АНАЛИЗ УЯЗВИМОСТЕЙ ПРОТОКОЛА МАРШРУТИЗАЦИИ OSPF И МЕТОДЫ ИХ УМЕНЬШЕНИЯ В КОРПОРАТИВНЫХ СЕТЯХ

Долгая А.С., студент гр 361402

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мокеров В.С. – ассистент каф. ЗИ

Аннотация. В материалах статьи рассматриваются уязвимости протокола динамической маршрутизации OSPF, его основные типы атак и методы защиты. Защита OSPF в приоритете ставит внедрение криптографической аутентификации и фильтрацию маршрутной информации с целью исключения возможности несанкционированного изменения маршрутов.

Ключевые слова. OSPF, динамическая маршрутизация, уязвимости протоколов, LSA, аутентификация, корпоративная сеть, безопасность маршрутизации

Протокол OSPF (Open Shortest Path First) является одним из наиболее распространённых протоколов динамической маршрутизации в корпоративных сетях среднего и крупного размера. Благодаря быстрой сходимости, масштабируемости и поддержке бесклассовой адресации (CIDR) он широко используется как в государственных организациях, так и в коммерческих структурах. Однако вопросы безопасности OSPF часто остаются вне фокуса внимания сетевых администраторов, поскольку приоритетом при настройке обычно является доступность и производительность, а не защита от целенаправленных атак.

Данный протокол относится к классу протоколов состояния каналов. Его работа основана на обмене между соседними маршрутизаторами сообщениями о состоянии каналов – LSA (Link State Advertisement), которые хранятся в единой базе данных LSDB. Именно эта архитектура, обеспечивающая быструю сходимость и масштабируемость, создаёт ряд фундаментальных уязвимостей.

В протоколе отсутствует обязательная аутентификация. Базовая спецификация OSPFv2 (RFC 2328) определяет аутентификацию как опциональный механизм [1]. Администратор может полностью отключить проверку подлинности OSPF-пакетов, и любой маршрутизатор, подключившийся к сегменту сети, способен установить соседство и начать рассылку LSA. Передача данных происходит в открытом виде. Даже при включении аутентификации сам OSPF-трафик не шифруется. Пароль передаётся открыто (при plain text) либо содержимое LSA остаётся доступным для перехвата (при MD5/SHA). Злоумышленник получает детальную карту сети. Архитектура OSPF построена на допущении, что все участники домена являются доверенными. После установления соседства маршрутизаторы принимают LSA без дополнительной верификации источника. Как отмечается в документации Cisco, данная уязвимость позволяет злоумышленнику полностью контролировать таблицу маршрутизации OSPF-домена [2]. Процедура выбора DR/BDR крайне уязвима. Злоумышленник может объявить максимальный приоритет и захватить роль Designated Router, что даёт ему влияние на синхронизацию LSDB в сегменте. В протоколе отсутствет защита IP-заголовка. Механизмы аутентификации OSPF (RFC 2328, RFC 5709) не защищают IP-заголовок пакета, что позволяет подменять IP-адрес источника для сброса соседств. Механизмы безопасности OSPF рассмотрены в таблице 1.

Таблица 1 – Стандартные механизмы безопасности OSPF и их ограничения

Механизм безопасности	Что обеспечивает	Основные ограничения
Plain text authentication	Базовую проверку пароля	Пароль передаётся открыто, легко перехватывается анализатором трафика; не рекомендуется к использованию в корпоративных сетях
MD5 authentication	Хэширование пароля (128 бит)	MD5 считается устаревшим алгоритмом, подвержен коллизиям; не защищает IP-заголовок
SHA authentication (RFC 7474)	Криптостойкое хэширование (160-512 бит)	Требует более высокой вычислительной мощности; поддерживается не на всех устройствах
Passive-interface	Отключает рассылку Hello на указанных интерфейсах	Не защищает от атак внутри сегмента, где OSPF должен работать; не предотвращает сниффинг трафика
Отсутствие шифрования в OSPFv2	–	Вся маршрутная информация передаётся открыто; топология сети доступна для пассивного перехвата

Атаки на OSPF можно разделить на три основные категории в зависимости от цели злоумышленника: нарушение доступности (DoS), перенаправление трафика (MITM) и сбор информации о топологии сети. Для удобства рассмотрения категории были разделены на 6 типов основных атак (таблица 2). Наиболее опасными с точки зрения последствий для корпоративной сети являются атаки первых двух типов.

Таблица 2 – Основные типы атак на OSPF

Тип атаки	Краткое описание	Уровень опасности
Внедрение ложного LSA	Злоумышленник рассылает фальшивые LSA с изменёнными параметрами маршрутов	Высокий
MaxAge LSA	Отправка LSA с возрастом 3600 секунд для удаления маршрута из LSDB	Высокий
MaxSequenceNumber	Отправка LSA с максимальным значением sequence number для «перетирания» легитимных записей	Высокий
Подмена DR/BDR	Захват роли Designated Router через объявление максимального приоритета	Средний
Сниффинг	Пассивный перехват OSPF-пакетов для получения карты сети	Средний
Атака на соседство	Установление поддельного соседства для внедрения ложной маршрутной информации	Высокий

Атака MaxAge LSA заключается в отправке специально сформированного LSA-пакета с возрастом 3600 секунд (максимальное значение). В уязвимых реализациях OSPF это приводит к удалению легитимного маршрута из таблицы маршрутизации, что создаёт «чёрную дыру» (отказ в обслуживании). Данная уязвимость подтверждена CVE-2017-8147 и затрагивает даже оборудование Huawei [3]. Внедрение ложного LSA Type 5 позволяет злоумышленнику объявить внешний маршрут с низкой метрикой, что приводит к перенаправлению трафика через атакующий узел. Такая атака даёт возможность перехватывать и анализировать трафик (MITM) (рисунок 1). Атака MaxSequenceNumber (CVE-2017-3224) использует недостатки RFC 2328 при определении «свежести» LSA. Злоумышленник может «перетереть» легитимные записи в LSDB, что приводит к нарушению маршрутизации в домене [4].

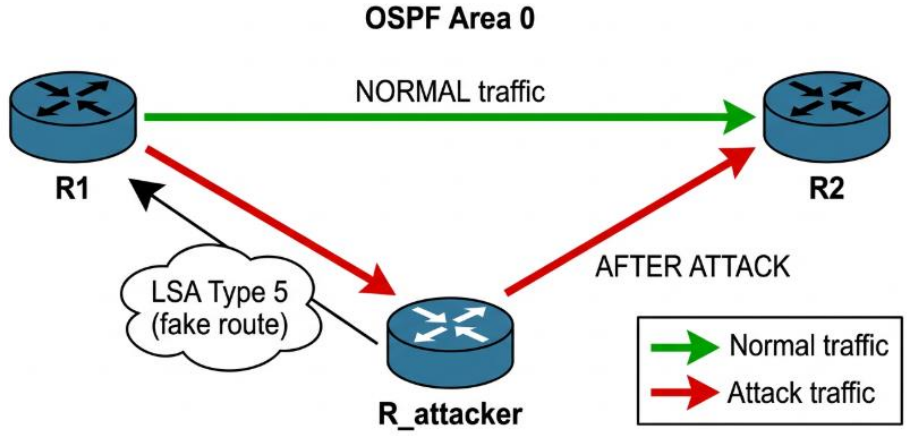

Рисунок 1 – Схема атаки MITM с внедрением ложного маршрута

Для защиты OSPF-домена от рассмотренных выше атак необходим комплексный подход, сочетающий криптографические, фильтрующие и мониторинговые меры. Ни одна из рассмотренных далее мер не является абсолютной, однако их совместное применение значительно снижает риски.

Основной мерой защиты является обязательное включение криптографической аутентификации. Рекомендуется использовать SHA-аутентификацию (RFC 7474) вместо устаревших MD5 и тем более plain text. Для OSPFv3 оптимальным решением является использование IPsec, обеспечивающего не только аутентификацию, но и шифрование всего трафика. Ключи аутентификации необходимо регулярно обновлять с помощью механизма key chain [5]. На интерфейсах, где нет соседей OSPF, следует включать режим passive-interface, который отключает рассылку Hello-пакетов и предотвращает установление поддельных соседств. Дополнительно рекомендуется использовать фильтрацию LSA с помощью distribute-list (inbound) и ограничивать максимальное количество соседей на интерфейс. Для предотвращения resource exhaustion-атак (флуд LSA) на маршрутизаторах следует настраивать CoPP (Control Plane Policing), ограничивающее скорость обработки OSPF-пакетов. На уровне коммутаторов необходимо применять port security и

DHCP snooping, чтобы затруднить физическое подключение злоумышленника в сегмент сети. Для своевременного выявления атак рекомендуется вести логирование изменений соседства (команда log-adjacency-changes), периодически анализировать LSDB на предмет аномальных записей, а также использовать системы IDS/IPS с правилами для обнаружения подозрительных OSPF-пакетов. Перечисленные далее меры защиты в совокупности позволяют существенно снизить вероятность успешной реализации атак на OSPF-домен и минимизировать их последствия для корпоративной сети.

Таблица 3 – Соответствие мер защиты типам атак

Мера защиты	Какие атаки блокирует или обнаруживает
SHA-аутентификация (RFC 7474)	Внедрение ложного LSA, MaxAge, MaxSequenceNumber, подмена DR/BDR
IPsec для OSPFv3	Внедрение ложного LSA, сниффинг, подмена DR/BDR
Passive-interface	Установление поддельного соседства, внедрение ложного LSA
Фильтрация LSA (distribute-list)	Внедрение ложного LSA, MaxAge, MaxSequenceNumber
CoPP (Control Plane Policing)	Resource exhaustion (LSA flood)
Логирование и мониторинг LSDB	Обнаружение всех типов атак (постфактум)
Port security на коммутаторах	Физическое подключение злоумышленника, установление соседства

Как мы видим, в современных корпоративных сетях созданы технические возможности для защиты протокола OSPF. Технологии аутентификации и фильтрации совершенствуются, как и методы обнаружения атак. Однако главной проблемой остаётся человеческий фактор – невнимание администраторов к настройке безопасности OSPF. Нарушители активно используют эти упущения, поэтому необходимо регулярно повышать уровень компетенции специалистов в области безопасной настройки протоколов маршрутизации.

Список использованных источников:

1. RFC 2328 – OSPF Version 2 [Электронный ресурс]. – Режим доступа : https://www.ietf.org/rfc/rfc2328.txt – Дата доступа : 06.04.2026.

2. Cisco Systems. OSPF Security Recommendations [Электронный ресурс]. – Режим доступа : https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13689-18.html. Дата доступа: 06.04.2026.

3. Huawei Security Advisory – MaxAge LSA Vulnerability (CVE-2017-8147) [Электронный ресурс]. – Режим доступа: https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170720-01-ospf-en Дата доступа : 06.04.2026.

4. CVE-2017-3224 – OSPF MaxSequenceNumber Vulnerability [Электронный ресурс]. – Режим доступа: https://cve.ics-csirt.io/cve/CVE-2017-3224 Дата доступа : 08.04.2026.

5. RFC 7474 – OSPF HMAC-SHA Cryptographic Authentication [Электронный ресурс]. – Режим доступа: https://www.rfc-editor.org/rfc/rfc7474.html Дата доступа : 08.04.2026.