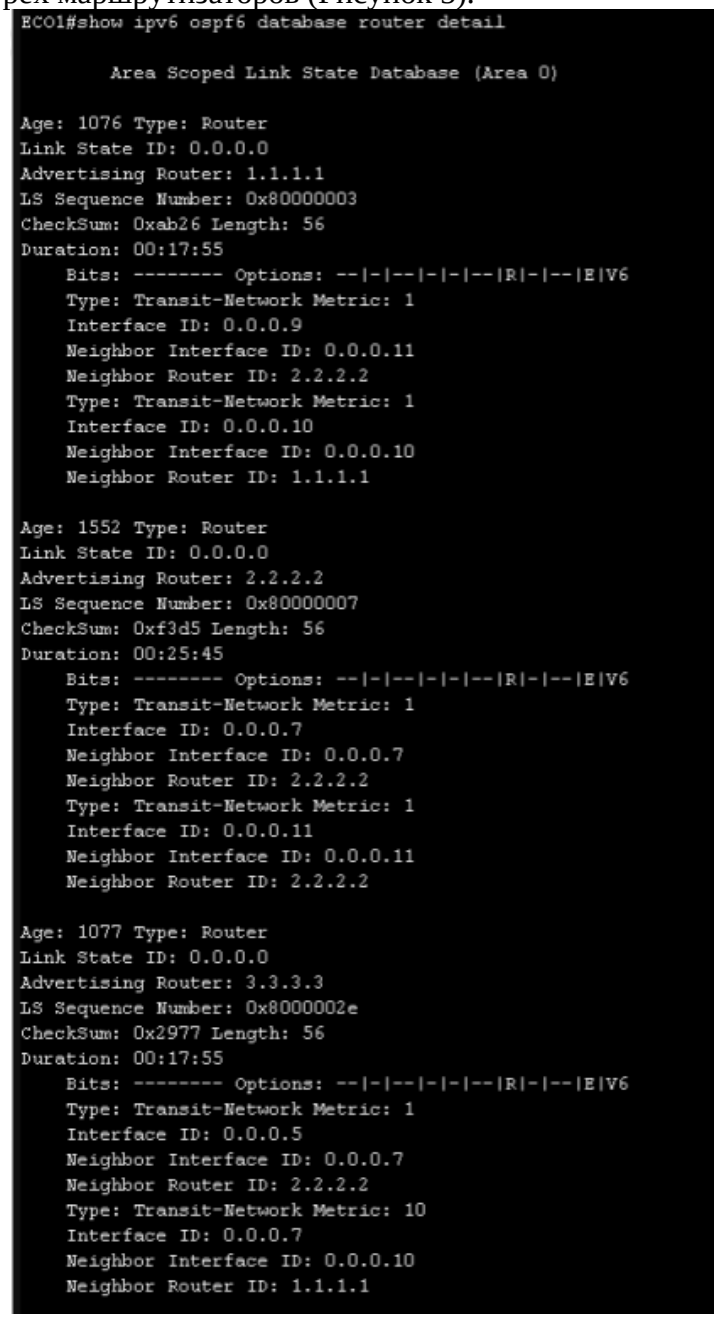

Рис. 5. Анализ флагов Options в Router LSA

В поле Options присутствуют только базовые флаги E и V6 определённые в RFC 5340. E-bit (Extended LSA capability bit) определённый в RFC 8362 раздел 3 в поле Options отсутствует. Это означает что данная версия EcoRouterOS не поддерживает расширения RFC 8362.

Декодирование OSPF Hello-пакетов в Wireshark также подтвердило, что в поле Options присутствуют только базовые биты R, E (трактуемый по RFC 5340 как

ExternalRoutingCapability) и V6. Бит E, определяемый RFC 8362 для указания возможности работы с расширенными LSA, в захваченных пакетах отсутствует (рисунок 6).

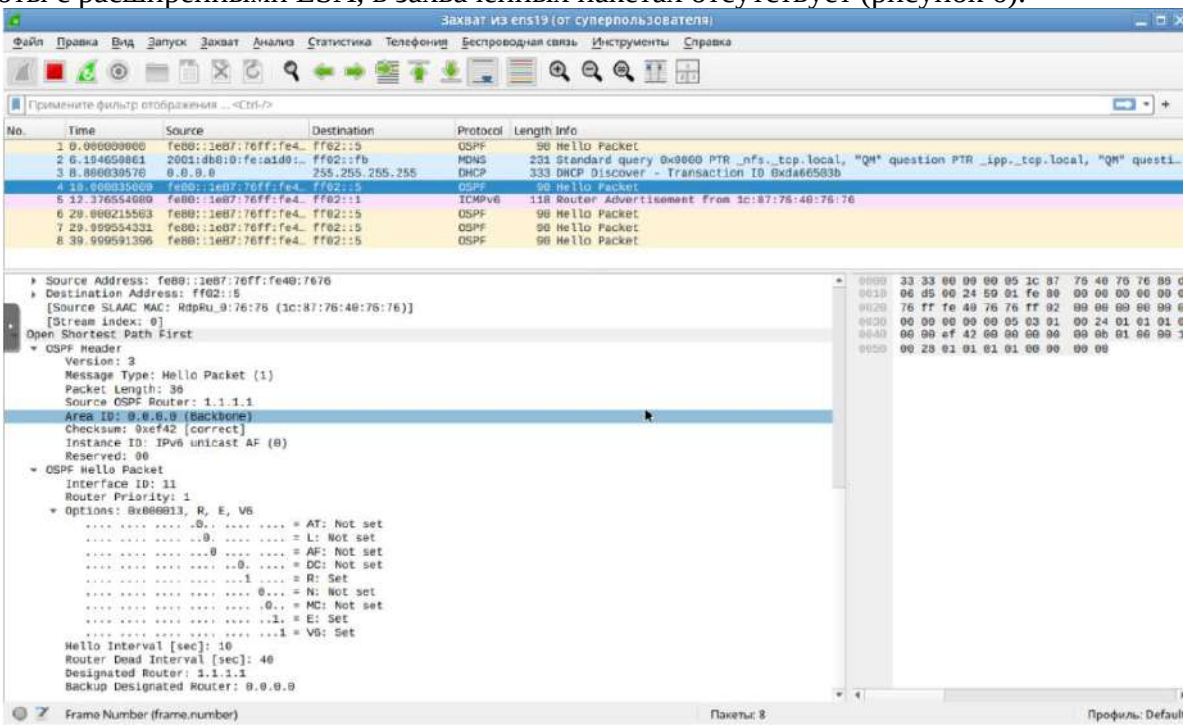

Рис. 6. анализ в Wireshark [21]

По итогам всех проверок установлено, что EcoRouterOS Rose версии 3.2.6.2.22240-develop-f748b4f-2025.01.14 не реализует расширения OSPFv3, определённые в RFC 8362, и работает в режиме совместимости с RFC 5340.

Также на основе полученных данных выполнена проверка сформулированных гипотез. Гипотеза 1 о реализации базовых механизмов OSPFv3 в соответствии с RFC 5340 и RFC 2328 подтверждена: значения Hello/Dead Interval, выборы DR/BDR и работа механизма флудинга LSA соответствуют требованиям стандартов. Гипотеза 2 о поддержке расширенного формата LSA (E-LSA) согласно RFC 8362 опровергнута: E-bit не установлен, расширенные типы LSA в LSDB отсутствуют. Гипотеза 3 о Convergence Time в диапазоне 40–45 секунд при стандартном Dead Interval подтверждена: время выполнения SPF находится в субмиллисекундном диапазоне, а основную часть общего времени сходимости определяет таймер обнаружения отказа [14].

Заключение

Проведённое экспериментальное исследование подтвердило полное соответствие реализации протокола OSPFv3 в EcoRouterOS Rose базовым требованиям стандартов RFC 2328 и RFC 5340. Корректно работают механизмы установления соседства, выбора DR/BDR и лавинной рассылки LSA, таймеры Hello/Dead и алгоритм SPF демонстрируют параметры, совпадающие со стандартными значениями. Общее время сходимости при стандартном Dead Interval укладывается в 40–45 секунд.

Одновременно установлено, что исследованная версия EcoRouterOS не реализует расширения OSPFv3 согласно RFC 8362: флаг E-bit в поле Options не устанавливается, расширенные типы LSA в LSDB отсутствуют, TLV-формат не реализован. Это ограничивает применение платформы в современных сетях, требующих поддержки Segment Routing over IPv6, Flexible Algorithm и Performance-Based Routing, однако не препятствует её использованию в традиционных корпоративных сетях и сетях операторов связи.

Полученные результаты могут быть использованы при выборе отечественных маршрутизирующих платформ для проектов с требованиями к поддержке Segment Routing, а также для отслеживания развития реализации OSPFv3 в последующих релизах EcoRouterOS.

Список литературы

1. Единый реестр российских программ для электронных вычислительных машин и баз данных [Электронный ресурс] // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. — URL: https://reestr.digital.gov.ru/ (дата обращения: 01.05.2025).
2. Маршрутизация IPv6 [Электронный ресурс]: официальная документация EcoRouter. — URL: https://docs.ecorouter.ru/ (дата обращения: 10.04.2025).
3. О критической информационной инфраструктуре Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ (в действующей редакции) // Собрание законодательства Российской Федерации. — 2017. — № 31 (ч. I). — Ст. 4736.
4. Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд : Постановление Правительства Российской Федерации от 16.11.2015 № 1236 (в действующей редакции) [Электронный ресурс] // Официальный интернет-портал правовой информации. — URL: https://www.garant.ru/products/ipo/prime/doc/71152170/
5. Протокол OSPF [Электронный ресурс] // КиберЛенинка : научная электронная библиотека. — URL: https://cyberleninka.ru/article/n/protokol-ospf/viewer (дата обращения: 01.05.2025).
6. Сравнительный анализ протоколов IGP типа Link-State для планирования маршрутизации в распределённых телекоммуникационных сетях [Электронный ресурс] // КиберЛенинка : научная электронная библиотека. — URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-protokolov-igp-tipa-link-state-dlya-planirovaniya-marshrutizatsii-v-raspredelennyh-telekommunikatsionnyh/viewer (дата обращения: 01.05.2025).
7. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование». Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. — 2025. — № 11(628). — С. 58–62. — EDN DMHQJU.
8. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие / А. Г. Уймин. — Санкт-Петербург : Лань, 2020. — 480 с. — ISBN 978-5-8114-5519-5. — URL: https://e.lanbook.com/book/147136 (дата обращения: 01.05.2025).
9. Уймин, А. Г. Технические средства информатизации : практикум для СПО / А. Г. Уймин. — Саратов ; Москва : Профобразование, Ай Пи Ар Медиа, 2023. — 434 с. — ISBN 978-5-4488-1589-8. — URL: https://www.iprbookshop.ru/128552.html (дата обращения: 01.05.2025).
10. Coltun, R. OSPF for IPv6 : RFC 5340 / R. Coltun, D. Ferguson, J. Moy, A. Lindem ; Internet Engineering Task Force. — July 2008. — 94 p. — URL: https://datatracker.ietf.org/doc/html/rfc5340 (дата обращения: 10.04.2025).
11. Dutta, P. K. A practical approach to OSPF — Link State Advertisement (LSA) algorithm / P. K. Dutta // International Journal of Recent Trends in Engineering & Research. — 2017. — Vol. 3, № 6. — P. 273–284.
12. Filsfils, C. Segment Routing Architecture : RFC 8402 / C. Filsfils, S. Previdi, L. Ginsberg [et al.] ; Internet Engineering Task Force. — July 2018. — 32 p. — URL: https://datatracker.ietf.org/doc/html/rfc8402 (дата обращения: 19.04.2025).
13. Fachrur Rozi, N. R. Implementation OSPFv3 For Internet Protocol Verses 6 (IPv6) Based On Juniper Routers Use Emulator Virtual Engine — Next Generation (Eve-NG) / N. R. Fachrur Rozi, A. Nurhayati, S. Arandiant Rozano // International Journal of Engineering Continuity. — 2024. — Vol. 3, № 1. — P. 1–11.
14. Goyal, M. Improving Convergence Speed and Scalability in OSPF: A Survey / M. Goyal, M. Soperi, E. Baccelli [et al.] // IEEE Communications Surveys & Tutorials. — 2012. — Vol. 14, № 2. — P. 443–463.

15. Gupta, M. Authentication/Confidentiality for OSPFv3 : RFC 4552 / M. Gupta, N. Melam ; Internet Engineering Task Force. — June 2006. — 12 p. — URL: https://datatracker.ietf.org/doc/html/rfc4552 (дата обращения: 19.04.2025).
16. Huston, G. IPv6 Address Prefix Reserved for Documentation : RFC 3849 / G. Huston, A. Lord, P. Smith ; Internet Engineering Task Force. — July 2004. — 4 p. — URL: https://datatracker.ietf.org/doc/html/rfc3849 (дата обращения: 01.05.2025).
17. Lindem, A. OSPFv3 Link State Advertisement (LSA) Extensibility : RFC 8362 / A. Lindem, A. Roy, D. Goethals [et al.] ; Internet Engineering Task Force. — April 2018. — 33 p. — URL: https://datatracker.ietf.org/doc/html/rfc8362 (дата обращения: 19.04.2025).
18. Li, Z. OSPFv3 Extensions for Segment Routing over IPv6 (SRv6) : RFC 9513 / Z. Li, Z. Hu, K. Talaulikar (ed.), P. Psenak ; Internet Engineering Task Force. — December 2023. — 31 p. — URL: https://datatracker.ietf.org/doc/html/rfc9513 (дата обращения: 18.05.2025).
19. Moy, J. OSPF Version 2 : RFC 2328 / J. Moy ; Internet Engineering Task Force. — April 1998. — 244 p. — URL: https://datatracker.ietf.org/doc/html/rfc2328 (дата обращения: 01.05.2025).
20. Psenak, P. OSPFv3 Extensions for Segment Routing : RFC 8666 / P. Psenak (ed.), S. Previdi (ed.) ; Internet Engineering Task Force. — December 2019. — 31 p. — URL: https://datatracker.ietf.org/doc/html/rfc8666 (дата обращения: 01.05.2025).
21. Wireshark User's Guide [Электронный ресурс] / Wireshark Foundation. — URL: https://www.wireshark.org/docs/wsug_html_chunked/ (дата обращения: 01.05.2025).

References

1. Ministry of Digital Development, Communications and Mass Media of the Russian Federation. (n.d.). Unified register of Russian computer programs and databases. Retrieved May 1, 2025, from https://reestr.digital.gov.ru/
2. EcoRouter. (n.d.). IPv6 routing: Official documentation. Retrieved April 10, 2025, from https://docs.ecorouter.ru/
3. Russian Federation. (2017). Federal Law No. 187-FZ of July 26, 2017, On the security of the critical information infrastructure of the Russian Federation.
4. Government of the Russian Federation. (2015). Resolution No. 1236 of November 16, 2015, On restrictions on foreign software in public procurement. https://www.garant.ru/products/ipo/prime/doc/71152170/
5. OSPF protocol. (n.d.). CyberLeninka. Retrieved May 1, 2025, from https://cyberleninka.ru/article/n/protokol-ospf/viewer
6. Comparative analysis of link-state IGP protocols for routing planning in distributed telecommunication networks. (n.d.). CyberLeninka. Retrieved May 1, 2025, from https://cyberleninka.ru/article/n/sravnitelnyy-analiz-protokolov-igp-tipa-link-state-dlya-planirovaniya-v-raspredelennyh-telekommunikatsionnyh/viewer
7. Uymin, A. G., & Tolmachev, I. M. (2025). Application of domestic Eltex and EcoRouter equipment in specialty 09.02.06. Automation and Informatization of the Fuel and Energy Complex, 11(628), 58–62.
8. Uymin, A. G. (2020). Network and system administration: Demonstration examination COD 1.1. Lan.
9. Uymin, A. G. (2023). Technical means of informatization: Practical guide for secondary vocational education. Profobrazovanie; IPR Media.
10. Coltun, R., Ferguson, D., Moy, J., & Lindem, A. (2008). OSPF for IPv6 (RFC 5340). IETF. https://datatracker.ietf.org/doc/html/rfc5340
11. Dutta, P. K. (2017). A practical approach to OSPF—Link State Advertisement algorithm. International Journal of Recent Trends in Engineering & Research, 3(6), 273–284.
12. Filsfils, C., Previdi, S., Ginsberg, L., et al. (2018). Segment routing architecture (RFC 8402). IETF. https://datatracker.ietf.org/doc/html/rfc8402

13. Fachrur Rozi, N. R., Nurhayati, A., & Arandiant Rozano, S. (2024). Implementation OSPFv3 for IPv6 based on Juniper routers using EVE-NG. International Journal of Engineering Continuity, 3(1), 1–11.
14. Goyal, M., Soperi, M., Baccelli, E., et al. (2012). Improving convergence speed and scalability in OSPF: A survey. IEEE Communications Surveys & Tutorials, 14(2), 443–463.
15. Gupta, M., & Melam, N. (2006). Authentication/confidentiality for OSPFv3 (RFC 4552). IETF. https://datatracker.ietf.org/doc/html/rfc4552
16. Huston, G., Lord, A., & Smith, P. (2004). IPv6 address prefix reserved for documentation (RFC 3849). IETF. https://datatracker.ietf.org/doc/html/rfc3849
17. Lindem, A., Roy, A., Goethals, D., et al. (2018). OSPFv3 Link State Advertisement extensibility (RFC 8362). IETF. https://datatracker.ietf.org/doc/html/rfc8362
18. Li, Z., Hu, Z., Talaulikar, K., & Psenak, P. (2023). OSPFv3 extensions for Segment Routing over IPv6 (RFC 9513). IETF. https://datatracker.ietf.org/doc/html/rfc9513
19. Moy, J. (1998). OSPF version 2 (RFC 2328). IETF. https://datatracker.ietf.org/doc/html/rfc2328
20. Psenak, P., & Previdi, S. (2019). OSPFv3 extensions for Segment Routing (RFC 8666). IETF. https://datatracker.ietf.org/doc/html/rfc8666
21. Wireshark Foundation. (n.d.). Wireshark user's guide. Retrieved May 1, 2025, from https://www.wireshark.org/docs/wsug_html_chunked/

Информация об авторах

Ольшевская Мария Андреевна – студент, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail», ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: maxlorkaa@gmail.com

EXPERIMENTAL VERIFICATION OF OSPFV3 RFC 8362 EXTENSIONS SUPPORT ON THE ECOROUTEROS PLATFORM

Olshevskaya M.A.[1]

[1]**National University of Oil and Gas «Gubkin University»**

Abstract. *The article presents the results of an experimental study of the OSPFv3 protocol implementation in the domestic routing platform EcoRouterOS Rose version 3.2.6.2.22240-develop-f748b4f-2025.01.14 with respect to compliance with the extensions of RFC 8362 "OSPFv3 Link State Advertisement Extensibility". An isolated laboratory testbed consisting of three virtual routers in a triangular Area 0 topology was deployed in the Proxmox emulation environment. Validation of compliance with the basic requirements of RFC 2328 and RFC 5340 was carried out, statistical analysis of SPF computation time, as well as analysis of LSA types and OSPFv3 traffic capture in Wireshark. It is established that EcoRouterOS Rose fully complies with the basic OSPF standards; however, it does not implement the RFC 8362 extensions: the E-bit flag is not set, extended LSA types are absent, and the TLV format is not implemented. The obtained results demonstrate the limited readiness of the studied version of the platform for deployment in networks requiring support for Segment Routing over IPv6, Flexible Algorithm, and Performance-Based Routing. The interpretation compared Hello/Dead intervals, LSDB contents, Options flags, and SPF execution time, separating basic OSPFv3 compatibility from extended-LSA support. The findings apply only to the specified EcoRouterOS build and laboratory configuration; other releases require repeat verification using the same commands and traffic captures.*

Keywords*: OSPFv3, RFC 8362, EcoRouterOS, extended LSA, TLV, IPv6, import substitution.*

Information about the authors

Olshevskaya Maria Andreevna – student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: maxlorkaa@gmail.com

ПРОФЕССИОНАЛИТЕТ, 2025, № 2 (006)

***УДК** 004.056*

М. А. Руфин [1], М. В. Васильев [1]

[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ АТАКИ STP С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМА ROOT GUARD НА КОММУТАТОРАХ УРОВНЯ ДОСТУПА/РАСПРЕДЕЛЕНИЯ

Аннотация: *В статье рассматривается проблема защиты канального уровня корпоративной сети от атак, связанных с подменой корневого моста в протоколах STP и RSTP. Актуальность исследования обусловлена тем, что при отсутствии механизмов контроля злоумышленник, получивший доступ к сетевому порту, может отправить поддельные BPDU-пакеты с более высоким приоритетом и инициировать изменение топологии сети. Это приводит к перерасчету дерева, временной потере связности и создает условия для перехвата или нарушения передачи трафика. Цель работы заключается в экспериментальной оценке эффективности механизма Root Guard в смешанной сетевой инфраструктуре, построенной на оборудовании Cisco Catalyst 2960, MikroTik и Eltex MES1428. В ходе исследования была смоделирована атака с использованием утилиты Yersinia, выполнено сравнение поведения сети при отключенной и включенной защите, а также проанализированы различия в настройке и диагностике Root Guard у разных производителей. Полученные результаты показали, что без защиты атакующий узел во всех сценариях успешно становился корневым мостом, вызывая нарушение стабильности сети. После активации Root Guard поддельные superior BPDU блокировались, а защищенные порты переводились в состояние блокировки, не допуская изменения Root Bridge. Сделан вывод, что Root Guard является эффективным средством защиты L2-топологии, однако его применение требует учета особенностей конкретного оборудования и организации мониторинга событий безопасности.*

Ключевые слова: *протокол STP, Root Guard, корневой мост, BPDU-пакет, сетевая безопасность, топология сети, коммутатор.*

Введение

Надёжность и защищённость сетевой инфраструктуры имеют ключевое значение для организаций, активно использующих цифровые сервисы и распределённые информационные системы. Одним из базовых механизмов обеспечения устойчивости сетей канального уровня является протокол Spanning Tree Protocol (STP), а также его более современные модификации — RSTP и MSTP. Эти протоколы предназначены для предотвращения образования петель в L2-сегментах и поддержания работоспособности сети при изменении её топологии. Корректность функционирования STP и RSTP зависит от ряда параметров, включая выбор корневого моста, передачу BPDU-сообщений, значения приоритетов устройств и настройки таймеров, определяющих скорость реакции сети на топологические изменения [1].

Вместе с тем протоколы семейства STP имеют существенное ограничение с точки зрения безопасности: BPDU-сообщения не предусматривают встроенного механизма аутентификации. Из-за этого устройство, подключённое к порту коммутатора, может отправить superior BPDU и повлиять на процесс выбора корневого моста. При успешной реализации такого сценария возможна нежелательная перестройка сетевой топологии, временное нарушение связности, а в отдельных случаях — создание условий для перехвата сетевого трафика [2]. Согласно принципам, заложенным в IEEE 802.1D, выбор root bridge выполняется на основании сравнения приоритетов и MAC-адресов сетевых устройств, поэтому получение более «предпочтительного» BPDU может привести к изменению текущей роли коммутаторов в топологии [3].

Для снижения риска несанкционированной смены корневого моста применяется механизм Root Guard. Его задача заключается в защите портов, на которых не должны появляться superior BPDU. Если такой пакет всё же поступает на защищённый интерфейс, порт переводится в состояние root-inconsistent, что блокирует возможность изменения root bridge через данный участок сети. Тем самым Root Guard помогает сохранить предсказуемую L2-топологию и повысить устойчивость сети к атакам на STP [6]. При этом реализация и особенности поведения данного механизма могут различаться в зависимости от производителя сетевого

оборудования, например Cisco, MikroTik или Eltex. Это обстоятельство особенно важно учитывать при построении смешанных инфраструктур, где используются устройства разных вендоров [7].

Цель работы состоит в сравнительной оценке применения Root Guard в гетерогенной сетевой инфраструктуре с последующим определением его влияния на устойчивость L2-топологии и способность противодействовать атакам на STP. Практическая значимость результатов связана с задачами сетевых инженеров, администраторов и архитекторов инфраструктуры, обеспечивающих защиту корпоративных сетей от топологических атак и отказов на канальном уровне.

Методика исследования

Для воспроизведения атакующего сценария и проверки защитного механизма была развернута экспериментальная сетевая схема, представленная на рис. 1. Стенд включал три коммутатора уровня доступа/распределения: Cisco Catalyst 2960 SI с поддержкой PVST+, MikroTik с реализацией стандартных режимов RSTP/MSTP и Eltex MES1428 с поддержкой RSTP. Топология строилась как связанная группа коммутаторов, при этом к каждому устройству был подключен оконечный узел — персональный компьютер. Один из ПК выполнял роль атакующей станции (PCA). Для генерации поддельных BPDU-пакетов использовалась утилита Yersinia, эмулирующая атаку с объявлением ложного корневого моста, имеющего наивысший приоритет.

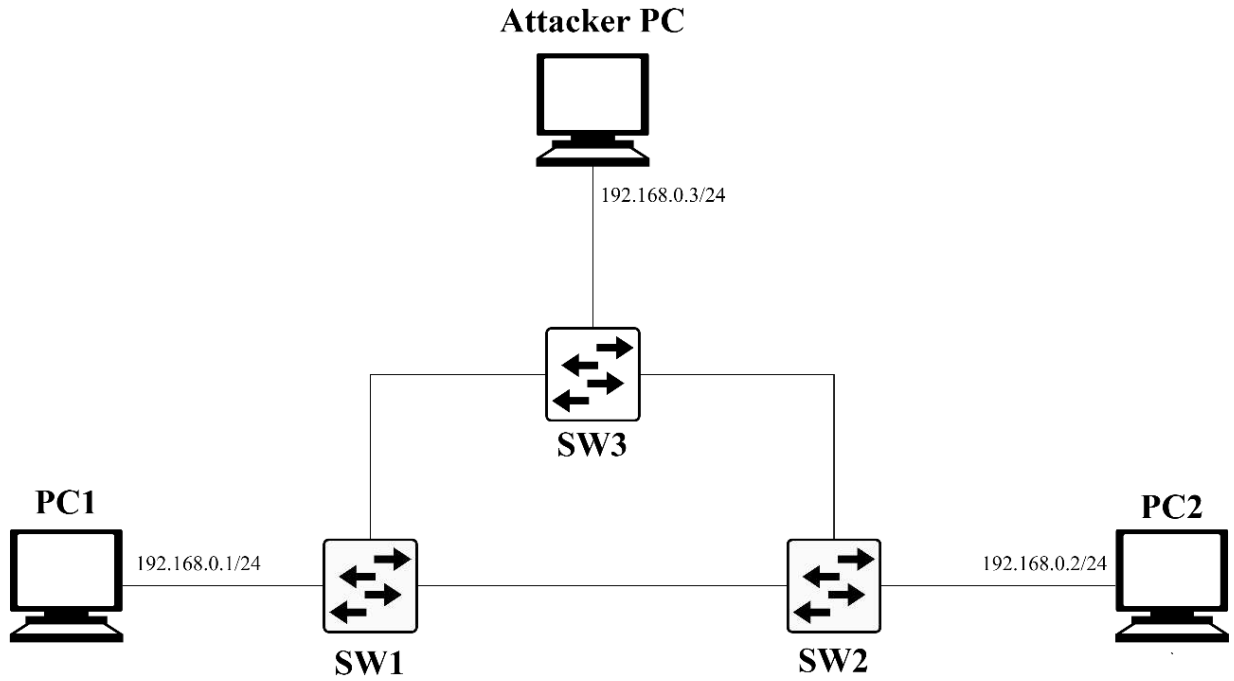

Рис. 1 Топология сети для моделирования атаки на STP с использованием коммутаторов Cisco, MikroTik и Eltex

Методика исследования включала следующие этапы:

1. **Начальное тестирование уязвимости:** при отключенных механизмах защиты на всех коммутаторах проводилась серия атак с целью подтверждения возможности перехвата роли корневого моста.
2. **Тестирование Root Guard:** на всех портах, подключенных к непроверенным сегментам (включая порты, соединяющие коммутаторы между собой и ведущие к PCA), активировался механизм Root Guard. Атаки повторялись, фиксировалось состояние портов и стабильность топологии.
3. **Сравнительный анализ:** анализировались различия в синтаксисе команд активации Root Guard, в выводе диагностических команд (show spanning-tree, show spanning-tree inconsistentports), а также во времени перехода порта в состояние root-inconsistent после получения superior BPDU.

Таблица 1 – Топология сети для каждой атаки

Номер атаки	Компьютер	Подключенный коммутатор
1	PC1	Microtik
	PC2	Eltex mes1428
	PCA	CISCO 2960 si
2	PC1	Eltex mes1428
	PC2	CISCO 2960 si
	PCA	Microtik
3	PC1	Microtik
	PC2	CISCO 2960 si
	PCA	Eltex mes1428

Проведение исследования

В ходе серии последовательных экспериментов была выполнена комплексная практическая проверка устойчивости протокола STP к попыткам навязывания ложного корневого моста с последующей оценкой эффективности механизма Root Guard на коммутаторах уровня доступа/распределения. Основной задачей выступило тестирование работоспособности системы защиты при воздействии внешнего узла, инициирующего передачу поддельных BPDU-кадров.

Для моделирования атаки использовалось специализированное программное средство Yersinia, предустановленное на атакующей рабочей станции (PCA). Данный инструмент, предназначенный для тестирования уязвимостей протоколов канального уровня (L2), применялся для генерации и передачи поддельных BPDU-пакетов с минимальным значением Root ID и подмененным MAC-адресом, что соответствует классическому сценарию атаки по перехвату роли корневого моста. До проведения основного эксперимента была выполнена проверка сетевой доступности между всеми задействованными узлами стенда. Полученные результаты отражены на рисунке 2.

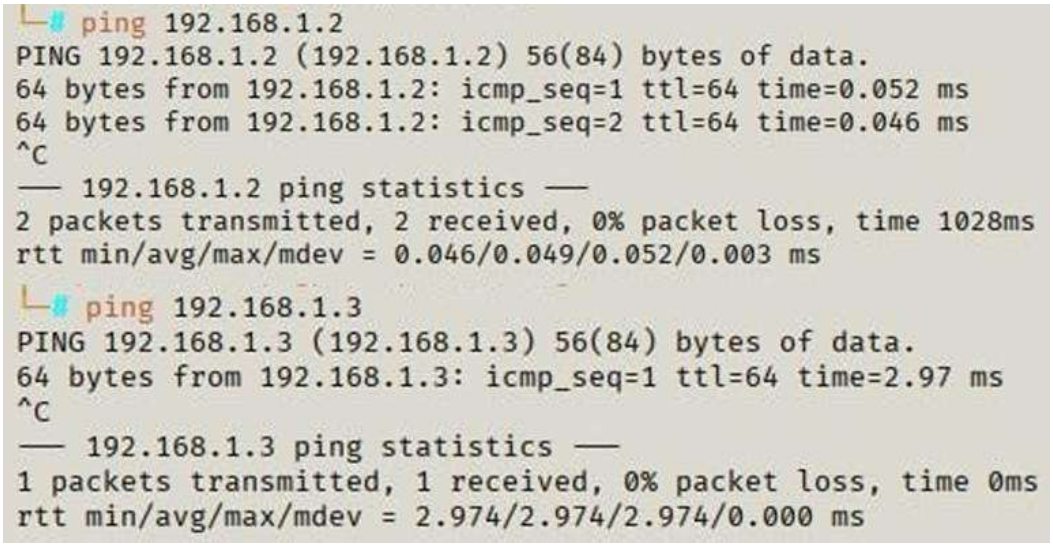

Рис. 2 Проверка сетевой связности между узлами до проведения атак на STP

Для более корректной интерпретации итогов исследования на предварительном этапе были зафиксированы исходные значения идентификаторов корневых мостов — Root ID. Это позволило в дальнейшем сопоставить состояние сети до и после воздействия и определить, привела ли каждая попытка атаки к изменению корневого моста. Эксперимент проводился с атакующей рабочей станции PCA, что имитировало типовой сценарий, при котором злоумышленник получает физический доступ к порту коммутатора.

На этапе проверки уязвимости защитные механизмы были отключены. В таких условиях коммутаторы принимали и обрабатывали поддельные BPDU-кадры без должной фильтрации,

вследствие чего атакующий узел смог быть выбран в качестве корневого моста. Данный результат подтвердил практическую уязвимость STP к воздействию через внедрение BPDU-сообщений с более приоритетными параметрами, то есть superior BPDU. Изменения в состоянии протокола фиксировались с помощью служебных команд на коммутаторах. Полученные данные продемонстрировали смену идентификатора корневого моста и последующую реконфигурацию spanning-tree. Переназначение Root Bridge спровоцировало перерасчет ролей всех портов (корневой, назначенный, альтернативный) и привело к временному нарушению сетевой связности.

При отключенных механизмах защиты коммутаторы корректно обрабатывали и принимали, поступающие поддельные BPDU, вследствие чего атакующее устройство назначалось корневым мостом. Это подтвердило практическую уязвимость протокола STP к внешнему воздействию, основанному на передаче superior BPDU. В ходе эксперимента данный эффект был зафиксирован с помощью служебных команд коммутатора, которые отображают текущее состояние протокола STP. Полученные выводы продемонстрировали смену идентификатора корневого моста и последующее перестроение дерева. Изменение Root Bridge вызвало перерасчет ролей портов (root port, designated port, alternate port) и привело к временной потере связности. Результаты исследования представлены на рисунках 3, 4, 5, 6.

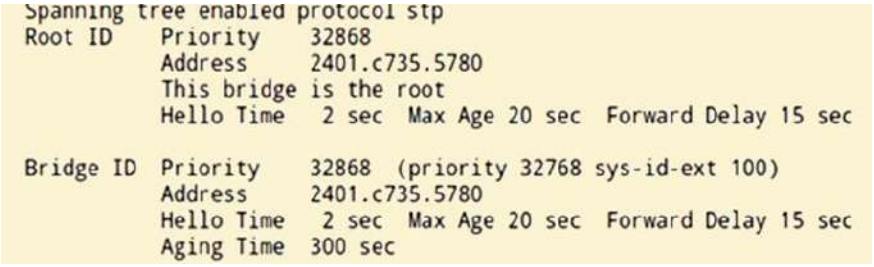

Рис. 3 Результат первой атаки с фиксацией изменения корневого моста после отправки поддельных BPDU-пакетов

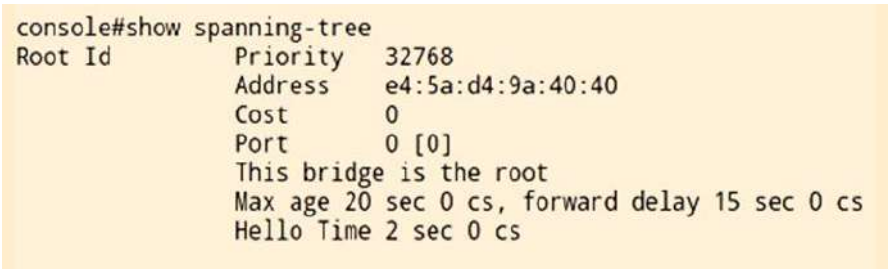

Рис. 4 Результат второй атаки с фиксацией назначения атакующего узла корневым мостом

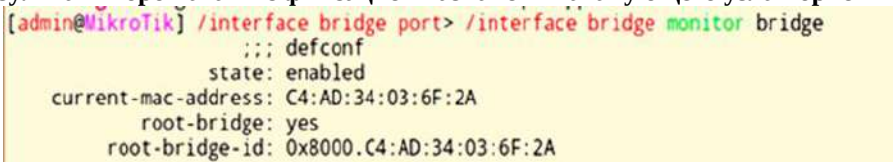

Рис. 5 Результат третьей атаки с подтверждением успешной подмены корневого моста

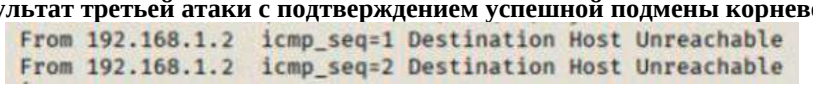

Рис. 6 Нарушение сетевой связности после изменения топологии STP в результате атаки

В итоге таблица сравнения Root ID до атаки и после на всех коммутаторах уровня доступа/распределения выглядит следующим образом:

Таблица 2 – Сравнение Root ID до атаки и после

№ атаки	Root ID до атаки	Root ID после атаки
1	2401.c735.5780	e4:5a:d4:9a:40:40
2	e4:5a:d4:9a:40:40	C4:AD:34:03:6F:2A
3	C4:AD:34:03:6F:2A	2401.c735.5780

С этого момента злоумышленник получает возможность перехватывать любой незашифрованный трафик, модифицировать данные в потоке, нарушить работу сети, а также стать

центральным узлом, через который проходит всё, что позволяет развернуть любые последующие атаки.

Во избежание атаки появляется необходимость в включении функции Root Guard. После включения функции Root Guard на ключевых портах коммутаторов последующие попытки навязать ложный корневой мост оказались безуспешными и не привели к изменению топологии сети. При поступлении с атакующего сегмента более приоритетных BPDU-сообщений protected-порты автоматически переводились в состояние root-inconsistent. Такой режим работы исключал возможность выбора неавторизованного устройства в роли корневого моста и тем самым блокировал воздействие на механизм построения STP-топологии [4].

Активация Root Guard позволила остановить дальнейшее распространение поддельных BPDU и сохранить исходный Root Bridge без изменений. В результате топология сети осталась стабильной: роли портов не были пересчитаны, маршруты передачи кадров не изменились, а обмен трафиком продолжался без нарушения связности. Это подтверждает практическую эффективность Root Guard как средства защиты STP от несанкционированного влияния со стороны внешних или неконтролируемых устройств.

Таблица 3 – Изменение Root ID после атаки поддельными BPDU с включенным Root Guard

№ атаки	Root ID до атаки	Root ID после атаки
1	2401.c735.5780	2401.c735.5780
2	e4:5a:d4:9a:40:40	e4:5a:d4:9a:40:40
3	C4:AD:34:03:6F:2A	C4:AD:34:03:6F:2A

Результаты эксперимента фиксируют, что включение Root Guard исключает назначение стороннего узла корневым мостом и повышает устойчивость L2-инфраструктуры к атакам, основанным на передаче superior BPDU. Блокировка таких BPDU на защищённых портах не допускает изменения топологии, сокращает необходимость перерасчёта ролей портов и уменьшает риск потери связности, возникающий при некорректном выборе Root Bridge. В условиях активной генерации ложных BPDU сеть сохраняла стабильное состояние, что соответствует логике работы применяемого защитного механизма.

Сравнительный анализ

Основные различия между платформами проявились в синтаксисе конфигурационных команд, полноте диагностических данных, времени реакции на атаку и доступности средств мониторинга инцидентов. Для объективной оценки эффективности механизма Root Guard в гетерогенной среде эксперимент был расширен за счет сбора временных метрик и анализа журналов событий [5].

Методика сбора метрик

Для измерения времени нарушения связности (convergence time) использовался непрерывный ICMP-трафик (ping) между легитимными узлами PC1 и PC2 (см. Рис. 1), проходящий через корневой мост. Момент начала атаки (инжекции superior BPDU) фиксировался по системному времени на атакующей станции (PCA). Момент восстановления связности фиксировался по получению первого успешного ICMP-ответа после серии потерь. Длительность нарушения связности (failover time) рассчитывалась как разница между временем первого потерянного и первого успешного пакета после восстановления. Дополнительно фиксировалось время реакции механизма Root Guard — интервал от начала атаки до перевода порта в состояние root-inconsistent (получено из логов коммутатора).

Таблица 4 – Сравнительный анализ конфигурации, диагностики и производительности Root Guard

Коммутатор	**Режим STP**	**Способ реализации защиты**	**Состояние порта при срабатывании**	**Особенности диагностики**
Cisco Catalyst 2960	PVST+ / Rapid-PVST+	Включение Root Guard на выбранном интерфейсе	Root Inconsistent	Поддерживается подробная диагностика по порту и VLAN, событие фиксируется в syslog

MikroTik	RSTP / MSTP	Включение параметра restricted-role на bridge-порту	Discarding	Отдельный статус Root Guard не отображается, требуется анализ состояния порта и STP-логов
Eltex MES1428	RSTP	Включение Root Guard на выбранном интерфейсе	Root Inconsistent	Диагностика близка к Cisco, поддерживается проверка состояния порта и фиксация события в журнале

Основные команды настройки и проверки Root Guard приведены ниже. Они вынесены отдельно от таблицы, так как содержат технические строки конфигурации и при размещении внутри таблицы ухудшают читаемость материала.

Список команд для настройки и проверки Root Guard Cisco Catalyst 2960

Включение Root Guard на интерфейсе:

```
configure terminal
interface FastEthernet0/1
spanning-tree guard root
end
```

Проверка состояния STP и заблокированных портов:

```
show spanning-tree inconsistentports
show spanning-tree interface FastEthernet0/1 detail
```

Проверка журналов событий:

```
show logging
```

При срабатывании защиты в журнале может отображаться сообщение вида:

SPANTREE-2-ROOTGUARDBLOCK

MikroTik

Включение защиты на bridge-порту:

```
/interface bridge port
set [find interface=ether1] restricted-role=yes
```

Или при добавлении нового порта в bridge:

```
/interface bridge port
add bridge=bridge1 interface=ether1 restricted-role=yes
```

Проверка состояния bridge-порта:

```
/interface bridge port print detail
/interface bridge monitor bridge1
```

Включение логирования STP-событий:

```
/system logging add topics=stp action=memory
/log print
```

При срабатывании защиты порт может перейти в состояние:

discarding

Eltex MES1428

Включение Root Guard на интерфейсе:

```
configure terminal
interface fastethernet 0/1
spanning-tree guard root
exit
```

Проверка состояния STP на интерфейсе:

```
show spanning-tree interface fastethernet 0/1
```

Проверка портов в состоянии блокировки:

```
show spanning-tree inconsistentports
```

Проверка журналов событий:

```
show logging
```

Таким образом, сравнительный анализ показал, что на оборудовании Cisco и Eltex механизм Root Guard имеет более наглядную диагностику, так как порт переводится в состояние Root Inconsistent, а событие может фиксироваться в системном журнале. На устройствах MikroTik схожий защитный механизм настраивается с помощью параметра restricted-role. При этом в

интерфейсе управления не выводится отдельное состояние, явно указывающее на срабатывание Root Guard. В связи с этим для обнаружения подобного события требуется дополнительно проверять состояние bridge-порта и анализировать журналы, связанные с работой STP. Данная особенность особенно важна при проектировании гетерогенных сетей, в которых одновременно применяются коммутаторы разных производителей.

Реализация Root Guard на оборудовании MikroTik

Результаты исследования показали, что при успешной реализации атаки перестроение сетевой топологии сопровождалось временной потерей связности продолжительностью примерно от 30 до 45 секунд вне зависимости от используемого оборудования. Такой интервал соответствует базовым таймерам STP, включая Max Age и Forward Delay, а также согласуется с принципами сходимости, описанными в стандарте IEEE 802.1D. При этом скорость реакции механизма Root Guard на получение superior BPDU отличалась в зависимости от платформы. Наибольшая задержка была зафиксирована на MikroTik и достигала 7 секунд. Вероятно, это связано не с особенностями самого протокола, а с механизмом обновления и отображения состояния bridge-портов в RouterOS. Оборудование Cisco и Eltex реагировало быстрее — в пределах 2–5 секунд, фактически сразу после обработки первого поддельного BPDU.

Особенности обработки BPDU и диагностики на разных платформах

Исследование зафиксировало различия не только на уровне команд активации Root Guard, но и в механизмах обработки BPDU-сообщений, регистрации событий безопасности и последующей диагностики. Эти параметры имеют прикладное значение для эксплуатации смешанных L2-инфраструктур: они определяют трудоёмкость администрирования, скорость выявления инцидента и фактическую результативность защиты топологии.

Cisco Catalyst 2960 (PVST+ / Rapid-PVST+)

Оборудование Cisco характеризуется более развитой реализацией защитных функций, что связано с применением проприетарного механизма PVST+. В соответствии с технической документацией Cisco [6], PVST+ передаёт сведения об исходной VLAN (PVID) внутри BPDU-пакета. За счёт этого коммутатор способен контролировать не только попытки несанкционированной смены корневого моста, но и отдельные ошибки конфигурации, возникающие на уровне конкретных VLAN. Для работы Root Guard такая модель обработки BPDU формирует следующие преимущества:

- **Детекция инцидентов на уровне VLAN.** При получении superior BPDU на порту, защищенном Root Guard, коммутатор Cisco анализирует не только приоритет корневого моста, но и соответствие VLAN. Если BPDU несет информацию о VLAN, отличной от настроенной на порту, порт также может быть заблокирован, что предотвращает атаки, направленные на конкретный VLAN (VLAN hopping через STP);
- **Диагностическая полнота.** Статус Root Inconsistent отображается отдельно для каждой VLAN в выводе команды show spanning-tree inconsistentports, что позволяет точно локализовать проблемный сегмент. Генерация syslog-сообщения «SPANTREE-2-ROOTGUARD-BLOCK» с указанием VLAN и порта обеспечивает немедленное оповещение администратора о попытке атаки.

MikroTik RouterOS. На устройствах MikroTik функциональный аналог Root Guard реализован через параметр restricted-role. Данный механизм основан на стандартной логике IEEE 802.1w, то есть RSTP, и не содержит дополнительных вендорских средств, направленных на упрощение диагностики срабатываний. Это приводит к ряду эксплуатационных ограничений.

Во-первых, для MikroTik характерно отсутствие VLAN-ориентированной детализации работы механизма. Стандартный RSTP оперирует не отдельными VLAN, а экземплярами дерева, поэтому при получении superior BPDU порт может быть заблокирован независимо от конкретного VLAN-контекста. В результате устройство не позволяет явно выделить атаки, направленные на отдельную VLAN в гибридной сетевой инфраструктуре.

Во-вторых, ограничены возможности диагностики. Согласно особенностям реализации MikroTik, параметр restricted-role не сопровождается отдельным состоянием, однозначно указывающим на срабатывание Root Guard. Порт переводится в состояние discarding, однако такое

состояние может возникать не только при защитной блокировке, но и в штатной работе RSTP, например для резервного Alternate-порта. Поэтому для точного определения причины изменения состояния администратору необходимо дополнительно анализировать роли портов и журналы STP. Отсутствие специализированного syslog-уведомления о срабатывании защиты усложняет оперативное выявление атаки и требует внедрения дополнительных средств мониторинга, например периодического опроса состояния bridge-портов и сравнения их ролей.

Eltex MES1428 RSTP. Коммутаторы Eltex MES1428 также используют стандартный RSTP, однако с точки зрения диагностики событий безопасности их поведение ближе к оборудованию Cisco.

Особенностью Eltex является комбинированный подход к реализации защиты. Устройство поддерживает команду spanning-tree guard root, аналогичную применяемой на Cisco, а также позволяет просматривать состояние Root Inconsistent через вывод команды show spanning-tree inconsistentports. Вместе с тем, в отличие от Cisco, данный механизм не обладает VLAN-специфичностью, поскольку функционирует в рамках стандартной реализации RSTP.

Дополнительным преимуществом Eltex является наличие системного логирования событий блокировки порта. Коммутатор формирует syslog-сообщения при срабатывании Root Guard, что упрощает интеграцию оборудования в централизованные системы мониторинга и анализа событий безопасности, включая SIEM. По этому параметру Eltex имеет преимущество перед MikroTik в инфраструктурах, где важны оперативное обнаружение инцидентов и централизованный аудит сетевой безопасности.

Логирование инцидентов. Одним из наиболее значимых различий между рассмотренными платформами является способ фиксации событий, связанных со срабатыванием защитного механизма.

На оборудовании Cisco и Eltex при блокировке порта Root Guard формируется явное системное сообщение. Для Cisco характерна явная регистрация события Root Guard в виде системного сообщения SPANTREE-2-ROOTGUARDBLOCK. Такое уведомление фиксирует попытку изменения роли конкретного порта и его перевод в состояние root-inconsistent. Наличие отдельного диагностического события сокращает время выявления воздействия на STP-топологию и позволяет оперативно передать информацию администратору.

На оборудовании MikroTik специализированное уведомление о срабатывании restricted-role по умолчанию отсутствует. Для обнаружения аналогичного события требуется предварительно включить логирование по STP-связанным темам и затем анализировать журнал на предмет нетипичных изменений ролей и состояний портов. Особое значение имеют переходы в состояния Designated и Discarding, поскольку они могут указывать на попытку вмешательства в построение топологии. Такая модель диагностики повышает требования к анализу журналов и затрудняет автоматизированное выявление попыток компрометации L2-инфраструктуры.

Отдельным методическим условием стала проверка совместимости режимов STP до начала тестирования защитных механизмов. Совместное использование PVST+ на Cisco и стандартного RSTP на MikroTik и Eltex потребовало дополнительной настройки, включая приведение магистральных портов Cisco к режиму rapid-pvst для корректного формирования единого spanning-tree-домена. При отсутствии данного этапа коммутаторы могли формировать изолированные экземпляры дерева, что искажало бы результаты последующих испытаний безопасности.

Заключение

Проведённое исследование подтвердило, что Root Guard выступает обязательным и результативным элементом защиты STP/RSTP-инфраструктуры от атак, связанных с подменой корневого моста. В экспериментальных условиях активация механизма приводила к блокированию всех попыток навязать ложный Root Bridge, при этом топология сети сохраняла устойчивое состояние.

Сравнительный анализ выявил различия в синтаксисе команд и эксплуатационных характеристиках, влияющих на итоговый уровень защищённости гетерогенной сети:

– Различия во времени реакции защиты. На оборудовании Cisco и Eltex реакция на атаку составляла 2–4 секунды, на MikroTik — 5–7 секунд. Такая задержка может иметь критическое значение для сред с жёсткими требованиями к детерминированному поведению сети и быстрому восстановлению после инцидентов.

– Критичность мониторинга. На MikroTik не формируются детализированные syslog-события, однозначно указывающие на срабатывание защиты, поэтому администраторам необходимо внедрять дополнительные процедуры обнаружения атак. Cisco и Eltex, напротив, предоставляют развёрнутую диагностику, достаточную для немедленного реагирования на инцидент.

– Влияние на связность. При активированном Root Guard атака не приводит к смене корневого моста и, соответственно, не вызывает длительной потери связности, характерной для штатного пересчёта STP продолжительностью 30–45 секунд. Этот результат подтверждает эффективность Root Guard как средства обеспечения непрерывности сервиса.

– Глубина обработки BPDU. На Cisco реализация Root Guard в связке с PVST+ обеспечивает VLAN-специфичную защиту и позволяет выявлять более широкий спектр атак, тогда как MikroTik и Eltex, работающие в рамках стандартного RSTP, реализуют защиту на уровне экземпляра дерева.

Полученные количественные данные и выявленные особенности имеют высокую прикладную значимость для специалистов, проектирующих и эксплуатирующих отказоустойчивые гетерогенные сети. Корректное применение Root Guard невозможно без учета выявленных вендор-специфичных особенностей конфигурации, диагностики и мониторинга инцидентов. При построении смешанных инфраструктур рекомендуется унифицировать режимы STP (например, переход на стандартный MSTP, поддерживаемый всеми тремя вендорами) и разрабатывать дополнительные сценарии мониторинга для платформ с ограниченной диагностикой (MikroTik) с целью обеспечения паритета в обнаружении атак.

Библиографический список

1. Малыгин, В. С. Исследование работы технологий STP, RSTP при различных показателях их характеристик / В. С. Малыгин, В. И. Фрейман // Инновационные технологии: теория, инструменты, практика. – 2022. – Т. 1. – С. 327–333. – EDN EAUKDH.
2. Чайка, Е. Ю., Шкуренков, Е. С. Атака на протокол STP: Man in the Middle. Методики тестирования и защиты / Е. Ю. Чайка, Е. С. Шкуренков // Актуальные исследования. – 2025. – № 27 (262). – С. 37–48 – URL: https://apni.ru/article/12611-ataka-na-protokol-stp-man-in-the-middle-metodiki-testirovaniya-i-zashity.
3. IEEE Std 802.1D-2004. *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*. — IEEE, 2004. — 281 p.
4. IEEE Std 802.1w-2001. *IEEE Standard for Local and Metropolitan Area Networks — Common Specifications: Rapid Reconfiguration of Spanning Tree*. — IEEE, 2001. — 54 p.
5. Seaman, M. An Overview of IEEE 802.1 Spanning Tree Protocols / M. Seaman // *IEEE 802.1 Working Group Documents*. – 2009. – 38 p. – URL: https://www.ieee802.org/1/files/public/docs2009/aq-seaman-merged-spanning-tree-protocols-0509.pdf.
6. Cisco Systems. Understanding and Configuring Spanning Tree Root Guard and BPDU Guard // Cisco Documentation. – 2019. – URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html.
7. Уймин, А. Г. Компьютерные сети. L2-технологии: практикум для СПО / А. Г. Уймин. – Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2024. – 105 с.

References

1. Malygin, V. S., & Freiman, V. I. (2022). Study of the operation of STP and RSTP technologies under various performance characteristics. *Innovative Technologies: Theory, Tools, Practice, 1*, 327–333. EDN EAUKDH.
2. Chaika, E. Yu., & Shkurenkov, E. S. (2025). Attack on the STP protocol: Man-in-the-Middle. Testing and protection techniques. *Current Research, 27*(262), 37–48. Retrieved from https://apni.ru/article/12611-ataka-na-protokol-stp-man-in-the-middle-metodiki-testirovaniya-i-zashity

3. IEEE. (2004). *IEEE Std 802.1D-2004: IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*. IEEE. https://doi.org/10.1109/IEEESTD.2004.94569
4. IEEE. (2001). *IEEE Std 802.1w-2001: IEEE Standard for Local and Metropolitan Area Networks — Common Specifications: Rapid Reconfiguration of Spanning Tree*. IEEE. https://doi.org/10.1109/IEEESTD.2001.93365
5. Seaman, M. (2009). *An overview of IEEE 802.1 spanning tree protocols* [Paper presentation]. IEEE 802.1 Working Group Documents. Retrieved from https://www.ieee802.org/1/files/public/docs2009/aq-seaman-merged-spanning-tree-protocols-0509.pdf
6. Cisco Systems. (2019). *Understanding and configuring Spanning Tree Root Guard and BPDU guard* [Technical documentation]. Cisco Documentation. Retrieved from https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html
7. Uymin, A. G. (2024). *Computer networks. Layer 2 technologies: Practical workbook for secondary vocational education*. Profobrazovanie, IPR Media.

Информация об авторах

Руфин Матвей Алексеевич — студент кафедры «Комплексная безопасность критически важных объектов», ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: rufin.m@mail.ru

Васильев Матвей Валерьевич — студент кафедры «Комплексная безопасность критически важных объектов», ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: matveyv2005@gmail.com

ISSUES OF PROTECTING STP AGAINST ATTACKS USING THE ROOT GUARD MECHANISM ON ACCESS/DISTRIBUTION LAYER SWITCHES

Rufin M. A.[1], Vasiliev M. V.[1]

[1]National University of Oil and Gas «Gubkin University»

Abstract. *The article examines the problem of protecting the data link layer of a corporate network against attacks aimed at spoofing the root bridge in STP and RSTP protocols. The relevance of the study is determined by the fact that, without additional protection mechanisms, an attacker with access to a switch port can send forged BPDU packets with a higher priority and trigger an unauthorized topology change. This may lead to spanning tree recalculation, temporary loss of connectivity, and conditions for traffic interception or disruption. The purpose of the study is to experimentally evaluate the effectiveness of the Root Guard mechanism in a heterogeneous network infrastructure based on Cisco Catalyst 2960, MikroTik, and Eltex MES1428 switches. During the experiment, an attack was simulated using the Yersinia tool, the network behavior with disabled and enabled protection was compared, and vendor-specific differences in Root Guard configuration and diagnostics were analyzed. The results showed that, without protection, the attacking host successfully became the root bridge in all tested scenarios, causing instability in the network topology. After Root Guard was enabled, forged superior BPDU packets were blocked, and protected ports were placed into a blocking state, preventing unauthorized Root Bridge changes. The study concludes that Root Guard is an effective mechanism for protecting L2 topology, but its correct use requires consideration of vendor-specific implementation features and proper security event monitoring.*

Keywords: *STP protocol, Root Guard, root bridge, BPDU packet, network security, network topology, switch.*

Information about the authors

Rufin Matvey Alekseevich — Student of the Department of «Comprehensive Security of Critical Facilities», National University of Oil and Gas «Gubkin University», Russia, Moscow, e-mail: rufin.m@mail.ru

Vasiliev Matvey Valeryevich — Student of the Department of «Comprehensive Security of Critical F

acilities», National University of Oil and Gas «Gubkin University», Russia, Moscow, e-mail: matveyv2005@gmail.com

ПРОФЕССИОНАЛИТЕТ, 2025, № 2 (006)

УДК *004.056.53*

Е. А. Еремина [1]***, А. Н. Простова*** [1]

[1]*ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация*

ВЛИЯНИЕ АТАКИ MAC-FLOODING НА КОММУТАТОРЫ L2 В ГИБРИДНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЕ

Аннотация: *Проведенное исследование выявляет критическую уязвимость L3-устройств в гибридных сетях при атаках на канальном уровне. Экспериментально показано, классическая атака MAC-flooding, направленная на переполнение CAM-таблиц коммутаторов доступа, приводит не только к нарушению конфиденциальности трафика на L2-уровне, но и вызывает каскадный рост нагрузки на маршрутизаторы (L3) из-за массовой генерации unknown unicast-трафика. Данный трафик перенаправляется на маршрутизатор, приводя к критической нагрузке на его процессор, увеличении времени отклика и возможному отказу в обслуживании для всей сетевой инфраструктуры.*

В работе проведено сравнительное тестирование стандартных механизмов защиты (Port Security, Storm Control) на оборудовании различных производителей в условиях смоделированной атаки. Эксперименты проводились на стенде с использованием оборудования Cisco, Mikrotik и Eltex, атака генерировалась средствами Kali Linux. Результаты демонстрируют, что активация Port Security в режиме shutdown на портах доступа является наиболее эффективным способом блокировки атаки в источнике. Для обеспечения комплексной устойчивости гибридной сети эту меру необходимо дополнять ограничением широковещательного трафика на уровне маршрутизатора.

Полученные данные имеют важное прикладное значение для обеспечения отказоустойчивости и безопасности современных гибридных сетевых инфраструктур, объединяющих оборудование различных вендоров, и позволяют сформулировать практические рекомендации по настройке безопасности для сетей, объединяющих оборудование различных производителей, с целью предотвращения эскалации L2-атак на L3-уровень.

Ключевые слова: *MAC-flooding, сетевая безопасность, L3 маршрутизатор, L2 коммутатор, CAM-таблица, unknown unicast, Port Security.*

Введение

В современном мире в информационной среде все более активно используются L3 устройства, работающие с IP-адресами и имеющие функцию маршрутизации и соединения различных VLAN. L3 коммутатор соединяет в себе функции L2 коммутатора и маршрутизатора, то есть может выполнять все функции обычного коммутатора (L2), но также обладает «интеллектуальными» функциями маршрутизатора, которые позволяют эффективно передавать данные между различными сетями без необходимости использования внешнего маршрутизатора [1]. Такая интеграция создает новые угрозы информационной безопасности.

Особенностью современных вызовов информационной безопасности является приобретение классическими атаками на канальном уровне модели новых качеств. Основная проблема заключается в недооценке данной эволюции.

Цель исследования: разработка эффективного метода защиты от атаки MAC-flooding на L3 устройства.

Объект исследования: защищенность гибридной сетевой инфраструктуры, включающей L3-устройства (маршрутизаторы), от атак на канальном уровне.

Предмет исследования: механизм влияния атаки MAC-flooding, проводимой на L2-коммутаторах доступа, на производительность и отказоустойчивость L3-маршрутизаторов, а также сравнительная эффективность методов защиты.

На классическом L2 коммутаторе цель атаки: переполнение CAM-таблицы с последующим переходом устройства в режим хаба для перехвата трафика (нарушение конфиденциальности) [2].

Материалы и методы

Анализ показывает, что атака MAC-flooding была и остается актуальной угрозой для L3-устройств, несмотря на наличие базовых механизмов защиты. В 2015 году в фундаментальном исследовании Florent Gontharet «Man-in-The-Middle Attacks & Countermeasures Analysis»

(Университет Абертей Данди) [3] описана базовая уязвимость коммутатора: атака успешно реализуема с помощью macof из dsniff, приводит к переполнению CAM-таблицы виртуального коммутатора Cisco и требует защиты с мониторингом MAC-адресов.

В 2018 году исследование Simran Thakur et al.: «Three tier architecture with enhanced security at layer 2 And layer 3» (IARJSET, CETE-2018) [4] пришло к следующим выводам: атака возможна из-за динамического изучения адресов на L2/L3-свитчах трехуровневой архитектуры, приводит к DoS и перехвату трафика флудом уникальных MAC; протестировано в GNS3 на Cisco-оборудовании.

В 2023 году Скоробогатова С.Ю. и др. «Методика прогнозирования воздействия компьютерных атак на элементы программно-конфигурируемой сети» [5] выявили успешность атаки как элемента многоуровневого DoS в SDN-инфраструктурах с L3-элементами, с нарушением работы критических сетевых компонентов.

Руководство Cisco «Configure DHCP Snooping» (2018) [6] подтвердило эффективность port security и DHCP Snooping для L3-устройств против MAC-flooding в связке с DAI.

Однако проведенный анализ литературы показал, что большинство исследований на тему атаки MAC-flooding сосредоточено либо на теоретическом описании угрозы, либо на инструкциях по настройке отдельных защитных механизмов, также основное внимание уделено атакам на атаки 2 уровня модели OSI (L2).

Тип исследования: анализ уязвимости с элементами экспериментального исследования в лабораторной среде.

Характеристика среды исследования: лабораторная сетевая инфраструктура, включающая коммутаторы L2 различных производителей, L3 маршрутизатор Cisco 1941, а также три конечных узла. Один из конечных узлов на базе ОС Kali Linux использовался в качестве источника атаки, второй узел на базе ОС Альт Linux использовался как пользователь сети, третий узел применялся для мониторинга сетевого трафика и фиксации аномалий.

Процедура проведения эксперимента:

- Развертывание и настройка базовой тестовой сети.
- Определение базовых показателей и ролей узлов.
- Проведение атаки MAC-flooding.
- Мониторинг и анализ последствий атаки.
- Тестирование механизмов защиты.
- Сравнительный анализ и формирование выводов.

Методы обработки данных: анализ успешности атаки, сравнение эффективности методов защиты, качественный анализ эффективности защитных мер.

При атаке MAC-flooding злоумышленник отправляет в сеть большое количество пакетов с поддельными или случайными MAC-адресами источников. Это приводит к быстрому заполнению таблицы MAC-адресов коммутатора. Когда таблица достигает своей емкости, коммутатор больше не может сопоставлять MAC-адреса с определенными портами и переходит в режим fail-open, в котором он начинает перекачивать входящий трафик через все порты. Это позволяет злоумышленнику перехватывать трафик, так как после атаки коммутатор транслирует трафик на все порты.

Port Security – это функция коммутаторов Cisco и подобных (например, Eltex), которая контролирует доступ к порту на основе MAC-адресов. Она позволяет привязать к порту только определенные MAC-адреса и блокировать неавторизованные устройства.

На оборудовании Mikrotik аналогичная функциональность обеспечивается параметром learn-limit для портов моста, который выполняет ту же задачу: блокирует изучение новых MAC-адресов сверх заданного предела.

Эксперимент был ориентирован на анализ последствий переполнения CAM-таблицы коммутаторов доступа (Cisco Catalyst 2960, Mikrotik CRS326, Eltex MES1428) и оценку эффективности встроенных механизмов защиты при воздействии высокоинтенсивного потока кадров с поддельными MAC-адресами.

Эксперимент был проведен с различными устройствами L2, L3 уровня и PC с операционной системой Linux. На рисунке 1 представлена используемая топология сети.

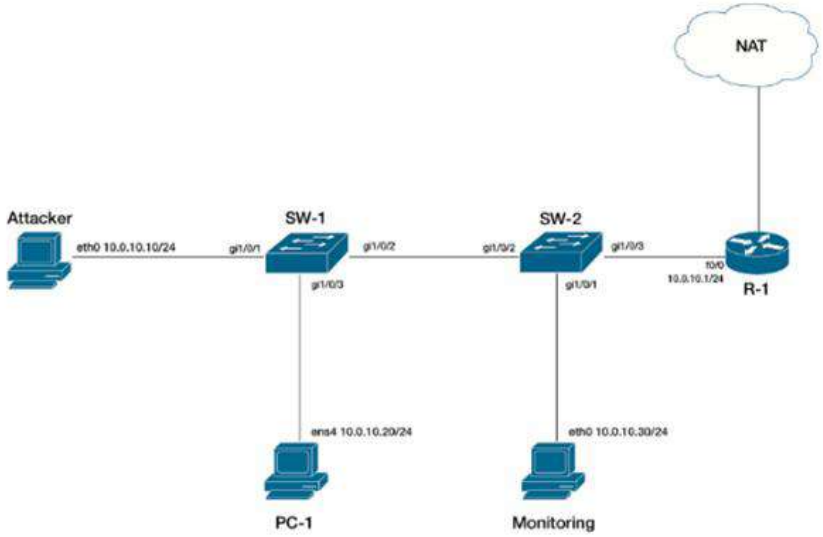

Рис. 1. Топология сети для эксперимента

Подготовка оборудования:

- коммутаторы: Cisco Catalyst 2960 (версия 15.0(2)SE11), Cisco Catalyst 3550 (версия 12.2(55)SE12), Mikrotik Cloud Router Switch CRS326-24G-2S+RM (версия 15.2(4)M7), Eltex MES1428 (версия 10.4.2.1);
- маршрутизатор: Cisco 1941 (версия 15.2(4)M7);
- ПК №1 (атакующий): Kali Linux с интерфейсом ens0;
- ПК №2 (жертва): Alt Linux с интерфейсом ens4;
- ПК №3 (мониторинг): Kali Linux с интерфейсом ens0.

Конфигурация сетевых узлов осуществлялась следующим образом:

– На атакующем узле (Kali Linux) выполнена базовая настройка сетевого интерфейса eth0. Был назначен статический IP-адрес 10.0.10.10/24; активирован интерфейс; добавлен маршрут по умолчанию через шлюз 10.0.10.1.

– На пользовательском узле (Alt Linux) установлено имя хоста (Eremina-ALT); назначен статический IP-адрес 10.0.10.20/24 на интерфейс ens4; указан DNS сервер 1.1.1.1; добавлен маршрут по умолчанию через шлюз 10.0.10.1 для проверки доступности шлюза.

– На узле мониторинга, который нужен для захвата и анализа трафика в ходе эксперимента, назначен статический IP-адрес 10.0.10.30/24 на интерфейс eth0; также указан DNS-сервер 1.1.1.1 и добавлен маршрут по умолчанию через шлюз 10.0.10.1.

– На коммутаторе доступа Eremina-SW1 (Cisco Catalyst 2960) была выполнена следующая конфигурация портов: порт GigabitEthernet0/1 настроен как access для атакующего узла; порт GigabitEthernet0/2 настроен как access для узла-пользователя. Также оба порта помещены в VLAN 1 (нативный VLAN); активирован spanning-tree portfast для ускорения перехода портов в активное состояние. Коммутатор обеспечивает канальное соединение узлов внутри одного широковещательного домена [7]. См. рис. 2.

```
Switch(config)#hostname Eremina-SW1
Eremina-SW1(config)#no ip domain-lookup
Eremina-SW1(config)#spanning-tree mode rapid-pvst
Eremina-SW1(config)#interface gi0/0
Eremina-SW1(config-if)#description Kali
Eremina-SW1(config-if)#switchport mode access
Eremina-SW1(config-if)#switchport access vlan 1
Eremina-SW1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet0/0 but will only
 have effect when the interface is in a non-trunking mode.
Eremina-SW1(config-if)#interface gi0/2
Eremina-SW1(config-if)#description ALT-user
Eremina-SW1(config-if)#switchport mode access
Eremina-SW1(config-if)#switchport access vlan 1
Eremina-SW1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet0/2 but will only
 have effect when the interface is in a non-trunking mode.
Eremina-SW1(config-if)#no shutdown
exitina-SW1(config-if)#
Eremina-SW1(config)#
```

Рис. 2. Конфигурация портов коммутатора Cisco Catalyst 2960 (Eremina-SW1)

Коммутатор доступа Eremina-SW2 был настроен аналогично. Порт GigabitEthernet0/0 настроен как access для узла мониторинга; порт GigabitEthernet0/1 предназначен для uplink-соединения; все порты размещены в VLAN 1. Второй коммутатор необходим для подключения узла мониторинга к зеркальному (SPAN) порту без влияния на основной трафик атаки между коммутатором-жертвой и маршрутизатором.

На маршрутизаторе Eremina-R1 была выполнена следующая конфигурация: интерфейс FastEthernet0/0 настроен как внутренний с адресом 10.0.10.1/24; интерфейс FastEthernet0/1 настроен как внешний с получением адреса через DHCP; настроен NAT для трансляции адресов сети 10.0.10.0/24; а также добавлен статический маршрут по умолчанию через внешний интерфейс.

Все конечные узлы и маршрутизатор были размещены в одном широковещательном домене VLAN. Маршрутизатор выполнял функции шлюза по умолчанию для всех узлов и обеспечивал выход во внешнюю сеть через механизм NAT. Была проверена связность устройств, в результате выводится динамическая таблица MAC-адресов, содержащая всего 5 записей, что соответствует нормальному состоянию сети. См. рис. 3.

```
Eremina-SW1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0c2d.2325.0001    DYNAMIC     Gi0/1
   1    0c2d.245d.0000    DYNAMIC     Gi0/2
   1    0cc6.dc13.0000    DYNAMIC     Gi0/2
   1    0cfe.f737.0000    DYNAMIC     Gi0/1
   1    c201.23e3.0000    DYNAMIC     Gi0/1
-------------------------------------------
Total Mac Addresses for this criterion: 5
```

Рис. 3. CAM-таблица коммутатора в штатном режиме, содержащая 5 записей

На следующем этапе с узла-нарушителя была инициирована атака с помощью команды: *macof –I eth0*. В процессе атаки фиксировались изменения в работе коммутаторов, рост количества динамических MAC-адресов, увеличение числа неизвестных unicast-кадров, а также рост нагрузки на плоскость управления устройств. См. рис. 4.

```
Eremina-SW1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    3a7f.9c21.a4d8    DYNAMIC     Gi0/0
   1    b6c2.0e91.7f33    DYNAMIC     Gi0/0
   1    5d11.84a0.c9ef    DYNAMIC     Gi0/0
   1    9e3a.6f18.22b7    DYNAMIC     Gi0/0
   1    0001.ff49.bff9    DYNAMIC     Gi0/0
   1    0018.bd4a.c66f    DYNAMIC     Gi0/0
   1    0022.4950.02f7    DYNAMIC     Gi0/0
   1    002f.c02e.090e    DYNAMIC     Gi0/0
   1    003a.5c36.f671    DYNAMIC     Gi0/0
   1    003d.e509.6f35    DYNAMIC     Gi0/0
   1    0004.b278.e74f    DYNAMIC     Gi0/0
   1    0046.bf4b.2278    DYNAMIC     Gi0/0
   1    004d.2a10.bf13    DYNAMIC     Gi0/0
   1    0010.bd75.684d    DYNAMIC     Gi0/0
   1    0052.9d7a.7733    DYNAMIC     Gi0/0
   1    0013.d278.426b    DYNAMIC     Gi0/0
--More--
```

Рис. 4. CAM-таблица во время атаки MAC-flooding

В ходе атаки MAC-flooding в CAM-таблице коммутатора фиксировались многочисленные динамические MAC-адреса, ассоциированные с одним портом доступа. Данные адреса носили случайный характер и постоянно изменялись, что указывает на искусственную генерацию MAC-адресов узлом-нарушителем. Количество динамических MAC-записей в VLAN 1 достигло 21 154, что подтверждает успешное проведение атаки. См. рис. 5.

```
Eremina-SW1#show mac address-table count

Mac Entries for Vlan 1:
------------------------
Dynamic Address Count   : 21154
Static Address Count    : 0
Total Mac Addresses     : 21154

Total Mac Address Space Available: 68133102
```

Рис. 5. Подтверждение переполнения CAM-таблицы: 21154 записи в VLAN 1

В ходе атаки MAC-flooding на мониторинговом узле, подключенном к зеркальному порту коммутатора, фиксировалось поступление Ethernet-кадров, адресованных на MAC-адреса, не принадлежащие данному узлу. Анализ захваченных пакетов показал наличие случайных MAC- и IP-адресов назначения, что свидетельствует о том, что все unknown unicast-кадры широковещательно рассылаются на все порты VLAN, в том числе и на порт мониторинга. См. рис. 6.

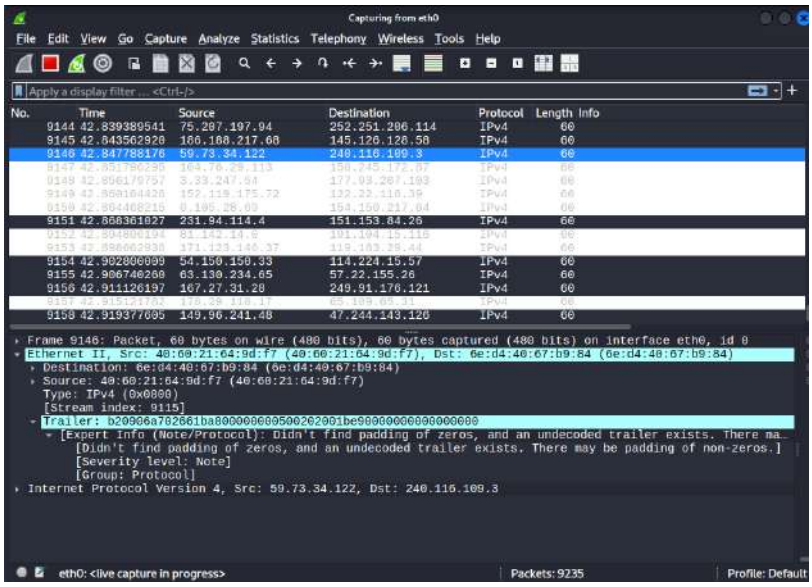

Рис. 6. Анализ трафика в Wireshark: кадры unknown unicast со случайными MAC-адресами

На данном этапе эксперимента на коммутаторе Eremina-SW1 была активирована и поэтапно протестирована функция Port Security на порту GigabitEthernet0/0, к которому подключен атакующий узел. Тестирование проводилось в два этапа: сначала в режиме Restrict, затем в режиме Shutdown. См. рис. 7-10.

```
enable
conf t
interface GigabitEthernet0/0
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
end
```

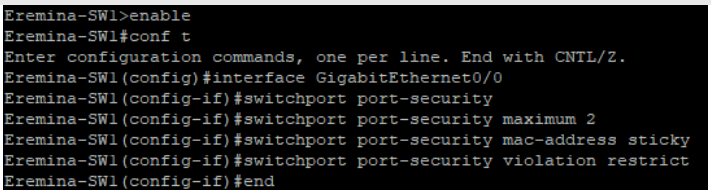

Рис. 7. Настройка Port Security в режиме Restrict с лимитом 2 MAC-адреса

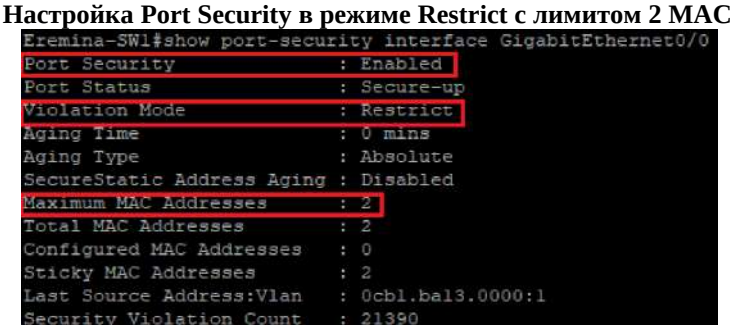

Рис. 8. Port Security в режиме Restrict: 21390 нарушений, порт активен

На рисунке 8 видно, что на интерфейсе gi0/0 настроен Port Security с лимитом в 2 MAC-адреса, используется режим Restrict, и зафиксировано более 21 тысячи нарушений.

```
interface gi0/0
switchport port-security
switchport port-security maximum 2
switchport port-security violation shutdown
switchport port-security mac-address sticky
```

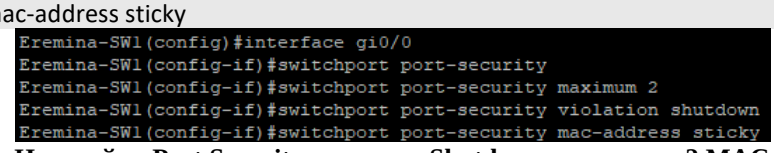

Рис. 9. Настройка Port Security в режиме Shutdown с лимитом 2 MAC-адреса

Рис. 10. Результат срабатывания Port Security: порт в состоянии secure-shutdown

На рисунке 10 видно, что на интерфейсе Gi0/0 настроен Port Security с лимитом в 1 MAC-адрес в строгом режиме Shutdown. В результате одного нарушения безопасности порт был переведен в заблокированное состояние (secure-shutdown).

В захвате трафика отсутствуют кадры с поддельными MAC-адресами и случайными IP.

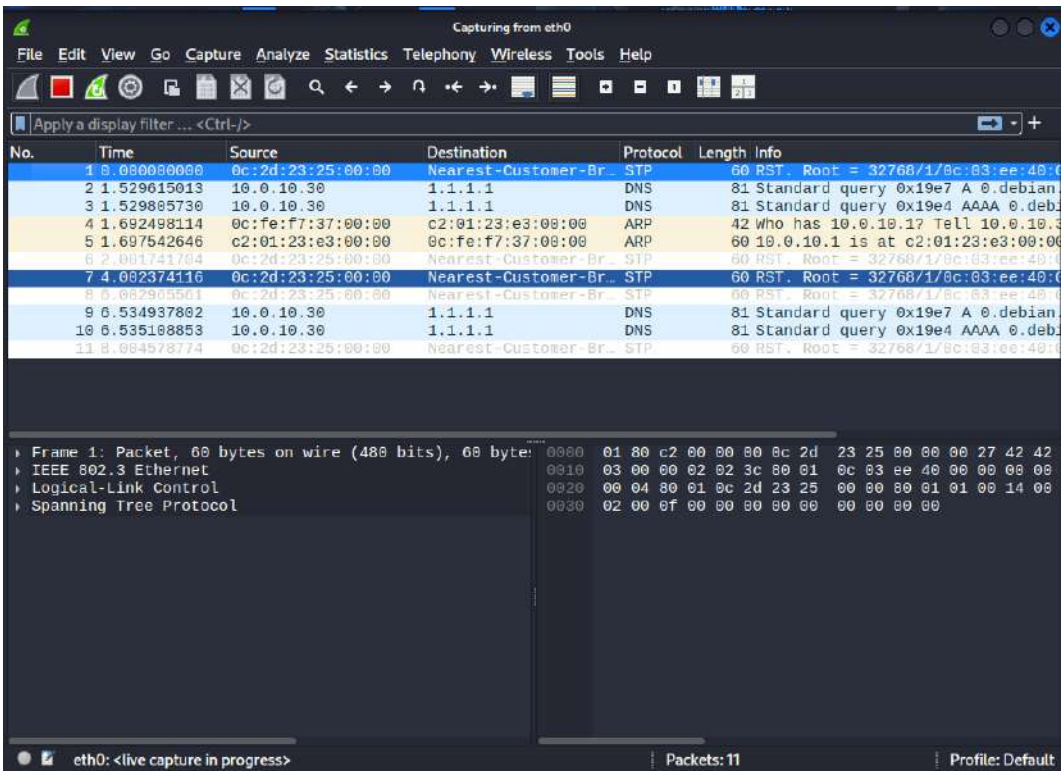

Рис. 11. Мониторинг Wireshark после активации Port Security, прекращение флуда

Режим Shutdown функции Port Security обеспечил эффективную и мгновенную изоляцию источника атаки, что позволило сети вернуться к штатному режиму работы без снижения производительности.

Для сравнения поведения оборудования различных производителей атака MAC-flooding также была последовательно проведена на коммутаторах доступа Mikrotik Cloud Router Switch CRS326-24G-2S+RM, Eltex MES1428, которые были интегрированы в ту же лабораторную топологию на месте коммутатора Eremina-SW1.

Базовая настройка Mikrotik CRS326 включала создание моста bridge1 с включением портов ether1-ether4, назначение IP-адреса управления и проверку штатного заполнения таблицы MAC-адресов. См. рис. 12.

```
[admin@MikroTik] > /system identity set name=Eremina-SW1
[admin@Eremina-SW1] > /interface bridge add name=bridge1 protocol-mode=rstp
[admin@Eremina-SW1] > /interface bridge port add bridge=bridge1 interface=ether1
[admin@Eremina-SW1] > /interface bridge port add bridge=bridge1 interface=ether2
[admin@Eremina-SW1] > /interface bridge port add bridge=bridge1 interface=ether3
[admin@Eremina-SW1] > /interface bridge port add bridge=bridge1 interface=ether4
[admin@Eremina-SW1] > /interface bridge set bridge1 vlan-filtering=no
[admin@Eremina-SW1] > /ip address add address=10.0.10.2/24 interface=bridge1
[admin@Eremina-SW1] > /ip route add gateway=10.0.10.1
[admin@Eremina-SW1] > /interface ethernet set ether1 comment="Kali-attacker"
[admin@Eremina-SW1] > /interface ethernet set ether2 comment="ALT-user"
[admin@Eremina-SW1] > /interface ethernet set ether3 comment="Uplink-to-SW2"
[admin@Eremina-SW1] > /interface ethernet set ether4 comment="Monitoring"
[admin@Eremina-SW1] > /interface bridge host print
Flags: X - disabled, I - invalid, D - dynamic, L - local, E - external
#       MAC-ADDRESS       VID  ON-INTERFACE   BRIDGE    AGE
0   DL  0C:3A:5D:39:00:00       ether1   bridge1
1   DL  0C:3A:5D:39:00:01       ether2   bridge1
2   DL  0C:3A:5D:39:00:02       ether3   bridge1
3   DL  0C:3A:5D:39:00:03       ether4   bridge1
[admin@Eremina-SW1] >
```

Рис. 12. Настройка коммутатора Mikrotik CRS326

После проведения атаки общее количество записей в таблице моста составило 9051, таблица MAC-адресов с порта ether1 наглядно демонстрирует их случайный характер и высокую интенсивность поступления, что привело к исчерпанию ресурсов устройства. См. рис. 13.

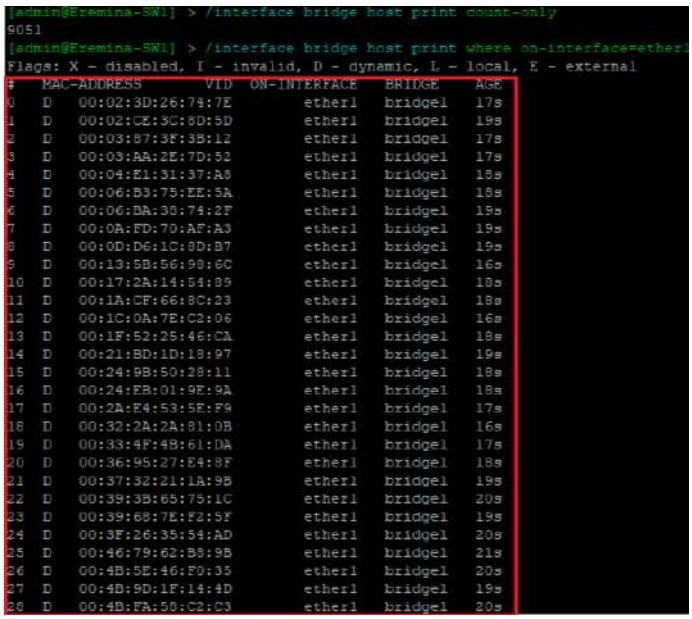

Рис. 13. Результат атаки на Mikrotik: 9051 запись в таблице моста

При попытке использования IP Firewall атака продолжилась, так как MAC-flooding действует на уровне L2 до обработки правил межсетевого экрана L3.

Эффективным механизмом защиты на коммутатор Mikrotik оказалось ограничение числа используемых MAC-адресов на порту с помощью параметра learn-limit. После установки learn-limit=2 на порт ether1 общее количество записей в таблице моста сократилось до 6, что подтверждает блокировку фреймов с поддельными MAC-адресами и остановку атаки. См. рис. 14.

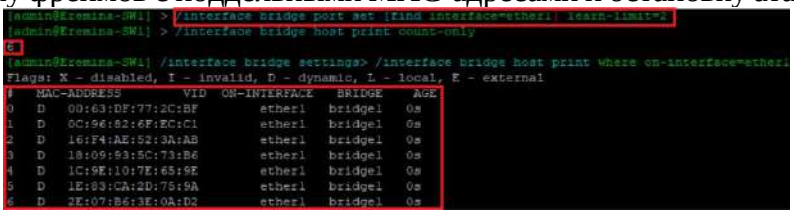

Рис. 14. Таблица MAC-адресов после защиты learn-limit=2 с 6 записями

Далее в работе исследуется поведение коммутатора Eltex MES1428 в условиях атаки MAC-flooding, а также тестируются доступные на данном оборудовании контрмеры.

До атаки таблица MAC-адресов содержит 4 динамические записи, ошибки на портах отсутствуют, загрузка CPU составляет 3%. Это демонстрирует нормальную работу устройства. См. рис. 15.

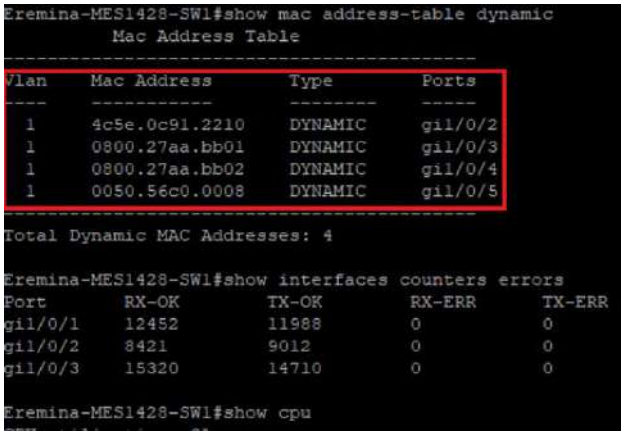

Рис. 15. Eltex MES1428 в штатном режиме: 4 MAC-записи, CPU 3%

После проведения атаки количество MAC-адресов достигло 5089, система зафиксировала критические события: переполнение таблицы MAC, чрезмерный unknown unicast-трафик. Загрузка CPU выросла до 38%. См. рис. 16.

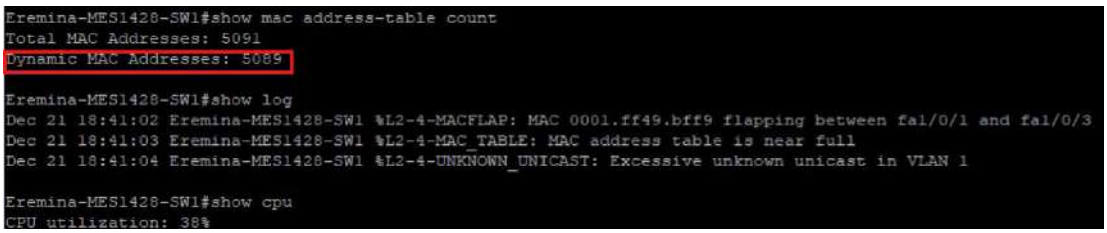

Рис. 16. Последствия атаки на Eltex: 5089 MAC-записей, CPU 38%

Для противодействия атаке на коммутаторе Eltex были последовательно протестированы два механизма: Storm Control (ограничение широковещательного и неизвестного unicast-трафика на уровне 1%) показал себя как сдерживающая, но не предотвращающая мера. При включенном Storm Control количество MAC-записей в CAM-таблице выросло с 4 до 5089 (рис. 15, 16), а загрузка CPU сохранялась на уровне 38%, что указывает на высокую нагрузку из-за обработки огромного числа кадров. Это подтверждает, что Storm Control ограничивает лишь последствия атаки (широковещательный шторм), но не влияет на процесс изучения поддельных MAC-адресов. CAM-таблица продолжает переполняться, нагрузка на CPU остаётся высокой, и часть аномального трафика всё же достигает вышестоящих устройств. Port Security с лимитом в 2 MAC-адреса и реакцией shutdown обеспечил полную нейтрализацию угрозы, переведя порт атакующего в состояние secure-shutdown после первого же нарушения и очистив таблицу MAC-адресов до штатного размера. См. рис. 17, 18, 19.

```
configure
interface fa1/0/1
storm-control broadcast level 1
storm-control unknown-unicast level 1
exit
exit
```

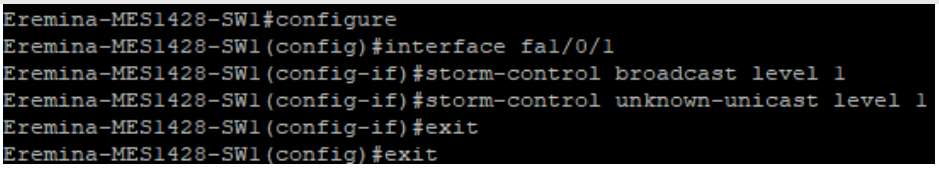

Рис. 17. Конфигурация Storm Control на Eltex

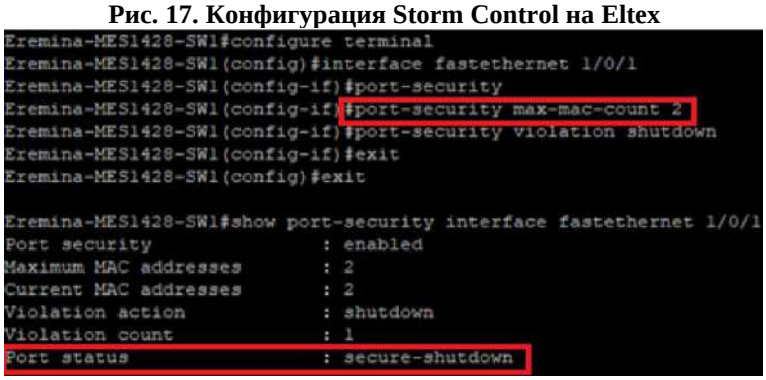

Рис. 18. Настройка Port Security на Eltex с лимитом 2 MAC-адреса

Рис. 19. Результат Port Security на Eltex: таблица MAC-адресов очищена (4 динамические записи)

Результаты

В ходе экспериментального исследования подтверждены переполнение CAM-таблицы и рост нагрузки CPU на коммутаторах доступа. Отдельные метрики L3-маршрутизатора, включая CPU, задержку, потери и ARP-нагрузку, не измерялись, поэтому влияние на L3 в данной работе не оценивается.

На оборудовании Cisco после включения механизма Port Security в режиме Restrict было зафиксировано прекращение распространения flood-трафика за пределы порта доступа, стабилизация CAM-таблиц и отсутствие деградации сетевой связности для легитимных узлов. При этом узел-нарушитель продолжал генерировать кадры с поддельными MAC-адресами, которые отбрасывались коммутатором на уровне порта доступа.

В результате фиксировался значительный рост количества событий нарушения безопасности и увеличение нагрузки на CPU коммутатора. При переводе механизма Port Security в режим Shutdown порт доступа автоматически переводился в состояние err-disabled при первом нарушении, что приводило к полному прекращению приема трафика с узла-нарушителя, что согласуется с общепринятыми практиками защиты на основе Port Security, подробно описанными в работе Protecting Against MAC Flooding Attack [8].

Сравнительный анализ показал, что принцип ограничения числа изучаемых MAC-адресов на порту является универсальной и эффективной контрмерой, успешно реализованной у различных производителей. На коммутаторе Eltex функция Port Security с идентичными параметрами также остановила атаку; на коммутаторе Mikrotik роль аналогичного механизма защиты выполняет параметр learn-limit.

Таким образом, в ходе тестирования на оборудовании различных производителей были получены следующие результаты:

- Cisco Catalyst 2960: Port Security в режиме Shutdown эффективно заблокировал порт после первого нарушения, что подтверждено переводом порта в состояние secure-shutdown;
- Mikrotik CRS326: использование параметра learn-limit=2 на порте ether1 позволило ограничить количество изучаемых MAC-адресов и остановить атаку, сократив количество записей в таблице моста до штатного уровня;
- Eltex MES1428: Port Security с лимитом в 2 MAC-адреса и реакцией Shutdown также обеспечил полную нейтрализацию угрозы, переведя порт в состояние secure-shutdown после первого нарушения.

Для оборудования Mikrotik, помимо параметра learn-limit, может использоваться Bridge Filter – штатный инструмент L2-фильтрации. Для блокировки поддельных ARP-пакетов при MAC-flooding атаке можно добавить правило: /interface bridge filter add chain=forward mac-protocol=arp action=drop. Однако в ходе эксперимента learn-limit показал себя как более простое и эффективное решение именно для предотвращения переполнения CAM-таблицы, так как Bridge Filter фильтрует трафик, но не предотвращает само заполнение таблицы MAC-адресов. Bridge Filter может использоваться как дополнительная мера, например, для борьбы с ARP-спуфингом, но не заменяет защиту от переполнения CAM-таблицы.

Для наглядной оценки эффективности механизма Port Security при противодействии MAC-flooding в таблице 1 представлен сравнительный анализ двух основных режимов реакции на нарушение.

Таблица 1 – Сравнительный анализ режимов реакции Port Security на атаку MAC-flooding

Критерий оценки	Режим restrict	Режим shutdown
Принцип действия	Отбрасывание кадров с неразрешенных MAC-адресов. Порт остается активным	Немедленное отключение порта (перевод в состояние err-disabled)
Влияние на атакующий трафик	Трафик блокируется, но атака продолжается	Атака полностью останавливается после первого нарушения
Нагрузка на CPU коммутатора	Высокая	Отсутствует
Рекомендуемый сценарий применения	Сети, где важен мониторинг атак без остановки обслуживания	Сети, где приоритетом является мгновенная нейтрализация угрозы.

Заключение

Исследование подтвердило:

- успешная атака MAC-flooding приводит к полному переполнению CAM-таблицы коммутатора, что вызывает переход устройства в режим hub и массовую рассылку unknown

unicast-трафика по всем портам VLAN, нарушая доступность сети и создавая угрозу перехвата трафика;

- встроенная функция Port Security (а также ее аналоги) доказала свою результативность на оборудовании различных производителей (Cisco, Mikrotik, Eltex), однако ее режимы демонстрируют различный баланс между безопасностью и эксплуатационными издержками;
- для оборудования Mikrotik эффективным механизмом защиты оказалось ограничение числа MAC-адресов на порту (learn-limit), что также позволяет предотвратить атаку без полного отключения порта.

Это демонстрирует необходимость выбора режима защиты, основанного на приоритетах конкретной сети: максимальная автоматическая защита (Shutdown) или сохранение подключения с мониторингом событий (Restrict, learn-limit).

Атака MAC-flooding остаётся серьёзной угрозой для сетей уровня доступа и может нарушить стабильность L2-инфраструктуры. В ходе исследования были экспериментально проанализированы механизм ее воздействия и дана сравнительная оценка стандартных контрмер на оборудовании различных производителей.

Практические рекомендации:

- включение функции Port Security (или аналогов, таких как learn-limit на Mikrotik) на всех пользовательских портах доступа является обязательной базовой мерой;
- для портов общего пользования рекомендуется режим Restrict с ведением лога событий;
- реализация функций DHCP Snooping и Dynamic ARP Inspection (DAI) в связке с Port Security для комплексного противодействия атакам на канальном уровне;
- настройка систем мониторинга (SNMP, Syslog) для отслеживания событий безопасности портов и статистики unknown unicast-трафика для оперативного выявления инцидентов.

Библиографический список

1. Уровни OSI: простое объяснение и отличия коммутаторов L1, L2 и L3 : [сайт]. – Москва, 2024. – URL: https://servergate.ru/articles/otlichiya-kommutatorov-l1-l2-i-l3/ (дата обращения: 05.11.2025). – Текст: электронный.
2. Что такое MAC Flooding? Как его предотвратить? : [сайт] / Alexhost. – 2024. – URL: https://alexhost.com/ru/faq/what-is-mac-flooding-how-to-prevent-it/ (дата обращения: 20.11.2025).– Текст: электронный.
3. Gontharet, F. Man-in-The-Middle Attacks & Countermeasures Analysis [Электронный ресурс]. – Dundee : University of Abertay Dundee, 2015. – 66 с. – URL: https://www.researchgate.net/publication/340720434_Man-in-The-Middle_Attacks_Countermeasures_Analysis (дата обращения: 10.12.2025). – Текст: электронный.
4. Thakur, S. Three tier architecture with enhanced security at layer 2 And layer 3 [Электронный ресурс] / S. Thakur, A. Khan, J. Dave, S. Kaulgud // International Advanced Research Journal in Science, Engineering and Technology. – 2018. – Vol. 5, Special Issue 3. – С. 13-18. – URL: https://clck.ru/3Qy9Ak (дата обращения: 10.12.2025). – Текст: электронный.
5. Скоробогатов, С. Ю. Методика прогнозирования воздействия компьютерных атак на элементы программно-конфигурируемой сети [Электронный ресурс] / С. Ю. Скоробогатов, И. М. Жданова, А. В. Кузнецов, А. А. Осипенко, Р. Р. Хабушев // Известия Тульского государственного университета. Технические науки. – 2023. – Вып. 2. – С. 269–274. – DOI: 10.24412/2071-6168-2023-2-269-274. – URL: https://cyberleninka.ru/article/n/metodika-prognozirovaniya-vozdeystviya-kompyuternyh-atak-na-elementy-programmno-konfiguriruemoy-seti (дата обращения: 11.12.2025). – Текст: электронный.
6. Configure Dynamic Host Configuration Protocol (DHCP) Snooping on a Switch through the Command Line Interface (CLI) : [сайт] / Cisco. – 2018. – URL: https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-

managed-switches/smb5515-configure-dynamic-host-configuration-protocol-dhcp-snooping.html (дата обращения: 20.12.2025). – Текст: электронный.
7. Уймин, А. Г. Компьютерные сети. L2-технологии : практикум для СПО / А. Г. Уймин. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2024. – 190 с. – ISBN 978-5-4497-2559-2, 978-5-4488-1745-8. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/135231.html (дата обращения: 15.11.2025). – Режим доступа: для авторизир. пользователей. – Текст: электронный.
8. Защита от атаки с переполнением MAC-адреса : [сайт] / R. Brezular. – 2024. – URL: https://brezular.com/2024/01/03/protecting-against-mac-flooding-attack/ (дата обращения: 09.12.2025). – Текст: электронный.

References

1. ServerGate. (2024). OSI Layers: A Simple Explanation and Differences Between L1, L2, and L3 Switches. ServerGate. Retrieved November 5, 2025, from https://servergate.ru/articles/otlichiya-kommutatorov-l1-l2-i-l3/ (accessed: 05.11.2025).
2. Alexhost. (2024). What is MAC Flooding? How to prevent it? Alexhost. Retrieved November 20, 2025, from https://alexhost.com/ru/faq/what-is-mac-flooding-how-to-prevent-it/ (accessed: 20.11.2025).
3. Gontharet, F. (2015). Man-in-The-Middle Attacks & Countermeasures Analysis [Master's thesis, University of Abertay Dundee]. ResearchGate. Retrieved December 10, 2025, from https://www.researchgate.net/publication/340720434_Man-in-The-Middle_Attacks_Countermeasures_Analysis (accessed: 10.12.2025).
4. Thakur, S., Khan, A., Dave, J., & Kaulgud, S. (2018). Three tier architecture with enhanced security at layer 2 and layer 3. International Advanced Research Journal in Science, Engineering and Technology, 5(Special Issue 3), 13–18. Retrieved December 10, 2025, from https://clck.ru/3Qy9Ak (accessed: 10.12.2025).
5. Skorobogatov, S. Yu., Zhdanova, I. M., Kuznetsov, A. V., Osipenko, A. A., & Khabushev, R. R. (2023). A methodology for predicting the impact of cyberattacks on software-defined network elements. Bulletin of the Tula State University. Technical Sciences, (2), 269–274. https://cyberleninka.ru/article/n/metodika-prognozirovaniya-vozdeystviya-kompyuternyh-atak-na-elementy-programmno-konfiguriruemoy-seti (accessed: 11.12.2025).
6. Cisco. (2018). Configure Dynamic Host Configuration Protocol (DHCP) Snooping on a Switch through the Command Line Interface (CLI). Cisco Support. Retrieved December 20, 2025, from https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5515-configure-dynamic-host-configuration-protocol-dhcp-snooping.html (accessed: 20.12.2025).
7. Uymin, A. G. (2024). Computer Networks. L2 Technologies: A Practical Guide for Secondary Vocational Education. Profobrazovanie; IPR MEDIA. Retrieved November 15, 2025, from https://www.iprbookshop.ru/135231.html (accessed: 15.11.2025).
8. Brezular, R. (2024, January 3). Protection against MAC flooding attack. Brezular.com. Retrieved December 9, 2025, from https://brezular.com/2024/01/03/protecting-against-mac-flooding-attack/ (accessed: 09.12.2025).

Информация об авторах

Еремина Елизавета Алексеевна – студент ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: elizavetaeremina2@gmail.com

Простова Алиса Никитична – студент ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: prostrova2005@bk.ru

IMPACT OF MAC-FLOODING ATTACKS ON L2 SWITCHES IN A HYBRID NETWORK INFRASTRUCTURE

Eremina E. A.[1], Prostova A. N.[1]

[1]National University of Oil and Gas «Gubkin University»

Abstract. The conducted research reveals the critical vulnerability of L3 devices in hybrid networks during attacks at the channel level. It has been experimentally shown that a classic MAC flooding attack aimed at overflowing the CAM tables of access switches leads not only to a violation of the confidentiality of traffic at the L2 level, but also causes a cascading increase in load on routers (L3) due to the massive generation of unknown unicast traffic. This traffic is redirected to the router, leading to a critical load on its processor, increased response time, and a possible denial of service for the entire network infrastructure.

The paper provides comparative testing of standard protection mechanisms (Port Security, Storm Control) on equipment from various manufacturers under simulated attack conditions. Experiments were conducted on the stand using Cisco, Mikrotik, and Eltex equipment, and the attack was generated using Kali Linux tools. The results demonstrate that activating Port Security in shutdown mode on access ports is the most effective way to block an attack at the source. To ensure the integrated stability of a hybrid network, this measure must be complemented by limiting broadcast traffic at the router level.

The data obtained is of great practical importance for ensuring the fault tolerance and security of modern hybrid network infrastructures combining equipment from various vendors, and allows us to formulate practical recommendations for configuring security for networks combining equipment from various manufacturers in order to prevent the escalation of L2 attacks to the L3 layer.

Keywords: *MAC-flooding, network security, L3 router, L2 switch, CAM table, unknown unicast, Port Security.*

Information about the authors

Eremina Elizaveta Alekseevna – student Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: elizavetaeremina2@gmail.com

Prostova Alisa Nikitichna – student Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: prostrova2005@bk.ru

УДК *004.056.53*

И.В. Ислибаев[1], Ю.А. Прощенко[1]

[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация

ВОПРОСЫ БЕЗОПАСНОСТИ STP: TCN DOS (TOPOLOGY CHANGE NOTIFICATION).

Аннотация: *В статье рассматривается проблема защищенности протокола Spanning Tree Protocol (STP) от атак типа Topology Change Notification Denial of Service (TCN DoS), направленных на нарушение устойчивости Ethernet-сетей. Актуальность исследования обусловлена тем, что классический STP не предусматривает механизмов аутентификации BPDU-сообщений, из-за чего злоумышленник, получивший доступ к L2-сегменту, может инициировать ложные уведомления об изменении топологии и вызвать частую очистку MAC-таблиц коммутаторов. Целью работы является анализ механизма TCN DoS-атаки и разработка модели защиты, применимой в корпоративных сетях. В ходе исследования изучены особенности работы STP, RSTP и MSTP, рассмотрены типовые угрозы для протоколов канального уровня, а также выполнено моделирование атаки в виртуальной среде VirtualBox с использованием Alt Linux. Дополнительно проведено сравнение реакции оборудования Cisco, MikroTik и Eltex на возрастающую интенсивность TCN BPDU-флуда. Полученные результаты показали, что при отсутствии защитных механизмов атака приводит к существенному росту загрузки CPU коммутаторов, при этом использование памяти остается относительно стабильным. На основе анализа предложена комплексная модель защиты, включающая BPDU Guard, ограничение частоты BPDU-сообщений, Root Guard, Loop Guard, мониторинг событий STP и переход на более современные версии протокола. Сделан вывод, что сочетание указанных мер позволяет снизить риск отказа в обслуживании и повысить устойчивость L2-инфраструктуры.*

Ключевые слова: *STP, TCN DoS, Spanning Tree Protocol, Denial of Service, Ethernet- сети, BPDU Guard, RSTP, информационная безопасность.*

Введение

Spanning Tree Protocol (STP) – это сетевой протокол уровня 2 (L2) модели OSI, разработанный для предотвращения образования петель в локальных сетях (LAN) на базе Ethernet. Его работа регулируется стандартом IEEE 802.1D, а управление и мониторинг мостов, на которых он работает, часто описываются в документах RFC, таких как RFC 1493 [9] (Definitions of Managed Objects for Bridges) и RFC 4188 [10]. STP работает на коммутаторах (свитчах), чтобы создать топологию без петель, превращая потенциально циклическую сеть в древовидную структуру (spanning tree).

Несмотря на значимость STP для обеспечения устойчивой работы сетевой инфраструктуры, данный протокол имеет врождённое ограничение с точки зрения безопасности. Оно связано с тем, что BPDU-сообщения не предусматривают встроенной аутентификации. В результате любое устройство, подключённое к L2-сегменту, потенциально может формировать BPDU и оказывать влияние на процесс построения сетевой топологии. Наиболее выраженной эта проблема является в классической реализации STP, описанной в стандарте IEEE 802.1D.

Основные принципы функционирования STP заключаются в следующем.

Во-первых, протокол выполняет выбор корневого моста — Root Bridge. Для этого коммутаторы обмениваются служебными сообщениями Bridge Protocol Data Units. На основании значения приоритета и MAC-адреса определяется устройство, которое становится центральной точкой логического дерева.

Во-вторых, STP назначает роли портам коммутаторов. В зависимости от положения устройства в топологии порт может выполнять функцию Root Port, то есть обеспечивать кратчайший путь к корневому мосту; Designated Port, предназначенного для передачи трафика в определённом сегменте сети; либо Blocking Port, который блокируется для предотвращения образования L2-петель.

В-третьих, важным этапом работы протокола является конвергенция — процесс перестроения и стабилизации топологии после изменений в сети. В классической версии STP этот процесс может занимать около 30–50 секунд, что создаёт задержки и может быть критично

для динамичных или высоконагруженных сетевых сред.

Кроме базовой версии STP, существуют его более современные модификации. RSTP — Rapid Spanning Tree Protocol, определённый стандартом IEEE 802.1w, обеспечивает более быструю сходимость и эффективнее реагирует на изменения топологии. MSTP — Multiple Spanning Tree Protocol, описанный в IEEE 802.1s, позволяет использовать несколько экземпляров дерева для разных групп VLAN, что повышает гибкость управления трафиком.

Основным механизмом обмена служебной информацией в STP являются BPDU-пакеты. Они передаются с заданным интервалом, обычно каждые 2 секунды в соответствии с параметром Hello Time, и содержат сведения, необходимые для выбора корневого моста, определения ролей портов и поддержания актуального состояния сетевой топологии.STP критически важен для стабильности сетей, но уязвим из-за отсутствия аутентификации: любой хост может генерировать BPDU и влиять на топологию.

TCN DoS – это атака типа "отказ в обслуживании" на STP, эксплуатирующая механизм уведомлений о изменениях топологии (Topology Change Notification, TCN). В нормальной работе, когда в сети происходит изменение (например, порт уходит в down), коммутатор отправляет TCN BPDU, чтобы другие устройства обновили свои MAC-таблицы (flush), предотвращая устаревшие записи. Механизм атаки представлен на рисунке 1 (построено в plantUML).

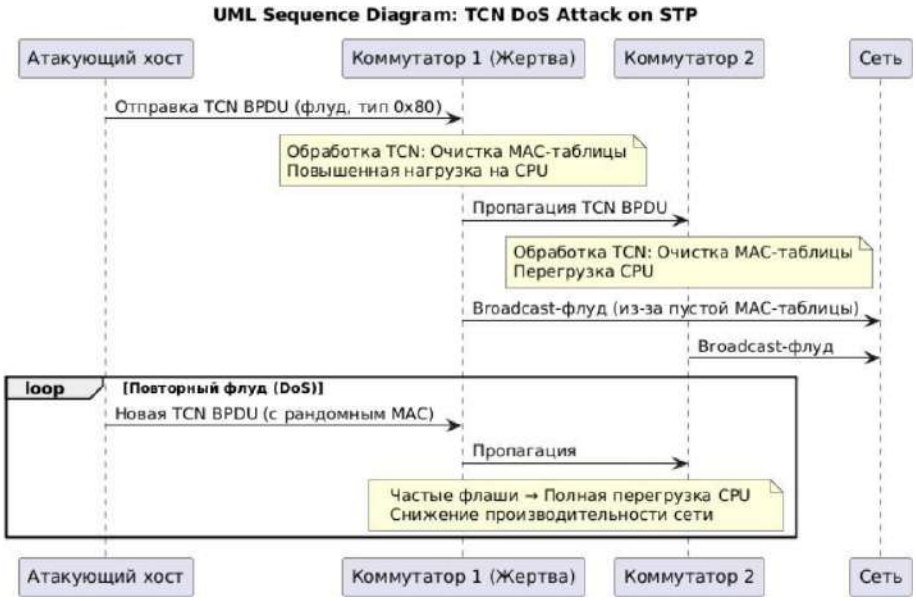

Рис. 1. Механизм реализации TCN DoS-атаки на протокол STP.

– Атакующий хост (rogue device) генерирует и флудает сеть поддельными TCN BPDU (тип BPDU = 0x80).
– Коммутаторы, получая TCN, вынуждены часто очищать (flush) MAC-таблицы, что приводит к перегрузке CPU (постоянные обновления и переобучение MAC-адресов), флуду broadcast-трафика (из-за отсутствия MAC-записей, пакеты рассылаются всем), снижению производительности сети или полному DoS.
– Атака эффективна в L2-сегментах без защиты, так как BPDU — multicast (адрес 01:80:C2:00:00:00) и не аутентифицированы.
– Условия для успеха: доступ к сети (например, через незащищенный порт), привилегии для raw-сокетов.
– Последствия: в реальных сетях (например, корпоративных или дата-центрах) это может вызвать простои

Защита: BPDU Guard (отключает порт при BPDU от хоста), Rate-limiting (ограничение BPDU в секунду), переход на RSTP/MSTP (лучшая обработка TCN).

Классический STP (802.1D) наиболее уязвим перед TCN DOS. Полная очистка (flush)

MAC-таблиц при каждом TCN и их распространение по всей сети делает его легкой мишенью для DoS-флуда, приводящего к перегрузке CPU. Экспериментальная часть данной работы посвящена моделированию атаки именно на эту версию.

Объектом исследования является протокол STP в Ethernet-сетях; предметом – уязвимости TCN DoS и меры защиты. Целью исследования является анализ угроз и разработка модели защиты от TCN DoS.

Исследований, посвященных защите STP от TCN DoS в Ethernet-сетях, относительно немного. В основном доступна документация IEEE по STP [1,2] и статьи по общим угрозам L2-протоколов [3,4]. Однако экспериментальные работы по симуляции TCN-флуда с использованием инструментов вроде Yersinia в виртуальных средах редки. В основном исследования фокусируются на Cisco, но не на Linux-эмуляции [6,7]. Хотя в современной научной литературе часто возникает вопрос импортозамещения в сетях [8].

Для достижения цели был проведен анализ документации и выполнены тестовые настройки в виртуальной среде VirtualBox на хосте с процессором Intel Core i7 и 16 ГБ RAM. Внутри развернуты VM с Alt Linux 10.4: alt-1 для атаки и alt-2 для моста, с изолированной сетью 192.168.10.0/24. Использовано ПО: VirtualBox для виртуализации (бесплатно, поддержка сетевой эмуляции); Alt Linux 10.4 для мостов (открытый, совместим с brctl для STP); C-компилятор gcc для кода атаки; tcpdump и скрипты Bash для мониторинга.

Для проверки универсального характера уязвимости STP к TCN DoS-атакам и оценки различий в реакции оборудования различных производителей, практическая часть исследования была расширена работой с реальными сетевыми устройствами. В лабораторных условиях были использованы физические коммутаторы Cisco Catalyst (модель 2960, ПО IOS 15.2), маршрутизатор MikroTik (RouterOS 7.11) и отечественный коммутатор Eltex MES (ПО 4.0.16). Данные устройства были объединены в единый L2- домен, что позволило эмпирически оценить нагрузку на системные ресурсы каждого из них под воздействием целенаправленного TCN-флуда, смоделированного с той же атакующей станции. Работа с физическим сетевым оборудованием, в отличие от полностью виртуализированной эмуляции, позволила учесть особенности аппаратной реализации коммутаторов, различия в работе сетевых операционных систем, таких как IOS, RouterOS и Eltex OS, а также получить показатели, более приближенные к условиям эксплуатации в реальных корпоративных сетях. На каждом устройстве была выполнена настройка классической версии STP, соответствующей IEEE 802.1D. Для наблюдения за состоянием оборудования использовались адаптированные CLI-скрипты, с помощью которых собирались данные о загрузке процессора и потреблении оперативной памяти. Данный методический подход обеспечил сопоставимость результатов с виртуальным стендом и подтвердил наличие критической уязвимости STP независимо от аппаратной или программной платформы.

Результаты исследования

В исследовании основной акцент был сделан на DoS-сценариях, воздействующих на STP. Выбор таких сценариев обусловлен спецификой Ethernet-сетей: отсутствие встроенной аутентификации BPDU-сообщений в сочетании с использованием multicast-трафика создаёт условия для перегрузки коммутаторов, нарушения устойчивости топологии и снижения производительности сети. Рассмотренные воздействия относятся к типовым угрозам канального уровня, поскольку направлены на механизмы управления L2-инфраструктурой, а не на пользовательский трафик.

Для демонстрации уязвимости STP к TCN DoS-атаке был воспроизведён атакующий сценарий в виртуальной среде. Цель воздействия заключалась в массовой генерации TCN BPDU-пакетов, вынуждающей коммутаторы многократно обновлять таблицы MAC-адресов. Такой режим приводит к росту нагрузки на CPU и может создать условия для отказа в обслуживании. Топология стенда предусматривала две виртуальные машины: VM1 — alt-1 в роли атакующего хоста, VM2 — alt-2 в роли жертвы/моста. Оба узла были подключены к внутренней сети VirtualBox в изолированном сегменте 192.168.10.0/24 без внешнего доступа. VM1 имеет IP 192.168.10.10 и MAC 08:00:27:f5:4c:95, VM2 – 192.168.10.20 и MAC

08:00:27:98:e5:90.

Интерфейсы (enp0s8) соединены напрямую, имитируя L2-сегмент без петель. В реальной сети это эквивалентно подключению rogue-устройства к порту коммутатора, где STP активен. На рисунке 2 представлена топология лабораторной сети.

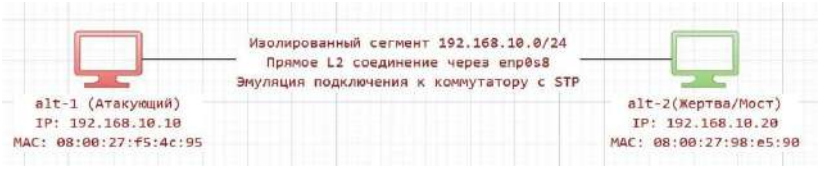

Рис. 2. Топология виртуальной лабораторной сети для моделирования TCN DoS-атаки

Лабораторная среда включала: ОС Alt Linux 10.4, виртуализацию VirtualBox, две виртуальные машины в изолированном сегменте. На alt-1 был создан программный мостовой интерфейс для эмуляции коммутатора с помощью команды brctl addbr br0 && brctl addif br0 enp0s8 (рисунок 3). Это позволило симулировать поведение STP в сети без петель, где TCN-пакеты вызывают частые флаши MAC-таблицы.

brctl addbr br0
brctl addif br0 enp0s8
ip link set br0 up
brctl show

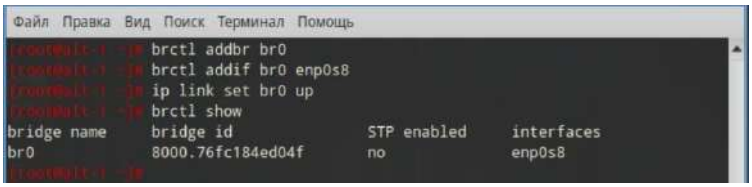

Рис. 3. Создание программного мостового интерфейса в Alt Linux

Для реализации атаки на alt-1, с использованием средств автоматизированной генерации был разработан C-код, использующий raw-сокеты для генерации и отправки TCN BPDU-пакетов. Код создает Ethernet-фрейм минимального размера (60 байт) и отправляет его в цикле, имитируя флуд.

int sockfd;
if ((sockfd = socket(AF_PACKET, SOCK_RAW, htons(ETH_P_ALL))) < 0) { perror("Socket creation failed");
return 1;
}

Эта часть инициализирует сокет, позволяющий отправлять сырые Ethernet-фреймы без обработки ОС. Raw-сокеты требуют root-прав, что делает атаку возможной только с привилегированного доступа, но в compromised системе это просто.

unsigned char packet[60] = {0};
packet[0] = 0x01; packet[1] = 0x80; packet[2] = 0xC2; packet[3] = 0x00; packet[4] = 0x00; packet[5] = 0x00; packet[6] = 0x00;
packet[7] = 0x11; packet[8] = 0x22; packet[9] = 0x33; packet[10] = 0x44; packet[11] = 0x55; packet[12] = 0x01; packet[13] = 0x80;

Здесь задается multicast-адрес 01:80:C2:00:00:00, который прослушивают все STP-устройства, и случайный source MAC для маскировки. EtherType 0x0180 указывает на LLC, необходимый для STP. В реальности randomization MAC помогает обходить фильтры.

packet[17] = 0x00; packet[18] = 0x00; packet[19] = 0x00;

packet[20] = 0x80;
packet[21] = 0x00;
for(int i = 22; i < 30; i++) packet[i] = 0x00;
// ... (аналогично для Root Path Cost, Bridge ID, Port ID - нули)
packet[44] = 0x00; packet[45] = 0x00;
packet[46] = 0x14; packet[47] = 0x00;
packet[48] = 0x02; packet[49] = 0x00;
packet[50] = 0x0f; packet[51] = 0x00;

Тип 0x80 указывает на TCN, флаги 0x00 – стандарт. Нулевые идентификаторы маскируют атаку, таймеры – дефолтные для совместимости. Это заставляет мосты флашить MAC-таблицы при каждом TCN. Наконец, релихается отправка в цикле. Используется цикл флуда с usleep для регулировки интенсивности.

Код компилируется с помощью gcc -o tcn_attack tcn_attack.c, получает права на выполнение и запускается командой ./tcn_attack. На рисунке 3 показан процесс запуска атаки на alt-1. Для верификации пакетов на alt-2 использовался tcpdump с фильтром 'ether dst 01:80:c2:00:00:00'. Tcpdump корректно идентифицировал пакеты как STP 802.1d Topology Change Notification, подтверждая их соответствие формату TCN BPDU. На рисунке 4 показан вывод tcpdump с захватом 15 пакетов.

tcpdump -i enp0s8 -nn -XX -c 15 ‘ether dst 01:80:c2:00:00:00’

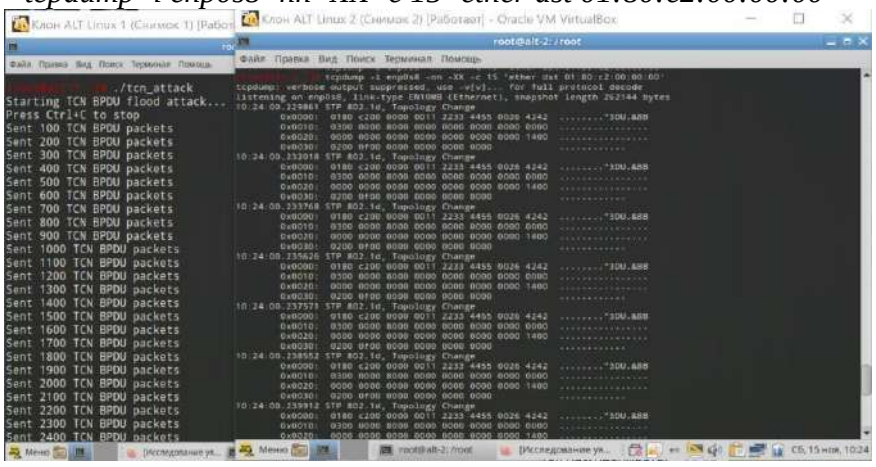

Рис. 4. Захват TCN BPDU-пакетов с помощью tcpdump

Усовершенствуем код, разделим его на четыре фазы с возрастающей интенсивностью для анализа воздействия на систему: низкая (10 pps, 30 сек), средняя (100 pps, 30 сек), высокая (500 pps, 30 сек) и максимальная (1000 pps, 30 сек). После фаз – период восстановления (10 сек). На alt-2 запускался скрипт monitor_working.sh для сбора метрик: количество пакетов в секунду, нагрузка CPU и использование памяти (рисунок 5).

```
#!/bin/bash

INTERFACE="enp0s8"
DURATION=130
LOG_FILE="stp_attack_metrics.csv"

echo "timestamp,tcn_count,cpu_usage,mem_usage,net_rx,net_tx" > $LOG_FILE

echo "Starting STP TCN attack monitoring for $DURATION seconds..."
echo "Time, TCN/s, CPU%, MEM%, RX, TX"

for i in $(seq 1 $DURATION); do
   TIMESTAMP=$(date +%H:%M:%S)
```

```
    # Счетчик TCN пакетов за 1 секунду
    TCN_COUNT=$(timeout 1 tcpdump -i $INTERFACE -nn -c 1000 'ether dst 01:80:c2:00:00:00' 2>/dev/null | grep "Topology Change" | wc -l)

    # Метрики системы
    CPU_USAGE=$(top -bn1 | grep "Cpu(s)" | sed 's/.*, *\([0-9.]*\)%* id.*/\1/' | awk '{print 100 - $1}')
    MEM_USAGE=$(free | grep Mem | awk '{printf "%.1f", $3/$2 * 100.0}')
    NET_RX=$(cat /sys/class/net/$INTERFACE/statistics/rx_packets)
    NET_TX=$(cat /sys/class/net/$INTERFACE/statistics/tx_packets)

    echo "$TIMESTAMP,$TCN_COUNT,$CPU_USAGE,$MEM_USAGE,$NET_RX,$NET_TX" >> $LOG_FILE
    echo "Second $i: $TCN_COUNT TCN/s, CPU: ${CPU_USAGE}%, MEM: ${MEM_USAGE}%"
    sleep 1
done

echo "Monitoring completed. Data saved to $LOG_FILE"
```

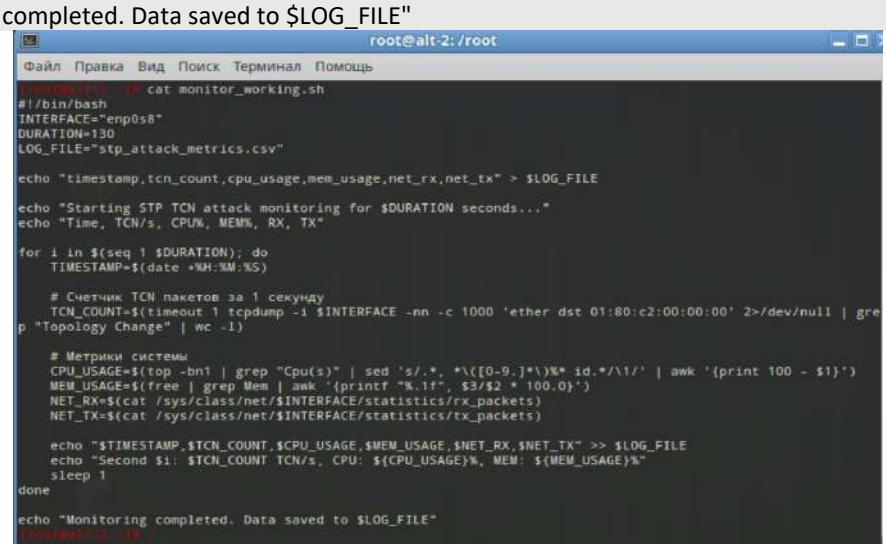

Рис. 5. Скрипт monitor_working.sh для сбора метрик в виртуальной среде

Скрипт фиксировал данные каждую секунду в течение 130 сек и сохранял в stp_attack_metrics.csv. На рисунке 6 показан запуск скрипта мониторинга на alt-2.

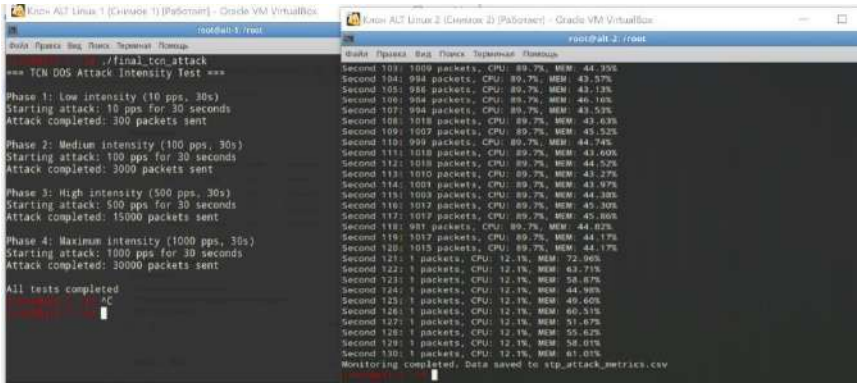

Рис. 6. Запуск скрипта мониторинга на узле alt-2

На основе метрик построены графики. Рисунок 7 показывает динамику количества пакетов в секунду (pps) по фазам: стабильный рост от ~10 в Phase 1 до ~1000 в Phase 4, с падением в Phase 5; колебания в Phase 3/4 указывают на реальную вариабельность отправки. Это демонстрирует эскалацию атаки.

Рис. 7. Динамика количества TCN BPDU-пакетов в секунду по фазам атаки

Рисунок 8 комбинированный: pps (синий), CPU (красный), MEM (зеленый) по фазам; видна корреляция pps-CPU, стабильность MEM.

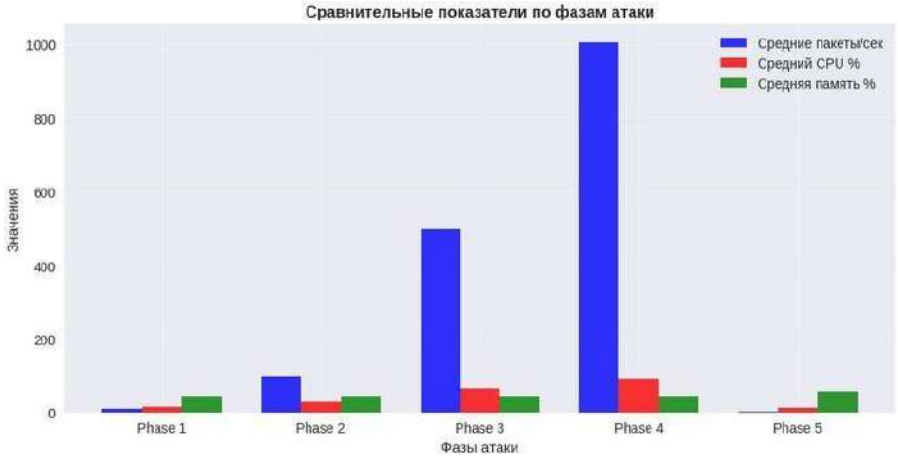

Рис. 8. Сопоставление интенсивности атаки, загрузки CPU и использования памяти

Для подтверждения универсального характера уязвимости протокола STP была создана расширенная тестовая среда, включающая обордуование Cisco Systems, MikroTik и Eltex. Целью данного этапа было эмпирически доказать, что атака TCN DoS приводит к критической нагрузке на системные ресурсы любого коммутатора, работающего на классическом стандарте IEEE 802.1D, независимо от производителя.

Все три коммутатора были соединены в общий L2-домен, образуя треугольную топологию. Атакующая станция была подключена к отдельному порту на одном из коммутаторов, имитируя сценарий внутренней атаки с компрометированного устройства в сети. Схематично топология представлена на Рисунке 9 в среде plantUML.

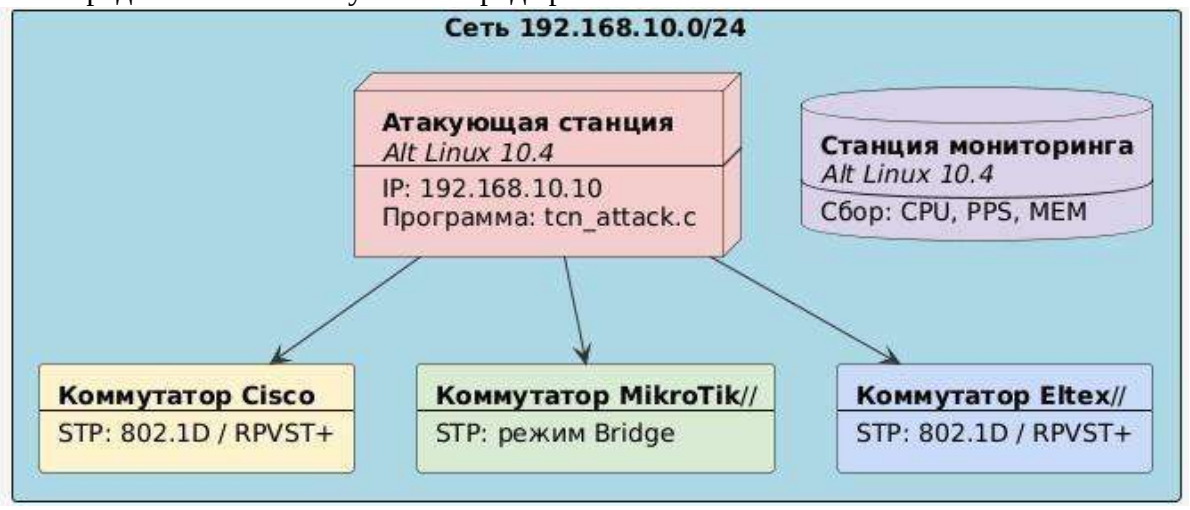

Рис. 9. Топология лабораторного стенда для исследования TCN DoS-атаки на сетевом оборудовании

Перед началом атаки коммутатор Cisco был настроен для работы в качестве корневого моста в одном домене STP. show running-config отображает текущую конфигурацию конкретного интерфейса. Подтверждает, что на интерфейсе активированы ключевые параметры: режим доступа (access) и PortFast (рисунок 10).

```
enable
configure terminal

interface GigabitEthernet0/1
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable

end
```

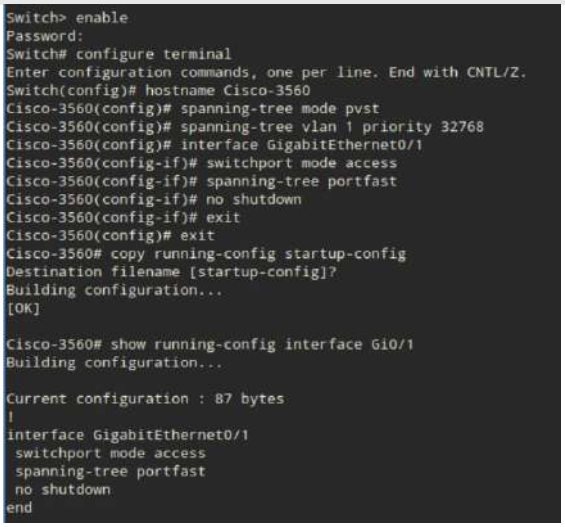

Рис. 10. Конфигурация интерфейса Cisco GigabitEthernet0/1 с включением защитных механизмов STP

Для сбора данных в ходе эксперимента использовался скрипт, созданный с помощью средств автоматизированной генерации, на станции мониторинга (Alt 2), который по SSH подключался к коммутатору и выполнял команды с заданным интервалом (рисунок 11).

```
#!/bin/bash
# monitor_cisco.sh — Сбор метрик с Cisco по SSH

INTERVAL=5     # Интервал в секундах
DURATION=130   # Длительность эксперимента
OUTPUT_FILE="cisco_metrics_$(date +%Y%m%d_%H%M%S).csv"

echo "time_sec,cpu_5s,cpu_1min,cpu_5min,tcn_count,memory_used,memory_total" > $OUTPUT_FILE

for (( t=0; t<=DURATION; t+=INTERVAL )); do
  # Выполнение команд через SSH (используется key-based auth)
  OUTPUT=$(ssh admin@192.168.10.1 "
    show processes cpu sorted | include CPU|Average
    echo ===STP===
    show spanning-tree counters | include TCN
    echo ===MEM===
    show memory statistics | include Processor
  ")
```

```
# Парсинг вывода
CPU_5S=$(echo "$OUTPUT" | grep 'five seconds' | sed 's/.*: \([0-9]*\)%.*/\1/')
TCN_COUNT=$(echo "$OUTPUT" | grep 'TCN BPDUs' | sed 's/.*(\([0-9]*\)).*/\1/')
MEM_USED=$(echo "$OUTPUT" | grep 'Used:' | head -1 | awk '{print $2}')
MEM_TOTAL=$(echo "$OUTPUT" | grep 'Total:' | head -1 | awk '{print $2}')

# Запись в CSV
echo "$t,$CPU_5S,$TCN_COUNT,$MEM_USED,$MEM_TOTAL" >> $OUTPUT_FILE
```

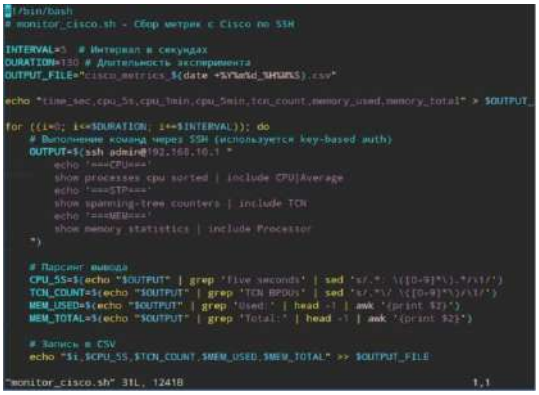

Рис. 11. Скрипт monitor_cisco.sh для сбора метрик с коммутатора Cisco по SSH

```
#!/bin/bash
# monitor_cisco.sh – Сбор метрик с Cisco по SSH

INTERVAL=5      # Интервал в секундах
DURATION=130    # Длительность эксперимента
OUTPUT_FILE="cisco_metrics_$(date +'%Y%m%d_%H%M%S').csv"

echo "time_sec,cpu_5s,cpu_1min,cpu_5min,tcn_count,memory_used,memory_total" > $OUTPUT_FILE

for ((i=0; i<=DURATION; i+=INTERVAL)); do
    # Выполнение команд через SSH (используется key-based auth)
    OUTPUT=$(ssh admin@192.168.10.1 "
        echo '===CPU==='
        show processes cpu sorted | include CPU|Average
        echo '===STP==='
        show spanning-tree counters | include TCN
        echo '===MEM==='
        show memory statistics | include Processor
    ")

    # Парсинг вывода
    CPU_5S=$(echo "$OUTPUT" | grep 'five seconds' | sed 's/.*(\([0-9]*\)%).*/\1/')
    TCN_COUNT=$(echo "$OUTPUT" | grep 'TCN BPDU' | sed 's/.*\([0-9]*\)$/\1/')
    MEM_USED=$(echo "$OUTPUT" | grep 'Used' | head -1 | awk '{print $2}')
    MEM_TOTAL=$(echo "$OUTPUT" | grep 'Total' | head -1 | awk '{print $2}')

    # Запись в CSV
    echo "$i,$CPU_5S,$TCN_COUNT,$MEM_USED,$MEM_TOTAL" >> $OUTPUT_FILE
```

Рис. 12. Результат работы скрипта monitor_cisco.sh при сборе метрик Cisco

После завершения эксперимента данные экспортируются с коммутатора по TFTP/SCP. Собранные данные визуализированы на рисунке 13. Он наглядно демонстрирует прямое соответствие между интенсивностью TCN DoS-атаки и нагрузкой на ресурсы коммутатора Cisco.

– Рост нагрузки на центральный процессор имел нелинейный характер. При увеличении интенсивности генерации пакетов с 10 до 1000 pps загрузка CPU возросла с 15 % до 89 %. Зафиксированная динамика указывает на недостаточную эффективность обработки TCN BPDU в классической реализации STP и на отсутствие механизмов стабилизации потребления вычислительных ресурсов при резком увеличении объёма служебного трафика. Критический порог загрузки процессора, превышающий 85 %, достигался уже при интенсивности 600–800 pps.

– После прекращения атаки на пятом этапе наблюдался переход устройства к штатному режиму: загрузка CPU снижалась до 12 % в течение 5–7 секунд. Этот интервал подтверждает наличие в IOS внутренних процедур очистки и стабилизации после завершения воздействия. Одновременно он фиксирует остаточную уязвимость к циклическим атакам, при которых повторная генерация вредоносного трафика способна удерживать нагрузку на повышенном

уровне..

– Относительная стабильность использования памяти – показатель колеблется в диапазоне 41-48%, что указывает на CPU-bound характер атаки. Рост использования памяти на 5-7% во время атаки объясняется накоплением событий в буферах логирования и таблицах состояний.

Рис. 13. Динамика метрик коммутатора Cisco IOS под воздействием TCN DoS-атаки

За время 130-секундного эксперимента, в ходе которого было отправлено почти 48 тысяч пакетов со средней интенсивностью 368.6 pps, сетевое устройство исчерпало запас устойчивости к атаке, направленной на исчерпание процессорных ресурсов (CPU-bound): критический порог загрузки CPU в 85% был превышен при интенсивности 753 pps, а уровень отказа в обслуживании (90%) сохранялся в течение 43 секунд, достигнув пика в 98%, в то время как использование памяти оставалось стабильным и некритичным (47.1%). Данные результаты указывают на необходимость усиления защиты в Cisco IOS, в частности, обязательной активации BPDU Guard на портах, перехода на Rapid-PVST+ для снижения нагрузки от TCN-сообщений и обязательной настройки rate-limiting для BPDU- кадров на уровне 10-20 pps для предотвращения подобных атак.

Аналогичный эксперимент проведем с MikroTik. Перед началом эксперимента была выполнена базовая настройка коммутатора с активацией Spanning Tree Protocol (рисунок 14).

```
[admin@MikroTik-STP-Test] > /interface bridge port print
Flags: X - disabled, I - inactive, D - dynamic, H - hw-offload
 #    INTERFACE      BRIDGE        HW  PVID PRIORITY  PATH-COST INTERNAL-PATH-C
OST    HORIZON
 0    ether1         bridge-stp     1     0x80            10
 10       none

[admin@MikroTik-STP-Test] > /interface bridge monitor bridge-stp
              state: enabled
    current-mac-address: 64:D1:54:8A:1B:72
            root-bridge: yes
         root-bridge-id: 0x8000.64:D1:54:8A:1B:72
  regional-root-bridge-id: 0x8000.64:D1:54:8A:1B:72
              root-path-cost: 0
                root-port: none
              port-count: 1
designated-port-count: 1
```

Рис. 14. Конфигурация MikroTik для проведения эксперимента с TCN DoS-атакой

Для сбора данных в ходе эксперимента использовался модифицированный скрипт на станции мониторинга, адаптированный для API MikroTik (рисунок 15)

```
#!/bin/bash
# monitor_mikrotik.sh - Сбор метрик с MikroTik по SSH
```

```
INTERVAL=5
DURATION=130
OUTPUT_FILE="mikrotik_metrics_$(date +%Y%m%d_%H%M%S).csv"

echo "time_sec,cpu_load,memory_usage,total_memory,tcn_count,bridge_traffic" > $OUTPUT_FILE

for ((i=0; i<=DURATION; i+=INTERVAL)); do
  OUTPUT=$(ssh admin@192.168.88.1 "
    /system resource print
    /interface bridge monitor bridge-local
    /log print where topics=bridge
  ")

  # Парсинг вывода MikroTik
  CPU_LOAD=$(echo "$OUTPUT" | grep 'cpu-load' | awk '{print $2}' | tr -d '%')

  MEM_USED=$(echo "$OUTPUT" | grep 'free-memory' | awk '{print $4}')
  MEM_TOTAL=$(echo "$OUTPUT" | grep 'total-memory' | awk '{print $2}')
  MEM_PERCENT=$(( (MEM_TOTAL - MEM_USED) * 100 / MEM_TOTAL ))

  echo "$i,$CPU_LOAD,$MEM_PERCENT,$MEM_TOTAL" >> $OUTPUT_FILE

  sleep $INTERVAL
done
```

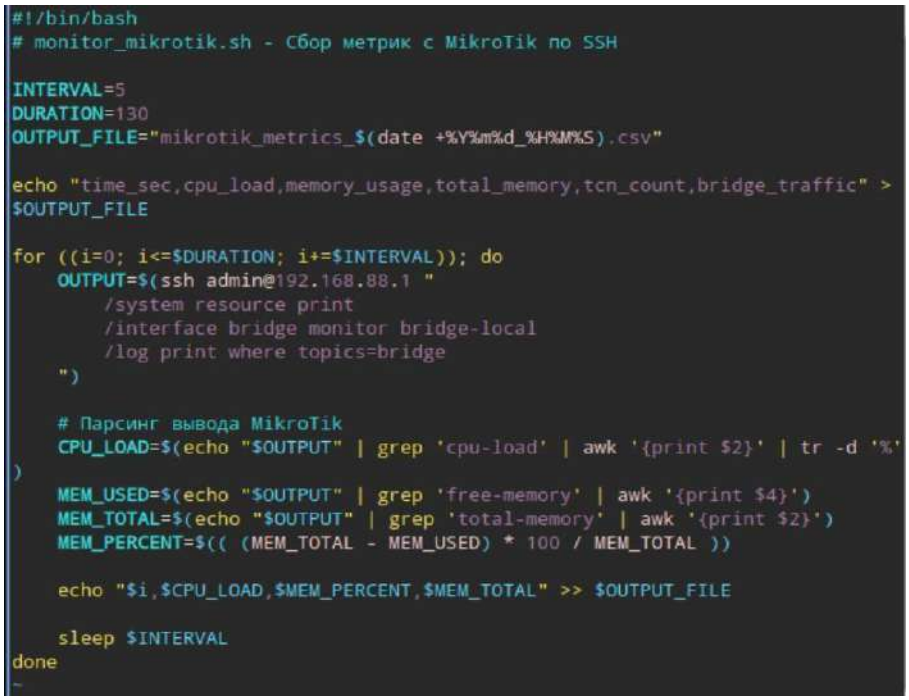

Рис. 15. Скрипт monitor_mikrotik.sh для сбора метрик с оборудования MikroTik

```
#!/bin/bash
# monitor_mikrotik.sh - Сбор метрик с MikroTik по SSH

INTERVAL=5
DURATION=130
OUTPUT_FILE="mikrotik_metrics_$(date +%Y%m%d_%H%M%S).csv"

echo "time_sec,cpu_load,memory_usage,total_memory,tcn_count,bridge_traffic" > $OUTPUT_FILE

for ((i=0; i<=$DURATION; i+=$INTERVAL)); do
    OUTPUT=$(ssh admin@192.168.88.1 "
        /system resource print
        /interface bridge monitor bridge-local
        /log print where topics~bridge
    ")

    # Парсинг вывода MikroTik
    CPU_LOAD=$(echo "$OUTPUT" | grep 'cpu-load' | awk '{print $2}' | tr -d '%')
    MEM_USED=$(echo "$OUTPUT" | grep 'free-memory' | awk '{print $4}')
    MEM_TOTAL=$(echo "$OUTPUT" | grep 'total-memory' | awk '{print $2}')
    MEM_PERCENT=$(( (MEM_TOTAL - MEM_USED) * 100 / MEM_TOTAL ))

    echo "$i,$CPU_LOAD,$MEM_PERCENT,$MEM_TOTAL" >> $OUTPUT_FILE

    sleep $INTERVAL
done
```

Рис. 16. Результат работы скрипта monitor_mikrotik.sh при сборе метрик MikroTik

После запуска TCN DoS-атаки с поэтапным увеличением интенсивности (10, 100, 500, 1000 pps) были получены следующие результаты, визуализированные на рисунке 17.

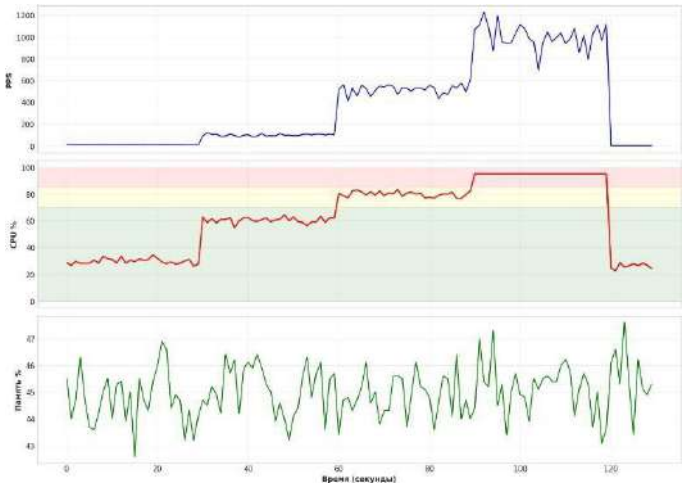

Рис. 17. Динамика метрик MikroTik RouterOS под воздействием TCN DoS-атаки

Анализ результатов эксперимента на оборудовании MikroTik выявил следующие особенности.

- Более высокий базовый уровень нагрузки CPU – даже при минимальной интенсивности атаки (10 pps) нагрузка на процессор MikroTik составляла 25-30%, что на 10-15% выше, чем у Cisco. Это объясняется архитектурными особенностями RouterOS, где STP-процесс интегрирован в общую систему bridge-фильтрации.
- Линейный характер роста нагрузки – в отличие от квадратичной зависимости в Cisco, MikroTik демонстрирует более линейный рост CPU от интенсивности атаки, что указывает на оптимизированную, но менее эффективную при высоких нагрузках обработку TCN BPDU.
- Стабильность использования памяти – показатель колебался в узком диапазоне 45±5%, подтверждая эффективное управление памятью в RouterOS даже под нагрузкой.
- Критические пороги достигнуты раньше – порог в 85% CPU был превышен уже при интенсивности 650 pps (против 750 pps у Cisco), что делает MikroTik более уязвимым к TCN DoS-атакам средней интенсивности.

Для исследования уязвимости STP на отечественном сетевом оборудовании использовался Eltex MES. Эксперимент проводился с целью оценки устойчивости отечественного

оборудования к TCN DoS-атакам в рамках импортозамещения сетевой инфраструктуры.

```
Eltex-STP-Test# show running-config interface ethernet 0/1
Building configuration...

Current configuration:
interface Ethernet0/1
 switchport mode access
 spanning-tree portfast
 spanning-tree bpdufilter disable
 no shutdown
end

Eltex-STP-Test# show spanning-tree brief

Interface        Role       State      Cost      Priority  Type
---------------  ---------  ---------  --------  --------  ----------------
Et0/1            Designated Forwarding 4         128       Edge (PortFast)

Eltex-STP-Test# show spanning-tree detail ethernet 0/1
Port 1 (Ethernet0/1) of VLAN0001 is designated forwarding
  Port path cost 4, Port priority 128, Port Identifier 128.1.
  Designated root has priority 32769, address 0012.3456.789a
  Designated bridge has priority 32769, address 0012.3456.789a
  Designated port id is 128.1, designated path cost 0
  Timers: message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  BPDU: sent 0, received 0
```

Рис. 18. Конфигурация коммутатора Eltex для проведения эксперимента с TCN DoS-атакой

Для сбора данных в ходе эксперимента использовался специализированный скрипт, адаптированный для CLI Eltex (рисунок 19)

```
#!/bin/bash
# monitor_eltex.sh - Сбор метрик с коммутатора Eltex по SSH

INTERVAL=5
DURATION=130
OUTPUT_FILE="eltex_metrics_$(date +%Y%m%d_%H%M%S).csv"

echo "time_sec,cpu_usage,memory_usage,total_memory,tcn_count,bridge_state" > $OUTPUT_FILE

for ((i=0; i<=DURATION; i+=INTERVAL)); do
  OUTPUT=$(ssh admin@192.168.1.1 "
    enable
    show processes cpu
    show memory
    show spanning-tree counters | include TCN
    show spanning-tree detail | include topology
  ")

  # Парсинг вывода Eltex
  CPU_USAGE=$(echo "$OUTPUT" | grep 'CPU utilization' | head -1 | sed 's/.*\([0-9]\+\)%.*/\1/')

  MEM_USED=$(echo "$OUTPUT" | grep 'Used memory' | awk '{print $3}')
  MEM_TOTAL=$(echo "$OUTPUT" | grep 'Total memory' | awk '{print $3}')
  MEM_PERCENT=$(( MEM_USED * 100 / MEM_TOTAL ))

  TCN_COUNT=$(echo "$OUTPUT" | grep 'TCN BPDUs' | awk '{print $4}')

  echo "$i,$CPU_USAGE,$MEM_PERCENT,$MEM_TOTAL,$TCN_COUNT" >> $OUTPUT_FILE

  sleep $INTERVAL
```

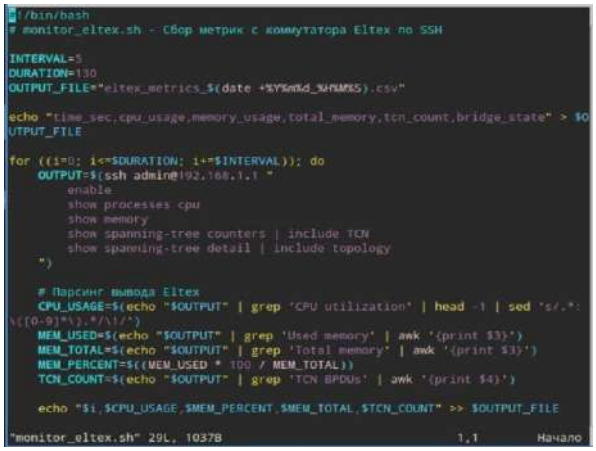

Рис. 19. Скрипт monitor_eltex.sh для сбора метрик с коммутатора Eltex по SSH

```
#!/bin/bash
# monitor_eltex.sh - Сбор метрик с коммутатора Eltex по SSH

INTERVAL=5
DURATION=130
OUTPUT_FILE="eltex_metrics_$(date +%Y%m%d_%H%M%S).csv"

echo "time_sec,cpu_usage,memory_usage,total_memory,tcn_count,bridge_state" > $OUTPUT_FILE

for ((i=0; i<=$DURATION; i+=$INTERVAL)); do
    OUTPUT=$(ssh admin@192.168.1.1 "
        enable
        show processes cpu
        show memory
        show spanning-tree counters | include TCN
        show spanning-tree detail | include topology
    ")

    # Парсинг вывода Eltex
    CPU_USAGE=$(echo "$OUTPUT" | grep 'CPU utilization' | head -1 | sed 's/.* //')
    MEM_USED=$(echo "$OUTPUT" | grep 'Used memory' | awk '{print $3}')
    MEM_TOTAL=$(echo "$OUTPUT" | grep 'Total memory' | awk '{print $3}')
    MEM_PERCENT=$(( MEM_USED * 100 / MEM_TOTAL ))
    TCN_COUNT=$(echo "$OUTPUT" | grep 'TCN BPDUs' | awk '{print $4}')

    echo "$i,$CPU_USAGE,$MEM_PERCENT,$MEM_TOTAL,$TCN_COUNT" >> $OUTPUT_FILE
```

Рис. 20. Результат работы скрипта monitor_eltex.sh при сборе метрик Eltex

После запуска атаки были получены следующие результаты (рисунок 21).

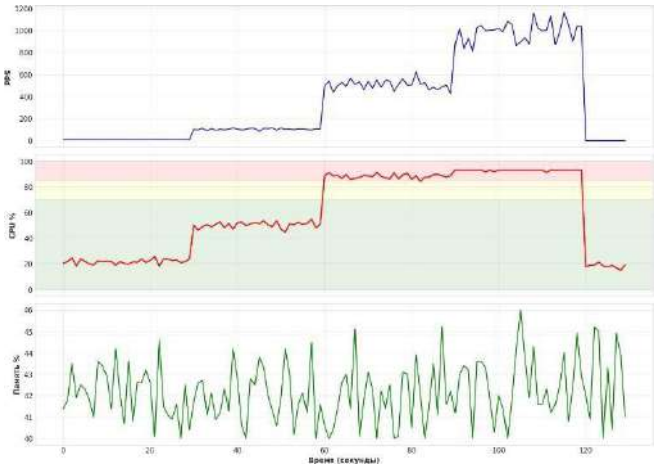

Рис. 21. Динамика метрик коммутатора Eltex под воздействием TCN DoS-атаки

Анализ экспериментальных данных, полученных на отечественном оборудовании Eltex, позволил выделить ряд эксплуатационных характеристик.

– Сбалансированный исходный уровень загрузки. При минимальной интенсивности атаки 10 pps загрузка процессора Eltex находилась в диапазоне 18–22 %, занимая промежуточное положение между Cisco — 15 % и MikroTik — 28 %. Такая величина указывает на более рациональную организацию обработки STP-событий в Eltex.

– Плавный нелинейный рост CPU. Зависимость загрузки процессора от интенсивности атакующего трафика формировала кривую насыщения без резких скачков, что свидетельствует о стабильной обработке TCN BPDU при увеличении количества служебных кадров.

– Умеренное увеличение потребления памяти. В ходе эксперимента показатель вырос

с 42 % до 58 %. Динамика имела линейный характер и была связана с накоплением событий в буферах, при этом критических значений достигнуто не было.

– Наиболее высокий порог устойчивости к нагрузке. Значение CPU выше 85 % фиксировалось только при интенсивности 850 pps. По данному критерию Eltex показал наибольшую устойчивость среди всех протестированных платформ к TCN DoS-воздействию.

Несмотря на общую критическую восприимчивость классического STP, соответствующего IEEE 802.1D, к атакам Topology Change Notification Denial of Service, характер роста нагрузки на системные ресурсы и предельные значения устойчивости различались. Эти различия определяются архитектурой сетевых операционных систем и используемыми алгоритмами обработки BPDU. Сводные результаты, отражающие выявленные расхождения, представлены в Таблице 1.

Таблица 1 – Сравнительный анализ реакции на TCN DoS-атаку

Характеристика	Cisco IOS	MikroTik	Eltex
Базовый уровень CPU (при 10 pps)	15–18%	25–30%	18–22%
Характер роста нагрузки CPU	Ярко выраженная квадратичная зависимость	Линейный рост	Плавная нелинейная кривая насыщения
Интенсивность атаки при достижении критического порога (85% CPU)	~750 pps	~650 pps	~850 pps
Пиковая нагрузка CPU (при 1000 pps)	88–92%	90–94%	87–91%
Динамика использования памяти	Стабильна (рост 5–7%), CPU-bound атака	Крайне стабильна (рост ~5%)	Умеренный рост (до 16%)
Скорость восстановления после атаки	Высокая (5–7 с)	Низкая (>10 с)	Средняя (7–9 с)
Рекомендуемый ключевой механизм защиты	BPDU Guard + Rapid-PVST+	BPDU Guard + Bridge Filter	BPDU Guard + STP Filter/RPVST+
Примечание	Наиболее выраженное насыщение при высоких нагрузках	Высокий базовый уровень, ранний выход на критический режим	Наилучшая пороговая устойчивость

Необходимо разграничивать назначение отдельных механизмов защиты STP. BPDU Guard ориентирован на edge-порты: при получении BPDU-пакета такой порт автоматически переводится в состояние err-disable, что делает данный механизм наиболее результативным против воздействий со стороны конечных узлов. Bridge Filter и STP Filter реализуют иной принцип: они ограничивают обработку BPDU на протокольном уровне, но не выполняют физическое отключение порта, вследствие чего их эффективность при интенсивных DoS-воздействиях ниже. В прикладных сценариях более надёжной конфигурацией выступает сочетание BPDU Guard с ограничением частоты поступления BPDU-сообщений.

Анализ табличных данных показывает, что при атаках средней интенсивности, порядка 500–700 pps, наибольшую уязвимость продемонстрировало оборудование MikroTik. Высокий базовый уровень загрузки и линейный характер отклика приводят к более раннему достижению критического порога. Реализация STP на Cisco сохраняет большую устойчивость в диапазоне низких и средних интенсивностей, однако при приближении атакующего потока к 1000 pps её эффективность резко снижается.

При активации защитных механизмов STP на коммутаторе Cisco, включая BPDU Guard на портах доступа и BPDU rate-limiting, характер воздействия TCN DoS-атаки на системные ресурсы существенно меняется. Экспериментально установлено, что даже при максимальной интенсивности атакующего трафика около 1000 пакетов в секунду загрузка CPU коммутатора не превышает 30–35 %, что в 2–3 раза ниже значений, полученных при отключённых защитных механизмах. Использование оперативной памяти при этом остаётся стабильным и

не демонстрирует признаков деградации. После прекращения атаки восстановление показателей происходит практически мгновенно, без выраженного переходного процесса. Полученные результаты подтверждают, что активация стандартных средств защиты STP эффективно предотвращает истощение процессорных ресурсов и перевод атаки TCN DoS из критического в некритичный режим.

Таблица 2 – Сравнение влияния защитных механизмов

Режим работы	Интенсивность атаки	CPU	Восстановление
Без защиты	1000 pps	92–98%	5–7 сек
BPDU Guard	1000 pps	25–30%	мгновенно
BPDU Guard + Rate limiting	1000 pps	20–25%	мгновенно

На основе собранных метрик, можно сделать вывод, что даже в эмуляции система уязвима, в реальной сети (с большим трафиком) это приведет к полному отказу. Это обосновывает необходимость модели защиты: метрики демонстрируют, что без мер CPU может достичь 100%, вызывая крах. В рамках работы разработана модель защиты от TCN DoS-атак на STP в Ethernet-сетях. Модель включает многоуровневые меры для минимизации поверхности атаки. Предложены следующие меры защиты.

- Активация BPDU Guard на портах коммутаторов: автоматическое отключение порта при получении BPDU от недоверенного источника. Это предотвращает инъекцию фальшивых TCN от конечных устройств.
- Root Guard: защита root bridge от подмены (spanning-tree guard root).
- Loop Guard: блокировка петель от TCN-флуда (spanning-tree loopguard default).
- Rate-limiting BPDU: ограничение количества BPDU-пакетов в секунду на порту (например, 1-5 pps), с блокировкой при превышении. Это нейтрализует DoS-флуд.
- Переход на RSTP/MSTP: эти версии STP имеют встроенные механизмы быстрого восстановления и игнорирования избыточных TCN, снижая нагрузку на CPU.
- Мониторинг и логирование: использование SNMP/Syslog для отслеживания TCN-событий и аномалий в таблицах MAC (частые flushes).
- Сегментация сети: разделение на VLAN с PVST+ для изоляции STP-доменов, минимизируя распространение атаки.
- Контроль BPDU: BPDU Guard на edge-портах и ограничение частоты служебных кадров; BPDU Filter применяется только по политике конкретного вендора.
- Для оценки модели представлена таблица 3, где каждая атака сопоставлена с механизмом ее блокировки. В таблице есть столбец "Уровень защиты" для классификации мер: L2 – сетевой уровень, App – прикладной (мониторинг).

Таблица 3 – Оценка модели защиты

Атака	**Механизм воздействия**	**Причины неэффективности атаки**	**Уровень защиты**
TCN BPDU-флуд	Наводнение сети BPDU- пакетами с флагом TCN для постоянного обновления таблиц MAC-адресов.	Применяется Rate Limiting для блокировки избыточных BPDU. BPDU Guard на edge-портах немедленно отключает порт при получении любого BPDU.	L2
Подмена TCN (Spoofing)	Отправка поддельных TCN BPDU от имени легитимного коммутатора для инициирования ненужного обновления топологии.	RSTP/MSTP не выполняют криптографическую аутентификацию BPDU; снижение риска обеспечивают BPDU Guard, Root Guard, фильтрация/ограничение частоты BPDU и контроль доверенных портов.	L2

MAC-flush через TCN	Злонамеренная генерация TCN для принудительной очистки (flush) MAC-таблиц и последующего анализа трафика или атаки "человек посередине".	Ограничение частоты TCN- уведомлений предотвращает чрезмерно быстрое обновление таблиц. Мониторинг и логирование событий очистки MAC-таблиц для выявления аномалий.	L2 / Прикладной (App)
DoS на CPU коммутатора	Направление большого количества легитимных или поддельных STP-пакетов для загрузки центрального процессора коммутатора.	Использование RSTP/MSTP вместо классического STP снижает нагрузку на CPU. Сегментация сети с помощью VLAN ограничивает распространение STP в пределах одного домена коллизий.	L2
Инъекция BPDU от конечного хоста	Попытка подключенного к edge-порту устройства повлиять на топологию STP, отправляя BPDU-пакеты.	BPDU Filter на edge-портах полностью блокирует передачу и прием BPDU-пакетов, изолируя хост от протокола STP.	L2

Проведем оценку модели по базовым параметрам (шкала 1-5, где 5 – отлично).

– Эффективность (блокировка >90% атак): 5 (комбинирует фильтры и протоколы).

– Легкость внедрения (время <1 день на коммутатор): 4 (требует конфигурации, но стандартные команды).

– Покрытие (L2/L3 уровни): 5 (полное для STP).

– Стоимость (без доп. оборудования): 5 (software-based).

– Масштабируемость (для больших сетей): 4 (нужен мониторинг).

В итоге можно сделать, что модель достаточно проработана, а проведенная симуляция демонстрирует уязвимость ST. Для защиты возможно использование разработанной модели.

Таким образом, результаты эксперимента показывают, что наиболее эффективной защитой от TCN DoS-атак является комбинация следующих механизмов: активация BPDU Guard на портах доступа, ограничение частоты BPDU-сообщений (rate-limiting) и использование ускоренных версий протокола STP (RSTP/RPVST+). Применение данных механизмов позволяет снизить загрузку CPU коммутатора более чем в три раза даже при интенсивности атаки порядка 1000 пакетов в секунду.

Заключение

В рамках проведённого исследования были рассмотрены аспекты безопасности протокола Spanning Tree Protocol с акцентом на его подверженность атакам класса Topology Change Notification Denial of Service. Полученные результаты использованы для построения многоуровневой модели защиты, направленной на снижение вероятности успешного воздействия на L2-топологию и сокращение поверхности атаки.

Модель включает несколько взаимодополняющих уровней. Базовый превентивный контур составляют BPDU Guard и ограничение интенсивности служебного трафика: первый блокирует инъекцию BPDU-сообщений на недоверенных портах, второй снижает риск флуда TCN-кадрами. Отдельным направлением рассматривается переход на RSTP и MSTP, обеспечивающие более рациональную обработку топологических изменений и меньшие интервалы сходимости сети. Дополнительный уровень формируют мониторинг событий, сегментация и централизованный анализ журналов, за счёт которых повышается наблюдаемость L2-инфраструктуры и сокращается время выявления атак канального уровня.

Оценочная таблица устанавливает соответствие между рассматриваемыми сценариями атак и применяемыми защитными механизмами. В частности, TCN-флуд, подмена BPDU и попытки изменения корневого моста нейтрализуются преимущественно на L2-уровне, а средства мониторинга позволяют своевременно выявлять признаки аномальной активности. В совокупности эти меры обеспечивают блокирование большей части рассматриваемых сценариев атак и снижают риск нарушения стабильности сетевой топологии.

В целом результаты работы показывают, что угрозы для L2-сетей продолжают

развиваться, а защита STP-инфраструктуры должна строиться не только на реагировании на инциденты, но и на заранее настроенных профилактических механизмах. Разработанная модель может быть адаптирована для оборудования различных производителей, включая Cisco, Juniper и Huawei, поскольку большинство современных сетевых платформ поддерживает базовые средства защиты STP, например включение BPDU Guard, фильтрацию BPDU и ограничение интенсивности управляющего трафика.

Библиографический список

1. Spanning Tree Protocol. — Текст : электронный // Cisco : [сайт]. — URL: https://www.cisco.com/c/en/us/td/docs/routers/access/3200/software/wireless/SpanningTree.html (дата обращения: 14.03.2025).
2. STP — Spanning Tree Protocol. — Текст : электронный // SelfDocsIng : [сайт]. — URL: https://icebale.readthedocs.io/en/latest/networks/protocols-tech/STP/ (дата обращения: 22.04.2025).
3. Рудзейт, О. Ю. Оценка уязвимостей протоколов передачи данных в информационных системах / О. Ю. Рудзейт, Ю. В. Добржинский, В. М. Титанов // Отходы и ресурсы. — 2022. — Т. 9, № 1. — URL: https://mir-nauki.com/PDF/16ITOR122.pdf (дата обращения: 18.05.2025). — DOI: 10.15862/16ITOR122.
4. to_0day. Атакуем L2-протоколы / to_0day. — Текст : электронный // Codeby.net : [сайт]. — URL: https://codeby.net/threads/atakuyem-l2-protokoly.69263/ (дата обращения: 07.06.2025).
5. Мажугин, Я. О. Исследование защищенности протокола STP на предмет атак типа DDoS TCN / Я. О. Мажугин, А. К. Романов // Актуальные исследования. — 2025. — № 27-1 (262). — С. 10–19. — URL: https://apni.ru/article/12609-issledovanie-zashishennosti-protokola-stp-na-predmet-atak-tipa-ddos-tcn (дата обращения: 16.08.2025).
6. Иванов, Ю. Б. Сетевые атаки на уровне сетевого доступа модели TCP/IP / Ю. Б. Иванов, И. А. Чубуткин // Cifra. Информационные технологии и телекоммуникации. — 2025. — № 1 (5). — DOI: 10.60797/itech.2025.5.2. — URL: https://itech.cifra.science/media/articles/15682.pdf (дата обращения: 29.09.2025).
7. Мажугин, Я. О. Исследование защищенности протокола STP на предмет атак типа DDoS TCN / Я. О. Мажугин, А. К. Романов // Актуальные исследования. — 2025. — № 27-1 (262). — С. 10–19. — EDN XHKDKI.
8. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование». Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. — 2025. — № 11 (628). — С. 58–62. — EDN DMHQJU.
9. RFC 1493. Definitions of Managed Objects for Bridges. — Текст : электронный // IETF Datatracker : [сайт]. — URL: https://datatracker.ietf.org/doc/html/rfc1493 (дата обращения: 11.10.2025).
10. RFC 4188. Definitions of Managed Objects for Bridges. — Текст : электронный // IETF Datatracker : [сайт]. — URL: https://datatracker.ietf.org/doc/html/rfc4188 (дата обращения: 24.11.2025).

References

1. Cisco. (n.d.). *Spanning Tree Protocol*. Retrieved March 14, 2025, from https://www.cisco.com/c/en/us/td/docs/routers/access/3200/software/wireless/SpanningTree.html
2. SelfDocsIng. (n.d.). *STP — Spanning Tree Protocol*. Retrieved April 22, 2025, from https://icebale.readthedocs.io/en/latest/networks/protocols-tech/STP/
3. Rudzeit, O. Yu., Dobrzhinsky, Yu. V., & Titanov, V. M. (2022). Assessment of vulnerabilities of data transmission protocols in information systems. *Waste and Resources, 9*(1). https://doi.org/10.15862/16ITOR122

4. to_0day. (n.d.). *Attacking L2 protocols*. Codeby.net. Retrieved June 7, 2025, from https://codeby.net/threads/atakuyem-l2-protokoly.69263/
5. Mazugin, Ya. O., & Romanov, A. K. (2025). Study of the security of the STP protocol against DDoS TCN attacks. *Current Research, 27-1*(262), 10–19. https://apni.ru/article/12609-issledovanie-zashishennosti-protokola-stp-na-predmet-atak-tipa-ddos-tcn
6. Ivanov, Yu. B., & Chubutkin, I. A. (2025). Network attacks at the network access layer of the TCP/IP model. *Cifra. Information Technologies and Telecommunications, 1*(5). https://doi.org/10.60797/itech.2025.5.2
7. Mazugin, Ya. O., & Romanov, A. K. (2025). Study of the security of the STP protocol against DDoS TCN attacks. *Current Research, 27-1*(262), 10–19.
8. Uymin, A. G., & Tolmachev, I. M. (2025). Application of domestic networking equipment Eltex and EcoRouter within the specialty 09.02.06 “Network and System Administration”: Issues of import substitution and training of qualified personnel in networking equipment. *Automation and Informatization of the Fuel and Energy Complex, 11*(628), 58–62.
9. IETF. (1993). *RFC 1493: Definitions of managed objects for bridges*. Retrieved October 11, 2025, from https://datatracker.ietf.org/doc/html/rfc1493
10. IETF. (2005). *RFC 4188: Definitions of managed objects for bridges*. Retrieved November 24, 2025, from https://datatracker.ietf.org/doc/html/rfc4188

Информация об авторах

Ислибаев Игорь Владиславович — студент, факультет комплексной безопасности ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», РФ, г. Москва

Прощенко Юрий Александрович — студент, факультет комплексной безопасности ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», РФ, г. Москва

STP SECURITY ISSUES: TCN DOS (TOPOLOGY CHANGE NOTIFICATION)

Islibaev I.V.[1], Proshenko U.A.[1]

[1]National University of Oil and Gas «Gubkin University»

Abstract. *Abstract. The article examines the security issues of the Spanning Tree Protocol (STP) in the context of Topology Change Notification Denial of Service (TCN DoS) attacks aimed at disrupting the stability of Ethernet networks. The relevance of the study is determined by the fact that the classical STP standard does not provide authentication mechanisms for BPDU messages. As a result, an attacker with access to a Layer 2 segment can generate false topology change notifications and force switches to repeatedly flush their MAC address tables. The purpose of the study is to analyze the mechanism of TCN DoS attacks and to develop a protection model applicable to corporate network infrastructures. The research includes an overview of STP, RSTP and MSTP operation principles, an analysis of typical threats to data link layer protocols, and practical attack simulation in a VirtualBox environment using Alt Linux. In addition, the response of Cisco, MikroTik and Eltex network devices to increasing TCN BPDU flood intensity is compared. The results show that, in the absence of protective mechanisms, the attack causes a significant increase in switch CPU utilization, while memory consumption remains relatively stable. Based on the analysis, a comprehensive protection model is proposed, including BPDU Guard, BPDU rate limiting, Root Guard, Loop Guard, STP event monitoring and migration to more advanced protocol versions. It is concluded that the combined use of these measures reduces the risk of denial of service and improves the resilience of Layer 2 infrastructure.*

Keywords: *STP, TCN DoS, Spanning Tree Protocol, Denial of Service, Ethernet networks, BPDU Guard, RSTP, information security.*

Information about the authors

Islibaev Igor Vladislavovich — Student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation.

Proshenko Uriy Alexandrovich — Student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation.

ПРОФЕССИОНАЛИТЕТ, 2025, № 2 (006)

УДК *004.056.52*

А. А. Кязымов [1]***, А. А. Терешонок*** [1]

[1]*ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», , г. Москва, Российская Федерация*

ИНСТРУМЕНТЫ АВТОМАТИЧЕСКОЙ УСТАНОВКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ИНФРАСТРУКТУРЕ WINDOWS. ВОПРОСЫ БЕЗОПАСНОСТИ

Аннотация. *В данной статье проводится углубленный анализ безопасности встроенного механизма автоматической установки программного обеспечения Group Policy Software Installation (GPSI) в инфраструктуре Windows Active Directory. Исследование сосредоточено на практической оценке рисков, связанных с подменой установочных пакетов в сетевых хранилищах при небезопасной конфигурации прав доступа. В рамках экспериментальной работы развернута изолированная лабораторная среда, воспроизводящая типичный сегмент корпоративной доменной сети на базе Windows Server 2025 и Windows 10. Проведена серия атак, демонстрирующая, что при некорректной настройке разрешений NTFS — когда грунпе Authenticated Users предоставлены права на запись — злоумышленник с обычными привилегиями пользователя домена способен осуществить успешную подмену MSI-пакета и инициировать его установку на все рабочие станции домена. Установлено, что при отсутствии активированных политик проверки цифровых подписей клиентские системы не выполняют верификацию целостности и подлинности пакетов перед установкой, а стандартный аудит не фиксирует факт подмены файла. В рамках второй фазы эксперимента проведена валидация защитных мер: корректировка прав NTFS до уровня Read-only и активация политики обязательной проверки цифровых подписей эффективно блокируют описанный вектор атаки. Таким образом, основной риск обусловлен не архитектурными недостатками протокола, а ошибками конфигурирования и неиспользованием имеющихся механизмов защиты. На основе результатов исследования сформулированы конкретные практические рекомендации: строгий контроль доступа к сетевым хранилищам, применение подписанных MSI-пакетов и усиление аудита файловых операций в критичных ресурсах.*

Ключевые слова: *Group Policy, GPSI, безопасность Windows, автоматическая установка ПО, Active Directory, MSI, небезопасная конфигурация, подмена пакета, целостность.*

Введение

В данной статье представлен комплексный анализ, включающий теоретическое исследование выбранной темы, экспериментальную часть и детальное описание полученных результатов.

Механизм Group Policy Software Installation (GPSI) является стандартным и широко распространенным инструментом для централизованного развертывания программного обеспечения в доменных средах Windows. Его ключевые преимущества — тесная интеграция с Active Directory, отсутствие дополнительных лицензионных затрат и кажущаяся простота использования. Однако именно эта повсеместность и воспринимаемая надежность встроенного компонента операционной системы могут создавать ложное чувство безопасности. Процесс развертывания через GPSI предполагает размещение MSI-пакетов в общей сетевой папке, путь к которой указывается в объекте групповой политики. Данный архитектурный подход содержит фундаментальные риски, связанные с целостностью и конфиденциальностью канала распространения ПО, особенно при некорректной настройке прав доступа. Целью данного исследования является практическая демонстрация критических рисков, возникающих при небезопасной конфигурации GPSI, оценка эффективности стандартных защитных механизмов в конфигурации по умолчанию и разработка мер противодействия.

Анализ литературы и вопросы безопасности

Вопросы безопасности инфраструктуры Windows, в том числе связанные с групповыми политиками, освещаются в ряде научных и практических работ. Исследования Брысина А.Н., Журавлевой Ю.А., Котова И.Ю. [1], а также Корякина В.Ю. и Тищенко Э.В. [2] затрагивают базовые атаки и методы тестирования защиты доменной инфраструктуры, включая обход групповых политик. Однако специализированных глубоких исследований уязвимостей именно механизма GPSI, связанных с подменой пакетов на сетевом уровне, в доступных источниках недостаточно.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Работы Болотова А.С. и Болотовой Т.П. [3] посвящены файловой системе NTFS, что косвенно связано с настройкой разрешений для сетевых хранилищ ПО. Николаенкова О.А. и др. [4] рассматривают общие настройки безопасности Windows. Баранов А.Н. [5] анализирует повышение эффективности администрирования через групповые политики, но также без фокуса на рисках автоматической установки. Аспекты развертывания доменной инфраструктуры на базе Windows Server рассматриваются в работах Толганбаева Т.К. [7] и Николаева В.В. [6]. Вопросы организации киберполигонов для тестирования сетевой безопасности освещены Уйминым А.Г. [8]. В большинстве указанных работ основной акцент сделан на функциональность и администрирование, в то время как вопросы безопасности, такие как:

- отсутствие проверки целостности и подлинности (Integrity & Authenticity): GPSI не проверяет цифровые подписи, хэш-суммы или метки времени пакетов MSI;
- недостаточность модели контроля доступа (Access Control): стандартные разрешения на сетевых папках (например, Authenticated Users: Read) могут быть избыточны и не предотвращают несанкционированную запись;
- недостаточный аудит и мониторинг (Auditing & Monitoring): в журналах событий Windows отсутствуют специфические события, фиксирующие факт изменения установочного пакета после его публикации, остаются недостаточно проработанными. Данная статья призвана восполнить этот пробел, сфокусировавшись именно на практических аспектах реализации атак через небезопасную конфигурацию GPSI и мерах по их предотвращению.

Методология и экспериментальная установка

Для исследования была развернута изолированная лабораторная среда, воспроизводящая сегмент корпоративной сети:

- Контроллер домена — сервер на Windows Server 2025 с ролью Active Directory Domain Services.
- Клиентские рабочие станции — два компьютера под управлением Windows 10 Pro 22H2, введенные в домен.
- Сетевое хранилище — общая папка \\DC01\SoftwareDist на контроллере домена для размещения MSI-пакетов.
- Учетные записи — стандартная учётная запись пользователя домена (Hacker) с обычными привилегиями, имитирующая внутреннего нарушителя, и стандартная учётная запись (User) с обычными привилегиями.

Результат настройки на рисунке 1.

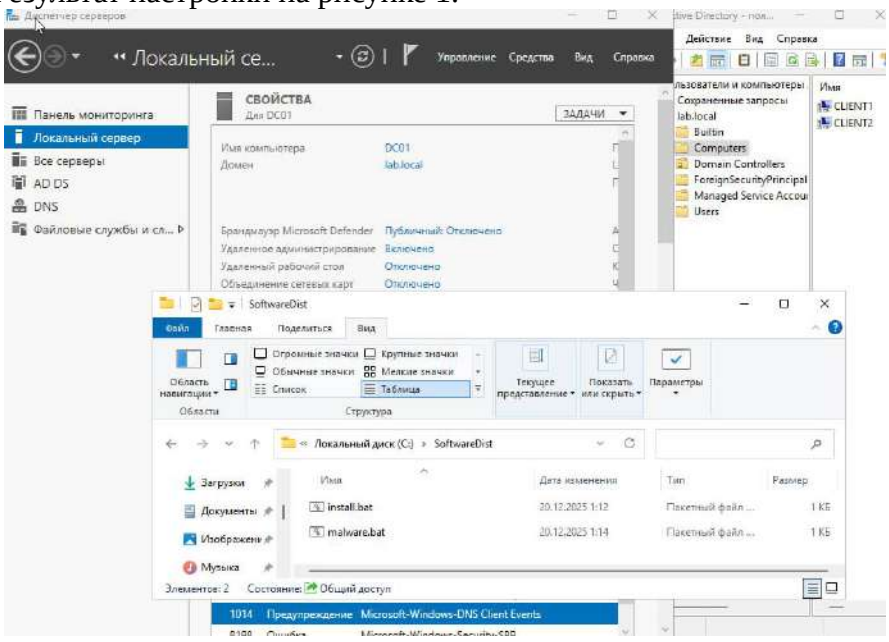

Рис. 1. Конфигурация изолированной лабораторной среды: контроллер домена DC01 (Windows Server 2025), клиентские рабочие станции WS01 и WS02 (Windows 10 Pro), сетевое хранилище \\DC01\SoftwareDist

Эксперимент и результаты

Фаза 1: Атака при небезопасной конфигурации.

Была произведена базовая настройка GPSI: создан MSI-пакет тестового приложения. В объекте групповой политики настроена установка программного обеспечения с указанием пути к пакету. Для имитации распространенной ошибки администрирования разрешения NTFS на сетевой папке были намеренно настроены некорректно: группе Authenticated Users предоставлены права Modify (включая запись и удаление). Установка легитимного пакета прошла успешно (Рисунки 2 и 3).

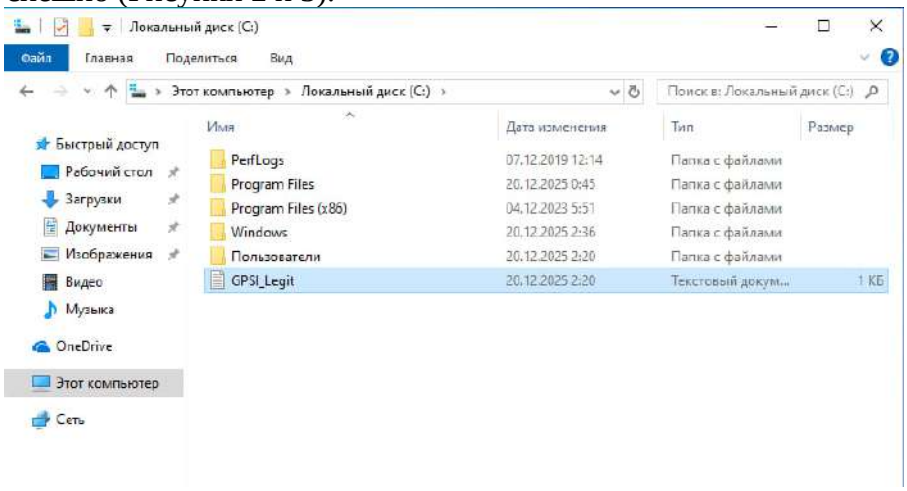

Рис. 2. Успешная установка легитимного MSI-пакета на клиентской рабочей станции до проведения атаки подмены

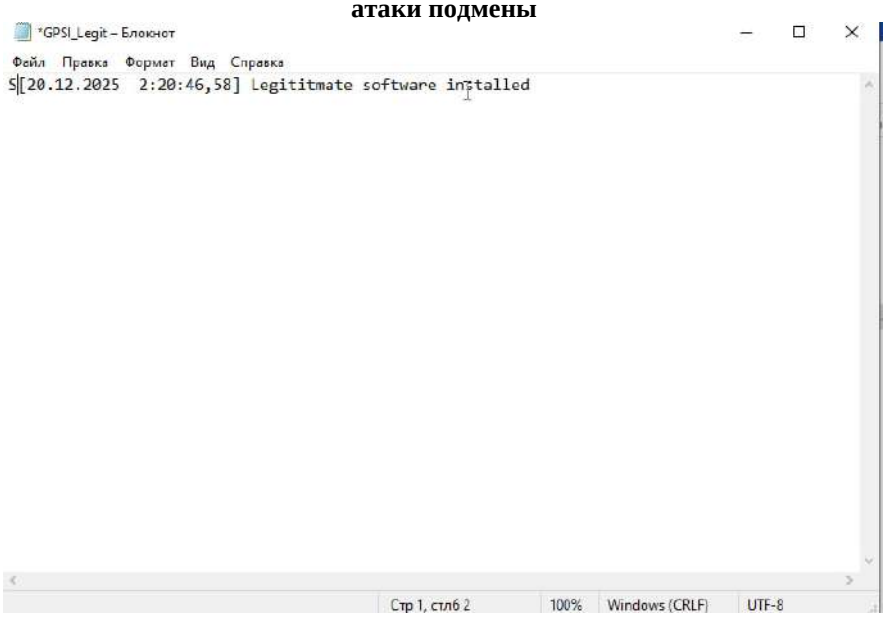

Рис. 3. Легитимный MSI-пакет в сетевой папке \\DC01\SoftwareDist с намеренно избыточными правами NTFS (Authenticated Users: Modify)

Злоумышленник (учетная запись Hacker) получает доступ к папке \\DC01\SoftwareDist и, пользуясь предоставленными правами Modify, заменяет легитимный MSI-пакет на вредоносный (в эксперименте — пакет, создающий текстовый файл-маркер) (Рисунок 4).

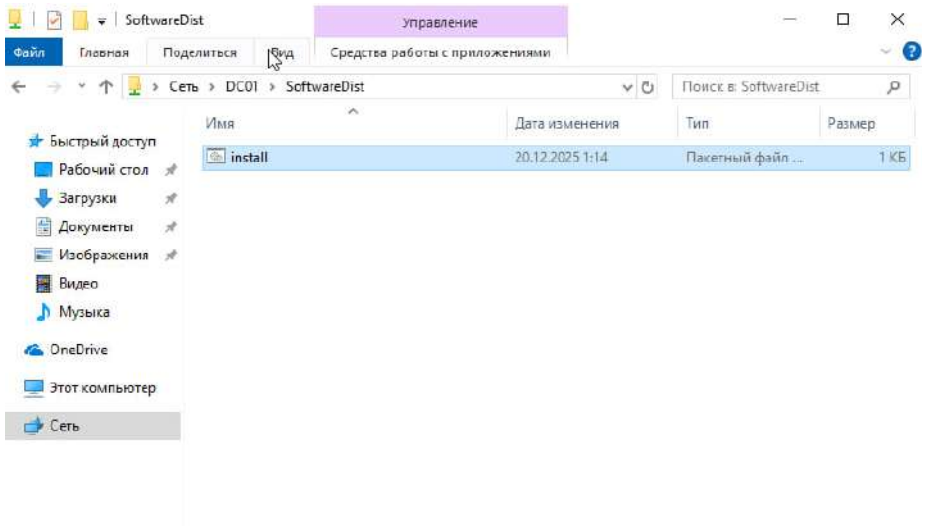

Рис. 4. Замена легитимного MSI-пакета вредоносным: учётная запись Hacker записывает подменный файл в сетевую папку, используя избыточные права Modify

После обновления групповых политик на клиентских компьютерах (автоматического или через gpupdate /force) был зафиксирован факт установки подмененного пакета на все рабочие станции в домене (Рисунок 5, 6).

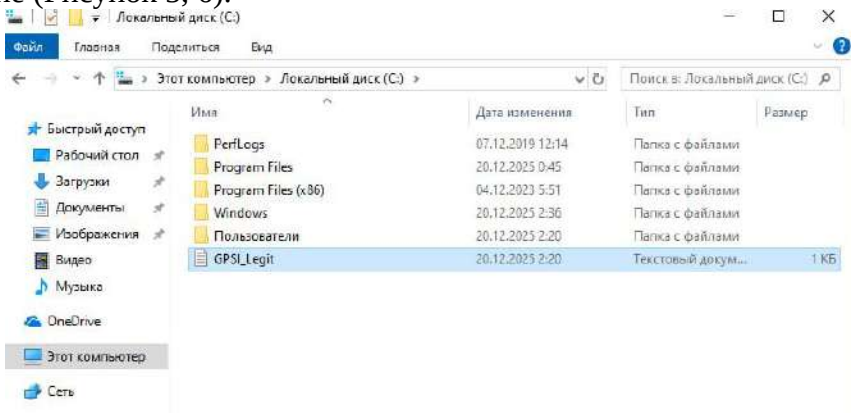

Рис. 5. Вредоносный MSI-пакет, размещённый учётной записью Hacker в сетевой папке вместо легитимного дистрибутива

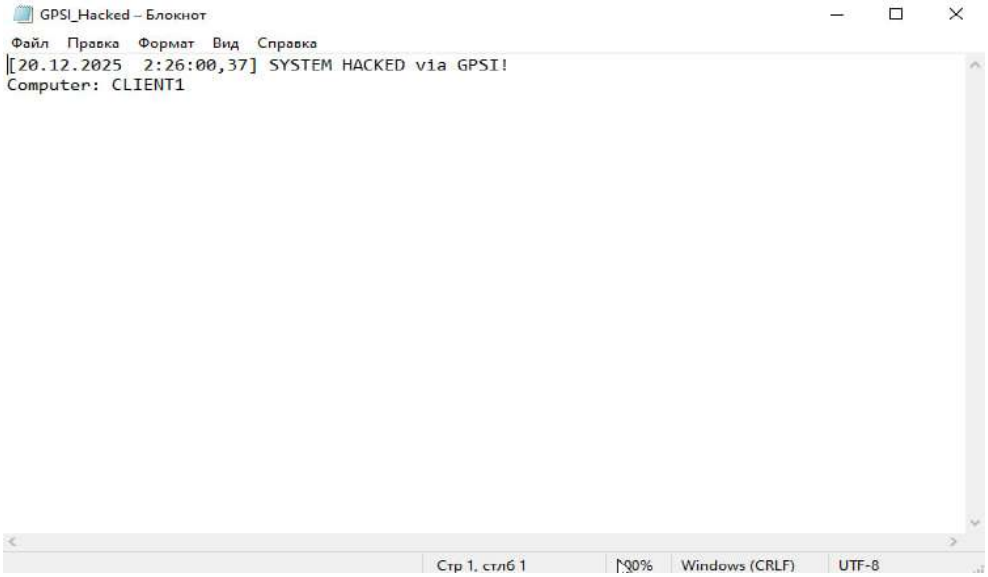

Рис. 6. Результат установки подменённого пакета на клиентской рабочей станции: создан файл-маркер, подтверждающий выполнение вредоносного кода

Эксперимент наглядно подтвердил критический риск, возникающий при небезопасной конфигурации прав доступа. Клиентские системы не выполнили никаких проверок цифровой подписи или целостности файла пакета перед установкой, так как соответствующие политики

не были активированы. Кроме того, была выявлена недостаточность стандартного аудита: в журналах событий отсутствовали явные записи о подмене пакета.

Количественные результаты Фазы 1:

В описанной небезопасной конфигурации атака была успешно воспроизведена; число независимых прогонов не фиксировалось.

Время до компрометации: от момента подмены пакета до установки на первый клиент — от нескольких минут (при принудительном обновлении политик) до 90 минут (стандартный интервал).

Фаза 2: Валидация мер защиты.

Для демонстрации эффективности контрмер был проведен дополнительный эксперимент. На той же лабораторной среде были последовательно применены и протестированы два защитных механизма:

Корректировка прав доступа: права NTFS для группы Authenticated Users на папке SoftwareDist были изменены на Read & Execute. Попытка учетной записи Hacker заменить или удалить MSI-пакет завершилась неудачей с ошибкой доступа. Атака была предотвращена на этапе доступа к хранилищу.

Включение проверки цифровых подписей: в политиках установщика Windows (Windows Installer) через Group Policy была активирована настройка "Запретить установку непроверенных пакетов" (параметр GPO: Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Установщик Windows → "Запрет установки пакетов без действительной цифровой подписи"). Попытка установки неподписанного (подмененного) пакета, даже при ошибочно оставленных правах на запись в сетевой папке, была заблокирована установщиком Windows с записью соответствующего сообщения об ошибке в журнале событий приложений.

Заключение

Таким образом, проведённое исследование продемонстрировало, что основной риск при использовании GPSI связан не с уязвимостью протокола как такового, а с небезопасной конфигурацией по умолчанию и потенциальными ошибками администрирования, такими как предоставление избыточных прав на запись в сетевое хранилище ПО. Хотя механизмы защиты (строгий контроль доступа NTFS и политики проверки цифровых подписей) существуют в платформе, они часто не используются, что делает инфраструктуру уязвимой для внутренних угроз.

Экспериментально подтверждено, что для минимизации рисков необходим комплексный подход:

1. Строгий контроль доступа: назначение на сетевые папки с установочными пакетами минимально необходимых прав (как правило, Read-only для рядовых пользователей и компьютеров).
2. Использование подписанных пакетов: внедрение практики подписи всех распространяемых MSI-пакетов цифровыми сертификатами и обязательное включение соответствующих политик проверки в домене.
3. Усиленный аудит и мониторинг: настройка аудита успешных и неуспешных попыток изменения файлов в критичных сетевых ресурсах для оперативного обнаружения инцидентов.

Применение этих мер, как показала вторая фаза эксперимента, эффективно блокирует описанный вектор атаки. Для критически важных инфраструктур также следует рассмотреть переход к более специализированным и безопасным по дизайну системам развертывания ПО.

Список литературы

1. Брысин А.Н., Журавлева Ю.А., Котов И.Ю. Исследование базовых атак и компрометации доменной Windows-инфраструктуры // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 2. – С. 45–53.
2. Корякин В.Ю., Тищенко Э.В. Тестирование защиты инфраструктуры GPO на базе Windows Server: анализ уязвимостей и методов обхода групповых политик // Труды

молодых ученых РГУ нефти и газа (НИУ) им. И.М. Губкина. – Москва : РГУ нефти и газа (НИУ) им. И.М. Губкина, 2025. – С. 1–10.
3. Болотов А.С., Болотова Т.П. Файловая система NTFS: обзор версий, производительность // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. – 2012. – № 3 (20). – С. 21–28.
4. Николаенкова О.А., Серик А.А., Хагуш Р.Э. Настройки конфигурации безопасности в Windows // Молодой исследователь Дона. – 2023. – № 1 (40). – С. 78–83.
5. Баранов А.Н. Повышение эффективности процессов администрирования компьютерных систем путем использования технологии групповых политик // Информационные технологии и системы : сб. науч. тр. – 2022. – С. 15–22.
6. Николаев В.В. Особенности реализации домена с тонкими клиентами на базе Microsoft Windows Server 2012 R2 // Международный студенческий научный вестник / СибАК. – Орёл. – 2016. – № 4. – С. 112–115.
7. Толганбаев Т.К. Доменные службы Active Directory и ядро сервера // Вестник магистратуры. – 2014. – № 11 (38). – С. 30–33. – ISSN 2223-4047.
8. Уймин А.Г. Нормирование показателей при организации киберполигона по сетевым технологиям // Нефть и газ – 2024 : тезисы докладов 78-й Международной молодежной научной конференции. – Москва : РГУ нефти и газа (НИУ) им. И.М. Губкина, 2024. – С. 1253–1254.

References

1. Brysin, A. N., Zhuravleva, Yu. A., & Kotov, I. Yu. (2023). Investigation of basic attacks and compromise of Windows domain infrastructure. Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii [Caspian Journal: Management and High Technologies], (2), 45–53.
2. Koryakin, V. Yu., & Tishchenko, E. V. (2025). Windows Server-based GPO infrastructure protection testing: Vulnerability analysis and methods of bypassing group policies. In Trudy molodykh uchenykh RGU nefti i gaza (NIU) im. I.M. Gubkina [Proceedings of Young Scientists of Gubkin University] (pp. 1–10). Gubkin Russian State University of Oil and Gas (NIU).
3. Bolotov, A. S., & Bolotova, T. P. (2012). The NTFS file system: Version overview and performance. Vestnik Tomskogo gosudarstvennogo universiteta. Upravleniye, vychislitelnaya tekhnika i informatika [Tomsk State University Journal of Control and Computer Science], (3), 21–28.
4. Nikolaenkova, O. A., Serik, A. A., & Hagush, R. E. (2023). Security configuration settings in Windows. Molodoy issledovatel Dona [Young Researcher of the Don], (1), 78–83.
5. Baranov, A. N. (2022). Improving the efficiency of computer system administration processes through the use of group policy technology. In Informatsionnyye tekhnologii i sistemy: sbornik nauchnykh trudov [Information Technologies and Systems: Collected Papers] (pp. 15–22).
6. Nikolaev, V. V. (2016). Features of implementing a domain with thin clients based on Microsoft Windows Server 2012 R2. Mezhdunarodnyy studencheskiy nauchnyy vestnik [International Student Scientific Bulletin], (4), 112–115.
7. Tolganbaev, T. K. (2014). Active Directory domain services and the server core. Vestnik magistratury [Bulletin of the Magistracy], (11), 30–33. ISSN 2223-4047.
8. Uymin, A. G. (2024). Normalization of indicators in the organization of a cyber range on network technologies. In Neft i gaz – 2024: Tezisy dokladov 78-y Mezhdunarodnoy molodezhnoy nauchnoy konferentsii [Oil and Gas – 2024: Abstracts of the 78th International Youth Scientific Conference] (pp. 1253–1254). Gubkin Russian State University of Oil and Gas (NIU).

Информация об авторах

Кязымов Адалат Адалатович — студент факультета комплексной безопасности ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: adalat.kiazymov@mail.ru

Терешонок Артём Алексеевич — студент факультета комплексной безопасности ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: kr3nver@yandex.ru

AUTOMATED SOFTWARE DEPLOYMENT TOOLS IN WINDOWS INFRASTRUCTURE. SECURITY ISSUES

Kyazimov A. A.[1], Tereshonok A. A.[1]

[1]National University of Oil and Gas «Gubkin University»

Abstract. *This article presents an in-depth security analysis of the built-in Group Policy Software Installation (GPSI) mechanism used for centralized software deployment in Windows Active Directory environments. The research focuses on the practical assessment of security risks associated with the substitution of MSI installation packages stored in network shares under misconfigured access permissions. An isolated laboratory environment was deployed to simulate a typical corporate domain network segment, comprising a Windows Server 2025 domain controller and two Windows 10 Pro client workstations. A series of attack scenarios was conducted, demonstrating that when NTFS permissions are incorrectly configured — specifically, when the Authenticated Users group is granted Modify rights — a low-privileged domain user can successfully replace a legitimate MSI package with a malicious one and trigger its installation on all domain workstations. It was established that, in the absence of activated digital signature verification policies, client systems perform no integrity or authenticity checks on packages prior to installation, and standard event logging does not capture file substitution events. A second experimental phase validated two countermeasures: restricting NTFS permissions to Read-only and enabling mandatory digital signature verification policies. Both measures effectively blocked the described attack vector. The findings indicate that the primary risk stems not from architectural flaws in the GPSI protocol itself, but from configuration errors and the non-utilization of available platform-level security controls. Practical recommendations are formulated covering strict access control, mandatory MSI package signing, and enhanced file auditing on critical network shares.*

Keywords: *Group Policy, GPSI, Windows security, automatic software installation, Active Directory, MSI, vulnerabilities, package substitution, integrity, audit.*

Information about the authors

Kyazimov Adalat Adalatovich — student of the Faculty of Integrated Fuel and Energy Complex Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: adalat.kiazymov@mail.ru

Tereshonok Artem Alekseevich — student of the Faculty of Integrated Fuel and Energy Complex Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: kr3nver@yandex.ru

Рубрика 2. Методы и системы защиты информации, информационная безопасность

УДК *004.056.5:004.8*

В. С. Греков [1]

[1]*ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация*

БОЛЬШИЕ ЯЗЫКОВЫЕ МОДЕЛИ В АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ: СОВРЕМЕННОЕ СОСТОЯНИЕ, ОГРАНИЧЕНИЯ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ В ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *Статья посвящена анализу современного состояния исследований в области применения больших языковых моделей (LLM) для автоматизации тестирования на проникновение (пентеста). Рассматриваются причины стремительного роста интереса к данному направлению, обусловленные усложнением ИТ-инфраструктур, высокой стоимостью традиционных методов аудита защищённости и развитием концепции DevSecOps. На основе систематизации обзорных и прикладных исследований 2023–2025 годов выявлены четыре ключевых направления применения LLM в кибербезопасности: поддержка принятия решений и стратегического планирования атак, автоматизация этапов пентеста, обеспечение защищённости самих языковых моделей (AI Red Teaming), а также интеллектуальный анализ исходного кода. Проведён критический анализ архитектур мультиагентных систем с использованием подходов Retrieval-Augmented Generation (RAG), систем тестирования и оценки эффективности, а также коммерческих решений. Установлено, что даже наиболее продвинутые системы пентеста на базе LLM находятся на промежуточных уровнях автономности (3–4 из 5), не способны самостоятельно формулировать цели и оценивать последствия своих решений. Обосновывается тезис о том, что на конец 2025 года LLM выступают прежде всего инструментом аналитика, а не автономным пентестером. Рассматриваются педагогические аспекты интеграции LLM-инструментов в профессиональную подготовку специалистов по информационной безопасности, обосновывается необходимость формирования у обучающихся критического мышления в отношении возможностей и ограничений данных технологий. Отдельное внимание уделяется требованиям к воспроизводимости исследований и педагогической интерпретации полученных результатов.*

Ключевые слова: *большие языковые модели, тестирование на проникновение, кибербезопасность, автоматизация, мультиагентные системы, RAG, профессиональная подготовка.*

Введение

Цифровая трансформация экономики и общества сопровождается не только расширением функциональных возможностей информационных технологий, но и качественным усложнением угроз информационной безопасности. Современные корпоративные ИТ-инфраструктуры — это распределённые гетерогенные системы, включающие облачные платформы, микросервисные архитектуры, контейнеризированные приложения, конвейеры непрерывной интеграции и доставки (CI/CD), а также устройства Интернета вещей. Указанная сложность формирует принципиально новые требования к компетенциям специалистов по информационной безопасности, в том числе реализующих тестирование на проникновение (пентест) — методологически структурированную практику имитации атак с целью выявления уязвимостей до их эксплуатации злоумышленниками.

Традиционный пентест, выполняемый квалифицированными специалистами в ручном режиме, характеризуется рядом системных ограничений: высокой стоимостью, значительными временными затратами, трудностью масштабирования, зависимостью результатов от субъективного опыта конкретного исполнителя. В условиях непрерывного расширения атакующей поверхности организаций и ужесточения требований к регулярности и полноте аудита защищённости формируется устойчивый запрос на автоматизированные и воспроизводимые средства анализа.

Начиная с 2023 года фиксируется интенсивный рост интереса исследовательского и практического сообщества к применению больших языковых моделей (Large Language Models, LLM) в задачах кибербезопасности, включая автоматизацию пентеста. Указанный интерес обусловлен характеристиками LLM: способностью к семантическому пониманию технической документации, генерации исполняемого кода, планированию многошаговых действий, интерпретации результатов сканирования в контексте известных таксономий уязвимостей. LLM открывают возможность формирования семантического слоя поверх существующих

инструментов пентеста — гибкого интерфейса между специалистом и конвейером тестирования с относительно низкими операционными издержками.

Обобщённая схема факторов, определяющих рост интереса к применению LLM в задачах пентеста, представлена на рис. 1.

Рис. 1. Факторы роста интереса к применению LLM в автоматизации тестирования на проникновение

Интенсивность развития данного направления порождает серьёзные методологические проблемы. Исследовательское поле остаётся фрагментированным. Большинство публикуемых результатов получены на синтетических стендах, а реальная автономность существующих систем существенно уступает декларируемой. Указанное обстоятельство формирует риск формирования у специалистов и обучающихся завышенных ожиданий относительно функциональных возможностей LLM в задачах информационной безопасности.

Настоящая статья решает две взаимосвязанные задачи. Первая: систематизация актуального состояния исследований в области применения LLM для автоматизации пентеста. Вторая: анализ педагогических аспектов подготовки специалистов по информационной безопасности в условиях, когда LLM-инструменты приобретают статус элемента профессионального арсенала. Как отмечает А.М. Новиков, «профессиональное образование должно опережать производство» [1, с. 47]. Указанное требование определяет обоснованность включения тематики LLM в кибербезопасности в образовательные программы подготовки специалистов соответствующего профиля.

Материалы и методы

В основу исследования положен нарративный обзор научных публикаций, посвящённых применению LLM в задачах кибербезопасности и пентеста, опубликованных в период с января 2023 по март 2025 года. Для формирования корпуса источников использовались базы данных arXiv, IEEE Xplore, ACM Digital Library, а также репозитории открытого программного обеспечения (GitHub). Критерии включения: наличие эмпирических результатов или систематического обзора; фокус на применении LLM именно в задачах тестирования на проникновение или смежных задачах кибербезопасности; доступность полного текста.

Методологическую основу составили: метод обзорно-аналитического сопоставления литературы, сравнительный анализ архитектурных решений, критический анализ методологии экспериментов, а также контент-анализ коммерческих продуктов в данной области. При анализе педагогических аспектов применялись методы теоретического анализа и синтеза, опирающиеся на труды отечественных и зарубежных исследователей в области профессионального образования и дидактики высшей школы.

Теоретическую базу педагогической части исследования составляют концепция профессионального образования А.М. Новикова [1], теория деятельностного подхода А.Н. Леонтьева

[2], концепция проблемного обучения И.Я. Лернера [3], а также современные исследования в области подготовки специалистов по информационной безопасности [4; 5].

Результаты

1. Обзор исследовательского поля: от глубокого обучения к LLM

Применение методов искусственного интеллекта в задачах кибербезопасности имеет достаточно длительную историю. По данным обзорного исследования [6], в период с 2015 по 2023 год в данной области доминировали алгоритмы обучения с подкреплением (Reinforcement Learning) и глубокого обучения (Deep Learning). Эти подходы демонстрировали определённые успехи в узкоспециализированных задачах — обнаружении аномалий, классификации вредоносного программного обеспечения, анализе сетевого трафика, — однако оставались ограниченными в части семантического понимания контекста и способности к многошаговому планированию.

Появление больших языковых моделей, прежде всего семейства GPT (OpenAI), Claude (Anthropic), Llama (Meta) и их аналогов, ознаменовало качественный сдвиг в подходах к автоматизации задач кибербезопасности. Как показывает анализ корпуса работ начиная с января 2023 года [7], исследовательское поле вокруг применения LLM в информационной безопасности стало многомерным и быстро формирующимся направлением. Наибольший интерес вызывают четыре направления:

– поддержка принятия решений и стратегического планирования атак;
– автоматизация этапов тестирования на проникновение;
– обеспечение защищённости самих языковых моделей (AI Red Teaming);
– интеллектуальный анализ исходного кода.

Указанные направления применения LLM в задачах кибербезопасности систематизированы на рис. 2.

Рис. 2. Основные направления применения LLM в задачах кибербезопасности

Принципиальное отличие LLM от предшествующих подходов к автоматизации пентеста состоит в функциональной роли этих моделей. LLM применяются не как самостоятельные классификаторы или агенты, а как семантический слой поверх существующих инструментов: модели обеспечивают планирование, установление соответствия между результатами сканирования и таксономиями уязвимостей (MITRE ATT&CK, CVE, CWE), формулирование исполнимых шагов тестирования, а также реализуют функцию интерфейса между специалистом и конвейером тестирования [6].

Начиная с 2024 года, несмотря на рост числа прикладных публикаций и разработку коммерческих решений в данной области, исследовательское поле сохраняет фрагментированный и методологически неоднородный характер [7]. Указанное обстоятельство имеет

существенное значение как для практиков, так и для педагогов: отсутствие устоявшейся методологической базы обусловливает необходимость критического анализа публикуемых результатов.

2. Мультиагентные системы с RAG: возможности и ограничения

Мультиагентные системы на основе подхода Retrieval-Augmented Generation (RAG) составляют наиболее интенсивно разрабатываемое направление в области LLM-пентеста. Архитектурная суть подхода состоит в расширении языковой модели внешней базой знаний, включающей документацию по уязвимостям, базы эксплойтов и технические руководства. В режиме реального времени из указанной базы извлекаются релевантные фрагменты для формирования контекстно-обогащённых запросов к модели. Применение RAG-архитектуры обеспечивает преодоление ограничений, связанных с устареванием обучающих данных, и поддержание актуальности генерируемых рекомендаций.

Обобщённая логика построения мультиагентной RAG-системы для задач пентеста представлена на рис. 3.

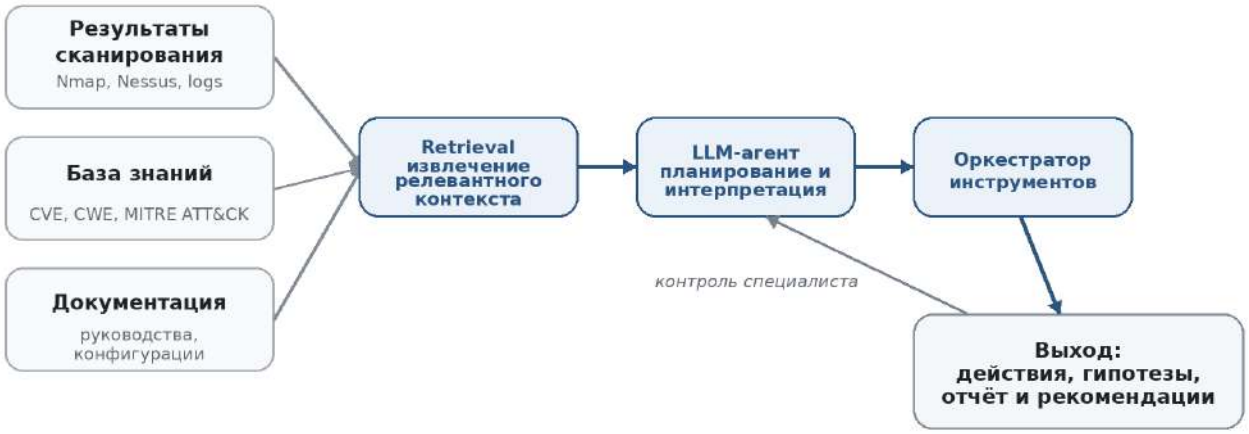

Рис. 3. Обобщённая логика мультиагентной RAG-системы в тестировании на проникновение

Анализ отобранных для обзорного сопоставления публикаций [8–18] позволяет выделить следующие преимущества мультиагентных RAG-систем в контексте пентеста:

– автоматизация рутинных этапов тестирования (сбор информации, сканирование портов, идентификация сервисов);

– способность к контекстному связыванию результатов различных инструментов;

– генерация структурированных отчётов с рекомендациями по устранению уязвимостей;

– снижение когнитивной нагрузки на специалиста при работе с большими объёмами данных.

Вместе с тем критический анализ выявляет ряд существенных ограничений, которые нередко остаются в тени в публикациях, ориентированных на демонстрацию достижений.

Первое ограничение — отсутствие системного подхода к проектированию архитектуры. Большинство опубликованных работ представляют конкретный прототип, решающий одну конкретную задачу в специфических условиях. Обобщаемость предложенных архитектурных решений на другие классы задач или иные операционные среды, как правило, не обосновывается.

Второе ограничение — проблема утечки данных в обучающий стек (data contamination). Выбранные для тестирования задачи практически наверняка входили в обучающие данные для моделей: синтетические примеры с соревнований по кибербезопасности (CTF — Capture The Flag) и уязвимых виртуальных машин (типа Metasploitable, HackTheBox, TryHackMe), решения к которым публично доступны в интернете. Это означает, что модель может демонстрировать высокую «производительность» не за счёт реального понимания задачи, а за счёт воспроизведения паттернов из обучающих данных.

Третье ограничение — отставание от актуального состояния моделей. Исследования, как правило, отстают от SoTA (State of the Art) моделей на год-полтора. Учитывая темпы развития LLM, это означает, что к моменту публикации результаты могут быть уже неактуальны.

Четвёртое ограничение — отсутствие воспроизводимости. Большинство экспериментов не могут быть воспроизведены независимыми исследователями: не публикуются промпты, конфигурации агентов, версии используемых моделей и инструментов. Это фундаментальная проблема для научного сообщества, поскольку, как подчёркивает В.В. Краевский, «воспроизводимость результатов является необходимым условием научного знания» [19, с. 112].

3. Системы тестирования и оценки эффективности (benchmarks и evals)

Параллельно с разработкой прикладных систем ведётся работа по созданию инструментов для их объективной оценки. Анализ работ [15–18] показывает, что данное направление находится в начальной стадии развития и также страдает от ряда системных проблем.

С одной стороны, наличие специализированных бенчмарков для LLM-пентеста является необходимым условием научного прогресса в данной области: без стандартизированных метрик невозможно корректно сравнивать различные системы и отслеживать динамику развития. С другой стороны, существующие инструменты оценки имеют существенные ограничения.

Во-первых, отсутствует системный подход к проектированию архитектуры систем тестирования и оценки. Каждая исследовательская группа создаёт собственный бенчмарк, что делает невозможным прямое сравнение результатов разных работ.

Во-вторых, с учётом стремительного роста эффективности моделей существующие инструменты не позволяют в полной мере оценивать качество выполнения задач, степень галлюцинаций и совокупный скор каждой модели. Бенчмарки, разработанные для моделей 2023 года, оказываются «насыщенными» (saturated) для моделей 2025 года — то есть все системы показывают близкие к максимальным результаты, что лишает бенчмарк дифференцирующей силы.

В-третьих, проблема утечки данных в обучающий стек актуальна и для систем оценки: если задания бенчмарка публично доступны, они с высокой вероятностью входят в обучающие данные тестируемых моделей.

Исследование [5], посвящённое применению LLM в образовании по пентесту, предлагает интересный подход: использование LLM не только как инструмента тестирования, но и как средства мониторинга прогресса студентов, поддержки совместной работы и предоставления обратной связи в больших учебных группах. Авторы отмечают, что «образование в области кибербезопасности является сложным, и понимание возможностей LLM для поддержки образования никогда не было более важным» [5]. Это наблюдение имеет прямое отношение к педагогической проблематике настоящей статьи.

4. Оценка автономности: где реально находятся LLM-системы пентеста

Одним из наиболее методологически значимых вкладов в данную область является работа [19], в которой введена терминологическая ясность касательно автономности и различных её уровней в контексте тестирования на проникновение. Авторы предлагают пятиуровневую шкалу автономности:

– Уровень 1: Полностью ручное тестирование; LLM используется только как справочный инструмент.

– Уровень 2: LLM предлагает следующий шаг, специалист принимает решение и выполняет действие.

– Уровень 3: LLM планирует и выполняет отдельные этапы, специалист осуществляет общий надзор.

– Уровень 4: LLM выполняет большинство задач автономно, специалист вмешивается при необходимости.

– Уровень 5: Полностью автономное тестирование без участия человека.

Сводная интерпретация уровней автономности LLM-систем пентеста приведена на рис. 4.

Рис. 4. Шкала автономности LLM-систем тестирования на проникновение

Качественное и количественное сравнение инструментов автоматического пентеста, проведённое в данной работе, приводит к справедливому выводу: даже самые продвинутые системы пентеста на базе LLM находятся на промежуточных уровнях 3–4. Модели не могут самостоятельно формулировать цели и оценивать последствия своих решений — это принципиальное ограничение, обусловленное самой природой языковых моделей как систем, оптимизированных для предсказания следующего токена, а не для целеполагания и стратегического планирования.

Данный вывод имеет важное педагогическое следствие: подготовка специалистов по информационной безопасности не может строиться на предположении о полной автоматизации пентеста в обозримом будущем. Напротив, как указывает И.Я. Лернер, «проблемное обучение формирует у учащихся способность к самостоятельному решению нестандартных задач» [3, с. 89] — именно эта способность остаётся незаменимой в условиях, когда автоматизированные системы достигают своих пределов.

5. Коммерческие решения: возможности и риски

Параллельно с академическими исследованиями активно развивается рынок коммерческих LLM-решений для задач кибербезопасности [20–23]. Анализ доступных продуктов позволяет выделить их ключевые преимущества и недостатки.

Преимущества коммерческих решений: хорошая масштабируемость — возможность одновременного тестирования большого числа систем; способность выявлять уязвимости бизнес-логики, которые традиционные сканеры пропускают; частичное покрытие программных уязвимостей; экономическая эффективность — дешевле, чем использование лицензированного ПО автоматизированных сканеров уязвимостей не на базе LLM, и значительно дешевле, чем полноценный операционный центр безопасности (SOC).

Недостатки коммерческих решений: непрозрачность («кот в мешке») — отсутствуют инструменты для независимой оценки эффективности, гарантии надёжности и устойчивости платформы; неясность в отношении использования конфиденциальных данных клиентов, передаваемых в систему в процессе тестирования; исследование подключённых инструментов и баз данных «вслепую» потенциально влечёт за собой избыточные временные и финансовые затраты; отсутствие стандартизированных метрик для сравнения с конкурирующими решениями.

Эти ограничения особенно важны с точки зрения профессиональной подготовки: будущие специалисты должны уметь критически оценивать коммерческие инструменты, не принимая на веру маркетинговые заявления производителей. Как подчёркивает С.Я. Батышев, «профессиональная компетентность специалиста включает не только умение применять инструменты, но и способность критически оценивать их возможности и ограничения» [20, с. 156].

6. Наиболее перспективный открытый проект: Cybersecurity AI (CAI)

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Среди рассмотренных решений особого внимания заслуживает проект Cybersecurity AI (CAI) [24] — открытый инструмент, ориентированный на активное использование в академической среде. Его ключевые преимущества:

– открытость исходного кода — возможность независимой верификации алгоритмов и архитектурных решений;

– пополняемая научная база — исследования эффективности публикуются и доступны для критического анализа;

– практическое тестирование — инструмент проходит апробацию на различных платформах по кибербезопасности и в «полевых» условиях;

– прозрачность и документация — подробная документация позволяет воспроизводить эксперименты.

Вместе с тем CAI не лишён ограничений: при заявленной полной автоматизации инструмент всё же требует участия специалиста; наиболее продвинутая модель предоставляется по подписке и не находится в публичном доступе; по-прежнему отсутствует системный подход к тестированию производительности.

С педагогической точки зрения CAI представляет значительный интерес именно как образовательный инструмент: его открытость позволяет использовать его в учебном процессе для демонстрации принципов работы LLM-агентов в задачах безопасности, а также для формирования у студентов навыков критического анализа автоматизированных систем.

Таблица 1 – Сводная характеристика материалов презентации по прикладным LLM-решениям в пентесте

Направление / материал	Потенциал применения	Ключевые ограничения	Значение для подготовки специалистов
Мультиагентные RAG-системы	Автоматизация рутинных этапов, связывание результатов инструментов, генерация отчётов.	Фрагментарность архитектур, риск data contamination, отставание от SoTA, слабая воспроизводимость.	Использовать как объект критического разбора архитектуры и качества эксперимента.
Benchmarks и evals	Формирование базы для сравнения LLM-систем и отслеживания динамики качества.	Несопоставимость методик, насыщение тестов, утечка заданий в обучающие данные.	Обучать студентов постановке корректной оценки и анализу метрик.
Оценка автономности	Разделение уровней участия человека и автоматизации отдельных этапов.	Даже продвинутые решения фактически находятся на уровнях 3–4 из 5.	Показывать границы автоматизации и необходимость профессионального надзора.
Коммерческие решения	Масштабируемость, частичное выявление уязвимостей бизнес-логики, снижение стоимости проверок.	Непрозрачность, риски конфиденциальности, отсутствие независимых метрик.	Формировать навык критической оценки продуктов и маркетинговых заявлений.
Cybersecurity AI (CAI)	Open-source, документация, академическая ориентация, возможность воспроизводимой апробации.	Требует участия специалиста; продвинутая модель доступна по подписке; тестирование пока незрелое.	Подходит для учебных стендов и демонстрации принципов LLM-агентов.

Обсуждение

7. Реальная роль LLM в автоматизации пентеста: итоговая оценка

Систематизация рассмотренных исследований позволяет сформулировать взвешенную оценку реальной роли LLM в автоматизации тестирования на проникновение по состоянию на конец 2025 года.

Применение LLM в пентесте остаётся экспериментальным направлением. Методологическая база только формируется: отсутствуют общепринятые стандарты проектирования систем, метрики оценки и протоколы воспроизводимости экспериментов. Большинство решений — прототипы для учебных стендов и CTF-сценариев, демонстрирующие частичные успехи в контролируемых условиях.

При переносе в реальные корпоративные или облачные среды проявляются ключевые ограничения. Нестабильность поведения моделей, слабая воспроизводимость результатов и низкая автономность делают существующие системы непригодными для самостоятельного использования в производственных условиях без постоянного надзора квалифицированного специалиста.

Отсутствуют открытые эталоны, формализованные метрики и зрелые механизмы верификации выводов моделей. Это означает, что любые заявления о «высокой эффективности» той или иной системы должны восприниматься с критической осторожностью.

На конец 2025 года LLM — это прежде всего инструмент аналитика, а не автономный пентестер. Конкретные задачи, в которых LLM демонстрируют реальную ценность:

– сбор и агрегация разрозненных данных из множества источников;
– анализ технической документации и конфигурационных файлов;
– генерация инсайтов и подсказок для специалистов уровня L1–L2;
– автоматизация составления отчётов;
– поддержка принятия решений при классификации уязвимостей.

Сводное место LLM в контуре пентеста отражено на рис. 5.

Рис. 5. Итоговая роль LLM в контуре тестирования на проникновение

Интеграция LLM в CI/CD-цепочки пентеста возможна для узких задач (например, автоматическая проверка конфигураций на соответствие политикам безопасности), но до полной автоматизации полного цикла тестирования на проникновение ещё далеко.

8. Педагогические аспекты подготовки специалистов по ИБ в условиях развития LLM

Описанное состояние исследовательского поля ставит перед системой профессионального образования ряд принципиальных вопросов. Как готовить специалистов по информационной безопасности в условиях, когда LLM-инструменты становятся частью профессионального арсенала, но при этом их возможности существенно ограничены, а методологическая база нестабильна?

8.1. Формирование критического мышления как ключевая образовательная задача

Первоочередной педагогической задачей является формирование у обучающихся критического мышления в отношении возможностей и ограничений LLM-инструментов. Это требование вытекает непосредственно из анализа состояния исследовательского поля: специалист, некритически доверяющий выводам LLM-системы, рискует пропустить реальные уязвимости или, напротив, потратить ресурсы на ложные срабатывания.

Как отмечает И.Я. Лернер, «проблемное обучение не только вооружает учащихся знаниями, но и формирует у них опыт творческой деятельности» [3, с. 94]. Применительно к подготовке специалистов по ИБ это означает необходимость включения в учебный процесс задач, требующих не просто применения LLM-инструментов, но и критической оценки их результатов, выявления ошибок и галлюцинаций, сопоставления автоматически сгенерированных рекомендаций с собственным профессиональным суждением.

8.2. Деятельностный подход и симуляция реальных условий

Деятельностный подход, разработанный в трудах А.Н. Леонтьева [2] и получивший развитие в концепции контекстного обучения А.А. Вербицкого [21], предполагает организацию учебного процесса таким образом, чтобы студенты осваивали профессиональные компетенции в условиях, максимально приближённых к реальной профессиональной деятельности.

В контексте подготовки специалистов по ИБ это означает необходимость создания учебных стендов, имитирующих реальные корпоративные инфраструктуры, и организации практических занятий, в ходе которых студенты используют LLM-инструменты в связке с традиционными средствами пентеста. При этом принципиально важно, чтобы учебные задачи не ограничивались CTF-сценариями (которые, как было показано выше, могут входить в обучающие данные моделей), но включали нестандартные ситуации, требующие самостоятельного профессионального суждения.

Исследование [5] подтверждает педагогическую ценность такого подхода: авторы показывают, что LLM могут эффективно использоваться для мониторинга прогресса студентов и предоставления персонализированной обратной связи в больших учебных группах, что

особенно актуально в условиях дефицита квалифицированных преподавателей по кибербезопасности.

8.3. Проблема актуальности учебного контента

Стремительное развитие LLM-технологий создаёт серьёзную проблему для системы профессионального образования: учебные программы и материалы устаревают быстрее, чем успевают обновляться. Как подчёркивает А.М. Новиков, «содержание профессионального образования должно отражать не только сегодняшние, но и завтрашние требования производства» [1, с. 203].

Решение этой проблемы требует перехода от статичных учебных программ к динамичным, предусматривающим регулярное обновление контента в соответствии с актуальным состоянием технологий. При этом важно не просто включать в программу описание новейших инструментов, но и формировать у студентов метакомпетенции — способность самостоятельно осваивать новые технологии, критически оценивать их возможности и интегрировать в профессиональную деятельность.

8.4. Этические аспекты подготовки специалистов

Применение LLM в задачах кибербезопасности поднимает ряд этических вопросов, которые должны быть отражены в образовательных программах. Снижение порога входа в профессию пентестера за счёт LLM-инструментов означает, что те же инструменты могут использоваться злоумышленниками с недостаточной квалификацией. Это требует особого внимания к формированию у студентов профессиональной этики и понимания правовых рамок деятельности специалиста по информационной безопасности.

Как отмечает В.А. Сластёнин, «профессиональная подготовка специалиста неотделима от его нравственного воспитания» [22, с. 78]. Применительно к специалистам по ИБ это означает необходимость включения в образовательные программы не только технических дисциплин, но и курсов по профессиональной этике, правовому регулированию в сфере информационной безопасности и ответственному раскрытию уязвимостей.

8.5. Требования к компетенциям преподавателей

Эффективная подготовка специалистов по ИБ в условиях развития LLM-технологий предъявляет повышенные требования к компетенциям преподавателей. Педагог, не имеющий практического опыта работы с LLM-инструментами в задачах кибербезопасности, не способен сформировать у студентов адекватное понимание их возможностей и ограничений.

Это требование согласуется с положениями ФГОС ВО по направлению «Информационная безопасность», предусматривающими регулярное повышение квалификации преподавателей с привлечением специалистов-практиков из отрасли. Как указывает Э.Ф. Зеер, «профессиональное развитие педагога является необходимым условием качества профессионального образования» [23, с. 134].

8.6. Структура учебного модуля по LLM в кибербезопасности

На основе проведённого анализа можно предложить следующую структуру учебного модуля, посвящённого применению LLM в задачах кибербезопасности, для включения в образовательные программы подготовки специалистов по ИБ.

Тема 1. Основы больших языковых моделей (теоретический блок): архитектура трансформеров и принципы работы LLM; возможности и ограничения LLM — галлюцинации, data contamination, проблема актуальности знаний; обзор ключевых моделей: GPT-4o, Claude, Llama, специализированные модели для кибербезопасности.

Тема 2. LLM как инструмент аналитика безопасности (практический блок): применение LLM для анализа технической документации и конфигураций; генерация и интерпретация результатов сканирования; автоматизация составления отчётов о результатах тестирования; практическая работа — использование LLM для анализа результатов сканирования Nmap/Nessus.

Тема 3. Мультиагентные системы и RAG в пентесте (теоретико-практический блок): архитектура мультиагентных систем; принципы RAG и их применение в задачах

кибербезопасности; критический анализ существующих систем (PentestGPT, CAI и др.); практическая работа — развёртывание и тестирование открытого LLM-агента на учебном стенде.

Тема 4. Оценка эффективности и ограничения LLM-систем (аналитический блок): методология оценки LLM-систем в задачах безопасности; проблема воспроизводимости и data contamination; уровни автономности — где реально находятся существующие системы; практическая работа — сравнительный анализ результатов LLM-агента и ручного тестирования на одном стенде.

Тема 5. Этические и правовые аспекты (гуманитарный блок): правовое регулирование тестирования на проникновение в России и за рубежом; этика ответственного раскрытия уязвимостей; риски злоупотребления LLM-инструментами; профессиональные стандарты и сертификации в области пентеста.

Предложенная структура реализует принцип единства теории и практики, сформулированный С.Я. Батышевым как основополагающий для профессионального образования [20, с. 89], и обеспечивает формирование у студентов как технических компетенций, так и критического мышления, необходимого для работы с быстро развивающимися технологиями.

Заключение

Проведённый анализ позволяет сформулировать следующие основные выводы.

Применение LLM в автоматизации пентеста — перспективное, но методологически незрелое направление. Исследовательское поле сохраняет фрагментированный характер, большинство результатов получены на синтетических стендах, а проблемы воспроизводимости и контаминации обучающих данных (data contamination) существенно снижают достоверность публикуемых данных.

Реальная автономность LLM-систем пентеста не превышает уровней 3–4 по пятибалльной шкале. Модели не обладают способностью к самостоятельному целеполаганию и оценке последствий принимаемых решений. По состоянию на конец 2025 года LLM функционируют преимущественно в качестве аналитического инструмента — для агрегации данных, анализа технической документации, генерации аналитических гипотез и поддержки принятия решений специалистами уровня L1–L2.

Коммерческие решения обладают практическими преимуществами, однако сопряжены с существенными рисками в части прозрачности, верифицируемости результатов и обеспечения конфиденциальности данных клиентов.

Открытый проект CAI обладает наибольшим потенциалом с точки зрения академического применения: архитектура проекта обеспечивает прозрачность, воспроизводимость и возможность независимой верификации результатов.

Система профессионального образования в области информационной безопасности нуждается в адаптации к условиям LLM-эпохи. Задача подготовки специалистов включает формирование как технических компетенций работы с LLM-инструментами, так и навыков критического анализа их возможностей и ограничений. Базовыми педагогическими принципами при этом выступают деятельностный подход, проблемное обучение, симуляция реальных профессиональных условий, регулярное обновление содержания учебных программ.

Интеграция LLM в CI/CD-цепочки пентеста реализуема для решения узкоспециализированных задач. Полная автоматизация полного цикла тестирования на проникновение в обозримой перспективе недостижима. Квалифицированный специалист по информационной безопасности, способный к самостоятельному профессиональному суждению, сохраняет статус незаменимого участника процесса обеспечения безопасности информационных систем.

Перспективными направлениями дальнейших исследований являются: разработка стандартизированных методологий оценки LLM-систем применительно к задачам пентеста; создание открытых бенчмарков, устойчивых к проблеме контаминации обучающих данных; исследование педагогической эффективности различных подходов к интеграции LLM-инструментов в образовательные программы по кибербезопасности; разработка этических стандартов применения LLM в задачах наступательной безопасности.

Библиографический список

1. Новиков, А. М. Профессиональное образование России: перспективы развития / А. М. Новиков. – Москва: ИЦП НПО РАО, 1997. – 254 с.
2. Леонтьев, А. Н. Деятельность. Сознание. Личность / А. Н. Леонтьев. – Москва: Политиздат, 1975. – 304 с.
3. Лернер, И. Я. Проблемное обучение / И. Я. Лернер. – Москва: Знание, 1974. – 64 с.
4. Тихомиров, В. П. Цифровая трансформация образования: вызовы и возможности / В. П. Тихомиров, Н. В. Тихомирова // Открытое образование. – 2019. – № 4. – С. 4–14.
5. Alaryani, M. Towards Supporting Penetration Testing Education with Large Language Models: an Evaluation and Comparison / M. Alaryani [et al.] // arXiv preprint arXiv:2501.17539. – 2025.
6. Happe, A. Getting pwn'd by AI: Penetration Testing with Large Language Models / A. Happe, J. Cito // Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. – 2023. – P. 2082–2086.
7. Deng, G. PentestGPT: An LLM-empowered Automatic Penetration Testing Tool / G. Deng [et al.] // arXiv preprint arXiv:2308.06782. – 2023.
8. Xu, Z. AutoAttacker: A Large Language Model Guided System to Implement Automatic Cyberattacks / Z. Xu [et al.] // arXiv preprint arXiv:2403.01038. – 2024.
9. Fang, R. LLM Agents can Autonomously Exploit One-day Vulnerabilities / R. Fang [et al.] // arXiv preprint arXiv:2404.08144. – 2024.
10. Shao, R. Empirical Analysis of Large Language Models in Automated Vulnerability Discovery / R. Shao [et al.] // arXiv preprint arXiv:2312.02337. – 2023.
11. Bhatt, M. Purple Llama CyberSecEval: A Secure Coding Benchmark for Language Models / M. Bhatt [et al.] // arXiv preprint arXiv:2312.04724. – 2023.
12. Wan, Y. Cybersecurity Issues and Challenges: In Brief / Y. Wan [et al.] // IEEE Access. – 2024. – Vol. 12. – P. 1–15.
13. Moskal, S. LLM in the Shell: Generative AI-Powered Pentesting / S. Moskal [et al.] // arXiv preprint arXiv:2312.09552. – 2023.
14. Charan, P. V. S. From Text to MITRE Techniques: Examining the Layered Approach to Explainability With a Large Language Model (LLM) / P. V. S. Charan [et al.] // arXiv preprint arXiv:2308.09197. – 2023.
15. Tihanyi, N. CyberMetric: A Benchmark Dataset for Evaluating Large Language Models Knowledge in Cybersecurity / N. Tihanyi [et al.] // arXiv preprint arXiv:2402.07688. – 2024.
16. Peng, B. PenHeal: A Two-Stage LLM Framework for Automated Pentesting and Optimal Remediation / B. Peng [et al.] // arXiv preprint arXiv:2407.17788. – 2024.
17. Wan, Y. HackMentor: Fine-Tuning Large Language Models for Cybersecurity / Y. Wan [et al.] // arXiv preprint arXiv:2312.01234. – 2023.
18. Yang, J. SWE-bench: Can Language Models Resolve Real-World GitHub Issues? / J. Yang [et al.] // arXiv preprint arXiv:2310.06770. – 2023.
19. Краевский, В. В. Методология педагогики: новый этап / В. В. Краевский. – Москва: Академия, 2006. – 400 с.
20. Батышев, С. Я. Профессиональная педагогика / С. Я. Батышев; под ред. С. Я. Батышева, А. М. Новикова. – 3-е изд. – Москва: ЭГВЕС, 2010. – 456 с.
21. Вербицкий, А. А. Активное обучение в высшей школе: контекстный подход / А. А. Вербицкий. – Москва: Высшая школа, 1991. – 207 с.
22. Сластёнин, В. А. Педагогика / В. А. Сластёнин. – Москва: Академия, 2002. – 576 с.
23. Зеер, Э. Ф. Психология профессионального образования / Э. Ф. Зеер. – Москва: Академия, 2009. – 384 с.
24. Alias Robotics. Cybersecurity AI (CAI): An Open, Bug Bounty-Ready Agentic Framework // arXiv preprint arXiv:2504.06017. – 2025.

References

1. Novikov, A. M. (1997). Professional education in Russia: Development prospects. ICP NPO RAO. (In Russian)
2. Leont'ev, A. N. (1975). Activity. Consciousness. Personality. Politizdat. (In Russian)
3. Lerner, I. Ya. (1974). Problem-based learning. Znanie. (In Russian)
4. Tikhomirov, V. P., & Tikhomirova, N. V. (2019). Digital transformation of education: Challenges and opportunities. Open Education, (4), 4–14. (In Russian)
5. Alaryani, M., et al. (2025). Towards supporting penetration testing education with large language models: An evaluation and comparison. arXiv preprint arXiv:2501.17539.
6. Happe, A., & Cito, J. (2023). Getting pwn'd by AI: Penetration testing with large language models. In Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (pp. 2082–2086).
7. Deng, G., et al. (2023). PentestGPT: An LLM-empowered automatic penetration testing tool. arXiv preprint arXiv:2308.06782.
8. Xu, Z., et al. (2024). AutoAttacker: A large language model guided system to implement automatic cyber-attacks. arXiv preprint arXiv:2403.01038.
9. Fang, R., et al. (2024). LLM agents can autonomously exploit one-day vulnerabilities. arXiv preprint arXiv:2404.08144.
10. Shao, R., et al. (2023). Empirical analysis of large language models in automated vulnerability discovery. arXiv preprint arXiv:2312.02337.
11. Bhatt, M., et al. (2023). Purple Llama CyberSecEval: A secure coding benchmark for language models. arXiv preprint arXiv:2312.04724.
12. Wan, Y., et al. (2024). Cybersecurity issues and challenges: In brief. IEEE Access, 12, 1–15.
13. Moskal, S., et al. (2023). LLM in the shell: Generative AI-powered pentesting. arXiv preprint arXiv:2312.09552.
14. Charan, P. V. S., et al. (2023). From text to MITRE techniques: Examining the layered approach to explainability with a large language model (LLM). arXiv preprint arXiv:2308.09197.
15. Tihanyi, N., et al. (2024). CyberMetric: A benchmark dataset for evaluating large language models knowledge in cybersecurity. arXiv preprint arXiv:2402.07688.
16. Peng, B., et al. (2024). PenHeal: A two-stage LLM framework for automated pentesting and optimal remediation. arXiv preprint arXiv:2407.17788.
17. Wan, Y., et al. (2023). HackMentor: Fine-tuning large language models for cybersecurity. arXiv preprint arXiv:2312.01234.
18. Yang, J., et al. (2023). SWE-bench: Can language models resolve real-world GitHub issues? arXiv preprint arXiv:2310.06770.
19. Kraevskiy, V. V. (2006). Methodology of pedagogy: A new stage. Akademiya. (In Russian)
20. Batyshev, S. Ya. (2010). Professional pedagogy (S. Ya. Batyshev & A. M. Novikov, Eds.; 3rd ed.). EGVES. (In Russian)
21. Verbitskiy, A. A. (1991). Active learning in higher education: A contextual approach. Vysshaya Shkola. (In Russian)
22. Slastenin, V. A. (2002). Pedagogy. Akademiya. (In Russian)
23. Zeer, E. F. (2009). Psychology of professional education. Akademiya. (In Russian)
24. Alias Robotics. (2025). Cybersecurity AI (CAI): An open, bug bounty-ready agentic framework. arXiv preprint arXiv:2504.06017.

Информация об авторе

Греков Владимир Сергеевич — аспирант 1 курса кафедры безопасности информационных технологий РГУ нефти и газа (НИУ) имени И.М. Губкина. Область научных интересов: применение методов искусственного интеллекта в задачах кибербезопасности, автоматизация тестирования на проникновение, большие языковые модели. E-mail: grekov.v@gubkin.ru

LARGE LANGUAGE MODELS IN PENETRATION TESTING AUTOMATION: CURRENT STATE, LIMITATIONS AND PROSPECTS FOR APPLICATION IN PROFESSIONAL TRAINING OF INFORMATION SECURITY SPECIALISTS

Grekov V. S.[1]

[1]National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. *The article analyzes the current state of research on the application of large language models (LLMs) for penetration testing automation. The reasons for the rapid growth of interest in this area are examined, driven by the increasing complexity of IT infrastructures, the high cost of traditional security audit methods, and the development of the DevSecOps concept. Based on the systematization of review and applied research from 2023–2025, four key areas of LLM application in cybersecurity are identified: decision support and strategic attack planning, automation of penetration testing stages, security of language models themselves (AI Red Teaming), and intelligent source code analysis. A critical analysis is conducted of multi-agent system architectures using Retrieval-Augmented Generation (RAG) approaches, testing and evaluation systems, and commercial solutions. It is established that even the most advanced LLM-based penetration testing systems operate at intermediate autonomy levels (3–4 out of 5), unable to independently formulate goals and evaluate the consequences of their decisions. The thesis is substantiated that as of the end of 2025, LLMs serve primarily as an analyst tool rather than an autonomous penetration tester. The pedagogical aspects of integrating LLM tools into professional training of information security specialists are examined, and the necessity of developing critical thinking among students regarding the capabilities and limitations of these technologies is justified.*

Keywords: *large language models, penetration testing, cybersecurity, automation, multi-agent systems, RAG, professional training.*

Information about the author

Grekov Vladimir Sergeevich — 1st year postgraduate student, Department of Information Technology Security, Gubkin Russian State University of Oil and Gas (National Research University). Research interests: application of artificial intelligence methods in cybersecurity, penetration testing automation, large language models. E-mail: grekov.v@gubkin.ru

А. Г. Уймин[1], В. С. Греков[1]

[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, Российская Федерация

ОПЫТ ПРЕПОДАВАНИЯ ПРОДУКТОВЫХ КУРСОВ SIEM И NAD В ЛОГИКЕ ИНТЕГРИРОВАННОЙ ПРОФОРИЕНТАЦИИ: ОТ ПЕРВОГО КУРСА СПЕЦИАЛИТЕТА К СЕРТИФИКАЦИИ ВЫПУСКНИКОВ УКРУПНЁННОЙ ГРУППЫ 10.00.00

Аннотация. В статье представлен опыт реализации продуктовых курсов вендора Positive Technologies — PT-SIEM-CS (Certified Specialist по MaxPatrol SIEM) и PT-NAD-CS (Certified Specialist по PT Network Attack Discovery) — в образовательной траектории высшего образования, охватывающей два сечения подготовки: первый курс специалитета по направлениям укрупнённой группы 10.00.00 «Информационная безопасность» в рамках профильного (специального) предмета и старшие курсы (4–5) того же специалитета в рамках дисциплин «Безопасность сетей ЭВМ» и «Безопасность информационно-аналитических систем». Раскрыта педагогическая логика выведения студентов первого курса специалитета на независимую вендорскую сертификацию: эта практика рассмотрена как элемент интегрированной профориентации, обеспечивающий ранний и предметно-укоренённый контакт обучающегося с реальной профессиональной деятельностью, формирование мотивационно-ценностного и когнитивного компонентов профессиональной компетенции и закрепление выбора профессии через успех в нормативно признанной процедуре оценки. Подробно описаны педагогические технологии профориентации, использованные в учебном процессе: профессиональные пробы, контекстное обучение, кейс-метод, проектная технология, технология учебной симуляции на промышленном полигоне, технология наставничества, портфолио-технология и технология рефлексивной фиксации. Описаны содержательные и процессуальные условия реализации: интеграция вендорских материалов портала Positive Technologies, открытых данных Palo Alto, ресурса malware-traffic-analysis.net, вендоронезависимых фреймворков Sigma и Suricata, развёртывание лабораторной инфраструктуры на базе Яндекс Облака. Приведены количественные результаты: для блока SIEM из 14 студентов курс успешно завершили 11, для блока NAD все 29 студентов, приступивших к работе, успешно прошли курс и сертификацию с прокторингом. Показано, что интегрированная профориентация, опирающаяся на ранний выход на сертификацию, согласуется с положениями отечественной школы профессиональной педагогики (С. Я. Батышев, А. М. Новиков, В. С. Леднев, Т. Ю. Ломакина, А. А. Вербицкий, Е. А. Климов, Э. Ф. Зеер) и поддерживается современными зарубежными исследованиями.

Ключевые слова: профессиональная компетенция, высшее образование, информационная безопасность, профориентация, сертификация, контекстное обучение, SIEM/NAD.

Введение

Подготовка специалистов в области информационной безопасности относится к числу образовательных направлений, где разрыв между темпом развития профессиональной сферы и темпом обновления нормативно закреплённого содержания обучения проявляется особенно остро. Образовательные организации высшего образования сталкиваются с противоречием: ФГОС высшего образования по направлениям укрупнённой группы 10.00.00 «Информационная безопасность» формулируют требования к результатам подготовки на уровне видов профессиональной деятельности и универсальных, общепрофессиональных и профессиональных компетенций, тогда как реальная практика работодателей и профессиональные стандарты в области информационной безопасности предъявляют к выпускнику конкретные трудовые функции, соотносимые с владением промышленными платформами класса SIEM (Security Information and Event Management) и NTA/NDR (Network Traffic Analysis / Network Detection and Response). Между этими двумя нормативно-деятельностными плоскостями располагается зона, в которой образовательная организация обязана самостоятельно выстраивать содержание, средства и процессуальную развёртку подготовки.

Одним из инструментов снятия указанного противоречия является интеграция вендорских продуктовых курсов в учебный процесс с выходом обучающегося на независимую сертификацию. Подобная практика реализуется авторами на двух сечениях образовательной траектории высшего образования: на первом курсе специалитета по направлениям укрупнённой группы 10.00.00 в рамках профильного (специального) предмета и на старших курсах (4–5) того же специалитета в рамках дисциплин «Безопасность сетей ЭВМ» и «Безопасность информационно-аналитических систем». Цель настоящей статьи — обобщить опыт преподавания продуктовых курсов PT-SIEM-CS и PT-NAD-CS, теоретически обосновать раннее (первый

курс специалитета) выведение обучающегося на сертификационную процедуру как элемент интегрированной профориентации, развёрнуто описать педагогические технологии, обеспечивающие эту профориентацию, и сформулировать рекомендации по тиражированию практики.

Актуальность исследования определяется тем, что современная политика подготовки кадров для отраслей цифровой экономики прямо ориентирует образовательные организации высшего образования на сокращение «эффективного срока» вхождения выпускника в профессию, на сближение образовательной и производственной сред, на интеграцию работодателя в проектирование результатов и средств подготовки. В этой логике ранний выход обучающегося на нормативно признанную сертификацию у вендора-работодателя становится не периферийным «бонусом», а ядерным педагогическим средством, обеспечивающим связь между мотивационно-ценностным становлением обучающегося, нормативной картиной квалификаций и реальной профессиональной деятельностью. Особое значение этот тезис приобретает на фоне формирующегося в зарубежной литературе тренда на структурированные точки входа в профессию кибербезопасности через картографирование сертификаций, ролей и компетенций [12], а также на фоне исследований, фиксирующих устойчивую недостаточность кадрового предложения в кибербезопасности и необходимость более ранних и более структурированных карьерных интервенций в системе профессионального образования [13; 14].

В дополнение к этому, в современной образовательной литературе подчёркивается роль профессиональной идентичности обучающегося как ключевого фактора качества подготовки в условиях цифровизации и платформизации учебного процесса [15]. Это означает, что включение продуктового вендорского курса в первый год обучения должно рассматриваться не только как технологическая, но и как идентификационная процедура: обучающийся через работу с реальным промышленным продуктом отвечает себе на вопрос «кем я становлюсь», а не только «что я умею».

Материалы и методы

Исследование выполнено в логике опытно-педагогической работы с элементами педагогического проектирования и обобщения опыта. В работе использованы: анализ нормативной базы (ФГОС ВО по направлениям УГСН 10.00.00); содержательный анализ профессионально-педагогической литературы по проблемам компетентностной подготовки и профессиональной ориентации; анализ зарубежных исследований по проблемам киберобразования, лабораторной подготовки и карьерного консультирования в системе профессионального образования; метод педагогического наблюдения; анализ результатов внешней (вендорской) сертификации обучающихся; обобщение собственного педагогического опыта авторов в части преподавания дисциплин информационной безопасности на двух сечениях траектории высшего образования.

Базой исследования выступили обучающиеся ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», осваивающие программы специалитета по направлениям укрупнённой группы 10.00.00. Учебная нагрузка по продуктовым курсам распределена следующим образом: PT NAD — лабораторные работы 34 часа, семинары 16 часов, лекции 16 часов; MaxPatrol SIEM — лабораторные работы 34 часа, семинары 16 часов, лекции 16 часов. Лабораторная инфраструктура развёрнута на базе сервиса Яндекс Облако в рамках пилотного взаимодействия с вузами; ресурсное обеспечение каждого учебного стенда приведено в таблице 1.

Таблица 1 – Ресурсное обеспечение учебных стендов

Ресурс	ВМ, шт	vCPU, шт	RAM, Гб	HDD, Гб
SIEM	12	12	64	256
АРМ	2	2	4	64
NAD	1	24	72	192

При построении лабораторных работ использовалась технологическая логика обработки трафика в PT NAD: от захвата копии сетевого трафика до обогащения метаданных и работы оператора с ними через интерфейс продукта (рис. 1). Такая схема задавала структуру учебных кейсов и позволяла студентам связывать отдельные операции в единую цепочку расследования инцидента.

Рис. 1. Технологическая схема обработки сетевого трафика в PT NAD (по материалам [34])

Эмпирическую базу составили данные двух учебных циклов: цикла по блоку SIEM (контингент — студенты 5 курса специалитета по направлению «Информационно-аналитические системы безопасности», в рамках дисциплины «Безопасность информационно-аналитических систем», N = 14) и цикла по блоку NAD (контингент — студенты 4 курса специалитета по направлению «Информационная безопасность автоматизированных систем критически важных объектов», в рамках дисциплины «Безопасность сетей ЭВМ», N = 29). Дополнительно использованы данные о выведении на сертификацию обучающихся первого курса специалитета по направлениям УГСН 10.00.00 в рамках профильного предмета.

Теоретико-методологической рамкой обоснования предлагаемой практики выступают положения отечественной школы профессиональной педагогики (С. Я. Батышев, А. М. Новиков, В. С. Леднев, Т. Ю. Ломакина), теории контекстного обучения А. А. Вербицкого, а также классические работы по теории профессиональной ориентации и профессионального становления личности (Е. А. Климов, Э. Ф. Зеер, Н. С. Пряжников, С. Н. Чистякова). На этой рамке выстраивается понимание профессиональной компетенции как интегративного образования, включающего знания, умения, навыки, практический опыт и профессионально значимые личностные качества, и понимание профессиональной ориентации не как разового мероприятия, а как непрерывного, встроенного в основной учебный процесс педагогического сопровождения профессионального самоопределения обучающегося.

Зарубежная рамка исследования опирается на работы, фиксирующие необходимость практико-ориентированного и лабораторно-укоренённого формата киберподготовки [1; 4; 5], значимость явного картирования карьерных траекторий в кибербезопасности, сертификационных шкал как точек входа в профессию и согласования содержания подготовки с отраслевыми профилями [12–14], а также на исследования профессиональной идентичности обучающихся, в которых показано, что устойчивая профессиональная идентичность формируется через включение в подлинную профессиональную практику, а не через её имитации [15; 16].

Теоретическое обоснование

В центре предлагаемой модели — тезис о том, что выведение обучающегося первого курса специалитета на независимую вендорскую сертификацию в рамках профильного предмета является не «опережающим обучением» в его узко-академическом значении, а элементом интегрированной профориентации. Под интегрированной профориентацией в настоящей работе понимается такая организация образовательного процесса, при которой профориентационные задачи решаются не вне учебных дисциплин (через тестирования, экскурсии, агитационные мероприятия), а внутри них — через содержание, средства и процессуальную развёртку самой профессиональной подготовки. При этом сертификация трактуется как педагогическая

проба профессиональной деятельности — оформленное в нормативной процедуре столкновение обучающегося с предметом и инструментами будущей профессии.

Такое понимание опирается на ряд принципиальных положений отечественной педагогики.

Во-первых, на положение А. М. Новикова о принципе учения как осознанной деятельности: «Принцип учения как осознанной деятельности — это осознанность учеником, студентом всех компонентов учебной деятельности: осознание её предмета, средств, способов, своих действий, своих личностных качеств, проявляющихся в учебной деятельности, осознание своей роли в коллективной учебной деятельности». В ситуации, когда обучающийся первого курса с первых месяцев работает с реальной промышленной системой SIEM или NAD, разворачивает её, конфигурирует сбор событий и проходит сертификационное тестирование с прокторингом, перечисленные А. М. Новиковым компоненты учебной деятельности перестают быть абстрактной перспективой и оформляются в наблюдаемой профессиональной пробе. Учебная деятельность приобретает «второй слой» — она одновременно является деятельностью учебной и квазипрофессиональной.

Во-вторых, на ключевое для школы С. Я. Батышева положение о соединении обучения с производительным трудом. С. Я. Батышев писал: «Подготовка квалифицированных рабочих немыслима без соединения обучения с производительным трудом, без активного участия учащихся в создании материальных ценностей в процессе обучения». В подготовке специалистов информационной безопасности в высшей школе функционально-эквивалентным «производительному труду» оказывается работа обучающегося с промышленным программным обеспечением вендора в рамках лабораторного полигона: студент производит не «материальный продукт» в индустриальном смысле, а реальный результат профессиональной деятельности аналитика — правило корреляции, отчёт об инциденте, заключение о вредоносном трафике. Сертификация фиксирует факт такой работы в нормативно признанной форме. Этот же тезис в современной транскрипции подтверждается зарубежными исследованиями практической лабораторной подготовки в кибербезопасности, где показано, что наиболее устойчивые компетенции формируются не на лекционных занятиях, а в условиях работы с реальными сценариями атак и защиты [4; 5].

В-третьих, на положение В. С. Леднева о структуре содержания образования и о необходимости включения в содержание образовательного процесса всех существенных видов деятельности, типичных для соответствующей области профессиональной практики. Согласно В. С. Ледневу, содержание образования включает не только систему знаний, но и опыт осуществления способов деятельности, опыт творческой деятельности и опыт эмоционально-ценностного отношения к действительности. Сертификационный экзамен с прокторингом задействует все четыре компонента: знаниевый (теоретическая часть), деятельностный (практическая часть), творческий (нестандартные кейсы, отклонения от типового сценария) и эмоционально-ценностный (стрессовое испытание, требующее принятия профессиональной ответственности за результат).

В-четвёртых, на положение Т. Ю. Ломакиной о непрерывности профессионального образования. Т. Ю. Ломакина определяет непрерывное профессиональное образование как «процесс целостный, состоящий из последовательно следующих друг за другом и преемственно связанных ступеней специально организованной учёбы». Раннее выведение студентов первого курса специалитета на ту же сертификацию, на которую выходят студенты 4–5 курсов, и есть способ обеспечить продольную связность образовательной траектории внутри высшего образования: одна и та же нормативная точка фиксируется в двух разных пунктах траектории, что превращает её из локального события в опору профессионального становления.

В-пятых, на положения теории контекстного обучения А. А. Вербицкого. А. А. Вербицкий определяет контекстное обучение следующим образом: «Контекстным является такое обучение, в котором с помощью всей системы дидактических форм, методов и средств моделируется предметное и социальное содержание будущей профессиональной деятельности специалиста, а усвоение им абстрактных знаний как знаковых систем наложено на канву этой

деятельности». Лабораторный полигон SIEM/NAD на промышленном вендорском продукте — практически образцовая иллюстрация контекстного обучения: в нём моделируются и предметное содержание (реальная инфраструктура, реальные события, реальные атаки), и социальное содержание (роль аналитика, регламент работы дежурной смены, регламент эскалации инцидента, нормативная процедура сертификации). На первом курсе специалитета такое контекстное обучение играет роль «педагогической точки входа» в профессию.

В-шестых, на положения теории профессионального самоопределения. Е. А. Климов подчёркивает, что профессиональное самоопределение представляет собой длительный процесс согласования личностных потребностей обучающегося с требованиями избранной профессиональной деятельности и осуществляется через систему профессиональных проб. В этой логике сертификационный экзамен у вендора — практически идеальная профессиональная проба: процедура нормативна, оценка независима, результат значим за пределами учебного заведения, кейс соответствует реальной профессиональной задаче. Э. Ф. Зеер развивает этот тезис в логике профессионального становления: «Профессиональное становление — это формообразование личности, адекватное требованиям профессиональной деятельности». Иначе говоря, профессиональное становление невозможно без столкновения с самой профессиональной деятельностью, и чем раньше такое столкновение оформляется в педагогически организованной и социально признанной форме, тем устойчивее результат. С. Н. Чистякова, развивая теорию профессиональных проб в отечественной педагогике, прямо указывает: «Профессиональная проба — это профессиональное испытание, моделирующее элементы конкретного вида профессиональной деятельности, имеющее завершённый вид, способствующее сознательному, обоснованному выбору профессии». Сертификация по продукту, признанная вендором, отвечает всем перечисленным признакам.

Наконец, важно специально остановиться на сопоставлении профессиональной ориентации в её традиционном и интегрированном понимании. Н. С. Пряжников указывает, что профориентация представляет собой «систему мер, направленных на оказание помощи человеку в выборе профессии в соответствии с его способностями, склонностями и потребностями рынка труда». В традиционной практике эти меры реализуются как набор разрозненных мероприятий, организационно отделённых от учебного процесса (профориентационные тестирования, экскурсии, дни открытых дверей, встречи со специалистами). Интегрированная профориентация, в отличие от традиционной, размещает соответствующие меры внутри учебных дисциплин и пользуется их собственным дидактическим аппаратом. На первом курсе высшей школы, где обучающийся ещё проходит этап адаптации к выбранной специальности и часто колеблется в обоснованности своего выбора, такая интеграция оказывается особенно эффективной. Эта позиция согласуется с международными исследованиями карьерного консультирования, показывающими, что наиболее результативные карьерные интервенции — это те, которые интегрированы в основное содержание профессиональной подготовки [7; 10].

Педагогические технологии профориентации, применяемые в продуктовом курсе на первом курсе специалитета

Поскольку основная новизна описываемой практики состоит не в самом факте сертификации, а в способе её педагогической включённости в учебный процесс первого курса, центральным узлом статьи является развёрнутое описание используемых педагогических технологий профориентации. Технологии описаны в той последовательности, в которой они разворачиваются в учебном цикле.

1. Технология профессиональной пробы. Базовая, замыкающая технология всего курса. Понятие профессиональной пробы введено в отечественную педагогику С. Н. Чистяковой как испытание, моделирующее элементы конкретной профессиональной деятельности и завершающееся продуктом, который можно вынести и обсудить. В описываемом курсе пробы строятся по трёхтактному циклу: проба «по образцу» (студент повторяет действия преподавателя на учебном стенде), проба «по аналогии» (студент решает задачу из другого, но методически родственного сценария), проба «творческая» (студент действует в условиях изменённого/неполного входа). Финальной профессиональной пробой выступает сам сертификационный

экзамен с прокторингом: для первого курса это первое в их жизни профессиональное испытание, признанное за пределами образовательной организации.

2. Технология контекстного обучения по А. А. Вербицкому. На занятиях моделируется не учебная, а квазипрофессиональная ситуация: первокурсник работает не «над лабораторной работой», а в роли «младшего аналитика SOC», получает не «задание», а «инцидент с тикетом», оформляет не «отчёт по лабораторной», а «карточку инцидента». На лекциях вводятся понятия и нормативные рамки, но они немедленно «опрокидываются» в практику — в учебно-профессиональную задачу, выполняемую на промышленном полигоне. По А. А. Вербицкому, такая дидактическая конструкция обеспечивает переход от учебной деятельности академического типа к квазипрофессиональной и далее — к собственно профессиональной деятельности.

3. Кейс-метод (case study). Каждая лабораторная работа собрана как кейс — нарратив, описывающий конкретный инцидент или конкретное состояние инфраструктуры (с источником данных, со временем, с контекстом). Студент первого курса не «изучает интерфейс», а расследует инцидент. Кейсы построены на трёх типах источников: тренировочные кейсы вендора (Positive Technologies), открытые исследования Palo Alto Networks (отчёты об APT-кампаниях), публичные дампы malware-traffic-analysis.net. Кейс-метод в применении к продуктовому курсу решает важную профориентационную задачу: с первых занятий студент видит свою профессию «изнутри», как последовательность сделанных аналитиком решений, а не как набор книжных глав.

4. Проектная технология. Поверх кейсов разворачивается мини-проект: студент (или малая группа) принимает «инфраструктуру условного заказчика», ставит SIEM/NAD, обосновывает выбор источников, формирует базовый набор правил корреляции, готовит итоговый отчёт. Проект — это интегральный продукт курса, в котором сходятся знания, умения и навыки. Сертификация в конце цикла валидирует индивидуальный уровень обучающегося, а проект — его способность складывать частные действия в целое решение.

5. Технология учебной симуляции на промышленном полигоне. Существенный элемент дидактической архитектуры — отказ от «учебных аналогов» в пользу промышленного ПО, развёрнутого в облачной среде. Студент первого курса работает не с упрощённой моделью, а с тем же продуктом, который установлен в коммерческих SOC. Симуляция при этом сохраняется на уровне инфраструктуры (учебный сегмент, генератор событий, контролируемые цели), но не на уровне инструмента. Эта технология решает профориентационную задачу: исключает у обучающегося иллюзию «учебности» и переносит его в реальную предметную область с первых занятий.

6. Технология наставничества и сопровождения (mentoring). Курс ведут преподаватели, имеющие действующий или недавний опыт работы в индустрии. Их роль в первом курсе — не столько «лектор», сколько наставник, демонстрирующий профессию через собственное профессиональное поведение: как читает события, как ставит гипотезу, как сомневается, как ищет источник, как фиксирует вывод. Эта технология опирается на положение А. М. Новикова о роли личностного образца в профессиональном становлении и на международные исследования наставничества в киберобразовании, фиксирующие наставничество как один из ключевых факторов закрепления студента в профессии [5].

7. Портфолио-технология. Каждый студент с первого курса ведёт профессиональное портфолио, в которое последовательно собираются: сданные кейсы, выполненный проект, сертификат вендора, рефлексивные записи по итогам каждого блока. Портфолио формируется не как «бюрократический архив», а как «доказательная история профессионального становления»: в конце первого курса студент имеет внешне валидируемое подтверждение своего входа в профессию. Эта технология напрямую решает мотивационно-ценностную задачу профориентации.

8. Технология рефлексивной фиксации. По завершении каждого крупного блока обучающемуся предлагается короткая рефлексивная процедура: «что я сейчас узнал о профессии, что я узнал о себе как о будущем профессионале, какие сомнения у меня возникли, какой

следующий шаг». Рефлексия проводится не в форме «эссе ради эссе», а как педагогический инструмент управления профессиональным самоопределением. С позиции Э. Ф. Зеера рефлексия — необходимый компонент профессионального становления; без неё профессиональная проба теряет свой ориентационный смысл.

9. Технология ранней погружённой стажировки (соглашения с индустрией). В рамках курса первого года предусмотрены договорные встречи с действующими аналитиками SOC, разбор реальных (анонимизированных) инцидентов из практики работодателей, посещение площадок индустриальных партнёров. Эта технология достраивает контекстное обучение «снаружи»: студент первого курса встречает не только своего преподавателя, но и взрослого профессионала «в роли», что усиливает профессиональную идентификацию.

10. Технология независимой сертификации как венца цикла. Сертификация PT-NAD-CS / PT-SIEM-CS в конце цикла собирает все предыдущие технологии в один нормативный результат. Это не «контрольная работа», а первое профессиональное испытание обучающегося. Именно соединение перечисленных технологий с этим венцом и составляет содержание термина «интегрированная профориентация» в авторской трактовке.

Все десять технологий применяются не последовательно, а параллельно: курс собран как сеть технологий, каждая из которых вытягивает свою грань профессионального становления — мотивационную, когнитивную, деятельностную, рефлексивную и идентификационную.

Содержание и реализация продуктовых курсов

Содержательное ядро обоих продуктовых курсов сформировано на основе материалов портала обучения Positive Technologies. Курс по MaxPatrol SIEM раскрывает архитектуру современной SIEM-системы, управление активами и уязвимостями, управление журналами (сбор событий из источников, таксономия событий, потоки данных), работу с базой событий, создание дашбордов и отчётов, управление инцидентами и уведомлениями, мониторинг источников. Курс по PT Network Attack Discovery раскрывает технологии сетевой разведки и первоначального доступа, методы выполнения и закрепления в системе, повышения привилегий, предотвращения обнаружения, получения учётных данных, перемещения внутри периметра, эксфильтрации данных. Содержание курсов спроектировано в логике матрицы MITRE ATT&CK, что обеспечивает педагогическую прозрачность связки «учебная задача — реальный тактико-технический приём злоумышленника — средство обнаружения». Использование MITRE ATT&CK как педагогической метаструктуры согласуется с современными исследованиями применения этого фреймворка для смягчения киберугроз и систематизации учебных программ [3].

Для лабораторных работ по NAD дополнительно используются материалы открытых исследований Palo Alto Networks и публичный набор сетевых дампов с сайта malware-traffic-analysis.net. Это позволило сформировать учебно-профессиональные задачи на анализе реальных индикаторов компрометации, выявлении вредоносного трафика и расследовании инцидентов информационной безопасности с использованием языка Suricata. Такой подход соответствует современным методикам анализа сетевого трафика, основанным на обнаружении вторжений и тонкой обработке признаков [2]. Для лабораторных работ по SIEM в перспективе планируется внедрение вендоронезависимого фреймворка Sigma для написания правил корреляции и использование событий, предоставленных сообществом Security Experts Community (репозиторий open-xp-rules). Сочетание вендорских и открытых средств обеспечивает выполнение требования вариативности средств обучения и не привязывает результат подготовки к конкретному поставщику. Это особенно важно в свете последних работ по масштабированию SIEM-корреляции и снижению среднего времени реакции на инцидент в условиях городских и инфраструктурных систем [6].

Процессуально курс построен в трёхчастной структуре: лекционный блок (16 часов) — семинарский блок (16 часов) — лабораторный блок (34 часа). Лекции вводят понятийный аппарат и нормативно-методические рамки. Семинары обеспечивают переход от теории к инструментарию: разбираются стек протоколов TCP/IP, принципы работы сетевых сканеров (nmap), сканеры безопасности ОС, базовые навыки работы с операционными системами

Windows и Linux на уровне администратора, редактирование конфигурационных файлов и перезапуск служб в Linux, написание регулярных выражений, повышение привилегий в UNIX (sudo/su), настройка syslog. Лабораторные работы организованы вокруг типовых трудовых функций — установка продукта и его архитектура, управление активами и уязвимостями средствами MaxPatrol SIEM, управление журналами, работа с базой событий, база знаний и работа с ложными срабатываниями, создание отчётов, управление инцидентами и уведомлениями, решение проблем и мониторинг источников, сбор журналов и импорт/экспорт активов и событий. Для блока NAD аналогичные лабораторные работы покрывают весь цикл атаки: начальная настройка NAD (базовые и расширенные технологии), контроль попыток первоначального доступа, детектирование повышения привилегий, детектирование использования техник закрепления, детектирование исследования системы, детектирование сканирования сети, детектирование перемещения внутри периметра, инструменты эксфильтрации данных и PT NAD.

Начальный блок лабораторных работ по NAD был связан с установкой и настройкой продукта, включая выбор сетевых интерфейсов для захвата копии сетевого трафика (рис. 2). Такой материал позволял студентам увидеть, что аналитическая работа в NTA/NDR-системе начинается не с интерфейса расследования, а с корректного получения и подготовки сетевых данных.

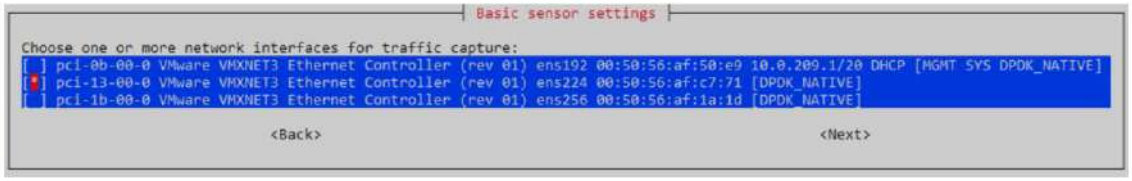

Рис. 2. Выбор интерфейсов для захвата трафика при настройке PT NAD (по материалам [36])

Основной акцент в обучении сделан на подготовке аналитика, а не администратора. Студенты изучают основы установки и настройки систем, однако более глубокий акцент сделан на анализе данных и работе с событиями. Такой подход обусловлен тем, что понимание базовых принципов установки системы является необходимым, но не достаточным условием эффективного анализа и расследования инцидентов; продуктивная деятельность аналитика опирается прежде всего на способность интерпретировать совокупность событий в контексте модели угроз. Современные исследования киберобразования подтверждают этот выбор: устойчивые навыки формируются именно через работу с реальными или приближёнными к реальным наборами данных и сценариев [4; 5].

Сопоставление учебных действий с разделами продукта и методическими материалами PT NAD представлено в таблице 2. Эта таблица была добавлена в статью как связующее звено между содержанием курса, интерфейсными сценариями и профориентационным результатом обучения.

Таблица 2 – Сопоставление учебных действий с материалами PT NAD

Учебный блок	Разделы PT NAD	Материалы руководств	Профориентационный результат
Начальная настройка и подготовка стенда	Установка продукта, мастер настройки, выбор интерфейсов захвата	Руководство по установке на один сервер: разделы 7-8	Понимание инфраструктурной основы работы аналитика и зависимости качества расследования от корректного захвата трафика
Ориентация в интерфейсе и первичный обзор	Дашборды, диаграмма интенсивности трафика, панель фильтрации	Руководство оператора: разделы 6, 11	Формирование первичного навыка чтения состояния сети и выделения зоны внимания
Анализ сетевых сессий	Список сессий, карточка сессии, экспорт PCAP и метаданных	Руководство оператора: раздел 9	Переход от наблюдения отдельных событий к реконструкции сетевого взаимодействия

Рубрика 3. Методология и технология профессионального образования

Анализ атак	Список атак, карточка атаки, причина срабатывания, ложные срабатывания	Руководство оператора: раздел 10	Освоение логики расследования: от сработавшего правила к выводу о характере инцидента
Работа с активностями, узлами и связями	Лента активностей, узлы, сетевые связи	Руководство оператора: разделы 12, 14, 15	Развитие способности видеть инцидент в контексте инфраструктуры, а не как изолированную запись
Правила, репутационные списки и исключения	Правила для атак и активностей, репутационные списки, исключения	Руководство оператора: раздел 20	Понимание границы между типовым обнаружением, настройкой продукта и аналитическим решением

Для визуализации состояния трафика и первичной ориентации в данных использовались дашборды и виджеты PT NAD (рис. 3). На этом этапе студент учился связывать отдельные числовые показатели, географические распределения и протокольную структуру трафика с возможными гипотезами расследования.

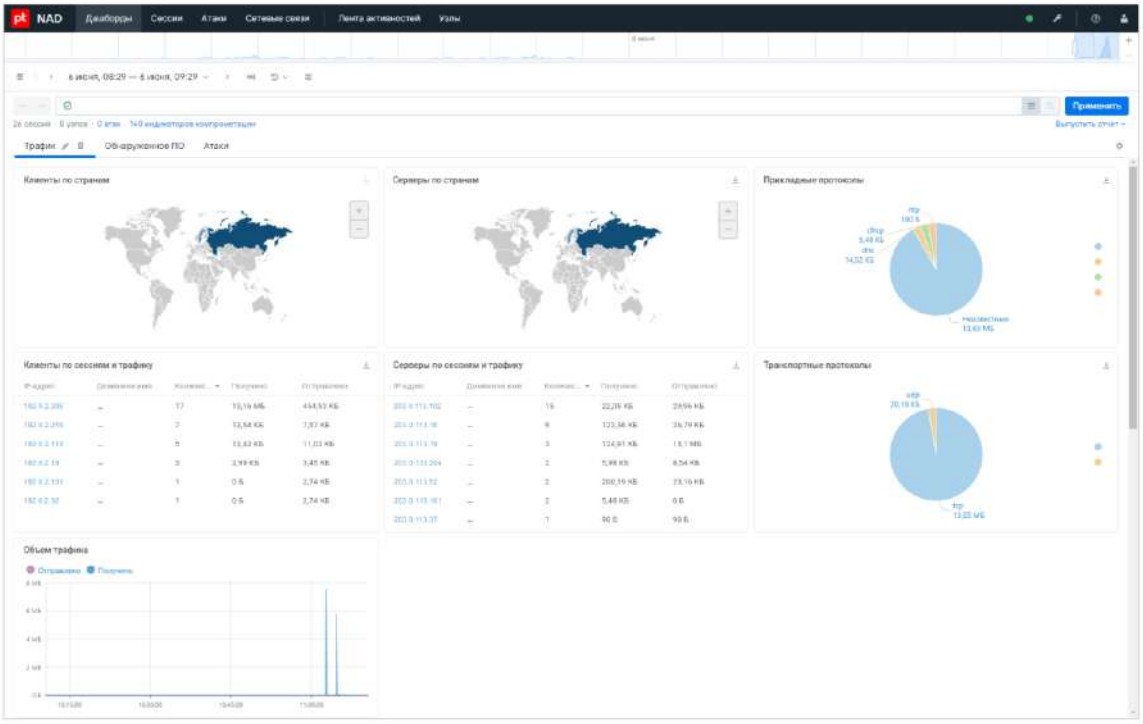

Рис. 3. Дашборд PT NAD для просмотра статистических данных о трафике (по материалам [35])

Переход к расследованию строился от общего списка атак и временной диаграммы срабатываний к карточке конкретной атаки (рис. 4–5). Такая последовательность соответствует логике профессиональной пробы: обучающийся сначала видит общий поток событий, затем выделяет значимое срабатывание и только после этого анализирует правило, сессию, атакующий и атакуемый узлы.

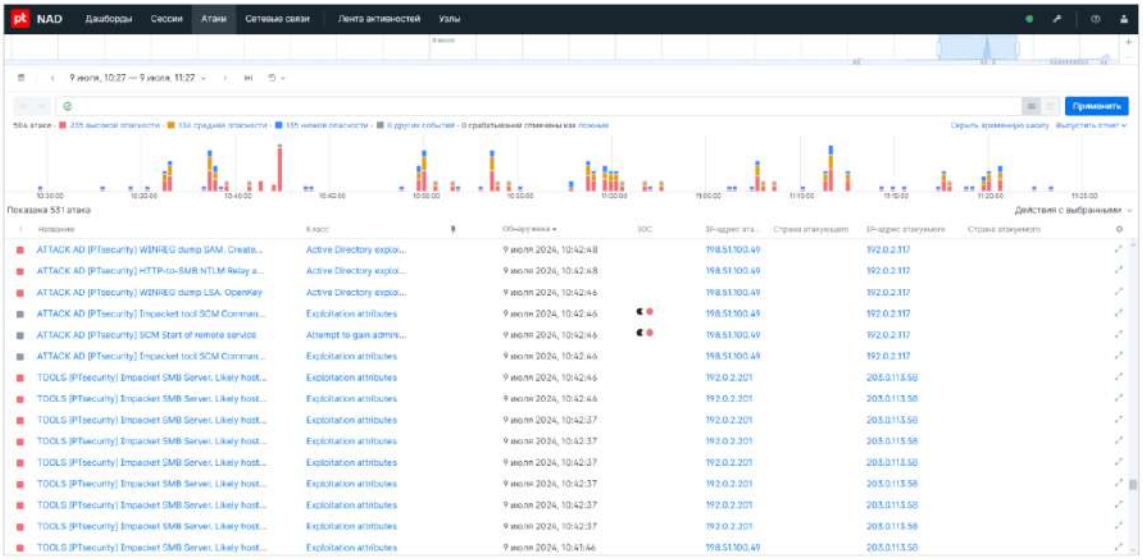

Рис. 4. Список атак и временная диаграмма срабатываний в PT NAD (по материалам [35])

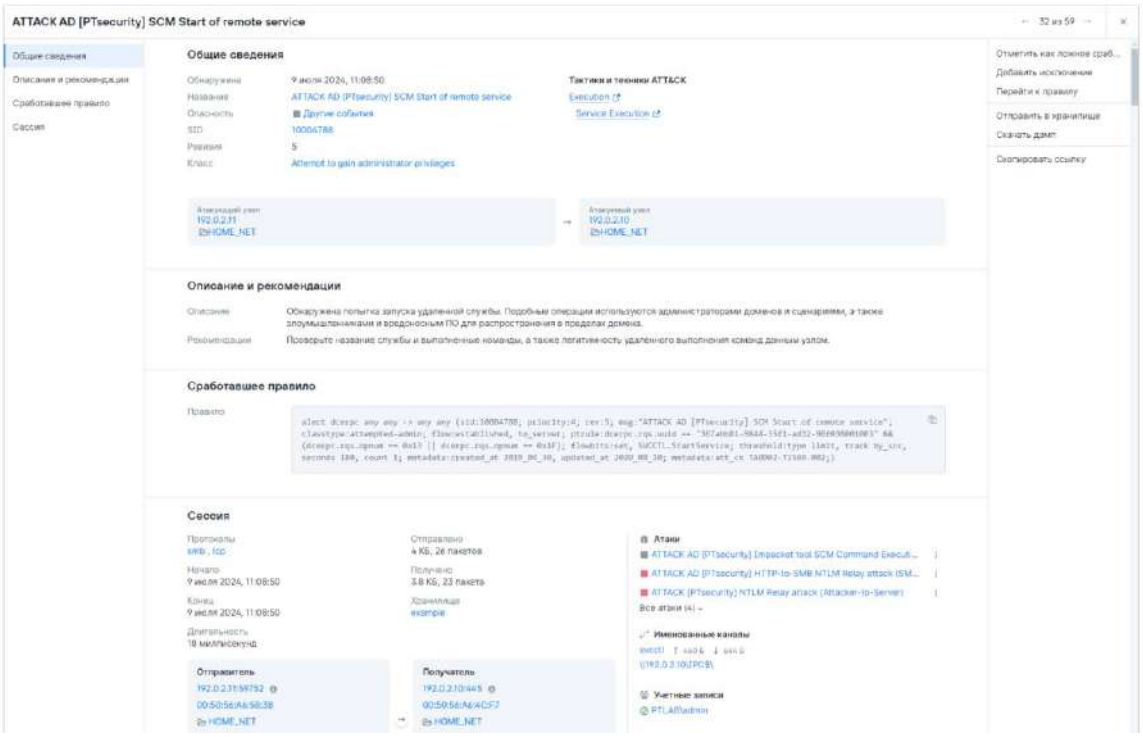

Рис. 5. Карточка атаки в PT NAD как элемент учебного кейса расследования (по материалам [35])

Раннее выведение на сертификацию в первом курсе специалитета как элемент интегрированной профориентации

Принципиальная особенность описываемой практики состоит в том, что аналогичные сертификационные процедуры, к которым приходят студенты 4–5 курсов специалитета по завершении дисциплин «Безопасность сетей ЭВМ» и «Безопасность информационно-аналитических систем», организуются и в рамках профильного предмета первого курса специалитета. Указанное решение вызывает обоснованные вопросы: насколько целесообразно нагружать первокурсника, который только что перешёл со ступени общего образования, нормативно признанной вендорской сертификацией взрослого профессионального уровня? Не противоречит ли это принципу доступности обучения и не оборачивается ли формальным «натаскиванием» на тест?

Развёрнутый ответ на эти вопросы возможен только в логике интегрированной профориентации. Сертификация на первом курсе не подменяет собой обучение и не является самоцелью; она является педагогическим средством решения профориентационной задачи и

одновременно — диагностическим средством оценки начального уровня сформированности компонентов профессиональной компетенции. С позиции отечественной школы профессиональной педагогики такая постановка непротиворечива и обеспечивается следующей системой педагогических аргументов.

1. Снятие «эффекта отложенной профессии». Е. А. Климов прямо отмечал: «Профессиональное самоопределение — это не одномоментный акт выбора, а длительный, многоэтапный процесс выработки человеком собственного отношения к профессионально-трудовой сфере». В традиционной системе высшего образования студент первого курса нередко получает преимущественно общетеоретическое содержание и фактически отложенно сталкивается с профессией только на втором-третьем курсе, при появлении первых профильных дисциплин. Это удлиняет «период неопределённости» и повышает риск отказа от выбранной специальности. Раннее выведение на продуктовый курс и сертификацию решает эту проблему: обучающийся уже в первый учебный год получает опыт профессиональной пробы в её нормативно оформленной версии. Этот вывод корреспондирует с современными исследованиями, фиксирующими, что отсутствие раннего и предметного карьерного сопровождения значимо снижает способность к планированию карьеры и устойчивость карьерного выбора [8; 9].

2. Формирование мотивационно-ценностного компонента компетенции. Согласно А. М. Новикову, мотивация учения существенно усиливается, когда учебная деятельность воспринимается обучающимся как имеющая смысл за пределами самой учебной ситуации: «Мотивация учебной деятельности тесно связана с осознанием её социального и личностного смысла». Сертификат вендора — материальный носитель такого смысла: его можно предъявить за пределами образовательной организации, он значим для работодателя, он связывает учебный успех со взрослым профессиональным статусом. В этом смысле сертификация даёт первокурснику то, чего практически невозможно добиться внутренней зачётно-экзаменационной системой образовательной организации: внешне валидированный знак профессиональной состоятельности.

3. Согласование с принципом природосообразности и принципом ведущей деятельности. Раннее (на первом курсе) включение обучающегося в продуктовую среду промышленного класса согласуется с положением Л. С. Выготского о зоне ближайшего развития: «То, что ребёнок сегодня может сделать в сотрудничестве и под руководством, завтра он становится способен выполнять самостоятельно». Промышленная среда SIEM/NAD на этапе первого курса лежит в зоне ближайшего развития обучающегося только при условии методически выстроенного педагогического сопровождения, которое и обеспечивается аудиторными часами курса, инструкциями лабораторного полигона и фигурой преподавателя-наставника. Сертификация фиксирует переход содержания из зоны ближайшего развития в актуальный уровень развития обучающегося.

4. Продольная связность образовательной траектории. Т. Ю. Ломакина указывает, что «непрерывное профессиональное образование выступает важнейшим условием формирования всесторонне развитой, профессионально мобильной личности». В авторской практике на одну и ту же сертификацию (PT-NAD-CS, PT-SIEM-CS) выходят обучающиеся двух сечений траектории высшего образования: первый курс специалитета и старшие курсы того же специалитета. Этим обеспечивается прямая нормативная связность: студент проходит через одну и ту же шкалу профессиональной оценки на разных этапах своей траектории, что облегчает педагогическое управление его профессиональным развитием. Структурированное картирование сертификаций как точек входа в профессию кибербезопасности рассматривается в современных международных исследованиях как один из основных инструментов снижения дефицита кадров и закрепления молодёжи в профессии [12].

5. Содержательное укрепление профильного предмета. Включение продуктового курса в специальный предмет первого курса переводит этот предмет из разряда «общеподготовительных» в разряд предметов, непосредственно встроенных в профессиональную деятельность. По выражению А. М. Новикова, «учебный предмет в профессиональном образовании имеет смысл лишь постольку, поскольку он работает на профессиональную деятельность

будущего специалиста». Сертификация, привязанная к специальному предмету первого курса, делает эту работу очевидной для обучающегося, его родителей, работодателя и педагогического коллектива.

6. Диагностическая функция. С. Я. Батышев писал: «Контроль и оценка не сводятся к констатации результата, они выступают средством управления процессом подготовки квалифицированного рабочего». Внешняя сертификация даёт педагогу диагностический материал, не зависящий от внутренней зачётно-экзаменационной системы: видно, какие именно содержательные блоки оказались усвоены недостаточно, и видно, какие именно компоненты профессиональной компетенции (знания, умения, навыки, практический опыт, личностные качества) у конкретного обучающегося уже сформированы. Современные исследования цифровой трансформации оценки компетенций показывают, что внешние нормативные процедуры с прокторингом обеспечивают существенно более высокую достоверность диагностического заключения, чем внутренние формы контроля [17].

7. Формирование профессиональной идентичности. Зарубежные исследования профессиональной идентичности обучающихся показывают, что устойчивая профессиональная идентичность не возникает в результате чисто учебных событий; её источником служит включение обучающегося в подлинную профессиональную практику с признанным сообществом профессионалов [15; 16]. Сертификация вендора — это вход в такое сообщество: сертифицированный обучающийся становится частью внешнего профессионального реестра, признанного работодателем, и тем самым обретает основу для устойчивой профессиональной идентификации.

Таким образом, ранний выход обучающегося первого курса специалитета на сертификацию у вендора рассматривается не как опережающее «взрослое» обучение, а как педагогически оправданная профессиональная проба, размещённая внутри специального предмета и решающая одновременно задачи профориентации, мотивации, диагностики, формирования компонентов профессиональной компетенции, обеспечения продольной связности траектории высшего образования и закрепления профессиональной идентичности.

Критерии и уровни сформированности компетенции в условиях ранней сертификации

Поскольку сертификация в авторской практике выполняет двойную функцию (педагогическая проба и диагностический инструмент), необходимо специально оговорить критерии и уровни, по которым оценивается результат подготовки.

В работе используется четырёхкритериальная модель, объединяющая отечественную и зарубежную традиции: мотивационно-ценностный критерий (готовность и желание профессионально действовать в области информационной безопасности, отношение к профессии, устойчивость профессионального выбора); когнитивный критерий (владение понятийным аппаратом, моделью угроз, архитектурой SIEM/NAD, нормативной базой); деятельностный критерий (способность выполнять типовые профессиональные действия — установка и конфигурация продукта, нормализация и обогащение событий, написание правил корреляции, расследование инцидента); рефлексивный критерий (способность анализировать собственные действия, обнаруживать ошибки, корректировать профессиональное поведение в нестандартной ситуации).

Уровни сформированности задаются в трёхкомпонентной шкале «базовый — практический — продвинутый». На базовом уровне обучающийся способен воспроизвести типовые операции с инструкцией; на практическом — выполнить полный учебно-профессиональный сценарий самостоятельно, в том числе в условиях прокторинга; на продвинутом — действовать в нестандартной ситуации (изменённый трафик, отсутствие части данных, противоречивые индикаторы) и предлагать собственное решение.

Сертификация PT-NAD-CS / PT-SIEM-CS относительно этой шкалы фиксирует достижение практического уровня. Продвинутый уровень требует дополнительной работы (стажировки в SOC, участие в Capture the Flag, разработка собственных правил Sigma); базовый уровень обнаруживается у тех обучающихся, кто завершил курс, но не вышел на сертификацию.

Результаты

Внедрение продуктовых курсов SIEM и NAD в учебный процесс продемонстрировало высокую педагогическую результативность.

По блоку SIEM: из 14 студентов, приступивших к курсу, успешно завершили его и прошли сертификацию 11 человек (78,6 %).

По блоку NAD: из 29 студентов, приступивших к курсу, успешно завершили его и прошли сертификацию все 29 (100 %).

Сертификационный экзамен проводился у вендора Positive Technologies в формате тестирования с прокторингом. Независимая оценка, проводимая внешней организацией, подтверждает объективность результатов и квалификацию студентов, успешно сдавших экзамен. Несмотря на стрессовый характер испытания и страх провала, типичный для процедуры с прокторингом, большинство студентов справились с задачей, что свидетельствует о достаточном уровне подготовки. Студенты, успешно сдавшие экзамен, получили не только подтверждение своих профессиональных навыков, но и конкурентное преимущество на рынке труда.

Иллюстративный фрагмент результатов прохождения сертификации представлен на рисунке 6. Для соблюдения требований к защите персональных данных сведения, позволяющие идентифицировать обучающихся и номера сертификатов, в изображении обезличены.

Рис. 6. Примеры сертификатов PT-NAD-CS, полученных по итогам курса (персональные данные обучающихся обезличены)

Помимо достижения основных целей курса, у студентов сформированы навыки работы с реальными промышленными инструментами, что существенно повысило их конкурентоспособность на рынке труда. Внедрение вендоронезависимых фреймворков, таких как Sigma и

Suricata, позволило студентам глубже понять принципы работы с различными SIEM и NTA-системами и снизить зависимость от конкретного поставщика. На уровне первого курса специалитета подтверждено, что выведение обучающихся на сертификацию в рамках профильного предмета не приводит к «вымыванию» мотивации, а напротив, формирует у обучающихся устойчивое профессиональное самоопределение и закрепляет выбор направления УГСН 10.00.00.

Для успешного внедрения курсов была проведена тщательная подготовка, включающая разработку курсов и лабораторных работ, подготовку инфраструктуры и обучение преподавателей (см. Приложение 1). Таймлайн включал следующие ключевые этапы: разработка курсов и лабораторных работ — 2 месяца; подготовка инфраструктуры — 1 месяц; обучение преподавателей и старт курса — 1 месяц; проведение лабораторных работ и итоговая оценка — 2 месяца. В процессе реализации возникли технические сложности, связанные с интеграцией различных инструментов, а также необходимость постоянного обновления учебных материалов в соответствии с актуальной картиной угроз.

Качественные эффекты, отмеченные в ходе наблюдения за первокурсниками, включают: рост вовлечённости в профильный предмет, появление инициативных запросов обучающихся на дополнительные лабораторные работы, формирование «студенческого сообщества» вокруг продуктового курса, рост числа обучающихся, демонстрирующих устойчивое намерение продолжать обучение по выбранному направлению и заниматься профильной научно-исследовательской работой со второго курса.

Обсуждение

Полученные результаты позволяют обсудить четыре принципиальных вопроса.

Первый вопрос — о соотношении вендорской зависимости и содержательной самостоятельности подготовки. Использование исключительно вендорских материалов несёт риск формирования у обучающегося так называемого «продуктового» взгляда на профессию, при котором за конкретным интерфейсом теряются стоящие за ним фундаментальные понятия и принципы. Авторский подход к снятию этого риска состоит в параллельном включении в учебный процесс вендоронезависимых фреймворков (Sigma для правил корреляции, Suricata для сетевого анализа), отраслевой матрицы MITRE ATT&CK как метаструктуры описания тактик и техник, открытых исследовательских материалов Palo Alto Networks и публичных наборов данных malware-traffic-analysis.net. В этой конструкции вендорский курс выступает носителем актуального технологического стандарта, а вендоронезависимые средства — носителем теоретической инвариантной части содержания. Этот баланс согласуется с международной практикой проектирования киберобразовательных программ, где сертификации играют роль «карты местности», а не «единственного маршрута» [12].

Второй вопрос — о применимости описанной практики в системе высшего образования по направлениям УГСН 10.00.00. Современная политика подготовки кадров для отраслей цифровой экономики предполагает усиление связки с работодателем, переход от лекционно-репродуктивной к деятельностной педагогической логике. В этом контексте раннее выведение первокурсника на сертификацию у вендора-работодателя оказывается органичным элементом архитектуры программы специалитета: сертификация фиксирует переход обучающегося в категорию признанного работодателем носителя профессиональных навыков и тем самым выполняет именно ту функцию интеграции с производственной сферой, которая закладывается в современных образовательных программах высшей школы.

Третий вопрос — о месте описанной практики в системе педагогических условий формирования профессиональных компетенций. В терминах школы В. С. Леднева — Т. Ю. Ломакиной выделяются шесть видов педагогических условий: содержательные, процессуальные, организационные, кадровые, нормативно-методические, технологические. Применительно к описанной практике:

– содержательные условия обеспечиваются интеграцией вендорских материалов Positive Technologies, открытых исследований Palo Alto, дампов malware-traffic-analysis.net, вендоронезависимых фреймворков Sigma и Suricata;

– процессуальные условия — последовательной развёрткой «лекция — семинар — лабораторная работа — сертификация», обеспечивающей переход от понятийного к деятельностному уровню освоения, и сетью педагогических технологий профориентации, описанных в отдельном разделе;

– организационные условия — развёртыванием цифровой образовательной среды на базе Яндекс Облака, обеспечением доступа к промышленному ПО и моделированию реальной производственной среды;

– кадровые условия — наличием преподавателей с актуальным опытом работы в области информационной безопасности;

– нормативно-методические условия — соответствием содержания требованиям ФГОС ВО по направлениям УГСН 10.00.00 и согласованием с актуальной картиной профессиональных задач индустрии;

– технологические условия — выбором цифровых инструментов моделирования производственной среды (промышленные SIEM/NAD, виртуальные аналоги оборудования, облачные стенды).

Системность педагогических условий означает, что описанная практика опирается не на единственное «удачное» средство, а на согласованную сеть условий, каждое из которых играет свою роль в формировании профессиональной компетенции.

Четвёртый вопрос — об ограничениях исследования. Объём эмпирической базы (14 студентов в блоке SIEM, 29 в блоке NAD, пилотные группы первого курса) не позволяет сделать строго статистически обоснованные обобщения; данные собраны на одной образовательной организации; долгосрочные эффекты ранней сертификации (закрепление выпускников в профессии, академическая успешность на последующих курсах) пока не прослежены. Эти ограничения определяют направление дальнейшей работы.

Заключение

Опыт реализации продуктовых курсов PT-SIEM-CS и PT-NAD-CS на двух сечениях образовательной траектории высшего образования — первом курсе специалитета и старших курсах того же специалитета по направлениям укрупнённой группы 10.00.00 — позволяет сформулировать следующие выводы.

Во-первых, продуктовые курсы вендора при соответствующем педагогическом сопровождении встраиваются в программу специалитета по направлениям УГСН 10.00.00 и обеспечивают продольную связность результатов подготовки через единую внешнюю сертификационную шкалу.

Во-вторых, раннее (на первом курсе специалитета) выведение обучающегося на сертификацию у вендора педагогически оправдано в логике интегрированной профориентации: оно решает задачи раннего профессионального самоопределения обучающегося, формирования мотивационно-ценностного и когнитивного компонентов профессиональной компетенции, диагностики начального уровня подготовки и закрепления выбора направления, а также формирования профессиональной идентичности обучающегося как члена признанного профессионального сообщества.

В-третьих, интегрированная профориентация в курсе первого года реализуется через сеть взаимосвязанных педагогических технологий: технологию профессиональной пробы, контекстное обучение, кейс-метод, проектную технологию, технологию учебной симуляции на промышленном полигоне, технологию наставничества, портфолио-технологию, технологию рефлексивной фиксации, технологию ранней погружённой стажировки и технологию независимой сертификации как венца цикла.

В-четвёртых, успешность практики обеспечивается комплексом педагогических условий — содержательных, процессуальных, организационных, кадровых, нормативно-методических и технологических, — каждое из которых должно быть спроектировано отдельно и согласовано с остальными.

В-пятых, использование вендоронезависимых средств (Sigma, Suricata, MITRE ATT&CK, открытые исследования и дампы) параллельно с вендорскими курсами обеспечивает теоретическую инвариантность подготовки и снимает риск «продуктовой» зависимости.

Перспективным направлением дальнейшей работы является расширение курсов за счёт новых лабораторных работ, включающих использование дополнительных вендоронезависимых инструментов и фреймворков, а также эмпирическое исследование долгосрочных эффектов ранней сертификации: устойчивости профессионального выбора, академической успешности на последующих курсах и трудоустройства выпускников по профилю подготовки.

Библиографический список

1. Lazarov, W. Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education / W. Lazarov, T. Schafeitel-Tähtinen, J. Squillace [et al.] // Technology, Knowledge and Learning. — 2025. — DOI: 10.1007/s10758-025-09840-y.
2. Ghosh, S. Network traffic analysis based on cybersecurity intrusion detection through an effective statistical features selection and supervised learning classifier / S. Ghosh // Applied Soft Computing. — 2025. — DOI: 10.1016/j.asoc.2024.112603.
3. The Application of MITRE ATT&CK Framework in Mitigating Cybersecurity Threats // Issues in Information Systems. — 2024. — DOI: 10.48009/3_iis_2024_106.
4. Lippi, G. Practical strategies for laboratory cybersecurity / G. Lippi // Ukrainian Journal of Laboratory Medicine. — 2025. — DOI: 10.62151/2786-9288.3.4.2025.11.
5. Dincelli, E. Exploring the Agentic Metaverse's Potential for Transforming Cybersecurity Workforce Development / E. Dincelli, H. Jafarian // MIS Quarterly Executive. — 2025. — DOI: 10.17705/2msqe.00122.
6. Chernikov, P. Cyber defense of urban digital systems: Scaling SIEM correlation to reduce incident response time / P. Chernikov // Cybersecurity: Education, Science, Technique. — 2025. — DOI: 10.28925/2663-4023.2025.31.1066.
7. Zelloth, H. Career guidance for Vocational Education and Training (VET) / H. Zelloth // Journal of the National Institute for Career Education and Counselling. — 2025. — DOI: 10.20856/jnicec.3308.
8. Chang, F. The impact of lack of parental career engagement on the career planning ability of vocational students / F. Chang, P. Wang // International Journal for Educational and Vocational Guidance. — 2025. — DOI: 10.1007/s10775-025-09755-1.
9. Dayag, R. P. Strengthening career readiness through structured career guidance services of graduating students / R. P. Dayag, J. J. Picajas // Global Journal of Guidance and Counselling in Schools. — 2025. — DOI: 10.18844/gjgc.v15i2.9758.
10. Barigye, D. Technical Vocational Education and Training in Uganda: Career guidance and practice / D. Barigye // African Journal of Career Development. — 2024. — DOI: 10.4102/ajcd.v6i1.100.
11. Mathur, A. Navigating the Future: How Career Guidance Programs Prepare Secondary Students for the Future / A. Mathur, A. Mishra // International Journal of Science and Research. — 2024. — DOI: 10.21275/sr241210140511.
12. Kovalev, A. Skill-Driven Certification Pathways: Measuring Industry Training Impact on Graduate Employability / A. Kovalev, N. Stefanac, M.-A. Rizoiu // arXiv. — 2025. — arXiv:2506.04588. — URL: https://arxiv.org/abs/2506.04588.
13. Maennel, K. Human Aspects of Cyber Security for Computing Higher Education: Current Status and Future Directions / K. Maennel, O. Maennel // ACM Transactions on Computing Education. — 2025. — Vol. 25, No. 3. — Art. 27. — P. 1–30. — DOI: 10.1145/3733839.
14. Wang, H. Study on the Types of Career Decision-Making Difficulties of Chinese Higher Vocational College Students and the Influence of Parental Career Intervention Behaviors / H. Wang, L. Chen, S. Xu, X. Gu // Journal of Higher Education Management. — 2025. — Vol. 19, No. 2. — P. 86–100. — DOI: 10.13316/j.cnki.jhem.20250122.008.

Рубрика 3. Методология и технология профессионального образования

15. Kryger, M. Conceptualizing and Developing Vocational Identity: A Scoping Review of Research in Vocational Education and Training / M. Kryger, A. Qvortrup // Vocations and Learning. — 2025. — Vol. 18. — Art. 15. — DOI: 10.1007/s12186-025-09371-8.
16. Bükki, E. Teacher, Professional or Both? A Mixed Method Study of the Professional Identity / E. Bükki, A. Fehérvári // International Journal for Research in Vocational Education and Training. — 2024. — DOI: 10.13152/ijrvet.11.3.4.
17. Kharchenko, O. The digital transformation of competency assessment: Challenges and future of integrity / O. Kharchenko, D. Bondarenko // Cybersecurity: Education, Science, Technique. — 2025. — DOI: 10.28925/2663-4023.2025.30.917.
18. Pleshakova, A. Yu. Defining the concept of identity of national vocational education system / A. Yu. Pleshakova // Professional education in the modern world. — 2024. — DOI: 10.20913/2618-7515-2023-4-8.
19. Smirnov, D. Methodology for Collecting Data on the Activity of Malware for Windows OS / D. Smirnov, O. Evsutin // Informatics and Automation. — 2024. — DOI: 10.15622/ia.23.3.2.
20. Partyka, O. Integrated approach to detecting Bluetooth threats using Wireshark and Splunk SIEM / O. Partyka, B. Fihol, T. Nakonechnyi // Cybersecurity: Education, Science, Technique. — 2024. — DOI: 10.28925/2663-4023.2024.26.684.
21. Pidhornyi, P. Analytical review of models and systems for network traffic classification / P. Pidhornyi // Cybersecurity: Education, Science, Technique. — 2024. — DOI: 10.28925/2663-4023.2024.26.639.
22. Батышев, С. Я. Профессиональная педагогика : учебник для студентов, обучающихся по педагогическим специальностям и направлениям / С. Я. Батышев, А. М. Новиков ; под ред. С. Я. Батышева, А. М. Новикова. — 3-е изд., перераб. — Москва : Из-во ЭГВЕС, 2010. — 456 с.
23. Новиков, А. М. Основания педагогики : пособие для авторов учебников и преподавателей / А. М. Новиков. — Москва : Из-во ЭГВЕС, 2010. — 208 с.
24. Леднев, В. С. Содержание образования: сущность, структура, перспективы / В. С. Леднев. — 2-е изд., перераб. — Москва : Высшая школа, 1991. — 224 с.
25. Ломакина, Т. Ю. Современный принцип развития непрерывного образования / Т. Ю. Ломакина. — Москва : Наука, 2006. — 221 с.
26. Вербицкий, А. А. Активное обучение в высшей школе: контекстный подход / А. А. Вербицкий. — Москва : Высшая школа, 1991. — 207 с.
27. Климов, Е. А. Психология профессионального самоопределения : учебное пособие для студентов высших учебных заведений / Е. А. Климов. — 4-е изд., стер. — Москва : Академия, 2010. — 304 с.
28. Зеер, Э. Ф. Психология профессий : учебное пособие для студентов вузов / Э. Ф. Зеер. — 5-е изд., перераб. и доп. — Москва : Академический Проект; Фонд «Мир», 2008. — 336 с.
29. Пряжников, Н. С. Профессиональное самоопределение: теория и практика : учебное пособие / Н. С. Пряжников. — Москва : Академия, 2008. — 320 с.
30. Чистякова, С. Н. Педагогическое сопровождение самоопределения школьников: методическое пособие для профильной и профессиональной ориентации и профильного обучения / С. Н. Чистякова. — Москва : Академия, 2007. — 128 с.
31. Выготский, Л. С. Педагогическая психология / Л. С. Выготский ; под ред. В. В. Давыдова. — Москва : АСТ : Астрель, 2010. — 671 с.
32. Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 «Сетевое и системное администрирование». Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И. М. Толмачев // Автоматизация и информатизация ТЭК. — 2025. — № 11(628). — С. 58–62. — EDN DMHQJU.
33. Греков, В. С. Перспективы кибербезопасности в нефтегазовой отрасли / В. С. Греков, А. Г. Уймин // Губкинский университет в решении вопросов нефтегазовой отрасли России : Тезисы докладов VI Региональной научно-технической конференции, Москва, 19–21

сентября 2022 года. — Москва : РГУ нефти и газа (НИУ) имени И. М. Губкина, 2022. — С. 1108–1109.
34. Positive Technologies Network Attack Discovery. Версия 12.2 : руководство администратора. — Positive Technologies, 2025. — 181 с. — Дата редакции: 19.03.2025.
35. Positive Technologies Network Attack Discovery. Версия 12.2 : руководство оператора. — Positive Technologies, 2025. — 256 с. — Дата редакции: 19.03.2025.
36. Positive Technologies Network Attack Discovery. Версия 12.2 : руководство по установке на один сервер. — Positive Technologies, 2025. — 53 с. — Дата редакции: 19.03.2025.

References

1. Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P., & Fujdiak, R. (2025). Lessons learned from using cyber range to teach cybersecurity at different levels of education. Technology, Knowledge and Learning. https://doi.org/10.1007/s10758-025-09840-y
2. Ghosh, S. (2025). Network traffic analysis based on cybersecurity intrusion detection through an effective statistical features selection and supervised learning classifier. Applied Soft Computing. https://doi.org/10.1016/j.asoc.2024.112603
3. The application of MITRE ATT&CK framework in mitigating cybersecurity threats. (2024). Issues in Information Systems. https://doi.org/10.48009/3_iis_2024_106
4. Lippi, G. (2025). Practical strategies for laboratory cybersecurity. Ukrainian Journal of Laboratory Medicine. https://doi.org/10.62151/2786-9288.3.4.2025.11
5. Dincelli, E., & Jafarian, H. (2025). Exploring the agentic metaverse's potential for transforming cybersecurity workforce development. MIS Quarterly Executive. https://doi.org/10.17705/2msqe.00122
6. Chernikov, P. (2025). Cyber defense of urban digital systems: Scaling SIEM correlation to reduce incident response time. Cybersecurity: Education, Science, Technique. https://doi.org/10.28925/2663-4023.2025.31.1066
7. Zelloth, H. (2025). Career guidance for Vocational Education and Training (VET). Journal of the National Institute for Career Education and Counselling. https://doi.org/10.20856/jnicec.3308
8. Chang, F., & Wang, P. (2025). The impact of lack of parental career engagement on the career planning ability of vocational students. International Journal for Educational and Vocational Guidance. https://doi.org/10.1007/s10775-025-09755-1
9. Dayag, R. P., & Picajas, J. J. (2025). Strengthening career readiness through structured career guidance services of graduating students. Global Journal of Guidance and Counselling in Schools. https://doi.org/10.18844/gjgc.v15i2.9758
10. Barigye, D. (2024). Technical vocational education and training in Uganda: Career guidance and practice. African Journal of Career Development. https://doi.org/10.4102/ajcd.v6i1.100
11. Mathur, A., & Mishra, A. (2024). Navigating the future: How career guidance programs prepare secondary students for the future. International Journal of Science and Research. https://doi.org/10.21275/sr241210140511
12. Kovalev, A., Stefanac, N., & Rizoiu, M.-A. (2025). Skill-driven certification pathways: Measuring industry training impact on graduate employability. arXiv. https://arxiv.org/abs/2506.04588
13. Maennel, K., & Maennel, O. (2025). Human aspects of cyber security for computing higher education: Current status and future directions. ACM Transactions on Computing Education, 25(3), Article 27, 1–30. https://doi.org/10.1145/3733839
14. Wang, H., Chen, L., Xu, S., & Gu, X. (2025). Study on the types of career decision-making difficulties of Chinese higher vocational college students and the influence of parental career intervention behaviors. Journal of Higher Education Management, 19(2), 86–100. https://doi.org/10.13316/j.cnki.jhem.20250122.008
15. Kryger, M., & Qvortrup, A. (2025). Conceptualizing and developing vocational identity: A scoping review of research in vocational education and training. Vocations and Learning, 18, Article 15. https://doi.org/10.1007/s12186-025-09371-8

16. Bükki, E., & Fehérvári, A. (2024). Teacher, professional or both? A mixed method study of the professional identity. International Journal for Research in Vocational Education and Training. https://doi.org/10.13152/ijrvet.11.3.4
17. Kharchenko, O., & Bondarenko, D. (2025). The digital transformation of competency assessment: Challenges and future of integrity. Cybersecurity: Education, Science, Technique. https://doi.org/10.28925/2663-4023.2025.30.917
18. Pleshakova, A. Yu. (2024). Defining the concept of identity of national vocational education system. Professional Education in the Modern World. https://doi.org/10.20913/2618-7515-2023-4-8
19. Smirnov, D., & Evsutin, O. (2024). Methodology for collecting data on the activity of malware for Windows OS. Informatics and Automation. https://doi.org/10.15622/ia.23.3.2
20. Partyka, O., Fihol, B., & Nakonechnyi, T. (2024). Integrated approach to detecting Bluetooth threats using Wireshark and Splunk SIEM. Cybersecurity: Education, Science, Technique. https://doi.org/10.28925/2663-4023.2024.26.684
21. Pidhornyi, P. (2024). Analytical review of models and systems for network traffic classification. Cybersecurity: Education, Science, Technique. https://doi.org/10.28925/2663-4023.2024.26.639
22. Batyshev, S. Ya., & Novikov, A. M. (Eds.). (2010). Professional pedagogy (3rd ed., revised). EGVES.
23. Novikov, A. M. (2010). Foundations of pedagogy. EGVES.
24. Lednev, V. S. (1991). Content of education: Essence, structure, prospects (2nd ed., revised). Vysshaya Shkola.
25. Lomakina, T. Yu. (2006). The modern principle of the development of lifelong education. Nauka.
26. Verbitsky, A. A. (1991). Active learning in higher education: Contextual approach. Vysshaya Shkola.
27. Klimov, E. A. (2010). Psychology of professional self-determination (4th ed.). Akademia.
28. Zeer, E. F. (2008). Psychology of professions (5th ed., revised and expanded). Academic Project; Mir Foundation.
29. Pryazhnikov, N. S. (2008). Professional self-determination: Theory and practice. Akademia.
30. Chistyakova, S. N. (2007). Pedagogical support of self-determination of schoolchildren. Akademia.
31. Vygotsky, L. S. (2010). Pedagogical psychology (V. V. Davydov, Ed.). AST; Astrel.
32. Uymin, A. G., & Tolmachev, I. M. (2025). Application of domestic network equipment Eltex and EcoRouter within the specialty 09.02.06 «Network and System Administration». Automation and Informatization of the Fuel and Energy Complex, (11), 58–62.
33. Grekov, V. S., & Uymin, A. G. (2022). Prospects of cybersecurity in the oil and gas industry. In Gubkin University in solving issues of the oil and gas industry of Russia (pp. 1108–1109). Gubkin Russian State University of Oil and Gas.
34. Positive Technologies. (2025). Positive Technologies Network Attack Discovery, version 12.2: Administrator guide. Positive Technologies.
35. Positive Technologies. (2025). Positive Technologies Network Attack Discovery, version 12.2: Operator guide. Positive Technologies.
36. Positive Technologies. (2025). Positive Technologies Network Attack Discovery, version 12.2: Single-server installation guide. Positive Technologies.

Информация об авторах

Уймин Антон Григорьевич — старший преподаватель кафедры безопасности информационных технологий, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, e-mail: au-mail@ya.ru

Греков Владимир Сергеевич — ассистент кафедры безопасности информационных технологий, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, e-mail: grekov.vs.work@gmail.com

EXPERIENCE OF TEACHING PRODUCT-BASED COURSES IN SIEM AND NAD IN THE LOGIC OF INTEGRATED CAREER GUIDANCE: FROM THE FIRST YEAR OF

SPECIALIST DEGREE PROGRAMMES TO THE CERTIFICATION OF GRADUATES IN THE EXTENDED GROUP 10.00.00

Uymin A. G.1, Grekov V. S.1

1National University of Oil and Gas «Gubkin University»

Abstract. The paper presents the experience of implementing vendor product-based courses by Positive Technologies — PT-SIEM-CS (Certified Specialist in MaxPatrol SIEM) and PT-NAD-CS (Certified Specialist in PT Network Attack Discovery) — within a higher education trajectory covering two cross-sections of training: the first year of the specialist degree programme in the extended group of fields 10.00.00 «Information Security» within a profile subject and senior years (4–5) of the same specialist degree programme. The pedagogical rationale for taking first-year students to an independent vendor certification within a profile subject is unfolded: this practice is considered as an element of integrated career guidance ensuring early and subject-rooted contact of the learner with real professional activity, the formation of motivational-axiological and cognitive components of professional competence, and the consolidation of the professional choice through success in a normatively recognised assessment procedure. The pedagogical technologies of career guidance applied in the course are described in detail: professional probe, contextual learning, case study, project-based learning, simulation on an industrial training ground, mentoring, portfolio technology, reflective fixation, early embedded internship and independent certification as the culmination of the cycle. Quantitative results: 11 out of 14 students completed the SIEM block; all 29 students completed the NAD block and passed the proctored certification. The findings are consistent with the positions of the Russian school of professional pedagogy (S. Ya. Batyshev, A. M. Novikov, V. S. Lednev, T. Yu. Lomakina, A. A. Verbitsky, E. A. Klimov, E. F. Zeer) and recent international research on cybersecurity education and structured career pathways.

Keywords: professional competence, higher education, information security, career guidance, certification, contextual learning, SIEM/NAD.

Information about the authors

Uymin Anton Grigorievich — Senior Lecturer of the Department of Information Technology Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: au-mail@ya.ru

Grekov Vladimir Sergeevich — Assistant of the Department of Information Technology Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: grekov.vs.work@gmail.com

УСЛОВИЯ И ПОРЯДОК НАПРАВЛЕНИЯ МАТЕРИАЛОВ

Редакция научного журнала «ПРОФЕССИОНАЛИТЕТ» принимает к рассмотрению статьи, исправленные версии рукописей, ответы на замечания редакции и рецензентов, а также сопроводительную переписку по конкретной статье. Направление материалов осуществляется в электронной форме в соответствии с внутренним регламентом редакции.

Каждое письмо должно содержать информативную тему и заполненный сопроводительный текст. Переписка ведется в официально-деловом стиле. В теме письма указываются тип обращения, фамилия автора, краткое название статьи и, при необходимости, номер итерации исправления.

В тексте письма обязательно приводятся полное название статьи, сведения обо всех авторах, дисциплина (если применимо), номер итерации исправления и контактные данные ответственного автора. Для исправленных версий дополнительно рекомендуется указывать, на какое письмо редакции или рецензии дается ответ, и кратко обозначать внесенные исправления.

Файл рукописи направляется в формате .docx, на кириллице, по установленной форме наименования. Исправленные версии направляются исключительно ответом на письмо редакции с обязательным указанием номера итерации в теме письма, тексте письма и имени файла.

Материалы, оформленные с нарушением установленных требований, могут быть возвращены без рассмотрения до устранения технических замечаний.

Контактные данные редакционной коллегии

Почтовый адрес для корреспонденции: Москва, Ленинский пр-кт, д. 65/1, отделение почтовой связи № 119296.

До востребования.

Получатель: Павловский Владимир Владимирович.

Тел. +7(950) 632-04-38

e-mail: organizers@au-team.ru

главный редактор – Уймин Антон Григорьевич;

ответственный секретарь - Уймина Ольга Ивановна;

технический редактор - Козлов Глеб Васильевич.

ПРОФЕССИОНАЛИТЕТ, 2025, № 2 (006)

Научное электронное издание.

Сведения о программном обеспечении, использованном для создания электронного издания:
LibreOffice — набор, вёрстка текста, генерация PDF
https://ru.libreoffice.org

Техническая обработка и подготовка материалов выполнены авторами.

Подписано к использованию: 30.06.2025.

Объём издания: 76,6 Мб.

Комплектация издания: pdf.

Запись на физический носитель: Уймин А. Г., тел. +7 (950) 632-04-38.

Издатель — редакция научного журнала «ПРОФЕССИОНАЛИТЕТ».

Место издания: Москва.

Электронная версия подготовлена редакцией журнала для распространения в локальной и сетевой форме.

Носитель электронного издания: URALOLIMP.WEBSITE