УДК 004.056.5

Мухаяров Владислав Альбертович - студент Цифровой Трансформации Института информационных технологий МИРЭА – Российского технологического университета.

Жучкова Александра Алексеевна – магистрант кафедры управляющих ЭВМ Института информационных технологий МИРЭА – Российского технологического университета.

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОТОКОЛА ARP И МЕТОДЫ ЗАЩИТЫ ОТ ARP-СПУФИНГА В КОРПОРАТИВНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Аннотация. В данной статье рассматриваются фундаментальные принципы работы протокола разрешения адресов (ARP), лежащего в основе взаимодействия узлов в локальных сетях IPv4. Проведен глубокий анализ архитектуры протокола и его критических уязвимостей, обусловленных историческим отсутствием встроенных механизмов криптографической аутентификации и проверки состояния (Stateless-природа). Подробно описаны векторы реализации атак на канальном уровне, в частности механизм ARP-спуфинга (ARP Poisoning) и его использование для организации атак типа «человек посередине» (Man-in-the-Middle) и «отказ в обслуживании» (DoS). В статье систематизированы современные методы противодействия данным угрозам. Особое внимание уделено практической реализации защиты на уровне коммутаторов доступа с использованием технологий DHCP Snooping и Dynamic ARP Inspection (DAI), а также рассмотрены перспективы перехода на протокол IPv6.

Ключевые слова: ARP, ARP-спуфинг, информационная безопасность, локальные вычислительные сети, MAC-адрес, MITM-атаки, сетевое оборудование, коммутаторы, Dynamic ARP Inspection.

Abstract. This article examines the fundamental principles of the Address Resolution Protocol (ARP), which underlies the interaction of nodes in IPv4 local area networks. A deep analysis of the protocol's architecture and its critical vulnerabilities, caused by the historical lack of built-in cryptographic authentication mechanisms and stateless nature, is carried out. The vectors of implementing data link layer attacks are described in detail, in particular the ARP spoofing (ARP Poisoning) mechanism and its use for organizing Man-in-the-Middle and Denial of Service (DoS) attacks. The article systematizes modern methods of countering these threats. Special attention is paid to the practical implementation of protection at the access switch level using DHCP Snooping and Dynamic ARP Inspection (DAI) technologies, and the prospects of transition to the IPv6 protocol are also considered.
Keywords: ARP, ARP spoofing, information security, local area networks, MAC address, MITM attacks, network equipment, switches, Dynamic ARP Inspection.

1. Введение

В эпоху глобальной цифровизации корпоративных процессов, активной миграции бизнес-инфраструктуры в облачные среды и интеграции технологий Интернета вещей (IoT) вопросы обеспечения комплексной информационной безопасности (ИБ) приобретают критическое значение. Традиционно основной фокус внимания ИБ-специалистов при проектировании сетей сосредоточен на защите внешнего периметра и прикладного уровня эталонной модели OSI (внедрение межсетевых экранов нового поколения NGFW, VPN-шлюзов, криптографических протоколов TLS/SSL). Однако, как показывает практика проведения аудитов безопасности и тестов на проникновение (Penetration Testing), внутренние сегменты локальных вычислительных сетей (ЛВС), функционирующие на канальном (L2) и сетевом (L3) уровнях, зачастую остаются наиболее уязвимым звеном корпоративной инфраструктуры.

Фундаментальной основой базовой связности и взаимодействия узлов в сетях стандарта IPv4 является протокол разрешения адресов ARP (Address Resolution Protocol), спецификация которого была утверждена в 1982 году документом RFC 826 [4]. Архитектура данного протокола разрабатывалась на ранних этапах развития сетевых технологий в парадигме абсолютного доверия к участникам информационного обмена. Вследствие этого протокол лишен встроенных механизмов криптографической аутентификации и проверки целостности сообщений. Данный архитектурный недостаток создает благоприятную поверхность для реализации сетевых атак внутри единого широковещательного домена, наиболее опасной и распространенной из которых является подмена ARP-ответов — ARP-спуфинг (ARP Poisoning).

Объектом данного исследования выступает информационная безопасность корпоративных локальных вычислительных сетей, построенных на базе стека протоколов TCP/IPv4.

Предметом исследования являются архитектурные уязвимости протокола ARP и современные аппаратно-программные методы противодействия деструктивным воздействиям на канальном уровне.

Цель работы заключается в проведении комплексного анализа механизмов эксплуатации уязвимостей протокола ARP и систематизации эффективных методов защиты сетевой инфраструктуры от атак типа «человек посередине» (Man-in-the-Middle) и «отказ в обслуживании» (DoS).

Для достижения поставленной цели в рамках исследования решаются следующие **задачи**:

1. Выполнить теоретический анализ принципов функционирования протокола ARP и выявить его ключевые структурные недостатки (Stateless-архитектура, отсутствие верификации).
2. Подробно описать механизм реализации атаки ARP-спуфинг с использованием поддельных немотивированных ответов (Gratuitous ARP) и оценить потенциальный ущерб для предприятия.

3. Проанализировать превентивные технологии защиты уровня доступа коммутаторов, в частности инструменты Dynamic ARP Inspection (DAI) и DHCP Snooping, а также специфику их внедрения.
4. Рассмотреть перспективы фундаментального устранения рассматриваемых уязвимостей в контексте перехода на протокол IPv6 и использования Neighbor Discovery Protocol (NDP).

2. Теоретический анализ протокола ARP и механика реализации атак канального уровня

2.1. Принципы штатного функционирования протокола ARP

Согласно эталонной модели взаимодействия открытых систем (OSI), маршрутизация пакетов между различными сетями осуществляется на сетевом (третьем) уровне на основе логических IP-адресов. Однако непосредственная передача данных (инкапсулированных кадров) внутри единого широковещательного домена локальной сети (LAN) происходит на канальном (втором) уровне и требует знания физического аппаратного адреса сетевого интерфейса — MAC-адреса.

Протокол ARP выполняет функцию связующего звена между этими двумя уровнями. Процесс штатного разрешения адреса подробно описан в фундаментальных работах по сетевым технологиям [1, 2] и включает следующие этапы:

1. Инициатор (отправитель) проверяет свой локальный ARP-кэш (таблицу соответствия IP и MAC-адресов). Если искомая запись найдена, кадр формируется и отправляется немедленно.
2. В случае отсутствия записи узел формирует широковещательный запрос (ARP Request), который инкапсулируется в кадр Ethernet с MAC-адресом назначения `FF:FF:FF:FF:FF:FF`. Запрос содержит логику: *Какой MAC-адрес соответствует IP-адресу X.X.X.X? Владельцу данного адреса необходимо ответить на мой MAC-адрес*.

3. Данный кадр доставляется всем узлам в текущем сегменте сети. Сетевые интерфейсы устройств, чей IP-адрес не совпадает с искомым, отбрасывают (Drop) пакет.
4. Легитимный владелец целевого IP-адреса формирует одноадресный ответ (ARP Reply), содержащий его физический MAC-адрес, и направляет его строго инициатору запроса.
5. Отправитель получает ответ, заносит новую динамическую связку IP – MAC в свою таблицу ARP для минимизации широковещательного трафика в будущем и начинает передачу пользовательских данных.

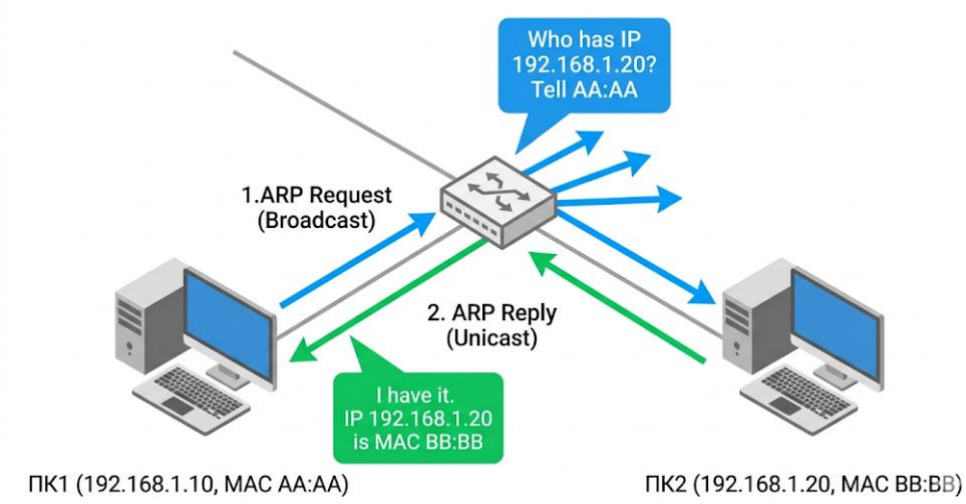

Рисунок 1 – Схема штатного обмена сообщениями ARP Request и ARP Reply

2.2. Архитектурные уязвимости и структурные недостатки

Анализ спецификации RFC 826 [4] показывает, что протокол создавался в условиях доверенной сетевой среды, что обусловило наличие в его архитектуре ряда критических функциональных недостатков:

- **Отсутствие криптографической аутентификации.** Протокол не содержит встроенных механизмов проверки цифровых подписей или сертификатов. Любой узел сети имеет техническую возможность сгенерировать легитимный по формату ответ, присвоив себе чужой IP-адрес, и сеть примет эту информацию как достоверную.
- **Отсутствие проверки состояния (Stateless-архитектура).** Как отмечается в анализе классических моделей сетевого взаимодействия

[1], отсутствие механизмов отслеживания состояния в протоколе ARP является критическим фактором уязвимости, так как позволяет узлам принимать немотивированные ответы без предварительного запроса

- **Безусловная перезапись кэша.** При получении нового ARP-ответа для уже существующего в таблице IP-адреса, устройство автоматически обновляет запись новым MAC-адресом. Последний пришедший ответ всегда считается приоритетным.

Особый вектор угрозы представляет механизм немотивированных ответов — **Gratuitous ARP (GARP)**. В штатном режиме GARP-пакеты рассылаются узлом в виде широковещательной рассылки при загрузке операционной системы или смене сетевых настроек для проверки сети на наличие дубликатов IP-адресов (IP Conflict Detection), а также при переключении виртуальных IP-адресов в кластерах высокой доступности (VRRP, HSRP). Именно GARP является основным инструментом злоумышленника при реализации атак канального уровня.

2.3. Вектор атаки: механика ARP-спуфинга и реализация MITM

Эксплуатация описанных уязвимостей позволяет реализовать атаку типа ARP-спуфинг (ARP Poisoning — отравление кэша). Стратегия атакующего базируется на генерации потока ложных GARP-сообщений для искажения таблиц маршрутизации соседних узлов.

Рассмотрим классический сценарий перехвата трафика по модели человек посередине (Man-in-the-Middle) между пользовательским узлом (Жертвой) и шлюзом по умолчанию (Маршрутизатором):

1. **Фаза инициализации:** Злоумышленник переводит свой сетевой интерфейс в неразборчивый режим (Promiscuous mode) и активирует функцию пересылки пакетов (IP Forwarding) на своем устройстве, чтобы не нарушать связность сети и скрыть факт своего присутствия.
2. **Отравление кэша Жертвы:** Злоумышленник направляет Жертве поддельный ARP-ответ, в котором указывает свой собственный MAC-

адрес в качестве аппаратного адреса Маршрутизатора. Жертва безусловно обновляет свой кэш.

3. **Отравление кэша Маршрутизатора:** Одновременно злоумышленник направляет поддельный ARP-ответ Маршрутизатору, связывая свой MAC-адрес с IP-адресом Жертвы.
4. **Перехват трафика:** С этого момента весь сетевой трафик (как исходящий в глобальную сеть, так и входящий) физически маршрутизируется через коммутатор на порт злоумышленника.

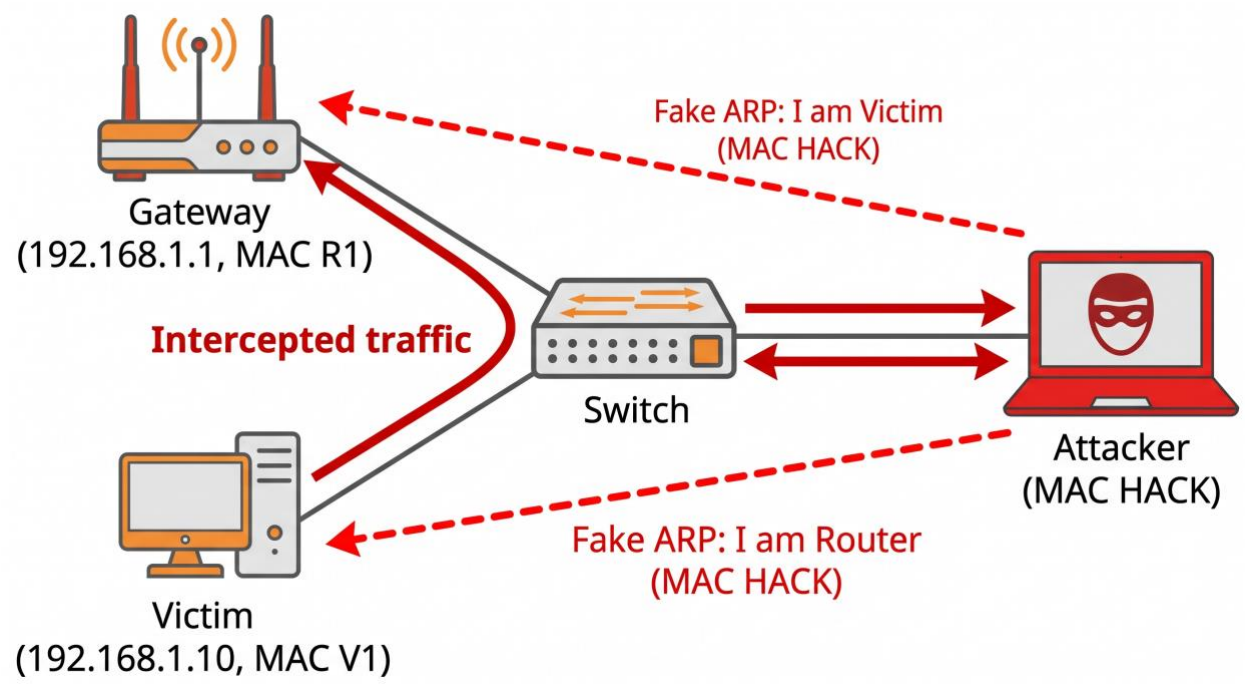

Рисунок 2 – Топология перехвата трафика (MITM) с использованием ARP-спуфинга

Находясь в позиции «посередине», атакующий получает возможность осуществлять пассивный сниффинг трафика (перехват паролей, сессионных токенов в незашифрованных протоколах HTTP, FTP, Telnet), активную модификацию передаваемых данных, а также реализацию Downgrade-атак (принудительное снижение уровня шифрования, например, SSL Stripping). Кроме того, если злоумышленник отключит пересылку пакетов или укажет несуществующий MAC-адрес (Blackhole), атака трансформируется в локальный «Отказ в обслуживании» (DoS), полностью изолируя жертву от сети передачи данных.

3. Практическая реализация механизмов защиты сетевой инфраструктуры

Переход от теоретического описания уязвимостей к практическому обеспечению безопасности требует внедрения эшелонированной защиты на канальном уровне. Поскольку ARP-спуфинг реализуется внутри одного широковещательного домена, фокус защиты должен быть смещен на коммутаторы уровня доступа (Access Layer), к которым непосредственно подключаются конечные узлы.

В рамках данного исследования проанализирована эффективность применения технологии аппаратной инспекции ARP-пакетов — **Dynamic ARP Inspection (DAI)** в связке с функцией **DHCP Snooping**. Данный подход является индустриальным стандартом де-факто и поддерживается большинством современных корпоративных коммутаторов, включая отечественные решения компании Eltex [3].

3.1. Механизм совместной работы DHCP Snooping и DAI

Технология DAI не может функционировать автономно в сетях с динамической IP-адресацией, так как коммутатору необходим эталонный источник доверенных данных о том, какому MAC-адресу легитимно принадлежит конкретный IP-адрес. Эту задачу решает функция DHCP Snooping.

Процесс защиты строится по следующему алгоритму:

1. **Построение базы данных привязок (DHCP Snooping Binding Database).** Коммутатор отслеживает процесс обмена DORA-сообщениями (Discover, Offer, Request, Acknowledge) между клиентами и легитимным DHCP-сервером. На основе этих перехваченных сообщений коммутатор формирует защищенную таблицу, в которой жестко связываются параметры: `MAC-адрес клиента — Выданный IP-адрес — Номер VLAN — Порт коммутатора`.
2. **Разделение портов на доверенные (Trusted) и недоверенные (Untrusted).** Порты, к которым подключены пользовательские

устройства, помечаются как недоверенные. Порты, ведущие к маршрутизатору или DHCP-серверу (аплинки), помечаются как доверенные.

3. **Инспекция ARP-трафика.** Функция DAI перехватывает все ARP-запросы и ARP-ответы (включая Gratuitous ARP), поступающие на недоверенные порты. Коммутатор извлекает из заголовка ARP-пакета IP-адрес и MAC-адрес отправителя (Sender IP и Sender MAC) и сверяет их с базой данных DHCP Snooping.
4. **Блокировка нелегитимного трафика.** Если пара «IP-MAC» в ARP-пакете злоумышленника не совпадает с легитимной записью, выданной DHCP-сервером для данного порта, коммутатор немедленно отбрасывает (Drop) данный кадр, предотвращая "отравление" кэша других узлов. При превышении порога подозрительных пакетов коммутатор может перевести порт нарушителя в состояние `err-disable` (аппаратная блокировка).

3.2. Пример базовой конфигурации оборудования

Для демонстрации практической применимости предложенного метода приведем фрагмент конфигурации коммутатора уровня доступа (на примере синтаксиса интерфейса командной строки CLI, применяемого в оборудовании Eltex [3]).

Предполагается, что пользовательские ПК находятся в VLAN 10, а порт `GigabitEthernet 1/0/24` является магистральным каналом (Uplink), ведущим к маршрутизатору.

```
! Глобальное включение функции слежения за DHCP
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10

! Глобальное включение динамической инспекции ARP
Switch(config)# ip arp inspection vlan 10
```

```
! Настройка магистрального порта (Uplink) как доверенного
Switch(config)# interface gigabitethernet 1/0/24
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip arp inspection trust
Switch(config-if)# exit

! Настройка пользовательского (недоверенного) порта
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# switchport access vlan 10
! (По умолчанию порты являются untrusted для DAI и DHCP Snooping)
! Ограничение скорости входящих ARP-пакетов для защиты CPU коммутатора (опционально)
Switch(config-if)# ip arp inspection limit rate 15
```

Листинг 1. Пример конфигурации механизмов защиты DAI и DHCP Snooping.

3.3. Оценка дополнительных мер: безопасность портов (Port Security)

В качестве дополнительного эшелона защиты в статье рассматривается функция Port Security. Она позволяет аппаратно ограничить количество уникальных MAC-адресов, с которых разрешена отправка кадров на конкретном физическом порту.

Хотя основное назначение Port Security — предотвращение атак типа MAC Flooding (переполнение таблицы коммутации), жесткая привязка 1-2 MAC-адресов к пользовательскому порту (`switchport port-security maximum 1`) существенно ограничивает возможности злоумышленника по генерации множества виртуальных сетевых интерфейсов для проведения комплексных MITM-атак.

3.4. Результаты анализа эффективности

Внедрение описанного комплекса мер на уровне коммутаторов доступа демонстрирует высокую практическую эффективность:

- **Полное предотвращение классического ARP-спуфинга.** Злоумышленник технически лишается возможности рассылать поддельные GARP-сообщения от имени шлюза по умолчанию.
- **Централизованность.** В отличие от использования статических ARP-записей на конечных ПК, настройка DAI выполняется единожды на сетевом оборудовании и легко масштабируется на сотни устройств.

К недостаткам (побочным эффектам) внедрения DAI следует отнести повышенную вычислительную нагрузку на центральный процессор (CPU) коммутатора, так как анализ каждого ARP-пакета происходит на программно-аппаратном уровне контроллера. Для нивелирования этого эффекта необходимо грамотно применять механизмы ограничения скорости ARP-трафика (`limit rate`).

Метод защиты	Преимущества	Недостатки / Ограничения
Статические ARP-записи	100% гарантия от подмены кэша на конкретном узле; не требует специального оборудования.	Крайне низкая масштабируемость; невозможность использования в сетях с DHCP и мобильными клиентами.
Безопасность портов (Port Security)	Снижает риск генерации множества поддельных MAC-адресов (защита от MAC Flooding).	Не защищает напрямую от поддельных ARP-ответов, если злоумышленник использует свой легитимный MAC-адрес.
Dynamic ARP Inspection (DAI)	Централизованная аппаратная защита всего	Требует настройки DHCP Snooping (базы привязок);

	L2-сегмента; автоматическая блокировка нелегитимного трафика.	создает дополнительную нагрузку на CPU коммутатора.

Таблица 1 – Сравнительный анализ методов противодействия ARP-спуфингу

4. Обсуждение результатов и анализ перспектив

Проведенный в рамках исследования теоретический анализ и оценка практической реализации механизмов защиты показывают, что фундаментальные архитектурные уязвимости протокола ARP (отсутствие аутентификации и Stateless-природа) не могут быть устранены путем простой модификации самого протокола, так как это нарушит обратную совместимость в сетях IPv4. Следовательно, перенос ответственности за верификацию канального трафика на коммутаторы уровня доступа (Access Layer) является единственным технически обоснованным решением.

4.1. Оценка эффективности предложенных методов

Внедрение связки технологий DHCP Snooping и Dynamic ARP Inspection (DAI) демонстрирует высокую эффективность в предотвращении атак типа ARP-спуфинг. Коммутатор начинает выполнять роль интеллектуального фильтра (L2-Firewall), который физически изолирует легитимный широковещательный домен от поддельных Gratuitous ARP-сообщений. Злоумышленник лишается возможности реализовать сценарий «человек посередине» (MITM) на канальном уровне, что автоматически снижает риски компрометации паролей и перехвата сессионных токенов.

4.2. Эксплуатационные ограничения и трудности внедрения

Несмотря на очевидные преимущества, практическое развертывание DAI в действующих корпоративных сетях (Legacy-инфраструктурах) сопряжено с рядом административных и аппаратных трудностей:

1. **Административные издержки (Overhead):** Технология DAI критически зависит от актуальности базы данных DHCP Snooping. Если в сети присутствуют узлы с легитимной статической IP-адресацией

(например, сетевые принтеры, серверы, технологическое оборудование), администратору необходимо вручную создавать статические списки контроля доступа (ARP Access Control Lists – ARP ACL) и привязывать их к портам. В крупных и динамично меняющихся сетях это значительно увеличивает трудозатраты ИТ-отдела.

2. **Аппаратная нагрузка на коммутаторы:** В отличие от стандартной коммутации кадров на основе таблиц MAC-адресов, выполняемой на скорости среды аппаратными чипами (ASIC), инспекция заголовков ARP-пакетов требует перенаправления трафика на центральный процессор (CPU) коммутатора. В случае массированного широковещательного шторма или целенаправленной DoS-атаки процессор коммутатора может быть перегружен. Для нивелирования этого риска критически важно использовать механизмы ограничения скорости входящих пакетов (Rate Limiting).
3. **Локальность защиты:** Рассмотренные механизмы защищают исключительно сегмент L2. Они не спасают от атак, инициированных с легитимно полученных IP-адресов на более высоких уровнях модели OSI (например, от эксплуатации уязвимостей веб-приложений или фишинга).

4.3. Перспективы развития и переход к протоколу IPv6

Глобальным стратегическим решением проблемы канальной маршрутизации является отказ от использования стека IPv4. В протоколе IPv6 механизм ARP полностью упразднен. Его функции перенесены в протокол обнаружения соседей — **NDP (Neighbor Discovery Protocol)**, который функционирует поверх протокола сообщений управления ICMPv6.

Хотя в базовой реализации NDP также подвержен атакам подмены (NDP Spoofing), спецификация стека IPv6 предусматривает использование расширения **SEND (Secure Neighbor Discovery — RFC 3971 [5])**. Архитектура SEND применяет криптографически сгенерированные адреса (CGA) и асимметричные алгоритмы шифрования (RSA) для строгой аутентификации

каждого узла, генерирующего ICMPv6-ответы. Таким образом, безопасность обеспечивается на уровне архитектуры протокола, а не за счет "надстроек" на коммутаторах.

Тем не менее, учитывая колоссальную долю сетей, продолжающих функционировать на базе протокола IPv4, использование технологий класса DAI останется безальтернативным и обязательным стандартом построения защищенных корпоративных ЛВС на ближайшее десятилетие.

5. Заключение

В ходе проведенного исследования был выполнен комплексный анализ уязвимостей протокола разрешения адресов (ARP) и механизмов реализации векторов атак на канальном уровне локальных вычислительных сетей. Теоретический анализ подтвердил, что исторически заложенные в спецификацию протокола архитектурные недостатки, в первую очередь отсутствие криптографической аутентификации и Stateless-архитектура, делают инфраструктуру IPv4 фундаментально уязвимой к перехвату трафика. Доказано, что обработка узлами немотивированных ответов (Gratuitous ARP) является главным инструментом злоумышленников для организации атак типа «человек посередине» (MITM) и локальных отказов в обслуживании (DoS).

Обосновано, что традиционные (базовые) методы защиты, такие как использование статических ARP-записей, обладают критически низкой масштабируемостью и не подходят для современных корпоративных сред. Практическая значимость работы заключается в систематизации и демонстрации методов эшелонированной защиты сетевой инфраструктуры на базе коммутаторов уровня доступа.

Показано, что обязательным стандартом проектирования безопасных ЛВС сегодня является внедрение технологии Dynamic ARP Inspection (DAI) в неразрывной связке с функцией DHCP Snooping. Данный аппаратно-программный комплекс переносит ответственность за верификацию пакетов

на сетевое оборудование, что позволяет эффективно блокировать поддельные ARP-ответы до того, как они скомпрометируют кэш конечных устройств.

Несмотря на то, что наиболее радикальным и перспективным решением проблемы канальной маршрутизации является миграция на протокол IPv6 с использованием защищенного механизма обнаружения соседей (SEND/NDP), доминирующее положение сетей стандарта IPv4 диктует необходимость повсеместного применения рассмотренных механизмов инспекции.

Таким образом, можно сделать вывод, что обеспечение надежной информационной безопасности современного предприятия невозможно без строгого контроля L2-сегмента. Грамотная конфигурация коммутационного оборудования выступает первичным, обязательным и наиболее действенным барьером на пути внутренних нарушителей.

Список литературы:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 6-е изд. – Санкт-Петербург : Питер, 2020. – 1008 с.
2. Танненбаум, Э. Компьютерные сети [Текст] / Э. Танненбаум, Д. Уэзерролл ; пер. с англ. В. Водолазского. – 5-е изд. – Санкт-Петербург : Питер, 2012. – 960 с.
3. Руководство по эксплуатации коммутаторов доступа серии MES [Электронный ресурс] // Официальный сайт предприятия «Элтекс» (Eltex). – URL: https://eltex-co.ru/support/downloads/ (дата обращения: 03.05.2024).
4. Plummer, D. An Ethernet Address Resolution Protocol: RFC 826 [Electronic resource] / D. Plummer // Internet Engineering Task Force (IETF). – 1982. – URL: https://datatracker.ietf.org/doc/html/rfc826 (дата обращения: 03.05.2024).

5. Arkko, J. Secure Neighbor Discovery (SEND): RFC 3971 [Electronic resource] / J. Arkko, J. Kempf, B. Zill, P. Nikander // Internet Engineering Task Force (IETF). – 2005. – URL: https://datatracker.ietf.org/doc/html/rfc3971 (дата обращения: 03.05.2024).