УДК 004.056

РАЗРАБОТКА И ЭКСПЕРИМЕНТАЛЬНАЯ АПРОБАЦИЯ МЕТОДА ОБНАРУЖЕНИЯ ARP-SPOOFING АТАК НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА И ARP-ТАБЛИЦ

Рамазанова Г.Р.,Марченко Р.О., студент, направление подготовки Информационная безопасность, Российский государственный университет нефти и газа им. И.М. Губкина, Москва,

Научный руководитель: Павловский В.В., кандидат технических наук, доцент кафедры информационной безопасности, Московский технический университет, Москва,

Аннотация. *В статье рассматривается проблема обеспечения безопасности локальных компьютерных сетей от атак типа ARP-spoofing. Актуальность исследования обусловлена ростом числа сетевых угроз и простотой реализации данной атаки, приводящей к перехвату трафика. Целью работы является разработка и практическая апробация метода, позволяющего своевременно обнаруживать ARP-spoofing. Предложенный метод основан на комплексном анализе двух факторов: фиксации поступления незапрошенного ARP-ответа и проверке последующего изменения в локальной ARP-таблице узла. Для проверки метода был разработан программный комплекс и проведен эксперимент на тестовом стенде с использованием реального оборудования и ПО для проведения атак. Результаты эксперимента подтвердили высокую эффективность и достоверность предложенного метода. Разработанное решение может быть использовано для защиты корпоративных сетей, а также в учебном процессе для демонстрации механизмов сетевых атак и методов противодействия.*

Ключевые слова: ARP-spoofing, обнаружение атак, сетевая безопасность, ARP-таблица, сетевой трафик, метод обнаружения, информационная безопасность.

DEVELOPMENT AND EXPERIMENTAL TESTING OF AN ARP-SPOOFING ATTACK DETECTION METHOD BASED ON NETWORK TRAFFIC AND ARP TABLE ANALYSIS

Рамазанова Г.Р.,Марченко Р.О., студент, направление подготовки Информационная безопасность, Российский государственный университет нефти и газа им. И.М. Губкина, Москва,

Научный руководитель: Павловский В.В., кандидат технических наук, доцент кафедры информационной безопасности, Московский технический университет, Москва,

Abstract. The article addresses the problem of securing local computer networks against ARP-spoofing attacks. The relevance of the research is driven by the growing number of network threats and the simplicity of implementing this attack, which leads to traffic interception. The aim of this work is to develop and practically test a method for timely detection of ARP-spoofing. The proposed method is based on a comprehensive analysis of two factors: detecting the receipt of an unsolicited ARP reply and verifying a subsequent change in the host's local ARP table. To validate the method, a software tool was developed, and an experiment was conducted on a testbed using real hardware and attack software. The experimental results confirmed the high efficiency and reliability of the proposed method. The developed solution can be used to protect corporate networks, as well as in the educational process to demonstrate the mechanisms of network attacks and countermeasures.

Keywords: ARP-spoofing, attack detection, network security, ARP table, network traffic, detection method, information security.

ВВЕДЕНИЕ

Актуальность. В современном мире, где информационные технологии пронизывают все сферы деятельности, обеспечение безопасности компьютерных сетей является одним из важнейших требований к инфраструктуре любого предприятия. Сетевые атаки становятся все более изощренными и могут нанести значительный финансовый и репутационный ущерб [3]. Одной из наиболее распространенных и опасных угроз для локальных сетей является атака типа ARP-spoofing. Ее суть заключается в отправке ложных ARP-ответов для перенаправления сетевого трафика через узел злоумышленника, что позволяет ему перехватывать, анализировать или модифицировать передаваемые данные [1]. Согласно данным аналитических отчетов, количество таких атак демонстрирует стабильный рост, что подтверждает актуальность проблемы.

Проблемой обнаружения и противодействия ARP-spoofing занимались многие исследователи. Так, А. Ю. Крылов и Н. А. Шитов предложили распределенную систему выявления и предотвращения атаки на основе объектного подхода и конечных автоматов, где атака рассматривается как объект, меняющий свое состояние [2]. Н. В. Шишов и В. А. Ломазов исследовали влияние ARP-spoofing атак на системы электронного документооборота, используя для моделирования аппарат сетей Петри-Маркова [3]. Эти работы заложили важную теоретическую основу.

Уже известно, что уязвимость лежит в самой архитектуре протокола ARP (Address Resolution Protocol), который не предусматривает механизмов проверки подлинности ARP-ответов [2, с. 18]. Это позволяет злоумышленнику с легкостью подменять MAC-адреса в ARP-таблицах легитимных узлов. Существуют теоретические модели обнаружения, такие как анализ последовательности событий в сети или отслеживание состояний потенциальной атаки.

Однако, как отмечает Р. М. Алиев, наряду с большим количеством теоретических публикаций, вопросы разработки и практической апробации конкретных программных комплексов, которые можно было бы легко развернуть и использовать для защиты или обучения, освещены недостаточно [1]. Часто предлагаемые модели остаются на теоретическом уровне без результатов экспериментов на реальном оборудовании. Настоящее исследование направлено на то, чтобы восполнить этот пробел путем разработки и тестирования конкретного, практически реализуемого метода обнаружения ARP-spoofing атак.

Объект исследования – процессы обеспечения информационной безопасности в локальных компьютерных сетях.

Предмет исследования – метод обнаружения атак типа ARP-spoofing, основанный на совместном анализе ARP-пакетов в сетевом трафике и динамических изменений в ARP-таблице узла сети.

Цель исследования – разработать и экспериментально апробировать программный комплекс, реализующий предложенный метод, для повышения уровня защищенности информационных процессов в компьютерных системах за счет своевременного обнаружения атак типа ARP-spoofing.

ЛИТЕРАТУРНЫЙ ОБЗОР

Для полного понимания проблематики необходимо определить ключевые термины.

Address Resolution Protocol (ARP) – это протокол, используемый для определения MAC-адреса (адреса канального уровня) узла по его известному IP-адресу (адресу сетевого уровня). Когда узлу необходимо отправить данные другому узлу в той же локальной сети, он проверяет свою ARP-таблицу. Если запись для нужного IP-адреса отсутствует, узел отправляет широковещательный ARP-запрос. Узел с искомым IP-адресом отвечает ARP-ответом, содержащим его MAC-адрес, который заносится в таблицу отправителя [2, с. 18].

ARP-таблица – это динамически обновляемый кэш на каждом сетевом узле, в котором хранятся соответствия между IP-адресами и MAC-адресами других устройств в сети.

ARP-spoofing (ARP-отравление) – тип сетевой атаки, при которой злоумышленник отправляет поддельные (ложные) ARP-сообщения в локальную сеть. Суть атаки заключается в том, что злоумышленник связывает свой MAC-адрес с IP-адресом другого узла (например, шлюза по умолчанию), в результате чего трафик от «жертвы» к этому узлу начинает проходить через компьютер злоумышленника. Это позволяет реализовать атаку «человек посередине» (Man-in-the-Middle) [2, с. 19].

На основе анализа литературы можно сформулировать следующие гипотезы исследования:

1. H1: Метод, основанный на одновременной фиксации получения unsolicited (незапрошенного) ARP-ответа и проверке факта изменения соответствующей записи в локальной ARP-таблице, позволяет с высокой степенью достоверности обнаруживать атаки типа ARP-spoofing.
2. H2: Программный комплекс, реализующий данный метод, является эффективным и низкоресурсным инструментом для обнаружения атак в реальных условиях и может быть использован как в практических целях для защиты сетей, так и в учебном процессе.

МЕТОДЫ ИССЛЕДОВАНИЯ

Тип исследования: экспериментальное исследование с использованием тестового стенда.

Характеристика выборки: в качестве выборки выступал тестовый сетевой сегмент, состоящий из трех персональных компьютеров в одной локальной сети Ethernet:

- Узел 1 («Атакующий»): ПК с ОС Parrot Security, на котором запускался инструмент для проведения атаки.
- Узел 2 («Жертва»): ПК с ОС Windows, на котором был установлен разработанный программный комплекс для обнаружения атаки.

- Узел 3 («Шлюз»): ПК, имитирующий маршрутизатор или другой легитимный узел, с которым взаимодействует «жертва».

Методы сбора данных: сбор данных осуществлялся с помощью разработанного программного комплекса [1], состоящего из двух модулей:

- Модуль сбора данных: выполнял захват и парсинг сетевого трафика (в частности, ARP-пакетов) с сетевого интерфейса узла-«жертвы».
- Модуль обнаружения: получал данные от первого модуля и анализировал их на предмет наличия атаки.

- Описание процедуры проведения исследования:

- На узле-«жертве» был запущен программный комплекс для обнаружения атак.
- На узле-«атакующего» с помощью инструмента «Ettercap» была инициирована атака ARP-spoofing командой ettercap -T -M arp -o. Целью атаки была подмена MAC-адреса узла-«шлюза» в ARP-таблице узла-«жертвы».
- Модуль сбора данных на узле-«жертве» перехватывал входящие ARP-ответы, отправленные атакующим.
- Модуль обнаружения анализировал полученные данные согласно заложенному алгоритму и фиксировал результат.

Методы обработки данных. Обработка данных производилась в реальном времени модулем обнаружения на основе следующей алгоритмической модели, описанной в [1]:

- На вход поступает сетевой трафик, из которого фильтруются только ARP-пакеты.
- Система ищет событие «получен ARP-ответ».
- При обнаружении такого события модуль немедленно проверяет локальную ARP-таблицу узла.
- Если в ARP-таблице обнаружено изменение MAC-адреса для IP-адреса, указанного в ARP-ответе, система генерирует оповещение об атаке.

На рисунке 1 представлена используемая топология сети.

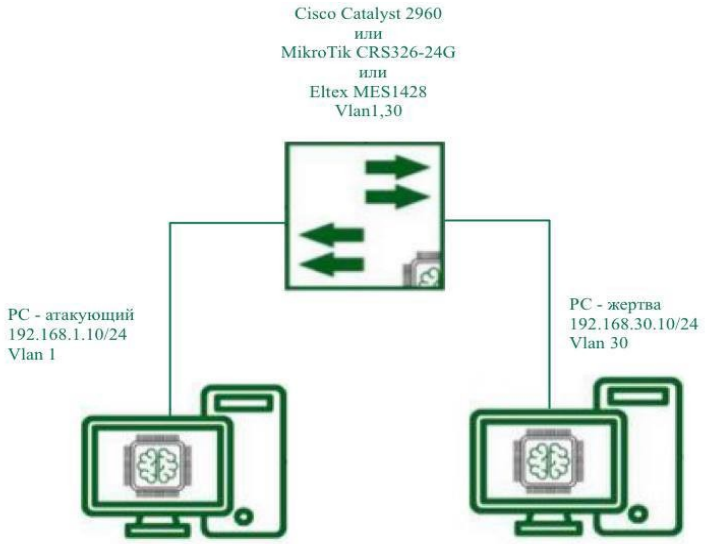

Рисунок 1 - Топология сети для эксперимента

ХОД ИССЛЕДОВАНИЯ

Рассмотрим настройку конкретных машин. Для начала покажем настройку Cisco Catalyst 2960 ,Eltex MES1428 и Mikrotik. Стоит понимать, что настройка производилась по отдельности каждый раз для каждого нового состава топологии, ведь в эксперименте участвуют три устройства: два PC и один коммутатор.

Начнём с объяснения настройки коммутатора Cisco Catalyst 2960. Создадим VLAN, настроим trunk-порт, настроим порты двух ПК (у одного - динамический режим, у другого - порт access). Данная настройка показана на рисунке 2.

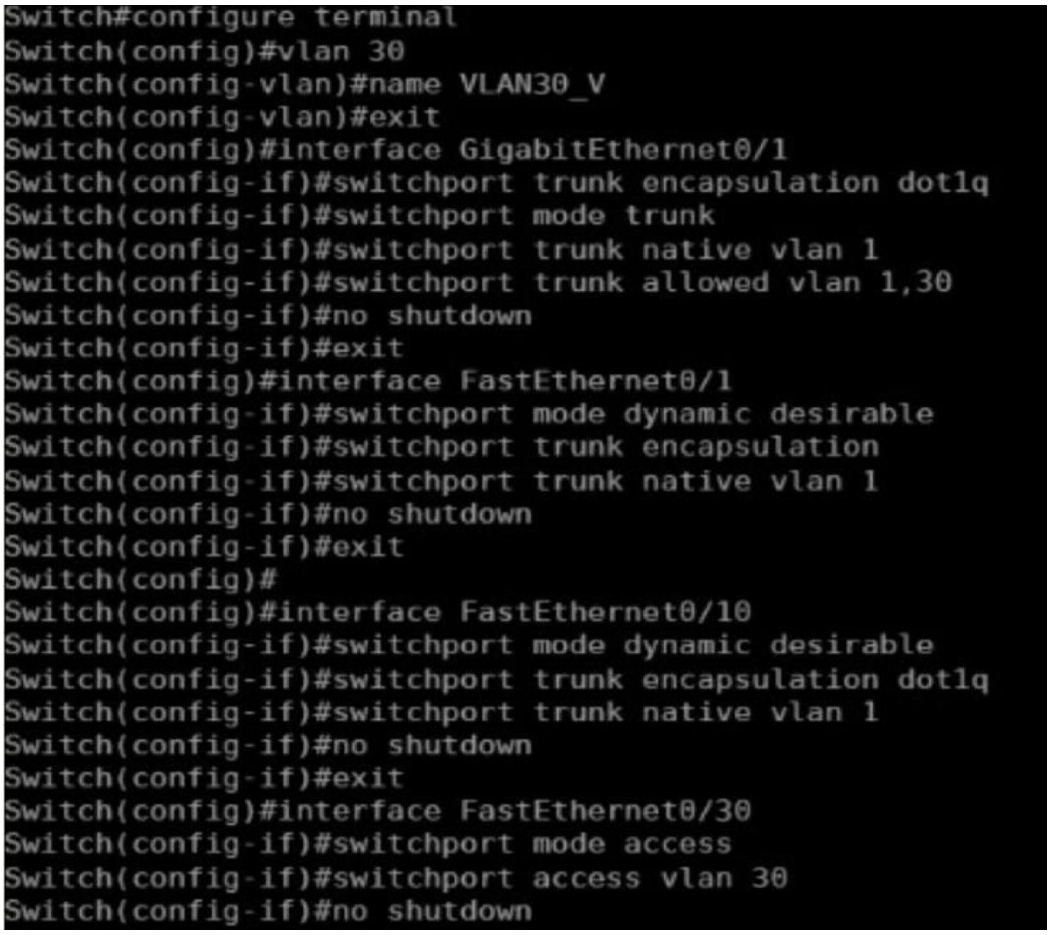

Рисунок 2- Настройка Cisco Catalyst 2960

Теперь покажем настройку для Eltex MES1428. Создадим VLAN 1 (native) и VLAN 30. Настроим порт для атакующего ПК (PC1) в режиме general (для trunk) interface GigabitEthernet 0/1. Настроим порт для жертвы (PC2) в VLAN 30. Данная настройка показана на рисунке 3.

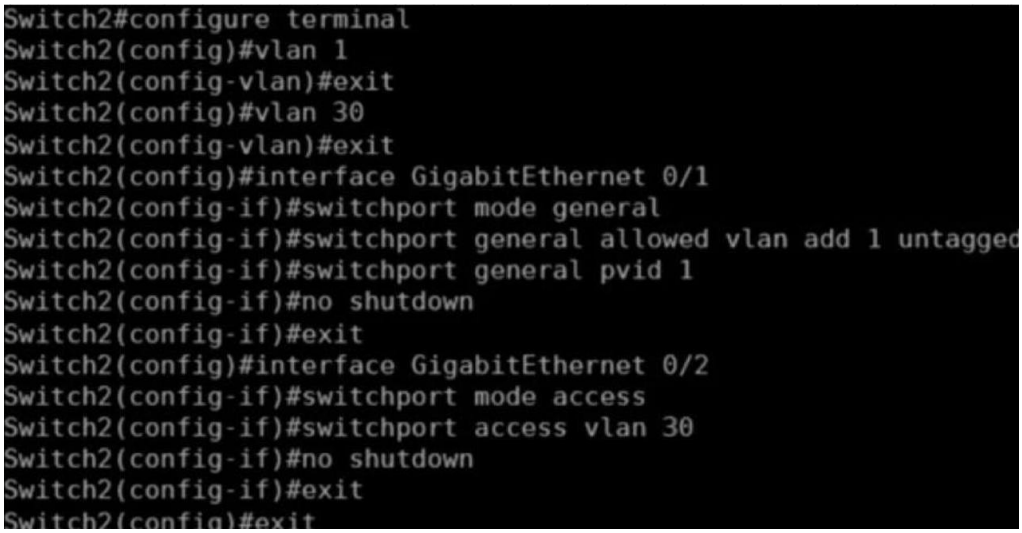

Рисунок 3- Настройка Eltex MES1428

Также продемонстрируем настройку MikroTik.

```
[root@MikroTik]> /interface bridge port add bridge=bridge1 interface=ether1
[root@MikroTik]> /interface bridge port add bridge=bridge1 interface=ether2
[root@MikroTik]> /interface bridge port add bridge=bridge1 interface=ether24
[root@MikroTik]> /interface bridge vlan add bridge=bridge1 tagged=ether24 vlan-ids=1,30
[root@MikroTik]> /interface bridge vlan add bridge=bridge1 untagged=ether1 vlan-ids=1
[root@MikroTik]> /interface bridge vlan add bridge=bridge1 untagged=ether2 vlan-ids=30
```

Рисунок 4 - Настройка MikroTik

Для того, чтобы осуществить атаку ARP-spoofing, можно использовать такие инструменты как: arspspoof, Ettercap, BetterCAP, но мы создадим двойной VLAN интерфейс на атакующем PC (рисунок 5).

```
[root@ALT ~]$ ip link add link eth0 name eth0.1 type vlan id 1
[root@ALT ~]$ ip link add link eth0.1 name eth0.1.30 type vlan id 30
[root@ALT ~]$ ip addr add 192.168.30.100/24 dev eth0.1.30
[root@ALT ~]$ ip link set eth0.1.30 up
[root@ALT ~]$
```

Рисунок 5 - Создание двойного VLAN интерфейса

А для проведения самой атаки потребуется следующая команда на PC: ping 192.168.30.10. Применение команды показано на рисунке 6.

```
[root@ALT ~]$ ping 192.168.30.10
PING 192.168.30.10 (192.168.30.10) 56(84) bytes of data.
64 bytes from 192.168.30.10: icmp_seq=1 ttl=64 time=0.474 ms
64 bytes from 192.168.30.10: icmp_seq=2 ttl=64 time=0.442 ms
64 bytes from 192.168.30.10: icmp_seq=3 ttl=64 time=0.220 ms
```

Рисунок 6 - Запуск атаки ARP-spoofing

Так же можно запустить атаку с помощью инструмента: sudo arpspoof -i eth0.30 -t 192.168.30.10 192.168.30.1

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Необходимо понять как именно работает атака.

Атакующий ПК подключается к обоим VLAN через двойной VLAN-интерфейс.

Через arpspoof он отправляет ложные ARP-ответы:

PC1 думает, что MAC PC2 – это MAC атакующего.

PC2 думает, что MAC PC1 – это MAC атакующего.

Весь трафик между PC1 и PC2 идет через атакующий ПК.

Вот некоторые методы защиты от атаки ARP-spoofing:

- Отключить DTP (Dynamic Trunking Protocol) на коммутаторах.
- Настроить порты как access, а не trunk (если не требуется меж-VLAN-маршрутизация).
- Использовать DHCP Snooping + ARP Inspection на коммутаторе.
- Статическая ARP-таблица (но это сложно масштабировать).

В ходе эксперимента была успешно смоделирована и обнаружена атака типа ARP-spoofing. Результаты работы программного комплекса представлены в таблице 1 и на рисунке 7.

Таблица 1. Результаты эксперимента по обнаружению атаки

№	Этап эксперимента	Действие на тестовом стенде	Результат на модуле обнаружения
1	Начальное состояние	Штатная работа сети, обмен трафиком отсутствует.	Активность не зафиксирована.
2	Запуск атаки	На «атакующем» узле запущена утилита Ettercap.	Модуль сбора данных фиксирует поступление ARP-ответов.
3	Обнаружение	Модуль обнаружения сопоставляет пришедший ARP-ответ с изменением в	Сгенерировано оповещение: «Обнаружена атака типа ARP-spoofing на ПК:

		ARP-таблице.	192.168.1.10».

Визуальное подтверждение результата работы модуля обнаружения представлено на скриншоте его интерфейса.

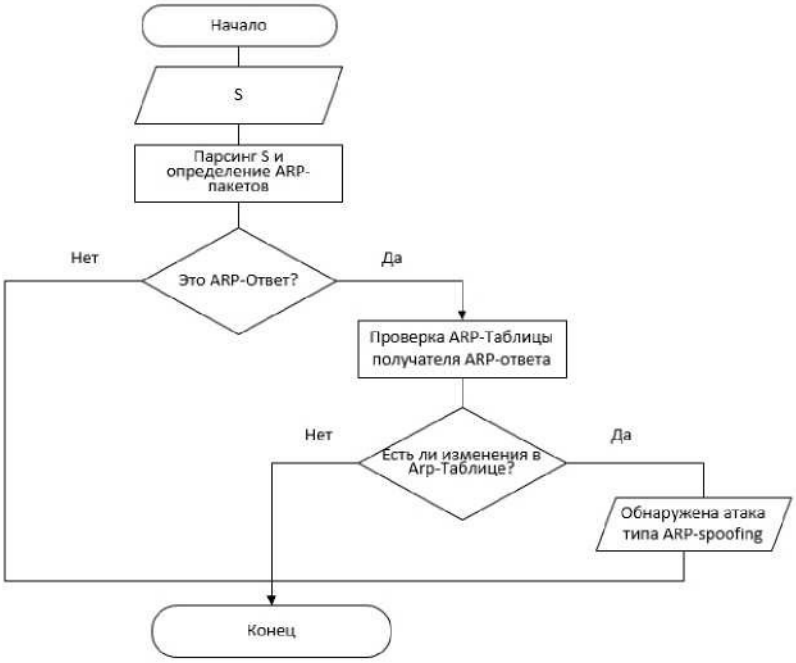

Рисунок 7 – Блок-схема

Как видно из представленных данных, программный комплекс, реализующий предложенный метод, успешно справился с поставленной задачей. Сразу после того, как утилита Ettercap отправила ложный ARP-ответ и ARP-таблица на узле-«жертве» была изменена, модуль обнаружения зафиксировал это событие и вывел соответствующее предупреждение в журнал. В сообщении указано точное время обнаружения и IP-адрес атакованного узла, что позволяет администратору оперативно отреагировать на инцидент. Результаты эксперимента подтверждают эффективность метода, который за счет учета двух факторов (наличие ARP-ответа и изменение в таблице) обеспечивает высокую достоверность срабатывания.

ЗАКЛЮЧЕНИЕ

В рамках данного исследования был рассмотрен и экспериментально апробирован метод обнаружения сетевых атак типа ARP-spoofing. Исследование показало, что, несмотря на простоту реализации самой атаки, существуют эффективные и низкоресурсные способы ее обнаружения. Предложенный метод, основанный на анализе входящих ARP-пакетов и проверке целостности локальной ARP-таблицы, продемонстрировал свою состоятельность в ходе практического эксперимента.

Результат проверки гипотез:

- Гипотеза H1 полностью подтвердилась. Эксперимент показал, что совместный анализ ARP-ответов и состояния ARP-таблицы позволяет точно и своевременно идентифицировать атаку, минимизируя ложные срабатывания.
- Гипотеза H2 также нашла свое подтверждение. Разработанный программный комплекс оказался простым в настройке, не требовательным к системным ресурсам и эффективно справился с обнаружением атаки в условиях, приближенных к реальным. Это делает его пригодным как для защиты сетей, так и для использования в качестве учебного пособия при подготовке специалистов по информационной безопасности.

Направления дальнейшего исследования:

Интеграция в программный комплекс модуля активного противодействия, который бы не только обнаруживал атаку, но и автоматически восстанавливал корректные записи в ARP-таблице.

тестирование метода в условиях высокой сетевой нагрузки и в более крупных и сложных сетевых инфраструктурах.

Разработка клиент-серверной архитектуры по аналогии с [2], где агенты на узлах собирали бы информацию, а центральный сервер анализировал бы ее и управлял бы защитой всей сети.

Адаптация метода для обнаружения других типов атак на канальном и сетевом уровнях.

СПИСОК ЛИТЕРАТУРЫ

1. Алиев Р. М. Разработка метода обнаружения атак типа ARP-spoofing // Шаг в науку. 2019. №2. URL: https://cyberleninka.ru/article/n/razrabotka-metoda-obnaruzheniya-atak-tipa-arp-spoofing (дата обращения: 28.06.2025).

2. Крылов А. Ю., Шитов Н. А., Галиаскаров Э. Г. Применение объектного подхода при создании распределенной системы выявления и предотвращения атаки типа ARP-spoofing // Объектные системы. 2010. №2 (2). URL: https://cyberleninka.ru/article/n/primenenie-obektnogo-podhoda-pri-sozdanii-raspredelennoy-sistemy-vyyavleniya-i-predotvrascheniya-ataki-tipa-arp-spoofing (да та обращения: 28.06.2025).

3. Шишов Н. В., Ломазов В. А. Моделирование процессов функционирования системы электронного документооборота при воздействии ARP-spoofing атак // Инженерный вестник Дона. 2022. №2 (86). URL: https://cyberleninka.ru/article/n/modelirovanie-protsessov-funktsionirovaniya-sistemy-elektronnogo-dokumentooborota-pri-vozdeystvii-arp-spoofing-atak (дата обращения: 28.06.2025).

4. Уймин А.Г. Компьютерные сети. L2-технологии [Электронный ресурс] // Ай Пи Ар Медия - Москва.- 2024.URL:https://www.iprbookshop.ru/epd-reader?publicationId=135231 –ISBN 978-5-4497-2539-4 -(дата обращения: 28.06.2025)