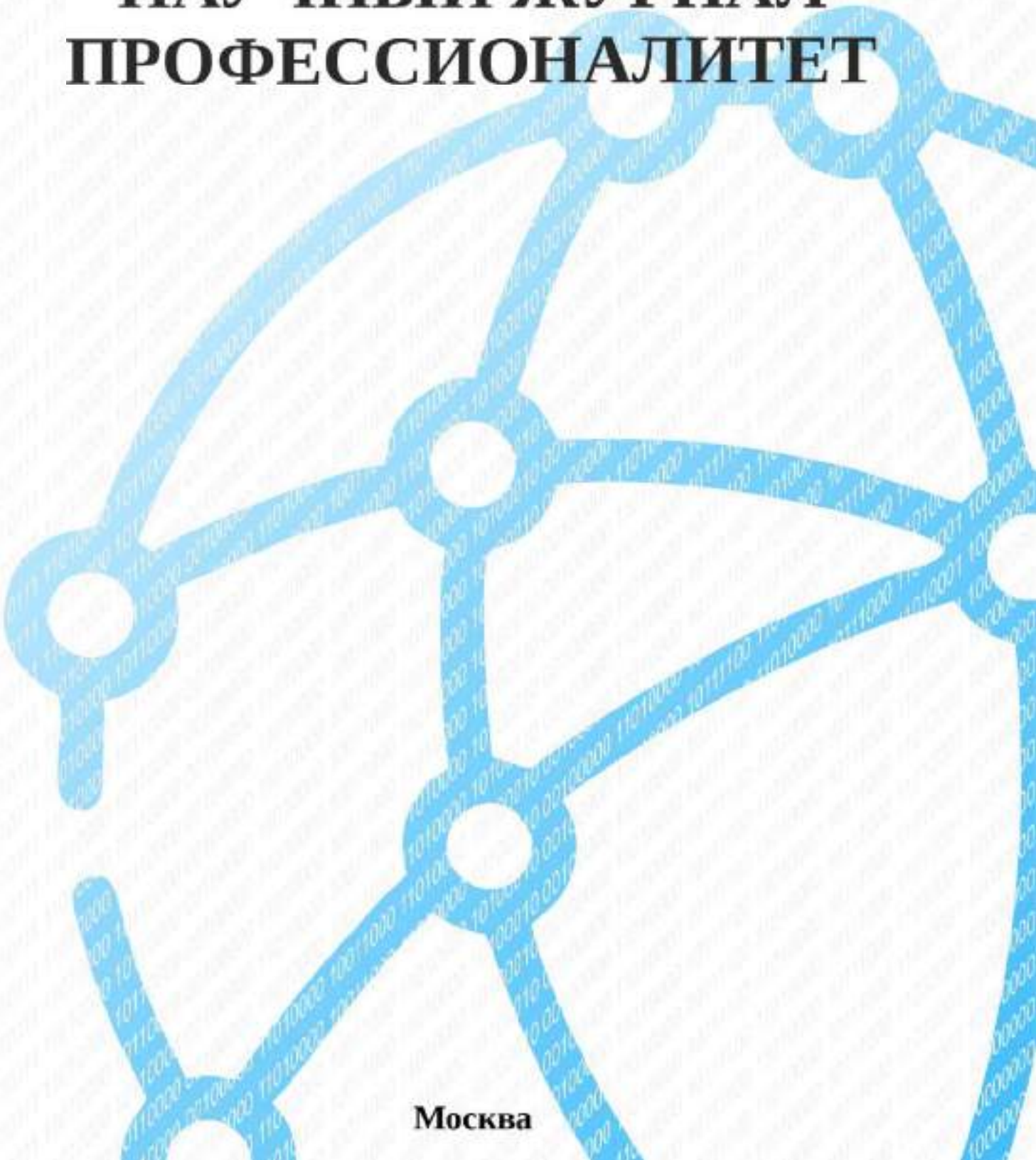
Выпуск 2 (4), 2025

НАУЧНЫЙ ЖУРНАЛ ПРОФЕССИОНАЛИТЕТ



Москва

ПРОФЕССИОНАЛИТЕТ

№ 2 (4), 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 119634, г. Москва, ул. Лукинская, д. 1, кв. 123

PROFESSIONALITET

No.2 (4), 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:

119634, Moscow, Lukinskaya St., 1, Apt. 123

СОДЕРЖАНИЕ

CONTENTS

Рубрика 1. Информатика и информационные процессы

УДК *004.45*

К. А. Лаврушова[1], Д. Р. Хабибов[1]

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

НАСТРОЙКА И ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ SMB СЕРВЕРА НА БАЗЕ WINDOWS SERVER. ВОПРОСЫ БЕЗОПАСНОСТИ

Аннотация: *В статье рассматриваются конфигурирование и функциональная проверка SMB-сервера на базе Windows Server, включённого в корпоративную доменную инфраструктуру. Предметный фокус сосредоточен на организации сетевого доступа к файловым ресурсам и устройствам, а также на анализе требований к защите данных при эксплуатации протокола SMB. Практический этап выполнен в виртуализированной среде, воспроизводящей типовую корпоративную схему: контроллер домена, файловый сервер, клиентские рабочие станции. Тестирование подтвердило корректность работы механизмов разграничения прав доступа и устойчивость файлового сервиса в заданной конфигурации. Отдельный блок исследования посвящён прикладной демонстрации критической атаки SMB Relay (NTLM Relay): описан её сценарий, определены условия успешного выполнения, включая отключённую цифровую подпись SMB и наличие возможности изменения DNS-записей. Показано, как при отсутствии обязательной подписи SMB-пакетов механизм ретрансляции аутентификации позволяет злоумышленнику получить несанкционированный доступ к ресурсам целевого сервера с привилегиями ретранслированной учётной записи. На основе проведённого анализа формулируются ключевые рекомендации по безопасной настройке SMB, включая отключение устаревшей версии протокола SMBv1, обязательное включение подписи пакетов и регулярное обновление программного обеспечения. Полученные результаты могут быть использованы при обучении специалистов в области информационной безопасности и системного администрирования, а также в практической деятельности для повышения защищённости корпоративных сетей.*

Ключевые слова: *SMB, Windows Server, файловый сервер, корпоративная сеть, информационная безопасность, сетевые протоколы.*

Введение

Современные корпоративные информационные системы невозможно представить без использования сетевых файловых сервисов, обеспечивающих централизованное хранение и совместный доступ к данным. В сетях на базе операционных систем семейства Windows для организации общего доступа к файлам и устройствам широко применяется протокол SMB (Server Message Block) [1].

Следует отметить, что термин CIFS (Common Internet File System) используется для обозначения одного из диалектов протокола SMB, тогда как Samba является программной реализацией данного протокола для UNIX-подобных операционных систем. В рамках данной работы рассматривается исключительно использование SMB как сетевого протокола общего доступа.

Актуальность данной работы обусловлена ростом числа сетевых атак, направленных на эксплуатацию сервисов общего доступа, а также необходимостью практического изучения принципов настройки и защиты SMB-серверов в корпоративных сетях. Это обусловлено тем, что файловые серверы зачастую содержат критически важную информацию организации, а уязвимости или ошибки конфигурации SMB-сервера могут привести к несанкционированному доступу, утечке данных или распространению вредоносного программного обеспечения внутри сети [2].

Объектом исследования в данной работе является файловый сервер в корпоративной сети на базе операционной системы Windows Server.

Предметом исследования являются процессы настройки, функционирования и обеспечения безопасности протокола SMB при организации общего доступа к файловым ресурсам в среде операционных систем Windows.

Целью исследования является изучение особенностей настройки SMB-сервера на базе Windows Server, проведение его функционального тестирования, а также анализ основных угроз информационной безопасности, связанных с использованием протокола SMB в корпоративных сетях.

Литературный обзор

Протокол SMB (Server Message Block) является одним из наиболее распространённых сетевых протоколов, применяемых для организации общего доступа к файловым ресурсам в локальных и корпоративных сетях [1]. Архитектура протокола, его клиент-серверная модель и механизмы взаимодействия с файловыми системами подробно рассматриваются в официальной технической документации Microsoft [1], а также в фундаментальных трудах по современным операционным системам и компьютерным сетям, в частности в учебных изданиях Э. Таненбаума и Н. Фимстера.

В работах, посвящённых администрированию серверных операционных систем Windows, SMB рассматривается как стандартный инструмент построения файловых серверов за счёт тесной интеграции с доменной инфраструктурой Active Directory и средствами управления доступом пользователей [3].

Значительное внимание в научной и учебной литературе уделяется вопросам информационной безопасности протокола SMB. Отмечается, что типовыми причинами инцидентов безопасности являются использование устаревших версий протокола, избыточные права доступа к общим ресурсам и недостаточный контроль сетевых соединений [2].

В аналитических материалах и методических рекомендациях по анализу киберугроз, включая базу знаний MITRE ATT&CK, протокол SMB рассматривается как один из распространённых векторов атак в корпоративных сетях, используемый при компрометации учётных данных и боковом перемещении злоумышленников внутри инфраструктуры [4, 5].

Методика исследования

На этапе теоретического исследования были применены методы анализа и обобщения научных и учебных источников [1], а также официальной технической документации, посвящённой операционным системам Windows, протоколу SMB и вопросам защиты сетевых файловых сервисов [6, 1]. Это позволило определить основные особенности работы протокола, его функциональные возможности и типовые уязвимости.

Основу практической части исследования составил экспериментальный метод. Для проведения эксперимента была использована среда виртуализации Oracle VirtualBox, позволяющая смоделировать типовую корпоративную сеть без применения физического оборудования. Схема экспериментальной сети представлена на Рисунке 1. В виртуальной среде были развернуты сервер и клиентские рабочие станции под управлением операционной системы Windows 11, а также отдельный узел атакующего (Attacker) на базе операционной системы Kali Linux. Узел Attacker подключён к той же виртуальной сети (Internal Network), что и остальные участники эксперимента, и использовался исключительно для запуска инструментов, моделирующих сценарий SMB Relay: krbrelayx и printerbug. Данный узел не является частью корпоративной доменной инфраструктуры и представляет внутреннего нарушителя, имеющего доменную учётную запись.

Рис. 1. Схема экспериментальной доменной сети для настройки и тестирования SMB-сервера

Для проверки работоспособности SMB-сервера был использован метод функционального тестирования, включающий проверку доступа к общим файловым ресурсам, а также корректность применения прав доступа пользователей.

Для анализа аспектов безопасности протокола SMB использовался метод анализа угроз. В частности, применялся анализ потенциальных векторов атак, связанных с получением учётных данных, боковым перемещением и несанкционированным доступом к данным в корпоративной сети [4, 5]. Результаты анализа сопоставлялись с практическими условиями эксплуатации SMB-сервера, выявленными в ходе эксперимента.

Настройка клиентского доступа к SMB-серверу

Для обеспечения совместного доступа профиль сетевого подключения был установлен в режим частной сети (Private). Включение компонентов SMB осуществлялось с использованием стандартных средств операционной системы Windows. В результате выполненной конфигурации клиентские рабочие станции получили возможность подключения к файловому серверу по сетевому имени и взаимодействия с общими ресурсами в рамках заданных прав доступа. Процесс активации компонентов SMB на клиентской системе представлен на рисунке 2.

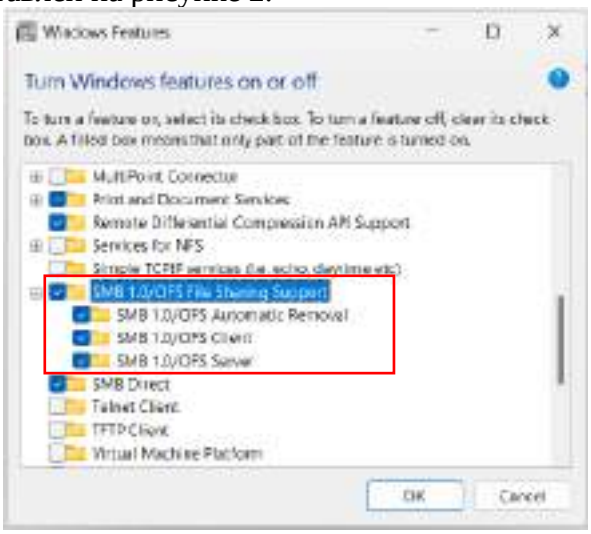


Рис. 2. Включение компонентов SMB на клиентской рабочей станции Windows

В ходе настройки файлового сервера были активированы необходимые роли и компоненты протокола SMB, обеспечивающие общий доступ в доменной среде. После установки сервер был приведён в рабочее состояние, что позволило предоставить сетевые

ресурсы клиентским рабочим станциям корпоративной инфраструктуры. Процесс активации компонентов файлового сервера и протокола SMB показан на рисунке 3.

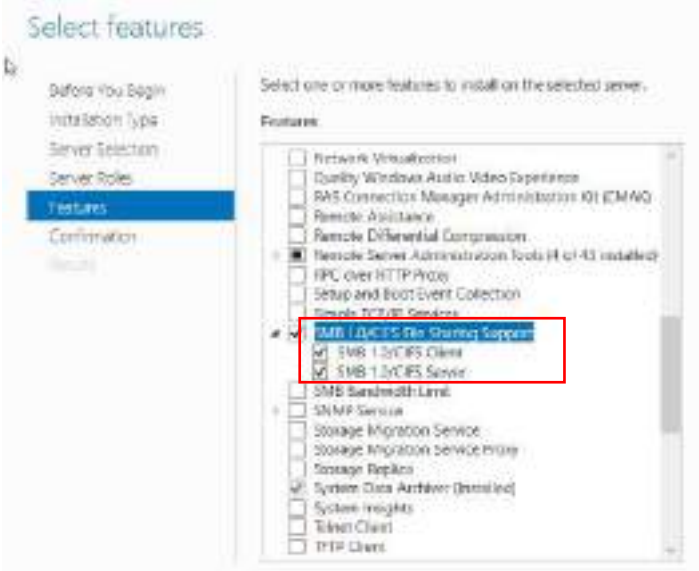


Рис. 3. Активация компонентов файлового сервера и протокола SMB в Windows Server

Следует отметить, что компонент SMB версии 1.0 был включён в экспериментальной среде исключительно в учебных целях для демонстрации известных уязвимостей протокола и анализа последствий его использования в корпоративной сети.

В реальных условиях эксплуатации SMBv1 считается устаревшим и небезопасным и не рекомендуется к использованию, что отдельно подчёркивается в разделе с рекомендациями по обеспечению безопасности.

Функциональное тестирование SMB-сервера

В рамках функционального тестирования была проведена проверка работоспособности SMB-сервера при организации общего доступа к файловым ресурсам в корпоративной сетевой среде. Для этого на сервере был создан общий сетевой каталог с заданными правами доступа для пользователей и групп домена, что показано на рисунке 4.

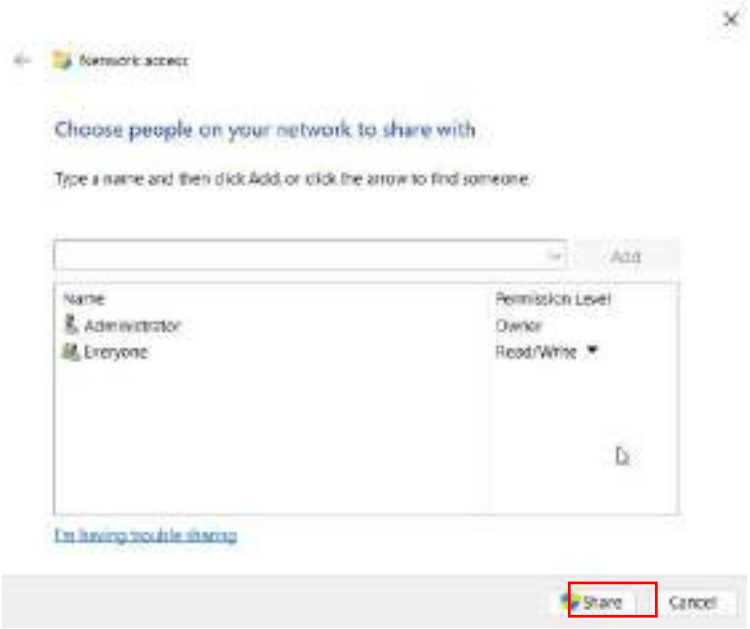


Рис. 4. Создание общего сетевого ресурса на SMB-сервере с настройкой прав доступа

Проверка показала, что клиентские рабочие станции успешно подключаются к общему ресурсу по сетевому имени сервера. Пользователи, обладающие соответствующими правами доступа, имели возможность просматривать содержимое

каталога, а также выполнять операции чтения, создания, изменения и удаления файлов. Факт корректного доступа к общему сетевому ресурсу с клиентской рабочей станции представлен на рисунке 5.

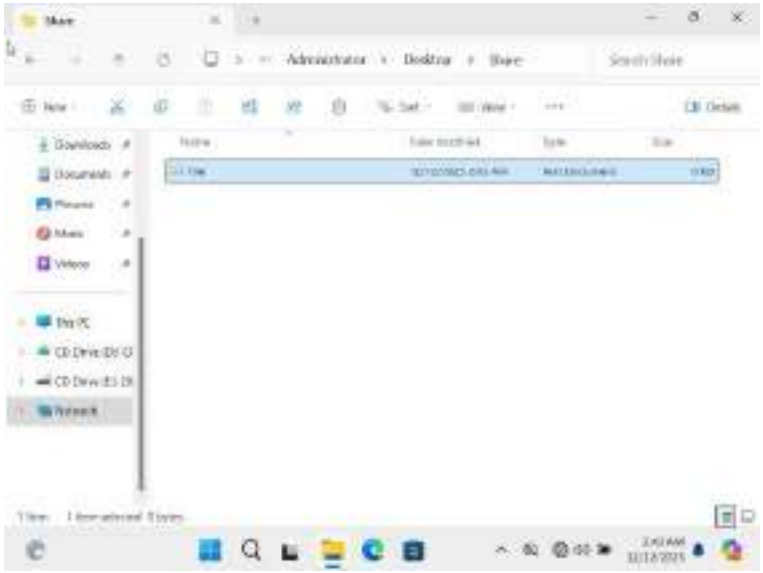


Рис. 5. Проверка подключения клиентской рабочей станции к общей сетевой папке SMB-сервера

Дополнительно была проведена проверка общего доступа к сетевым устройствам. На сервере был настроен общий доступ к сетевому принтеру, после чего клиентские рабочие станции успешно обнаруживали и подключали данное устройство через файловый сервер, что показано на рисунке 6.

Рис. 6. Подключение клиентской рабочей станции к сетевому принтеру через SMB-сервер

Вопросы безопасности SMB протокола

Согласно матрице атак MITRE ATT&CK, протокол SMB в корпоративных сетях чаще всего используется злоумышленниками в рамках следующих тактик: Credential Access, Lateral Movement и Collection. Эксплуатация уязвимостей и ошибок конфигурации SMB-сервисов позволяет получить учётные данные пользователей, осуществлять боковое перемещение между узлами сети и собирать конфиденциальную информацию, размещённую в общих сетевых ресурсах [5].

Средства и методы атак на SMB-протокол условно можно классифицировать по функциональному назначению на несколько групп.

Средства выявления и инвентаризации SMB-ресурсов применяются для определения доступных в сети общих каталогов, файловых хранилищ и назначенных пользователям прав доступа. Использование таких инструментов позволяет оценить организацию сетевой файловой инфраструктуры, обнаружить открытые ресурсы и определить узлы, которые потенциально могут требовать дополнительной настройки безопасности, без активного вмешательства в работу системы.

Атаки класса Man-in-the-Middle в отношении SMB связаны с перехватом, подменой или ретрансляцией сетевого обмена между клиентом и сервером. В доменной среде подобные сценарии особенно опасны, поскольку при недостаточной защите сетевого

взаимодействия злоумышленник может получить сведения об учётных записях и аутентификационных данных. Риск возрастает при отключённой или необязательной подписи SMB-сообщений, а также при использовании устаревших и небезопасных механизмов разрешения имён.

Подбор учётных данных для SMB-ресурсов основан на последовательной проверке различных комбинаций имени пользователя и пароля с целью получения доступа к сетевым папкам или службам. Вероятность успешной реализации такой атаки повышается при наличии простых паролей, типовых учётных записей, повторного использования паролей и отсутствии ограничений на количество неудачных попыток входа.

Инструменты, ориентированные на эксплуатацию SMB, обычно совмещают функции анализа доменной инфраструктуры, перечисления пользователей, групп и общих ресурсов, а также проверки доступных привилегий. При наличии недостаточно защищённых настроек или избыточных прав такие средства могут использоваться для выполнения несанкционированных действий в сети.

Следует отметить, что многие инструменты и методы могут одновременно относиться к нескольким указанным группам.

Атака на протокол SMB

В рамках исследования реализуется атака типа SMB Relay (NTLM Relay), основанная на архитектурных особенностях протоколов аутентификации в доменной среде. Успех атаки обеспечивается не наличием конкретного программного дефекта, а механизмом ретрансляции аутентификационных данных в сочетании с небезопасными настройками инфраструктуры: прежде всего отсутствием обязательной подписи SMB-пакетов (SMB Signing) и возможностью манипуляции DNS-записями. При соблюдении этих условий злоумышленник может ретранслировать перехваченные учётные данные на другой узел домена и получить к нему несанкционированный доступ с привилегиями исходного пользователя.

Сценарий атаки строится вокруг принудительного подключения жертвы к серверу, контролируемому злоумышленником. При этом узел атакующего перехватывает аутентификационный обмен по протоколу SMB и немедленно ретранслирует его на целевой сервер. Поскольку подпись SMB-пакетов не применяется, целевой сервер не в состоянии проверить подлинность источника запроса и устанавливает сессию с привилегиями ретранслированной учётной записи. Если ретранслируемая учётная запись обладает правами локального администратора на целевом узле, это открывает возможность удалённого выполнения команд, в том числе в контексте системного аккаунта SYSTEM. Для инициирования цепочки ретрансляции достаточно, чтобы пользователь попытался подключиться к поддельному узлу через специально созданный скрипт или ссылку.

Ключевые условия эксплуатации: отключение подписи SMB или установка значения «при согласовании» — эти параметры позволяют упростить принудительную аутентификацию.

На первом этапе производится анализ параметров безопасности SMB-сервера с целью определения режима работы подписи сообщений. В случае, если подпись SMB отключена либо используется в необязательном режиме, создаются предпосылки для перехвата и повторного использования аутентификационных данных при установлении сетевых соединений. Результат проверки конфигурации SMB-сервиса представлен на рисунке 7.

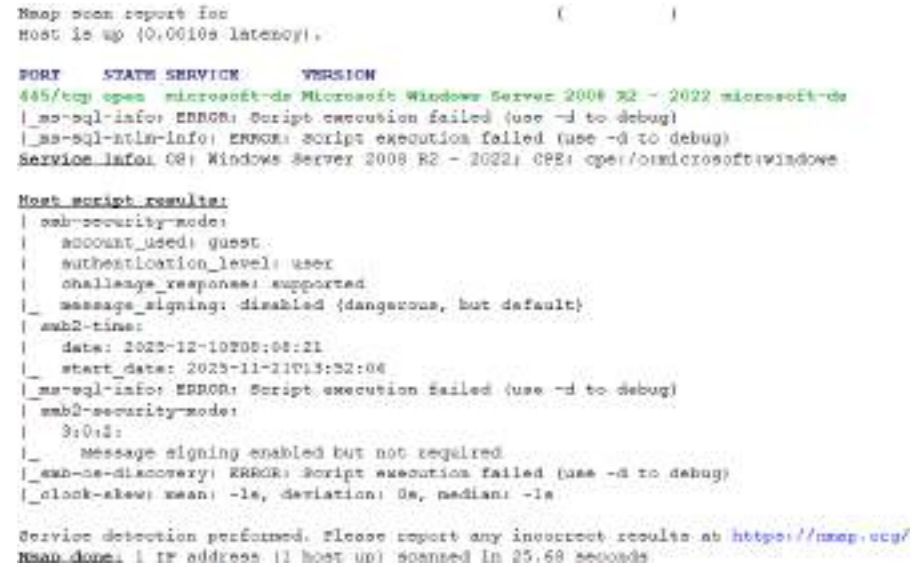


Рис. 7. Проверка параметров безопасности SMB-сервиса и режима подписи сообщений

На втором этапе используется особенность доменной инфраструктуры Active Directory, заключающаяся в том, что по умолчанию ряд пользователей обладает правами на добавление и изменение DNS-записей. В рамках экспериментального сценария моделируются действия внутреннего нарушителя. Злоумышленник может создать DNS-запись, указывающую на подконтрольный ему узел, что приводит к перенаправлению сетевых запросов легитимных пользователей. Факт успешного добавления DNS-записи показан на рисунке 8.

Рис. 8. Добавление DNS-записи в доменной среде Active Directory

На третьем этапе реализуется подмена ответов службы разрешения имён, в результате чего клиентская система инициирует соединение с поддельным сетевым ресурсом, полагая его доверенным элементом инфраструктуры. При отсутствии криптографической защиты SMB-аутентификации это позволяет осуществить ретрансляцию учётных данных и выполнить несанкционированные действия в доменной среде. Пример работы механизма подмены DNS-ответов представлен на рисунках 9–10:

Рис. 9. Настройка подмены разрешения сетевых имён в экспериментальной доменной сети

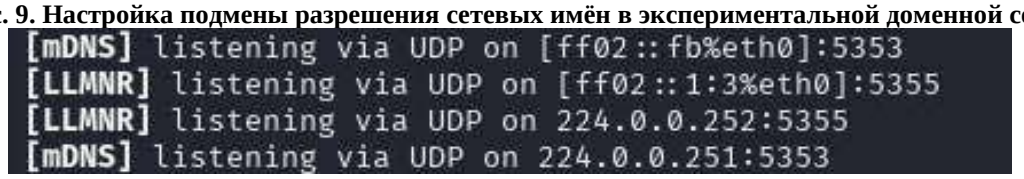


Рис. 10. Результат перенаправления сетевого запроса на подконтрольный узел атакующего

После завершения настройки службы разрешения имён был рассмотрен сценарий атаки ретрансляции аутентификации в доменной инфраструктуре. На данном этапе в экспериментальной среде был развёрнут SMB-листенер, предназначенный для приёма входящих попыток аутентификации и их последующей ретрансляции на целевой сервер. В качестве цели для ретрансляции использовалась служба SMB файлового сервера домена.

Для инициирования атаки применялся механизм принудительной аутентификации, при котором целевая система инициирует сетевое соединение с подконтрольным узлом. В результате данного воздействия сервер автоматически выполнял попытку аутентификации по протоколу SMB. Процесс принудительной аутентификации показан на рисунке 11 [7].

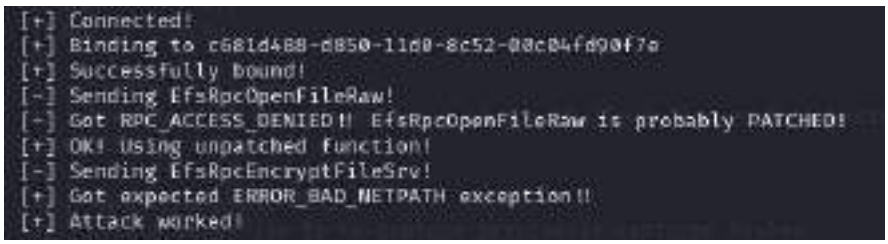


Рис. 11. Инициирование принудительной аутентификации целевой системы в доменной среде

В ходе эксперимента входящая попытка аутентификации была успешно ретранслирована на целевой сервер, что привело к получению доступа к системным данным безопасности. В частности, была подтверждена возможность удалённого получения информации из базы учётных данных локальной системы (Security Account Manager). Результат успешной ретрансляции и установления SMB-сессии представлен на рисунках 12–13.

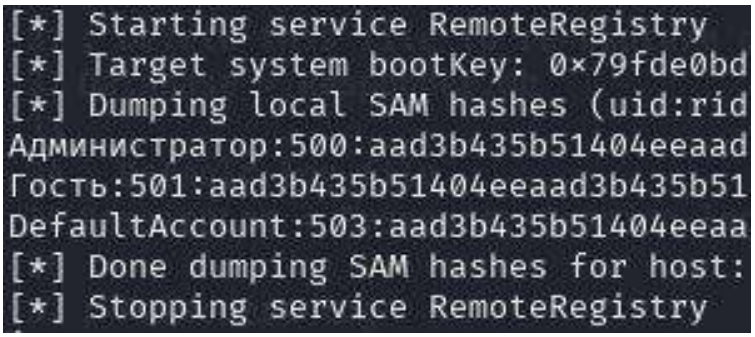


Рис. 12. Получение системных данных безопасности после ретрансляции SMB-аутентификации

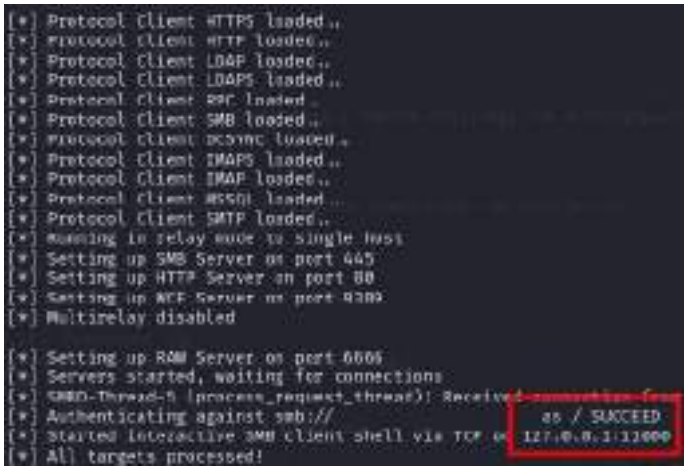


Рис. 13. Установление SMB-сессии с целевым сервером после успешной ретрансляции аутентификации

В качестве примера выполним команду на целевой системе после успешной ретрансляции с правами SYSTEM.

python3 krbrelayx.py -t smb://srv-1c-upp.mydomain.local -debug -c 'cmd /c "whoami /all & hostname & ipconfig"'

python3 printerbug.py 'mydomain.local/attacker:Qwerty123@srv-1c-upp.mydomain.local' srv-1c-upp1UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAAAwbEAYBAAAA

Теперь входящее соединение ретранслируется krbrelayx обратно на srv-1c-upp, и указанные команды выполняются на srv-1c-upp с привилегиями SYSTEM [8].

Результаты исследования

Результаты выполнения показали, что команды исполняются в контексте системного аккаунта **SYSTEM,** что свидетельствует о полном компрометировании целевого сервера. В

частности, была подтверждена возможность получения расширенной информации о правах текущего процесса, имени целевой системы и параметрах сетевой конфигурации.

Дополнительно было установлено, что повторная ретрансляция входящих соединений позволяет устойчиво поддерживать привилегированный доступ к целевой системе.

В итоге для успешной атаки нам необходимо выполнение следующих условий:

−пользовательская учетная запись домена;

−сетевой доступ к 445 порту атакуемого хоста и обратно;

−отсутствие подписи SMB;

−возможность добавления DNS-записей (либо spoofing DNS-записей в пределах широковещательного домена).

Чтобы минимизировать риски эксплуатации уязвимостей протокола SMB, рекомендуется:

−Регулярно обновлять операционную систему и любое программное обеспечение, использующее SMB — часто выпускаются исправления для устранения уязвимостей.

−Отключить устаревший протокол SMB версии 1 — эта версия не поддерживает современные механизмы безопасности и крайне уязвима. Начиная с Windows Server 2016, SMBv1 по умолчанию отключён.

−Использовать цифровую подпись SMB-пакетов — это не позволит злоумышленнику незаметно подменять или перехватывать файлы по сети.

−Не оставлять SMB доступным там, где это не нужно — по умолчанию Windows Firewall блокирует внешние подключения к SMB-портам (TCP 445).

Заключение

В рамках данной работы была рассмотрена настройка и функциональное тестирование SMB-сервера на базе операционной системы Windows Server в условиях корпоративной доменной инфраструктуры. В ходе экспериментального исследования была смоделирована типовая корпоративная сеть в виртуальной среде, что позволило на практике изучить особенности работы протокола SMB при организации общего доступа.

Проведённое функциональное тестирование подтвердило корректную работу SMB-сервера и его способность обеспечивать централизованный доступ к сетевым ресурсам с применением механизмов аутентификации и разграничения прав доступа. Эксперимент показал, что при корректной конфигурации файловый сервер стабильно функционирует в доменной среде и удовлетворяет требованиям, предъявляемым к корпоративным файловым сервисам.

В рамках анализа вопросов информационной безопасности были рассмотрены основные векторы атак на протокол SMB, а также условия, при которых возможна их успешная реализация. Установлено, что большинство рисков безопасности связано не с архитектурными недостатками самого протокола, а с ошибками конфигурации и нарушением базовых принципов безопасного администрирования, такими как использование устаревших версий протокола, отключение подписи SMB-сообщений и избыточные права пользователей в доменной инфраструктуре.

Реализация указанных мер позволяет существенно снизить вероятность компрометации файловых сервисов и повысить уровень информационной безопасности корпоративной сети.

Список литературы

1. Microsoft. SMB Protocol Overview : техническое описание протокола Server Message Block. — URL: https://learn.microsoft.com/windows-server/storage/file-server/smb-overview (дата обращения: 26.11.2025).
2. Microsoft. Windows Server security overview : обзор механизмов защиты Windows Server. — Microsoft Learn, 2024. — URL: https://learn.microsoft.com/windows-server/security/security-and-assurance (дата обращения: 10.10.2025).

3. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : практикум : учеб. пособие для вузов / А. Г. Уймин. — СПб. : Лань, 2024. — 116 с. — (Высшее образование). — ISBN 978-5-507-48647-2. — EDN BZJRIQ.
4. MITRE Corporation. MITRE ATT&CK Framework : база знаний по тактикам и техникам кибератак. — URL: https://attack.mitre.org (дата обращения: 17.10.2025).
5. MITRE ATT&CK. Network Share Discovery (T1135) : Обнаружение общего сетевого ресурса. — URL: https://attack.mitre.org/techniques/T1135/ (дата обращения: 14.11.2025).
6. Microsoft. Windows Server Documentation : официальная техническая документация. — URL: https://learn.microsoft.com/en-us/windows-server/ (дата обращения: 14.12.2025).
7. Russinovich, M., Ionescu, A., Solomon, D. Windows Internals. Part 2. — 7th ed. — Redmond : Microsoft Press, 2021. — 816 p.
8. Microsoft. Security Update Guide : официальная база уязвимостей и обновлений безопасности Microsoft. — URL: https://msrc.microsoft.com/update-guide (дата обращения: 14.12.2025).

References

1. Microsoft. (n.d.). SMB protocol overview. Microsoft Learn. Retrieved November 26, 2025, from https://learn.microsoft.com/windows-server/storage/file-server/smb-overview
2. Microsoft. (2024). Windows Server security overview. Microsoft Learn. Retrieved October 10, 2025, from https://learn.microsoft.com/windows-server/security/security-and-assurance
3. Uimin, A. G. (2024). Basic level demonstration exam. Network and system administration: Practical course. Lan Publishing.
4. MITRE Corporation. (n.d.). MITRE ATT&CK framework. Retrieved October 17, 2025, from https://attack.mitre.org
5. MITRE ATT&CK. (n.d.). Network Share Discovery (T1135). MITRE Corporation. Retrieved November 14, 2025, from https://attack.mitre.org/techniques/T1135/
6. Microsoft. (n.d.). Windows Server documentation. Microsoft Learn. Retrieved December 14, 2025, from https://learn.microsoft.com/en-us/windows-server/
7. Russinovich, M., Ionescu, A., & Solomon, D. (2021). Windows internals, part 2 (7th ed.). Microsoft Press.
8. Microsoft. (n.d.). Security Update Guide. Microsoft Security Response Center. Retrieved December 14, 2025, from https://msrc.microsoft.com/update-guide

Информация об авторах

Лаврушова Ксения Александровна — студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: ksenialive8@gmail.com

Хабибов Денис Рустамович — студент 3 курса факультета комплексной безопасности топливно-энергетического комплекса, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: deniskhab81@gmail.com

SETUP AND FUNCTIONAL TESTING OF AN SMB SERVER BASED ON WINDOWS SERVER. SECURITY ISSUES

Lavrushova K. A[1]., Khabibov D. R.[1]

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

Annotation: *This article examines the process of configuring and functionally testing an SMB server running Windows Server within a corporate domain infrastructure. It focuses on organizing shared access to file resources and network devices, as well as a comprehensive analysis of information security issues related to the operation of the SMB protocol. The experimental portion of the study was implemented in a virtual environment using virtualization software, which allowed us to simulate a typical corporate network infrastructure, including a domain controller, a file server, and client workstations. Functional testing was conducted, confirming the correctness of access rights delimitation and the stability of the service. Particular attention is given to a practical demonstration of one of the critical attacks—SMB Relay (NTLM Relay). The article describes in detail the attack scenario and the conditions for*

its successful implementation, including the lack of an SMB digital signature and the possibility of modifying DNS records. It also demonstrates how an attacker can gain privileged access to the system and execute code with SYSTEM privileges. Based on their analysis, the authors formulate key recommendations for secure SMB configuration, including disabling the outdated SMBv1 protocol, mandating packet signing, and regularly updating software. These findings can be used in training information security and system administration professionals, as well as in practical applications to improve the security of corporate networks.
Keywords: *SMB, Windows Server, file server, corporate network, information security, network protocols.*

Information about the authors

Lavrushova Ksenia Aleksandrovna – 3rd year student of the Department of Integrated Safety of Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National University), Moscow, e-mail: ksenialive8@gmail.com

Khabibov Denis Rustamovich – 3rd year student of the Department of Integrated Safety of Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National University), Moscow, e-mail: deniskhab81@gmail.com

ПРОФЕССИОНАЛИТЕТ, 2025, № 2 (4)

***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.

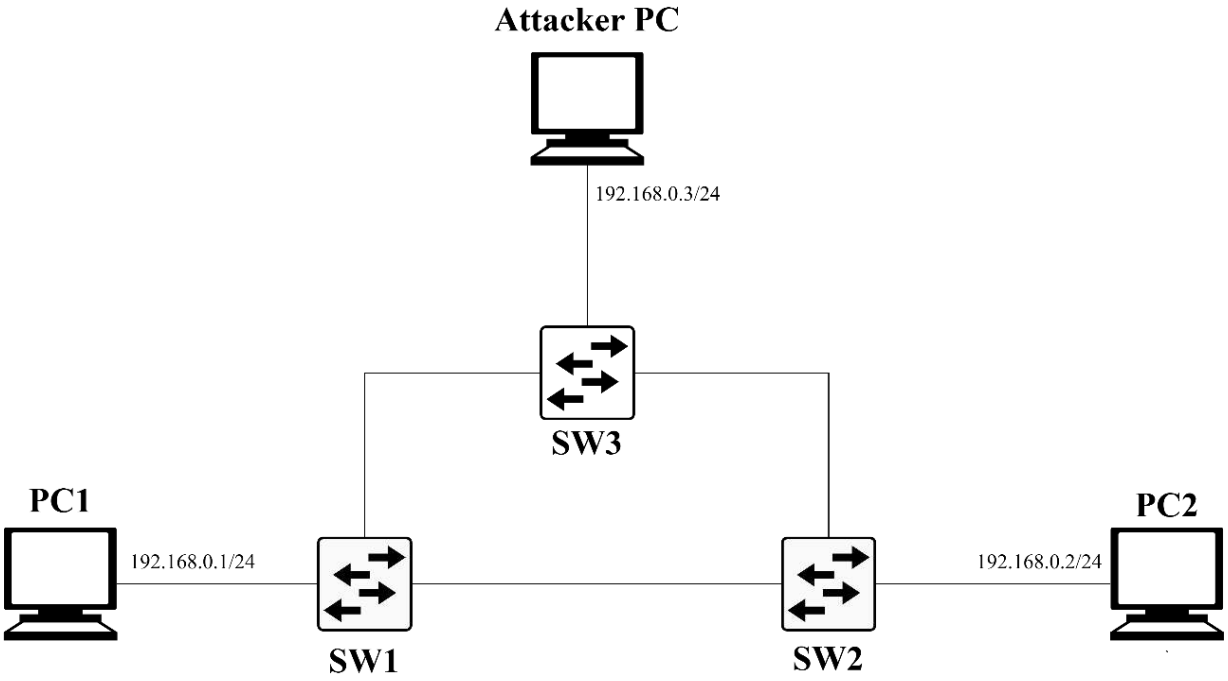


Рис. 1 Топология сети для моделирования атаки на STP с использованием коммутаторов Cisco, MikroTik и Eltex

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.

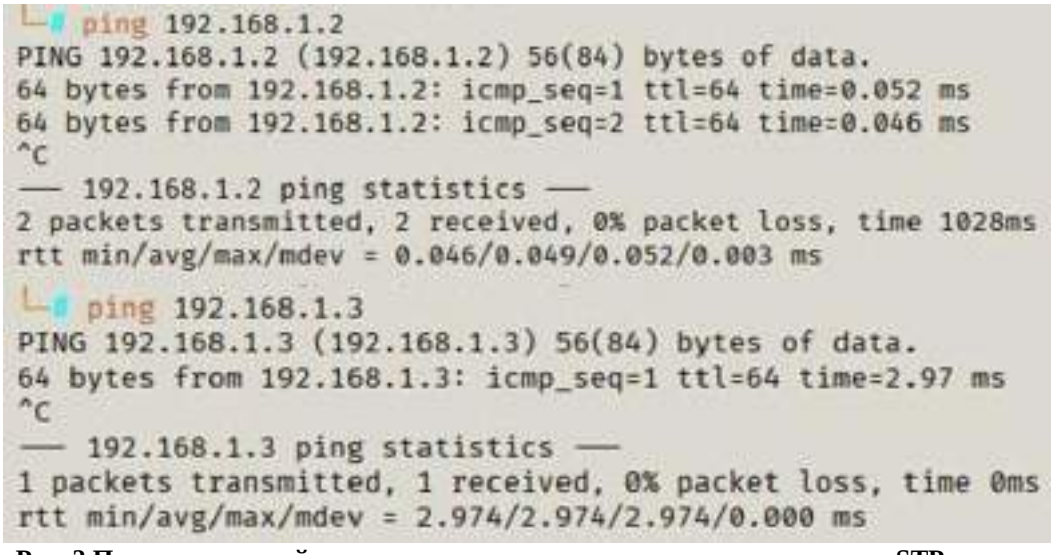


Рис. 2 Проверка сетевой связности между узлами до проведения атак на STP

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.

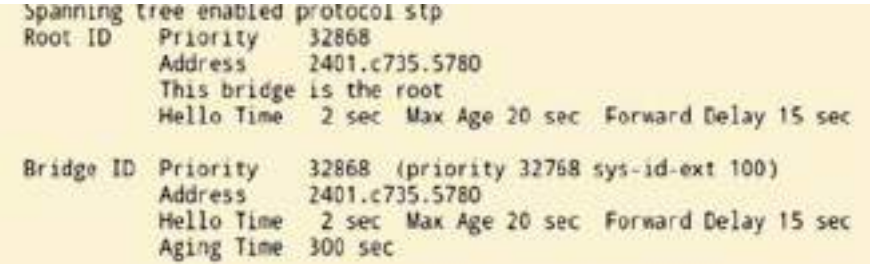


Рис. 3 Результат первой атаки с фиксацией изменения корневого моста после отправки поддельных BPDU-пакетов

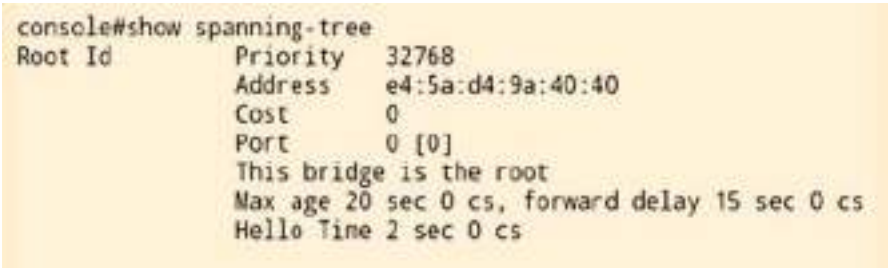


Рис. 4 Результат второй атаки с фиксацией назначения атакующего узла корневым мостом

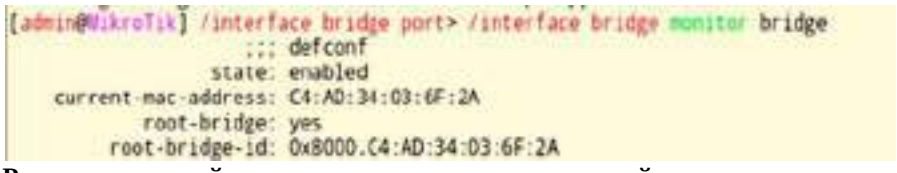


Рис. 5 Результат третьей атаки с подтверждением успешной подмены корневого моста

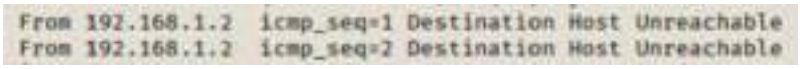


Рис. 6 Нарушение сетевой связности после изменения топологии STP в результате атаки

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-ROOTGUARDBLOCK» 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.

Список литературы

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

ПРОФЕССИОНАЛИТЕТ, 2025, № 2 (4)

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 L3-УСТРОЙСТВА 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.

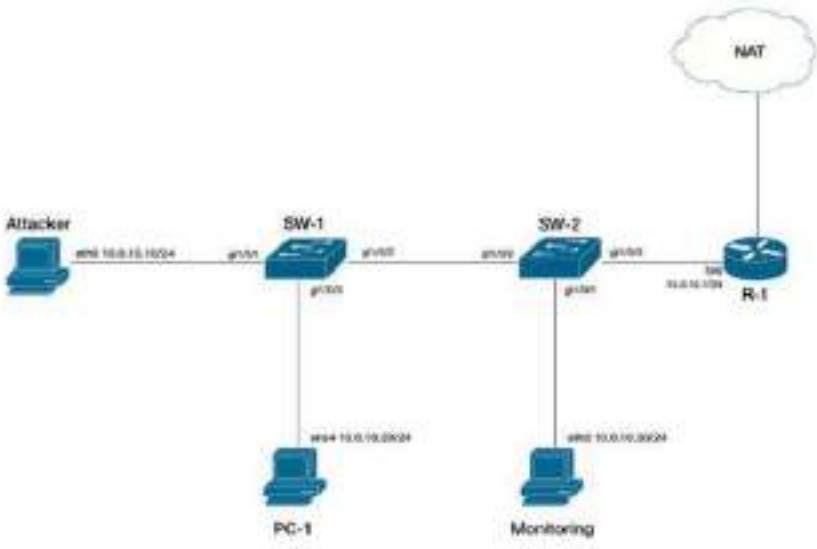


Рис. 1. Топология сети для эксперимента

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.

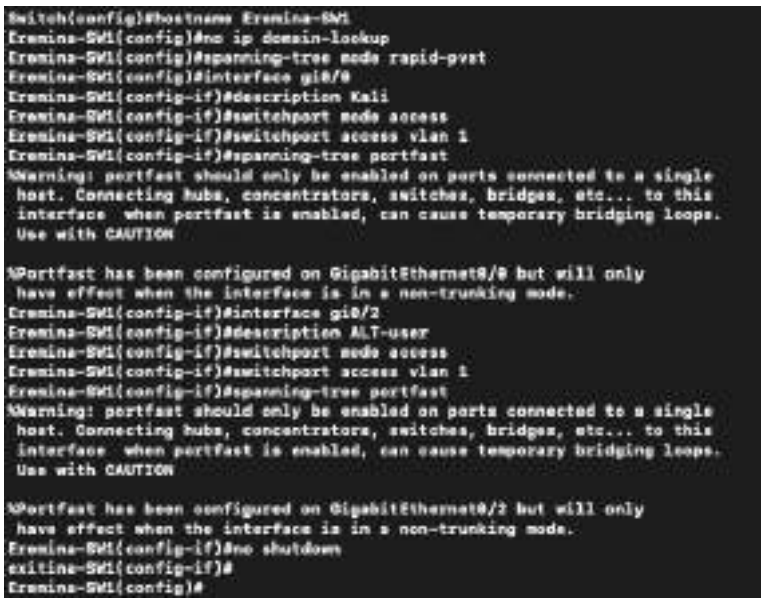


Рис. 2. Конфигурация портов коммутатора Cisco Catalyst 2960 (Eremina-SW1)

–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.

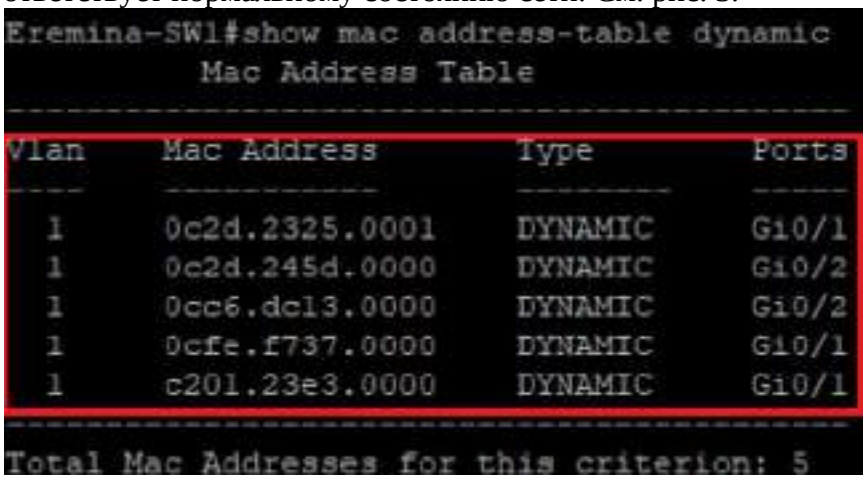


Рис. 3. CAM-таблица коммутатора в штатном режиме, содержащая 5 записей

–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.

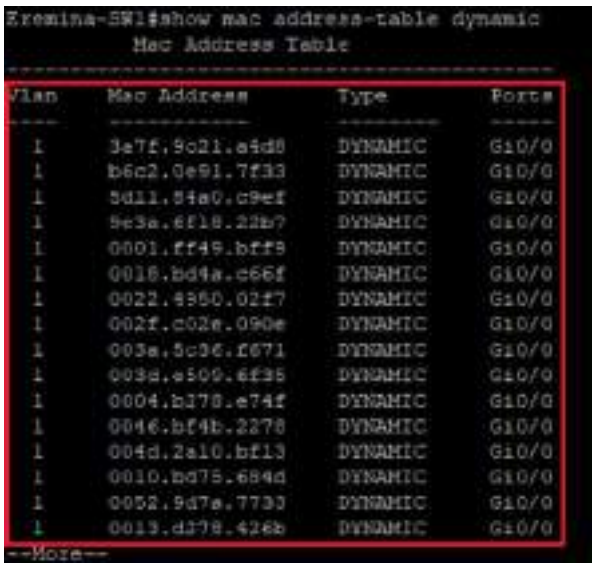


Рис. 4. CAM-таблица во время атаки MAC-flooding

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.

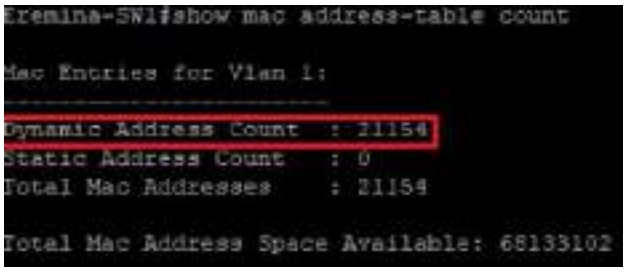


Рис. 5. Подтверждение переполнения CAM-таблицы: 21154 записи в VLAN 1

–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.

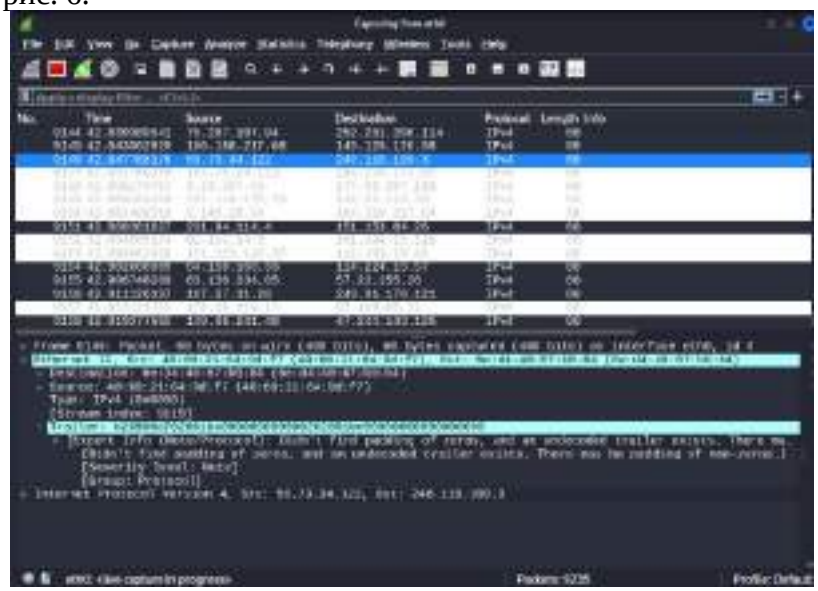


Рис. 6. Анализ трафика в Wireshark: кадры unknown unicast со случайными MAC-адресами

– 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.

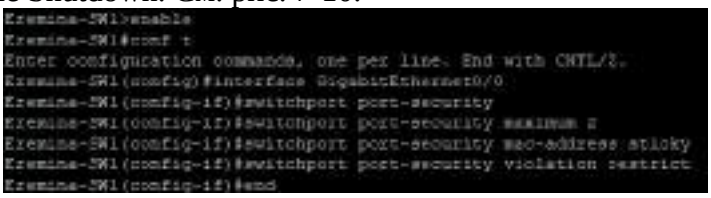


Рис. 7. Настройка Port Security в режиме Restrict с лимитом 2 MAC-адреса

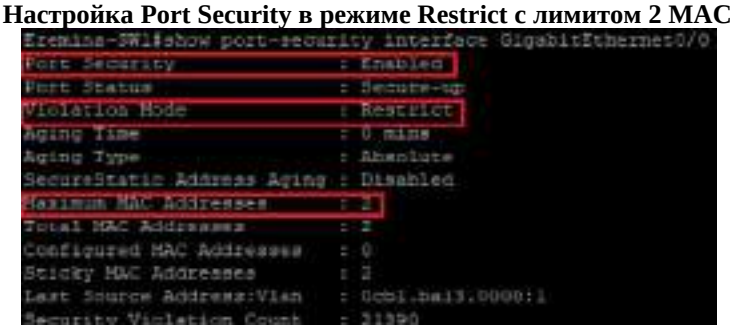


Рис. 8. Port Security в режиме Restrict: 21390 нарушений, порт активен

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.

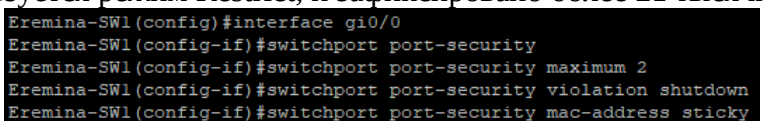


Рис. 9. Настройка Port Security в режиме Shutdown с лимитом 2 MAC-адреса

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.

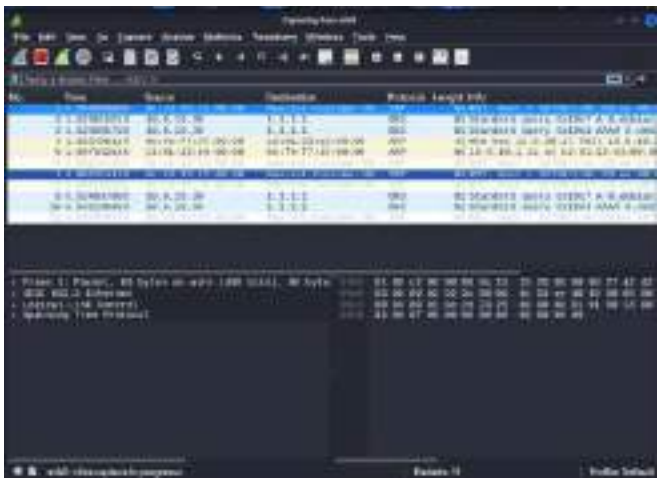


Рис. 11. Мониторинг Wireshark после активации Port Security, прекращение флуда

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.

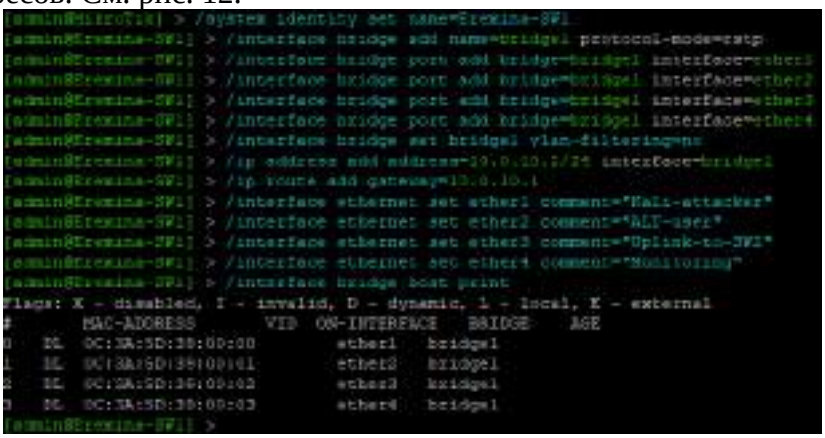


Рис. 12. Настройка коммутатора Mikrotik CRS326

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.

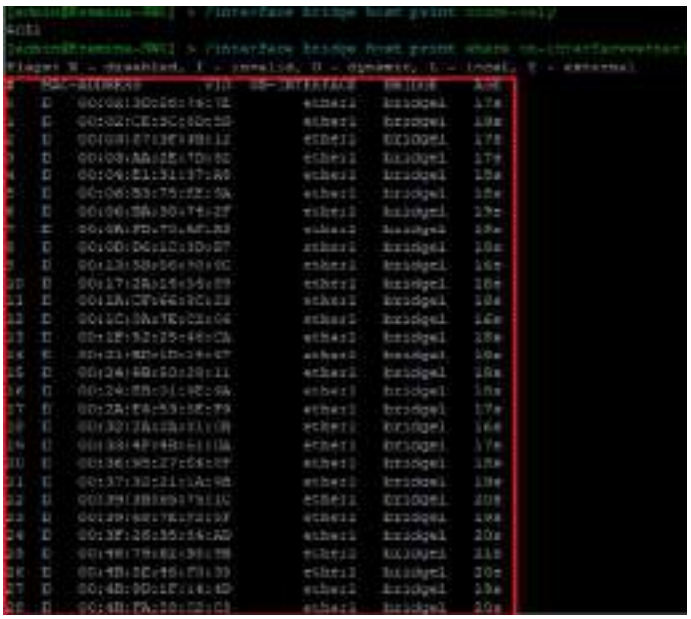


Рис. 13. Результат атаки на Mikrotik: 9051 запись в таблице моста

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.

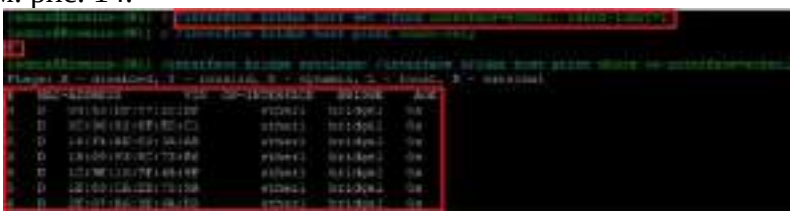


Рис. 14. Таблица MAC-адресов после защиты learn-limit=2 с 6 записями

–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.

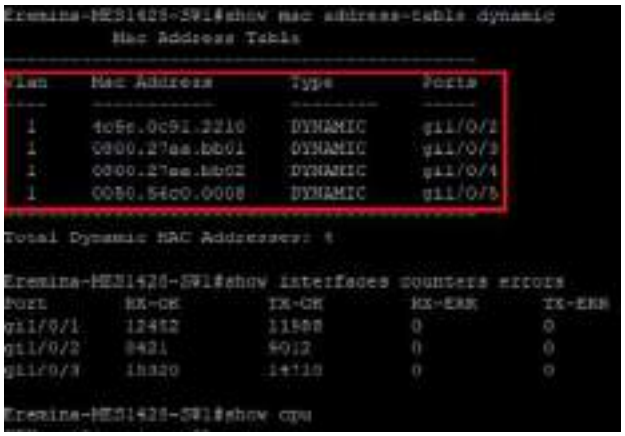


Рис. 15. Eltex MES1428 в штатном режиме: 4 MAC-записи, CPU 3%

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.

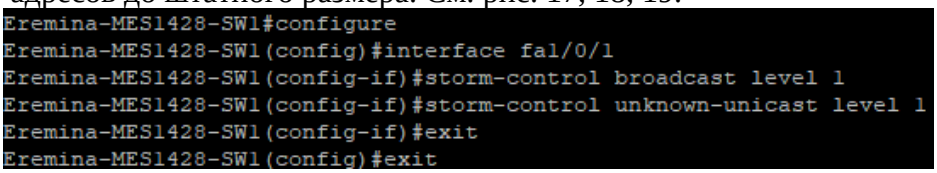


Рис. 17. Конфигурация Storm Control на Eltex

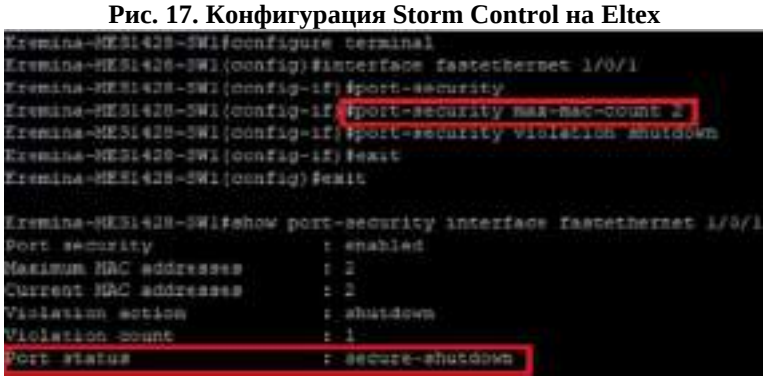


Рис. 18. Настройка Port Security на Eltex с лимитом 2 MAC-адреса

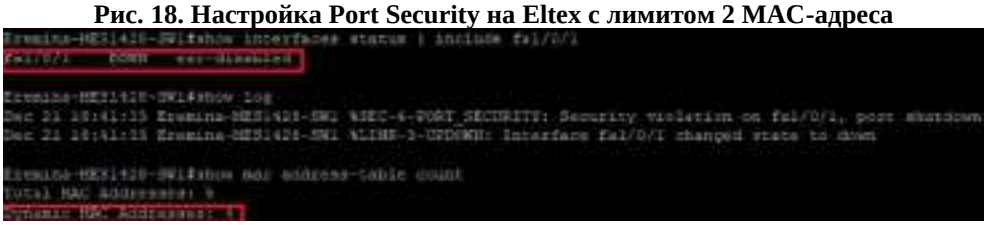


Рис. 19. Результат Port Security на Eltex: таблица MAC-адресов очищена (4 динамические записи)

Результаты

В ходе экспериментального исследования выявлено, что атака MAC-flooding на коммутаторы доступа приводит к увеличению нагрузки на L3 маршрутизатор из-за обработки ARP-запросов, а также unknown unicast-кадров.

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 остается серьезной угрозой для сетей уровня доступа, способной нарушить стабильность инфраструктуры даже при наличии маршрутизатора (L3) в топологии. 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.

Список литературы

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 L3 DEVICES 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

Рубрика 2. Методы и системы защиты информации, информационная безопасность

УДК *004.383.3*

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).

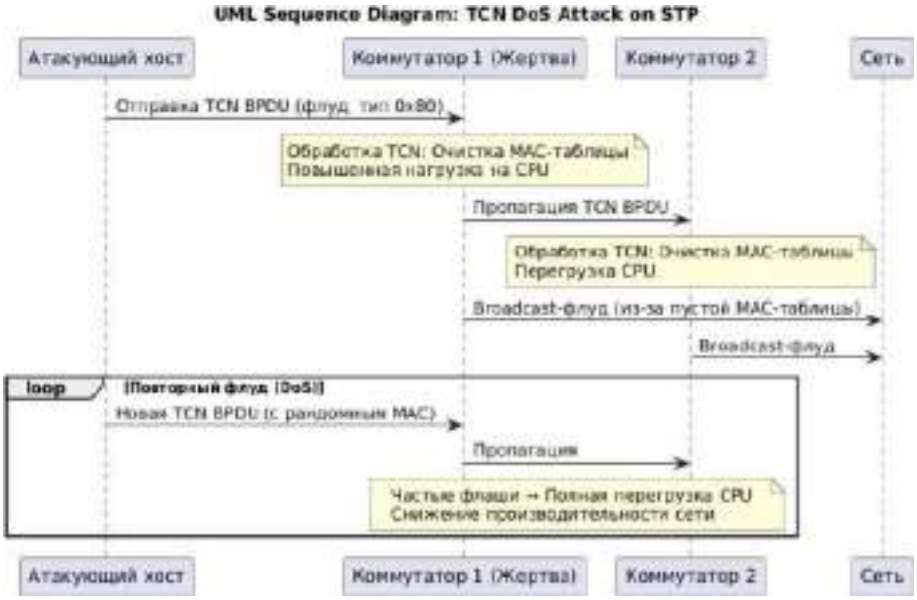


Рис. 1. Механизм реализации TCN DoS-атаки на протокол STP.

- 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 STPP 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 STPP 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 STPP 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.

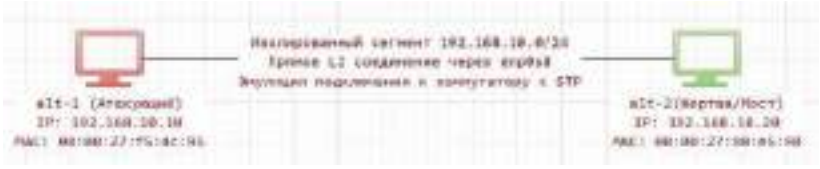


Рис. 2. Топология виртуальной лабораторной сети для моделирования TCN DoS-атаки

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
```

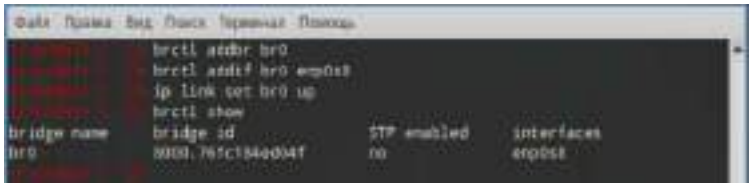


Рис. 3. Создание программного мостового интерфейса в Alt Linux

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).

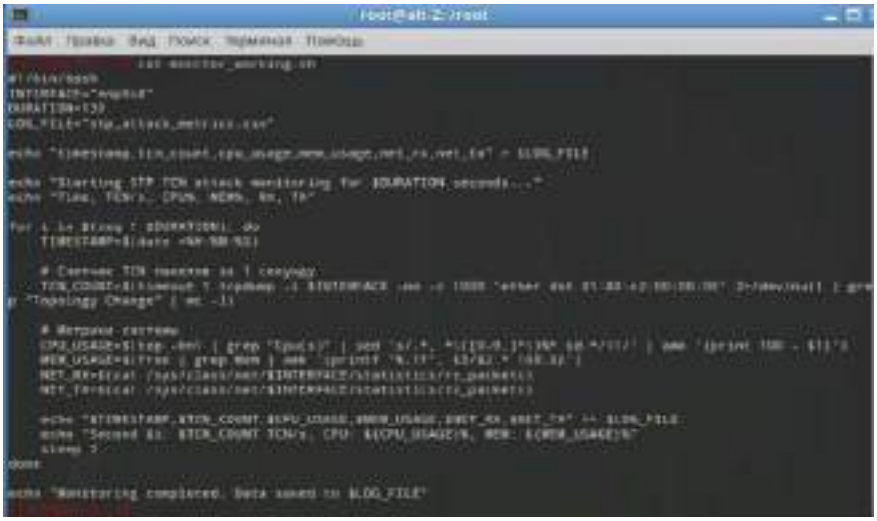


Рис. 5. Скрипт monitor_working.sh для сбора метрик в виртуальной среде

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.

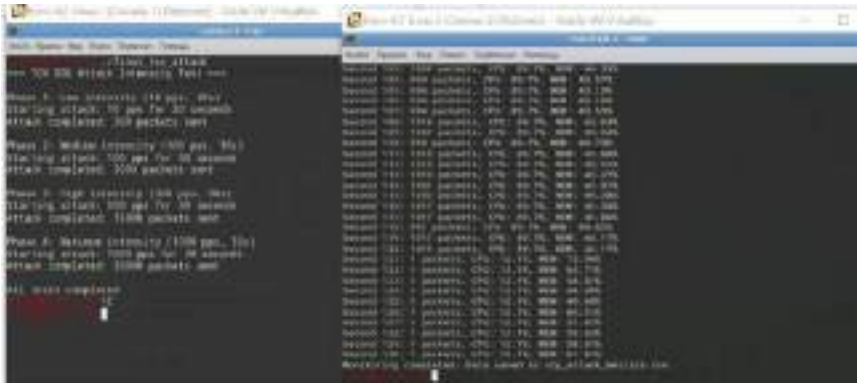


Рис. 6. Запуск скрипта мониторинга на узле alt-2

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.

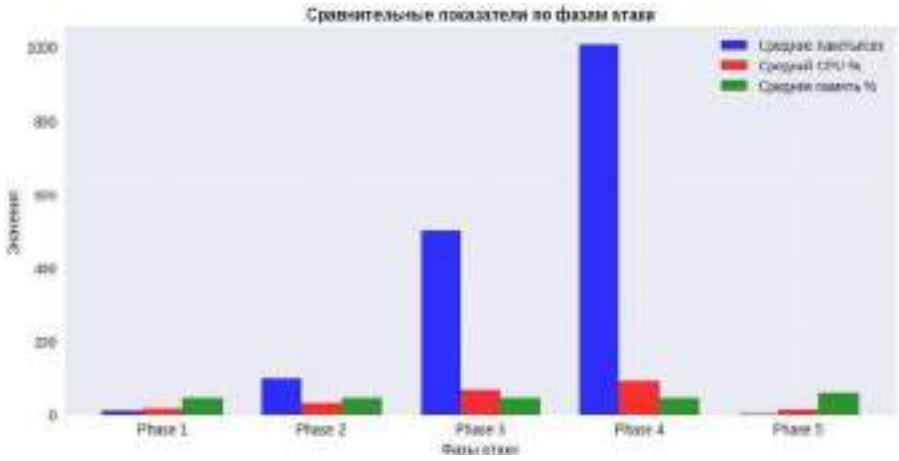


Рис. 8. Сопоставление интенсивности атаки, загрузки CPU и использования памяти

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.

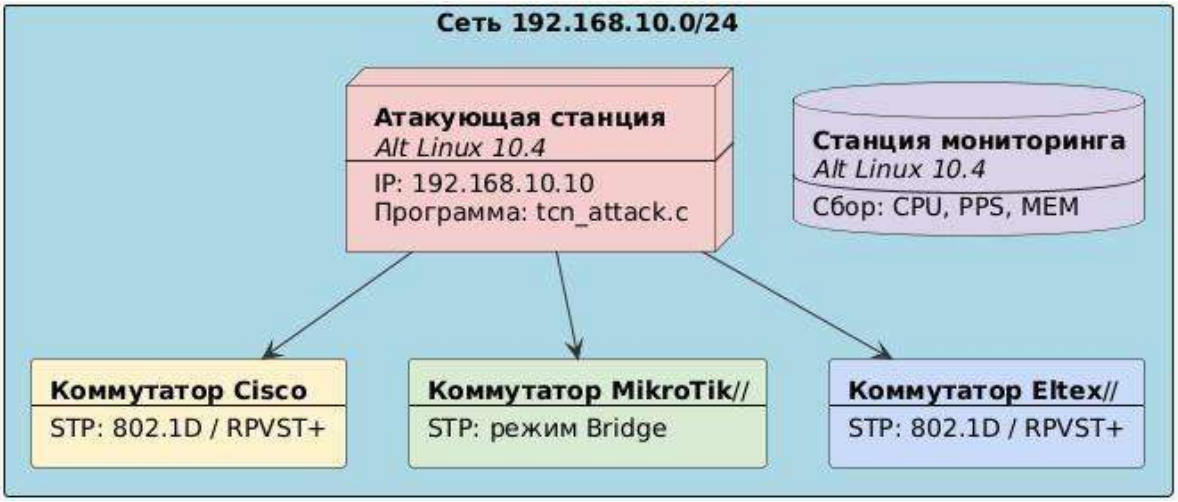


Рис. 9. Топология лабораторного стенда для исследования TCN DoS-атаки на сетевом оборудовании

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

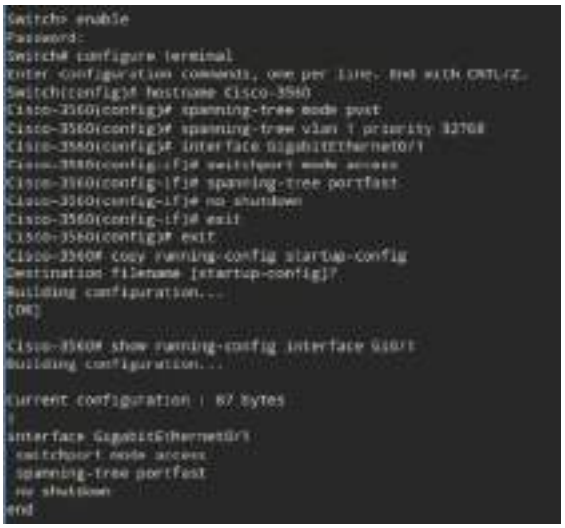


Рис. 10. Конфигурация интерфейса Cisco GigabitEthernet0/1 с включением защитных механизмов STP

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

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 12. 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).

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
```

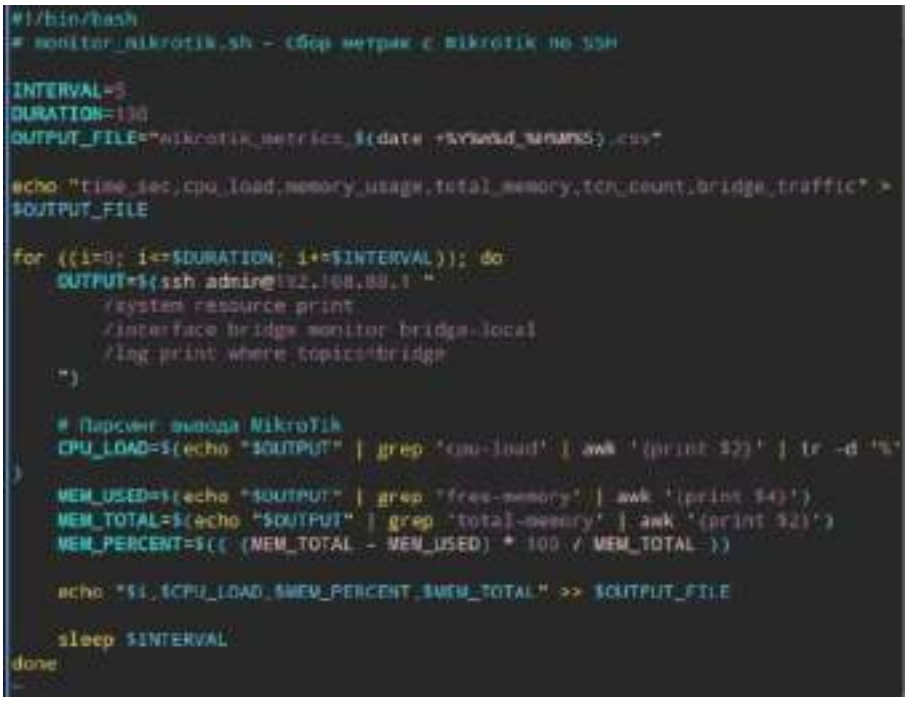


Рис. 15. Скрипт monitor_mikrotik.sh для сбора метрик с оборудования MikroTik

```
#!/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.

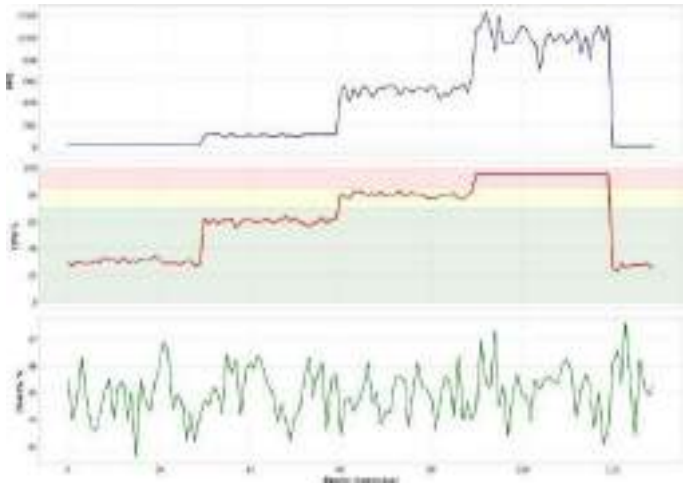


Рис. 17. Динамика метрик MikroTik RouterOS под воздействием TCN DoS-атаки

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 STPP на отечественном сетевом оборудовании использовался Eltex MES. Эксперимент проводился с целью оценки устойчивости

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

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=150
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 19).

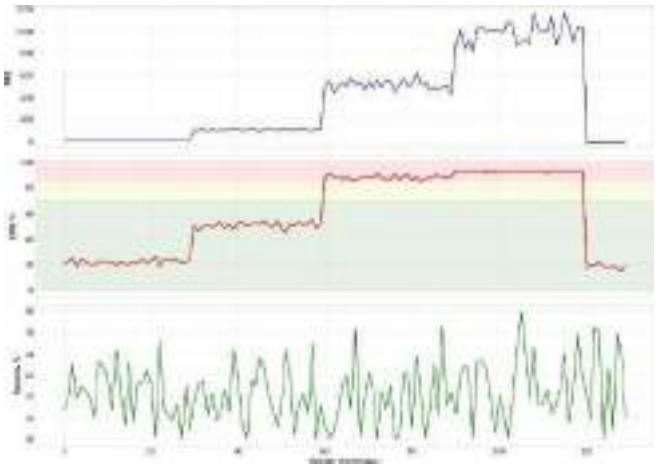


Рис. 21. Динамика метрик коммутатора Eltex под воздействием TCN DoS-атаки

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.
- Аутентификация: BPDU Filter на edge-портах (spanning-tree bpdufilter enable).
- 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.	Аутентификация в RSTP/MSTP проверяет легитимность источника BPDU. Порт-участник (non-Designated) в состоянии "Discarding" игнорирует BPDU.	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.

Список литературы

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.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

УДК *004.056*

А. В. Фоменко [1]***, Я. Ю. Зеленов*** [1]

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

ВОПРОСЫ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ В ДОМЕНЕ WINDOWS: ТОКЕН

Аннотация: рассматривается проблема повышения защищённости корпоративных информационных систем при помощи внедрения двухфакторной аутентификации (2FA) на основе аппаратного токена RuToken в доменной среде Windows. Выделены ключевые уязвимости традиционной парольной аутентификации: фишинг, перехват паролей и пользовательские ошибки. Рассматривается архитектура на основе открытых ключей — PKI, при которой закрытый ключ сохраняется только на физическом носителе, а открытый ключ размещается на компьютере пользователя. Выполнен сравнительный анализ нескольких методов аутентификации: Password-only, SMS / Email OTP, TOTP, FIDO2 / WebAuthn, RuToken + PKI. В результате определены их преимущества и уязвимые стороны. В качестве основных критериев сопоставления использованы устойчивость к фишингу и атакам Man-in-the-Middle, зависимость от интернет-соединения, возможность централизованного управления и сложность развёртывания. Отдельный акцент сделан на практическом внедрении RuToken + PKI в доменной среде, функционирующей без доступа к интернету. Показана настройка Active Directory Certificate Services (AD CS), групповых политик, шаблонов сертификатов, после которых возможен вход в учётную запись пользователя при помощи смарт карты в виде RuToken. При этом выявлены базовые неудобства использования данной архитектуры в доменной среде. Зависимость от криптодрайверов, риск потери физического носителя или PIN-кода и др. Эксперимент был проведён на базе Windows Server 2025 и Windows 11, развёрнутых на виртуальной машине Oracle VirtualBox. Результатом является демонстрация эффективность PKI-подхода в доменной среде по сравнению с классическими уровнями защиты

Ключевые слова: двухфакторная аутентификация, RuToken, инфраструктура открытых ключей (PKI), Active Directory Certificate Services (AD CS), Windows-домен, информационная безопасность

Введение

Основной целью кибератак в нынешнее время в основном являются корпоративные информационные системы из-за большого количества сотрудников в организации, именно компрометация пользовательских данных является главной проблемой при атаке. Привычная парольная аутентификация демонстрирует низкую устойчивость к различным векторам атак. Фишинг, перехват трафика и другим. Поэтому внедрение надёжной защиты учётных данных пользователей становится необходимостью в наше время. Для увеличения надёжности по всему миру развиваются двухфакторные аутентификации (2FA) при помощи различных решений, особенно актуально проблема в изолированных от интернета сетях, в которых невозможна интеграция с облачными сервисами.

Объектом исследования выступают информационные системы, построенные на базе доменной архитектуры Windows с централизованным управлением через Active Directory. Предметом исследования являются архитектурные особенности и эффективность реализации двухфакторной аутентификации на основе аппаратных токенов RuToken в условиях отсутствия интернет-соединения.

Целью работы является проведение сравнительного анализа методов двухфакторной аутентификации и обоснование лидерства PKI-подхода с использованием RuToken в offline доменных средах.

Проблема надёжной аутентификации широко освещена в нормативных и научных источниках. NIST SP 800-63B [1] формализует требования к многофакторной аутентификации и выделяет phishing-resistant методы — FIDO2/WebAuthn и PKI на основе аппаратных токенов. Однако стандарт ориентирован на современные облачные среды и не рассматривает особенности их применения в изолированных Windows-доменах. Для повышения надежности идентификации пользователей и устройств, в компании Google разрабатывают схемы двухэтапного подтверждения прав доступа к аккаунту [7],

основанные на одноразовых паролях и технологии открытого ключа. В российской практике ГОСТ Р 57580.1–2017 [4] закладывает основу для использования PKI с аппаратным хранением ключей, а документация Microsoft [5] и компании «Aktiv» [2] подтверждает техническую возможность интеграции RuToken в Active Directory. Практическая значимость положений ГОСТ Р 57580.1–2017 подтверждается результатами исследования Гнездилова [6], в котором показано, что использование аппаратной двухфакторной аутентификации способствует снижению количества инцидентов информационной безопасности. В отечественной научной литературе также уделяется внимание вопросам моделирования и отработки подобных механизмов в учебно-тренировочных средах, что отражено в работе В. С. Грекова и А. Г. Уймина [3].

Методология и критерии сравнения

Для определения эффективности различных способов реализации двухфакторной аутентификации в изолированной Windows-доменной инфраструктуре был использован метод сравнительного анализа. Оценка проводилась по шести основным критериям, позволяющим сопоставить рассматриваемые решения с точки зрения безопасности, удобства внедрения и применимости в корпоративной среде.

В рамках исследования были выбраны пять распространённых подходов к аутентификации: классическая парольная схема, одноразовые коды, передаваемые через SMS или электронную почту, временные одноразовые пароли TOTP, механизмы FIDO2/WebAuthn, а также PKI-аутентификация с использованием аппаратного токена RuToken. Выбор данных методов обусловлен их практическим распространением в организациях, а также существенными различиями в архитектуре и принципах работы. Это позволяет более наглядно определить преимущества, ограничения и потенциальные риски каждого варианта. Одним из основных критериев является устойчивость к фишинговой атаке. Фишинг-атаки остаются главным вектором компрометации учётных данных, поскольку пользователи вводят свои реквизиты на поддельных сайтах. Метод может считаться устойчивым к фишингу, только если злоумышленник не может повторно использовать полученные данные. Парольные и OTP-методы уязвимы, так как передаваемый ключ не привязан к домену. FIDO2 и PKI на аппаратных токенах используют иную модель: в процессе аутентификации формируется криптографическая подпись, связанная с конкретным доменом. За пределами легитимного контекста такая подпись не имеет практической ценности.

Следующим критерием сравнения выступает устойчивость к атакам типа «человек посередине» — MITM. Методы, при которых секрет передаётся по сети в открытом виде либо представлен динамическим кодом, при перехвате трафика теряют значительную часть защитных свойств, особенно при некорректной настройке или отсутствии защищённого TLS-соединения. PKI и FIDO2 демонстрируют более высокий уровень устойчивости к данному классу атак: закрытый ключ не покидает устройство, а процедура аутентификации строится по схеме «запрос — ответ», где каждое подключение имеет уникальный криптографический контекст.

Для изолированных корпоративных сетей отдельное значение имеет зависимость механизма аутентификации от интернета и внешних сервисов. SMS/Email OTP, а также облачные TOTP-решения требуют постоянного обращения к внешней инфраструктуре, поэтому их применение в offline-средах ограничено или невозможно. В то же время RuToken + PKI и локально развёрнутый TOTP могут функционировать без подключения к внешним ресурсам. Это делает их применимыми в инфраструктурах, изолированных от сети Интернет и облачных платформ.

Для корпоративных систем критически важна централизованная управляемость. Ключевыми требованиями являются настройка единых политик безопасности, отзыв доступа, управление параметрами аутентификации и принудительное применение правил через Active Directory. В рассматриваемой Windows-доменной среде полную интеграцию с

групповыми политиками и механизмами доменного администрирования обеспечивают только классическая парольная аутентификация и PKI-инфраструктура на базе AD CS.

FIDO2, несмотря на высокий уровень криптографической защищённости, в изолированной Windows-доменной среде без Azure AD или специализированных сторонних компонентов не обеспечивает сопоставимого уровня централизованного управления. По этой причине его использование в offline-инфраструктуре ограничивается как техническими, так и организационными условиями. Не менее значимым параметром является сложность развёртывания выбранного метода аутентификации. Парольная схема требует минимальных трудозатрат, поскольку изначально поддерживается доменной инфраструктурой Windows. В то же время внедрение PKI или FIDO2 предполагает настройку дополнительных компонентов: центра сертификации, шаблонов сертификатов, криптографических провайдеров, драйверов токенов, политик безопасности и механизмов управления жизненным циклом учётных данных. Несмотря на повышенную сложность развёртывания самого метода, это гарантия высокой степени защиты информационной системы.

Основным фактором безопасности является место и способ хранения закрытого ключа. Если ключ может быть извлечён из устройства в TOTP-приложениях, то система является уязвимой для атаки со стороны злоумышленника. В RuToken и FIDO2 закрытый ключ генерируется и хранится в аппаратном защищённом элементе и является невыгружаемым, что соответствует требованиям современных стандартов.

Для количественной оценки эффективности методов была проведена оценка трудоёмкости внедрения и замер времени аутентификации в ходе эксперимента. Результаты сведены в таблицу 1.

Таблица 1. Сравнительная оценка методов аутентификации

Метод	Время внедрения	Время входа	Стоимость внедрения	Риск отказа
Password-only	0 ч	3–5 сек	Бесплатно	Низкий (забывание пароля)
SMS/Email OTP	4–8 ч	15–30 сек	Средняя	Средний (задержки сети)
TOTP (App)	2–4 ч	10–15 сек	Бесплатно	Средний (рассинхронизация)
FIDO2/WebAuthn	8–12 ч	5–7 сек	Высокая	Низкий
RuToken + PKI	12–16 ч (AD CS + драйверы)	8–12 сек	Высокая	Низкий (ошибка PIN)

Экспериментальная часть

Сеть, состоящая из двух устройств на основе Windows Server 2025 и Windows 11 является полностью изолированной от глобальной сети интернет. Перед началом исследования устанавливаем необходимое программное обеспечение для корректной работы RuToken. Для этого через официальный сайт скачиваем драйвер поддержки Рутокена 2.0, устанавливаем на обе машины.

Установка и настройка операционных систем на машины. На машине DC создаём домен, настраиваем сеть, устанавливаем AD CS, DNS. В домен вводим машину CLI, устанавливаем необходимое ПО для работы Рутокена (драйвер и криптосервис) на обе машины, без этой установки машины будут воспринимать токен как обычную флешку

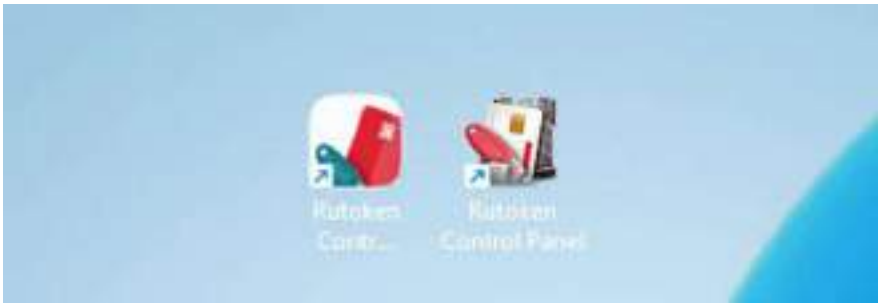


Рис. 1. Установка программного обеспечения и драйверов RuToken на виртуальных машинах доменной среды

Устанавливаем AD CS на машину DC с выбором типа Enterprise Root CA, обеспечивающего интеграцию с Active Directory и автоматическое распространение корневого сертификата на компьютеры домена. После установки выполнили начальную конфигурацию центра сертификации

Рис. 2. Добавление роли Active Directory Certificate Services на контроллере домена Windows Server

Создание и публикация пользовательского шаблона сертификата на основе стандартного шаблона «Smart Card User» под названием «Rutoken_Logon» с предоставленными разрешениями Enroll, Autoenroll. Важным этапом конфигурирования шаблона Rutoken_Logon является настройка криптографических параметров на вкладке Cryptography. В поле Cryptography Service Provider выбран поставщик, соответствующий установленному драйверу Рутокен Aktiv Co. RuToken CSP для CAPI-совместимых приложений, что гарантирует генерацию закрытого ключа непосредственно в защищённой памяти аппаратного носителя и исключает возможность его экспорта в программное хранилище. Минимальная длина ключа установлена на уровне 2048 бит, алгоритм хеширования — SHA-256, что соответствует требованиям ГОСТ Р 57580.1–2017 [4] к стойкости ключевой информации в инфраструктуре открытых ключей. Дополнительно активирована опция Request must use a specific provider, исключающая выпуск сертификата с ключом, сгенерированным сторонним криптопровайдером. Данные настройки обеспечивают выполнение ключевого требования безопасной архитектуры PKI: закрытый ключ никогда не покидает аппаратный токен, а все криптографические операции выполняются внутри защищённого элемента Рутокен.

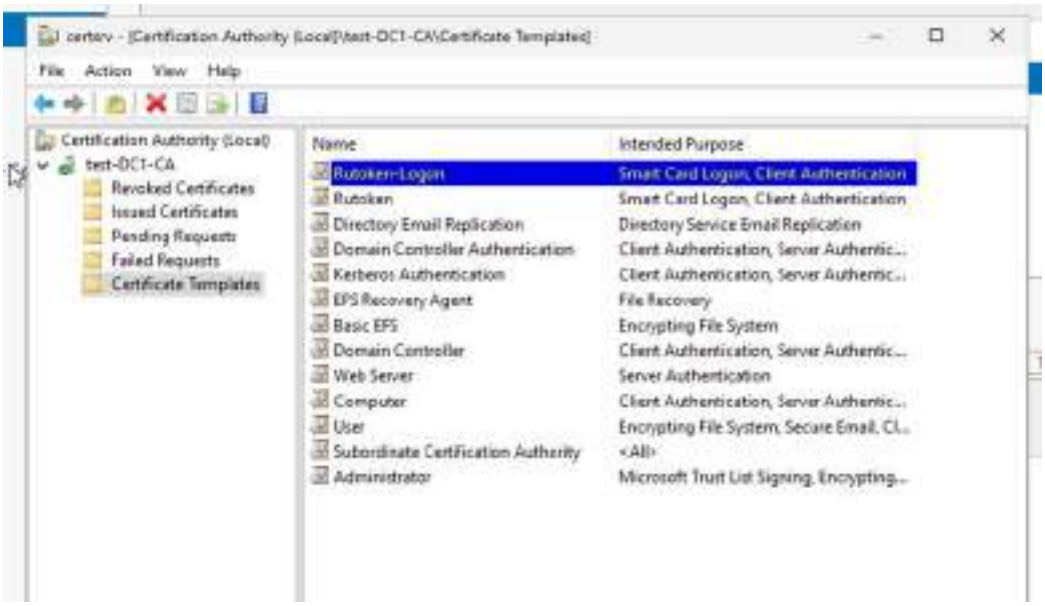


Рис. 3. Создание пользовательского шаблона сертификата Rutoken_Logon на основе шаблона Smart Card User

Для выпуска сертификатов пользователям домена, на клиентской машине через консоль MMC → Certificates (Current User) был запущен мастер Certificate Enrollment. Выбран целевой шаблон и инициирован запрос сертификата. После вставки токена и ввода PIN-кода, закрытый ключ создавался непосредственно на смарт-карте (токене), а полученный сертификат автоматически установился в соответствующее устройство. При успешной регистрации сертификат появлялся в хранилище Personal → Certificates, где можно было убедиться в наличии критических атрибутов «Smart Card Logon» и «Client Authentication»

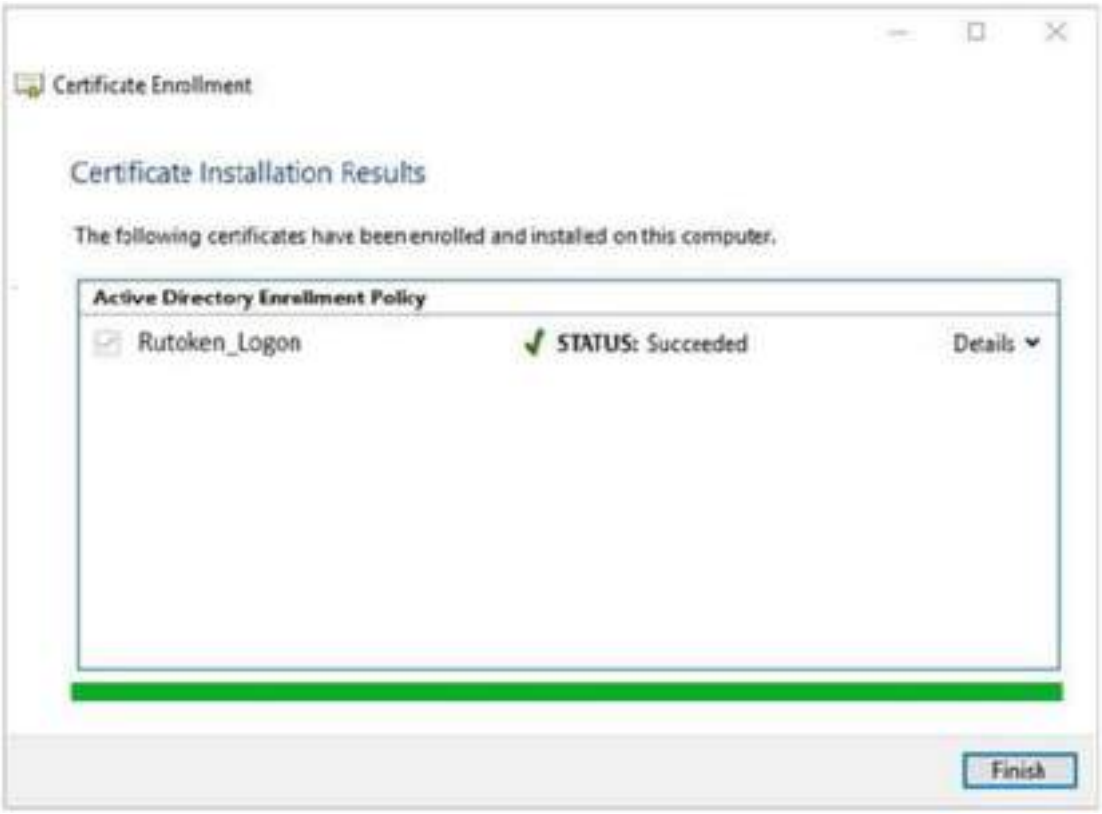


Рис. 4. Выпуск пользовательского сертификата Rutoken_Logon через мастер Certificate Enrollment

После настройки групповых политик для пользователя домена при входе на CLI требуется вводить не только пароль, но также обязательным требованием является

владение токеном, зарегистрированным на DC (контроллере домена)

Рис. 5. Проверка входа пользователя в доменную учётную запись с использованием аппаратного токена RuToken

Заключение

Таким образом анализ методов двухфакторной аутентификации показал, что в условиях изолированной Windows-доменной среде без доступа к интернет-соединению наиболее эффективным и безопасным решением является PKI-подход на основе аппаратного токена RuToken. В отличие от OTP-методов, уязвимых к фишингу и MITM-атакам, и FIDO2, RuToken обеспечивает высокий уровень защиты за счёт хранения невыгружаемого закрытого ключа на устройстве, полной совместимости с Active Directory и независимости от внешних сервисов. Экспериментальная верификация на основе Windows Server 2025 и Windows 11 подтвердила работоспособность решения, несмотря на операционные ограничения, связанные со сложностью развёртывания и зависимостью от криптодрайверов. В случаях, где приоритетом являются безопасность и возможность централизованного управления, данный подход представляет собой наиболее верное и практически применимое решение для защищённых информационных систем.

Список литературы

1. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management : special publication / P. A. Grassi, J. L. Fenton, E. M. Newton [et al.]. – Gaithersburg : National Institute of Standards and Technology, 2017. – URL: https://pages.nist.gov/800-63-3/sp800-63b.html (дата обращения: 02.01.2025). – Текст : электронный.
2. Гроссе, Э. Многофакторная аутентификация / Э. Гроссе, М. Упадхаяй // Информационная безопасность. – 2013. – № 4. – С. 42–47. – EDN SDXTOH.
3. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер : национальный стандарт Российской Федерации. – Москва :

Стандартинформ, 2017. – URL: https://regulhub.kaspersky.ru/upload/iblock/71a/k99732yk7w1rrz8d3yg3y4hwqzmg8bcw.pdf (дата обращения: 04.01.2025). – Текст : электронный.
4. Smart Card Logon Architecture // Microsoft Learn : official documentation portal. – Redmond, 2025. – URL: https://learn.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-architecture (дата обращения: 05.01.2025). – Текст : электронный.
5. Рутокен : документация для разработчиков и администраторов // Рутокен : официальный сайт / АО «Актив». – Москва. – URL: https://dev.rutoken.ru (дата обращения: 02.01.2025). – Текст : электронный.
6. Гнездилов, Р. Р. Многофакторная аутентификация и эффективность обеспечения безопасности информации при доступе к ресурсам телекоммуникационных сетей / Р. Р. Гнездилов // Гагаринские чтения – 2018 : сборник тезисов докладов XLIV Международной молодежной научной конференции, Москва – Ахтубинск – Байконур, 17–20 апреля 2018 года. – Москва ; Ахтубинск ; Байконур : Московский авиационный институт (национальный исследовательский университет), 2018. – Т. 1. – С. 193. – EDN XMKQST.
7. Греков, В. С. Стратегии создания модели сети предприятия в рамках киберполигона для эффективной подготовки кадров в области кибербезопасности / В. С. Греков, А. Г. Уймин // Вестник кибербезопасности. – 2024. – № 3. – С. 45–58. – URL: https://www.elibrary.ru/item.asp?id=80499001 (дата обращения: 04.01.2025). – Текст : электронный.

References

1. Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). National Institute of Standards and Technology. https://pages.nist.gov/800-63-3/sp800-63b.html
2. Grosse, E., & Upadhyay, M. (2013). Multi-factor authentication. *Information Security*, (4), 42–47.
3. GOST R 57580.1–2017. (2017). *Security of financial (banking) operations. Information protection of financial organizations. Basic set of organizational and technical measures*. Standartinform. https://regulhub.kaspersky.ru/upload/iblock/71a/k99732yk7w1rrz8d3yg3y4hwqzmg8bcw.pdf
4. Microsoft. (2025). *Smart card logon architecture*. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-architecture
5. Aktiv Co. (n.d.). *Rutoken: Documentation for developers and administrators*. Rutoken. https://dev.rutoken.ru
6. Gnezdilov, R. R. (2018). Multi-factor authentication and the effectiveness of information security in accessing telecommunication network resources. In *Gagarin Readings – 2018: Proceedings of the XLIV International Youth Scientific Conference, Moscow – Akhtubinsk – Baikonur, April 17–20, 2018* (Vol. 1, p. 193). Moscow Aviation Institute.
7. Grekov, V. S., & Uymin, A. G. (2024). Strategies for creating an enterprise network model within a cyber range for effective training of cybersecurity personnel. *Cybersecurity Bulletin*, (3), 45–58. https://www.elibrary.ru/item.asp?id=80499001

Информация об авторах

Фоменко Артём Владимирович — студент 3-его курса, факультет КБ ТЭК, группы КИ-23-01 ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail:

1studentnow1@gmail.com

Зеленов Ярослав Юрьевич — студент 3-его курса, факультет КБ ТЭК группы КИ-23-01 ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: mobzila567@gmail.com

A. V. Fomenko 1, Ya. Yu. Zelenov 1

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

TWO-FACTOR AUTHENTICATION ISSUES IN THE WINDOWS DOMAIN: TOKEN

Abstract. This article examines the problem of increasing the security of corporate information systems by implementing two-factor authentication (2FA) based on the RuToken hardware token in a Windows domain environment. Key vulnerabilities of traditional password authentication, phishing, password interception, and user errors are highlighted. A public key infrastructure (PKI) architecture is explored, where the private key remains only on the physical medium, and the public key is stored on the user's computer. A comparative analysis of several user authorization methods, such as password authentication (Password-only), SMS / Email OTP (One-Time Password), TOTP (Time-based One-Time Password), FIDO2 / WebAuthn, and RuToken + PKI, is conducted, as a result of which their vulnerabilities and advantages are identified. The main comparison criteria are vulnerability to phishing and MITM (Man-in-the-Middle) attacks, dependence on an internet connection, the possibility of centralized management, and the complexity of deployment. Particular attention is given to the practical implementation of RuToken + PKI in a domain environment without internet access. The article demonstrates the configuration of Active Directory Certificate Services (AD CS), group policies, and certificate templates, which enable user account login using a RuToken smart card. The article also identifies the key challenges of using this architecture in a domain environment, including dependence on cryptographic drivers, the risk of losing the physical drive or PIN, and more. The experiment was conducted using Windows Server 2025 and Windows 11, deployed on an Oracle VirtualBox virtual machine. The result demonstrates the effectiveness of the PKI approach in a domain environment compared to traditional security levels.

Keywords: two-factor authentication, RuToken, public key infrastructure (PKI), Active Directory Certificate Services (AD CS), Windows domain, information security

About the Authors

Artem Vladimirovich Fomenko, third-year student, Faculty of Design Bureau of Fuel and Energy Complex, group KI-23-01, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: 1studentnow1@gmail.com

Yaroslav Yuryevich Zelenov, third-year student, Faculty of Design Bureau of Fuel and Energy Complex, group KI-23-01, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: mobzila567@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

Почта России · Москва, Ленинский пр-кт, 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 (4)

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: 10.01.2024.

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