ОТКАЗОУСТОЙЧИВОСТЬ И ЗАЩИТА МАРШРУТИЗАЦИИ В КОРПОРАТИВНЫХ СЕТЯХ: OSPF, BGP И СМЕЖНЫЕ МЕХАНИЗМЫ

Карпекин Владимир Александрович, Рукавицин Эдуард Вячеславович

Алтайский государственный технический университет имени И.И. Ползунова, Барнаул
e-mail: ed.rukavitsin@yandex.ru; karpekin05@internet.ru

Аннотация. Доступность сети как одно из базовых свойств информационной безопасности напрямую зависит от отказоустойчивости маршрутизации. При проектировании резервируемых корпоративных сетей устойчивость к случайным отказам и устойчивость к целенаправленным воздействиям на маршрутизацию нередко рассматриваются раздельно. В статье на основе анализа протоколов OSPF и eBGP, а также туннелей GRE поверх IPsec, рассматривается, как архитектурные решения, повышающие отказоустойчивость, одновременно влияют на защищённость. Автоматическое восстановление маршрутов средствами OSPF и резервирование внешних каналов через eBGP расширяют поверхность атаки (подмена анонсов, установление соседства без аутентификации). Лабораторное наблюдение на RouterOS качественно иллюстрирует различие времени восстановления связности при статической маршрутизации и при OSPF с BFD и показывает, что аутентификация соседства OSPF не включена по умолчанию; количественные измерения не проводились. Рассматриваются меры защиты: HMAC-аутентификация OSPF, фильтрация префиксов и RPKI для BGP, TCP-AO и GTSM для сессии BGP, BFD (с учётом его двойственной роли). Делается вывод о необходимости проектировать отказоустойчивую маршрутизацию и её защиту как единую задачу.

Ключевые слова: маршрутизация, отказоустойчивость, OSPF, BGP, RPKI, перехват маршрутов, GRE, IPsec, BFD, аутентификация соседства.

ROUTING RESILIENCE AND SECURITY IN ENTERPRISE NETWORKS: OSPF, BGP AND RELATED MECHANISMS

Karpekin Vladimir Alexandrovitch, Rukavitsin Eduard Vyacheslavovitch

Polzunov Altai State Technical University, Barnaul
e-mail: ed.rukavitsin@yandex.ru; karpekin05@internet.ru

Abstract. Network availability, one of the core properties of information security, depends directly on routing resilience. When designing redundant enterprise networks, resilience to random failures and resilience to targeted attacks on routing are often treated separately. Based on an analysis of OSPF and eBGP, as well as GRE over IPsec, the article examines how architectural choices that improve fault tolerance affect security. Automatic route recoexpandsia OSPF and external-link redundancy via eBGP expand the attack surface. A RouterOS lab observation qualitatively illustrates the difference in failover time between static routing and OSPF with BFD and shows that OSPF neighbor authentication is not enabled by default; no quantitative measurements were made. Protective measures are discussed: OSPF HMAC authentication, prefix filtering and RPKI for BGP, TCP-AO and GTSM for the BGP session, and BFD (with its dual role). The article concludes that fault-tolerant routing and its security should be designed as a single task.

Keywords: routing, resilience, OSPF, BGP, RPKI, route hijacking, GRE, IPsec, BFD, neighbor authentication.

Доступность — наряду с конфиденциальностью и целостностью — одно из базовых свойств информации [1]. Для сетевой инфраструктуры доступность в первую очередь означает отказоустойчивость маршрутизации: способность сети автоматически восстанавливать связность при отказе канала, узла или сегмента. Достигается это преимущественно за счёт динамических протоколов: внутри автономной системы чаще всего OSPF [2], для резервирования внешних подключений — eBGP [3].

При проектировании таких решений вопрос отказоустойчивости обычно решается проработанными методами: несколько независимых каналов, автоматический пересчёт маршрутов, балансировка нагрузки [4]. Значительно реже на этом же этапе рассматривается, что динамическая маршрутизация, повышая устойчивость к случайным отказам, одновременно расширяет поверхность для целенаправленной атаки на маршрутизацию [5, 6].

Цель статьи — рассмотреть взаимосвязь отказоустойчивости и защищённости маршрутизации на примере OSPF, eBGP и GRE/IPsec и обобщить меры защиты. OSPF (IGP) и BGP (EGP) решают разные задачи, поэтому сопоставляются не сами протоколы, а конфигурации по времени сходимости и меры защиты каждого из них. Лабораторное наблюдение носит иллюстративный характер; атаки в эксперименте не моделировались, а тезис о расширении поверхности атаки опирается на литературу [5, 6].

Отказоустойчивость и защищённость: общая и разная стороны задачи

Статическая маршрутизация предсказуема и минимальна с точки зрения поверхности атаки: у неё нет протокола обмена анонсами.

Однако она не восстанавливает связность автоматически. Динамические протоколы решают эту проблему за счёт обмена служебной информацией, но именно этот обмен становится объектом атаки: устройство, способное установить соседство или внедрить поддельный анонс, может нарушить связность или перенаправить трафик. Отказоустойчивость и защищённость маршрутизации — две связанные задачи; рассматривать их изолированно рискованно: меры, решающие одну задачу, могут ослаблять другую.

OSPF: быстрая сходимость и её оборотная сторона

Протокол OSPF обеспечивает быструю сходимость за счёт полной топологической базы в пределах области. Для ускорения обнаружения отказов поверх OSPF нередко разворачивают BFD [7], снижающий время обнаружения разрыва до десятков–сотен миллисекунд. При типовых таймерах Hello/Dead 10/40 с и BFD с интервалом 50–300 мс и множителем 3 время обнаружения отказа сокращается на два–три порядка.

По умолчанию установление соседства OSPF не требует аутентификации (тип 0 по RFC 2328 [2]): любое устройство в сегменте может отправить Hello, установить соседство и внедрить LSA. Для устранения предусмотрена криптографическая аутентификация на основе HMAC-SHA [8]; её включение — отдельный шаг, который на практике нередко пропускается. BFD ускоряет обнаружение отказов (отказоустойчивость), но сам может быть целью атаки (подделка пакетов) и поддерживает аутентификацию (RFC 5880, разд. 6.7); его не следует относить исключительно к мерам защиты.

eBGP и резервирование внешних каналов

Резервирование внешнего подключения через двух и более провайдеров с eBGP — стандартное решение. Оборотная сторона документирована: BGP проектировался без встроенной проверки права на анонс префикса — основа случайных утечек и намеренного перехвата [9, 10]. Рекомендации по фильтрации обобщены в RFC 7454 [11]. Для проверки происхождения используется RPKI [12]; процедура — RFC 6811 [13] (и RFC 6482 о ROA). Более полная защита пути — BGPsec [14]; его практическое распространение остаётся ограниченным, поэтому на практике чаще применяют проверку происхождения на основе RPKI (оценку охвата следует брать из актуального мониторинга развёртывания).

Защита сессии BGP: TCP-AO [15], GTSM [16], ограничение числа префиксов. Для OSPF анализ угроз дан в RFC 6863 [5]; обобщающий документ — NIST SP 800-189 [6].

GRE поверх IPsec как дополнительный контур

Там, где резервные каналы проходят через сети общего пользования, отказоустойчивость дополняется защитой данных. Комбинация GRE [17] с IPsec [18] — распространённое решение. Механизм Dead Peer Detection [19] и таймеры IKE необходимо

согласовывать с параметрами BFD и Hello-таймерами, иначе переключение занимает больше времени, чем предполагалось.

Практическая проверка на лабораторном стенде

В рамках лабораторного стенда на базе RouterOS, воспроизводящего связность нескольких площадок через статическую маршрутизацию, OSPF, eBGP-резервирование и туннели GRE/IPsec, зафиксировано: отказ канала при статической маршрутизации с плавающими маршрутами обрабатывался за секунды–десятки секунд, тогда как OSPF с BFD восстанавливал связность за доли секунды. Попытка установления OSPF-соседства без аутентификации проходила успешно, что соответствует поведению по умолчанию по RFC 2328 [2]; поэтому аутентификация [8] должна включаться на этапе базовой настройки.

Наблюдение носит качественный характер: не указаны версия RouterOS, топология, точные значения таймеров (Hello/Dead, BFD, check-gateway) и способ имитации отказа [указать], а время восстановления не измерялось с повторами. Для eBGP без BFD следует ожидать десятков секунд и более (RFC 4271 предлагает hold time 90 с [3]). Для количественной оценки необходимы не менее 10 прогонов для каждой из 4–5 конфигураций (статика, OSPF с BFD и без, eBGP с BFD и без), в том числе с GRE/IPsec и DPD; это направление дальнейшей работы. Сходимость BGP в стенде не измерялась, атаки не воспроизводились.

Заключение

Отказоустойчивость и защищённость маршрутизации опираются на одни и те же протокольные механизмы. Решения, повышающие устойчивость к случайным отказам, нередко расширяют поверхность для целенаправленной атаки. Лабораторное наблюдение иллюстрирует, что аутентификация соседства OSPF не включена по умолчанию; аналогично фильтрация префиксов и проверка происхождения на основе RPKI для BGP требуют явной настройки [11, 13]. Целесообразно рассматривать отказоустойчивость и защиту маршрутизации как единую задачу уже на этапе проектирования, закладывая аутентификацию, фильтрацию анонсов и согласованные таймеры в базовую конфигурацию.

Библиографический список

1. ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary. — Geneva : ISO/IEC, 2018.

2. RFC 2328. OSPF Version 2 [Электронный ресурс] / J. Moy. — IETF, 1998. — URL: https://www.rfc-editor.org/rfc/rfc2328 (дата обращения: 07.10.2026).

3. RFC 4271. A Border Gateway Protocol 4 (BGP-4) [Электронный ресурс] / Y. Rekhter, T. Li, S. Hares (eds). — IETF, 2006. — URL: https://www.rfc-editor.org/rfc/rfc4271 (дата обращения: 07.10.2026).

4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. — 6-е изд. (юбилейное). — СПб.: Питер, 2020. — 1008 с.

5. RFC 6863. Analysis of OSPF Security According to the Keying and Authentication for Routing Protocols (KARP) Design Guide [Электронный ресурс] / S. Hartman, D. Zhang. — IETF, 2013. — URL: https://www.rfc-editor.org/rfc/rfc6863 (дата обращения: 07.10.2026).

6. NIST SP 800-189. Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation / K. Sriram, D. Montgomery. — Gaithersburg : NIST, 2019. DOI: 10.6028/NIST.SP.800-189.

7. RFC 5880. Bidirectional Forwarding Detection (BFD) [Электронный ресурс] / D. Katz, D. Ward. — IETF, 2010. — URL: https://www.rfc-editor.org/rfc/rfc5880 (дата обращения: 07.10.2026).

8. RFC 5709. OSPFv2 HMAC-SHA Cryptographic Authentication [Электронный ресурс] / M. Bhatia, V. Manral, T. Li [и др.]. — IETF, 2009. — URL: https://www.rfc-editor.org/rfc/rfc5709 (дата обращения: 07.10.2026).

9. RFC 7908. Problem Definition and Classification of BGP Route Leaks [Электронный ресурс] / K. Sriram, D. Montgomery, D. McPherson [и др.]. — IETF, 2016. — URL: https://www.rfc-editor.org/rfc/rfc7908 (дата обращения: 07.10.2026).

10. RFC 4272. BGP Security Vulnerabilities Analysis [Электронный ресурс] / S. Murphy. — IETF, 2006. — URL: https://www.rfc-editor.org/rfc/rfc4272 (дата обращения: 07.10.2026).

11. RFC 7454. BGP Operations and Security [Электронный ресурс] / J. Durand, I. Pepelnjak, G. Doering. — IETF, 2015. — URL: https://www.rfc-editor.org/rfc/rfc7454 (дата обращения: 07.10.2026).

12. RFC 6480. An Infrastructure to Support Secure Internet Routing [Электронный ресурс] / M. Lepinski, S. Kent. — IETF, 2012. — URL: https://www.rfc-editor.org/rfc/rfc6480 (дата обращения: 07.10.2026).

13. RFC 6811. BGP Prefix Origin Validation [Электронный ресурс] / P. Mohapatra, J. Scudder, D. Ward [и др.]. — IETF, 2013. — URL: https://www.rfc-editor.org/rfc/rfc6811 (дата обращения: 07.10.2026).

14. RFC 8205. BGPsec Protocol Specification [Электронный ресурс] / M. Lepinski, K. Sriram (eds). — IETF, 2017. — URL: https://www.rfc-editor.org/rfc/rfc8205 (дата обращения: 07.10.2026).

15. RFC 5925. The TCP Authentication Option [Электронный ресурс] / J. Touch, A. Mankin, R. Bonica. — IETF, 2010. — URL: https://www.rfc-editor.org/rfc/rfc5925 (дата обращения: 07.10.2026).

16. RFC 5082. The Generalized TTL Security Mechanism (GTSM) [Электронный ресурс] / V. Gill [и др.]. — IETF, 2007. — URL: https://www.rfc-editor.org/rfc/rfc5082 (дата обращения: 07.10.2026).

17. RFC 2784. Generic Routing Encapsulation (GRE) [Электронный ресурс] / D. Farinacci [и др.]. — IETF, 2000. — URL: https://www.rfc-editor.org/rfc/rfc2784 (дата обращения: 07.10.2026).

18. RFC 4301. Security Architecture for the Internet Protocol [Электронный ресурс] / S. Kent, K. Seo. — IETF, 2005. — URL: https://www.rfc-editor.org/rfc/rfc4301 (дата обращения: 07.10.2026).

19. RFC 3706. A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers [Электронный ресурс] / G. Huang [и др.]. — IETF, 2004. — URL: https://www.rfc-editor.org/rfc/rfc3706 (дата обращения: 07.10.2026).