

Е. А. Басыня¹✉, В. Ю. Сапегин¹

Методика сравнительного анализа методов обнаружения VPN-трафика с учетом сдвига домена и дрейфа данных

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: director@nii-ikt.ru

Аннотация. В работе представлена методика сравнительного анализа методов бинарного обнаружения VPN/non-VPN-трафика в условиях маскировки, изменения сетевой среды и дрейфа данных. Актуальность исследования определяется практической необходимостью сопоставления существующих решений не только по качеству классификации в лабораторном домене, но и по устойчивости при переходе к эксплуатационным сценариям. Методика основана на доменной постановке задачи, в которой условия наблюдения описываются совокупностью факторов: временным срезом, платформой клиента, типом сети, географией маршрута, режимом маскировки и используемым VPN-протоколом. В качестве базовых показателей используются F1 и AUPRC, а для сравнительного анализа дополнительно вводятся индекс переносимости, интегральная устойчивость к маскировке, показатель минимального качества на множестве целевых доменов и чувствительность метода к domain shift. Предлагаемая методика определяет единые правила формирования benchmark-сценариев, вычисления показателей и итогового сопоставления существующих методов обнаружения VPN, что позволяет использовать ее как воспроизводимую основу для последующих экспериментальных исследований.

Ключевые слова: VPN, обнаружение VPN, зашифрованный трафик, обфускация трафика, методика сравнения, информационная безопасность

Е. А. Басыня¹✉, V. Y. Sapegin¹

A methodology for comparative analysis of VPN traffic detection methods under domain shift and data drift

¹National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: director@nii-ikt.ru

Abstract. This paper presents a methodology for comparative analysis of binary VPN/non-VPN traffic detection methods under obfuscation, changing network conditions and data drift. The study is motivated by the need to compare existing solutions not only by their classification quality in a laboratory domain, but also by their robustness when transferred to operational scenarios. The methodology is based on a domain-oriented problem formulation in which observation conditions are described by a set of factors including time slice, client platform, network type, route geography, obfuscation mode and VPN protocol. F1 and AUPRC are used as the main quality indicators, while transferability index, integrated robustness to obfuscation, minimum quality over target domains and sensitivity to domain shift are introduced as comparative criteria. The proposed methodology defines unified rules for constructing benchmark scenarios, computing indicators and performing the final comparison of VPN detection methods, thus providing a reproducible basis for further experimental studies.

Keywords: VPN, VPN detection, encrypted traffic, obfuscation, comparative benchmark, information security

Введение

В условиях цифровой трансформации выявление скрытых виртуальных защищенных каналов связи становится значимой задачей обеспечения информационной безопасности корпоративных сетей. Технологии сокрытия сетевой активности, изначально ориентированные на защиту конфиденциальности, могут использоваться для обхода фильтрации, организации скрытых каналов передачи данных и маскировки вредоносной активности. По данным F.A.C.C.T. [1], в 2023 году сохранялась тенденция применения VPN-технологий при целевых атаках на корпоративные сети Российской Федерации. Современные исследования предлагают различные подходы к решению данной задачи: Wu Н. и соавторы [2, 3] показывают эффективность нейросетевой классификации при детекции сложных протоколов, включая V2Ray и Shadowsocks, Канатьев К. Н. и соавторы [4, 5] отмечают ограничения существующих подходов и необходимость новых аналитических методов, а работы научной школы под руководством Е. А. Басыни рассматривают механизмы обхода фильтрации и методы его детекции на примере оверлейных сетей Tor и I2P [6–8].

Последние зарубежные исследования показывают, что пассивное обнаружение VPN-трафика в корпоративных и операторских сетях остается сложной задачей, поскольку современные VPN активно используют шифрование, обфускацию и многоуровневую инкапсуляцию. Вследствие этого сигнатурный анализ и отдельные статистические признаки уже не отражают реальную эксплуатационную устойчивость методов. Akbari и соавторы указывают на зависимость классификации зашифрованного трафика от «ленивых» TLS-признаков [9], Хуе и соавторы демонстрируют детектируемость OpenVPN на реальном провайдерском трафике [10] и уязвимость обфусцированных проху/VPN-подобных туннелей к отпечаткам инкапсулированного TLS [11]. Отдельное значение имеют исследования устойчивости методов при изменении условий эксплуатации: Malekghaini и соавторы показывают снижение качества моделей глубокого обучения при временном дрейфе данных [12], Lv и соавторы рассматривают one-class постановку и устойчивость к неизвестным типам трафика [13], а Hanlon и соавторы демонстрируют возможности protocol-agnostic эвристики на основе поведения инкапсулированного TCP [14].

Таким образом, научная проблема состоит не только в разработке способов обнаружения виртуальных защищенных каналов связи, но и в формировании методики их корректного сравнительного анализа в условиях маскировки трафика. Обзоры Razzoqi, Pekar и Guerra-Manzanares [15, 16] фиксируют слабую сопоставимость опубликованных результатов из-за устаревших лабораторных датасетов, недостаточного учета сдвигов данных и отсутствия общей benchmark-рамки; эти выводы согласуются с методологическими рекомендациями Arp и соавторов для ML-систем в задачах кибербезопасности [17]. Дополнительную актуальность задаче придает нормативное регулирование: Приказ Роскомнадзора № 168 от 08.11.2023 [18], предусматривающий создание Единого реестра VPN- и прокси-

сервисов, подчеркивает прикладную значимость эффективных и воспроизводимых методов мониторинга VPN-соединений в корпоративных сетях.

Постановка задачи

Целью настоящей работы является разработка методики сравнительного анализа существующих методов бинарного обнаружения VPN/non-VPN-трафика на семействе эксплуатационных доменов. Методика должна обеспечивать воспроизводимое сопоставление как моделей машинного обучения, так и эвристических либо протольно-ориентированных методов по интегральным и эксплуатационным показателям качества.

Пусть X – пространство наблюдаемых фрагментов сетевого трафика. Элемент $x \in X$ может представлять собой поток, сессию или окно наблюдения, сформированное по доступным наблюдателю признакам: последовательностям длин пакетов, временным интервалам, признакам рукопожатия, метаданным транспортного и прикладного уровней. Каждому объекту x ставится в соответствие бинарная метка y , характеризующая наличие или отсутствие VPN.

$$Y \in \{0, 1\}, \quad 0 = \text{nonVPN}, \quad 1 = \text{VPN} \quad (1)$$

$$\xi = (\tau, p, n, g, o, v) \in \Xi \quad (2)$$

Вектор ξ задает условия эксплуатации метода: τ – временной срез наблюдения, p – платформу или VPN-клиент, n – тип сети, g – географию маршрута, o – режим маскировки, v – протокол или реализацию VPN.

$$D_\xi = P_\xi(X, Y), \quad \text{hm}: X \rightarrow \hat{Y}, \quad \hat{Y} \in \{0, 1\} \quad (3)$$

Каждому вектору ξ соответствует собственный домен эксплуатации D_ξ . Сравнимый метод m рассматривается как отображение hm , преобразующее наблюдаемый объект x в решение $\hat{y}$. Если метод использует пороговый score, то решение может быть записано в виде $\hat{y} = 1 [s_m(x) \geq \theta_m]$.

Выделяется базовый домен ξ_0 , соответствующий in-domain сценарию, и множество целевых доменов Ξ_{tar} , включающее temporal shift, cross-platform shift, cross-protocol shift, obfuscation shift и изменение сетевого маршрута. Задача сравнительного анализа состоит в получении воспроизводимой оценки поведения метода m на ξ_0 и на множестве Ξ_{tar} .

Методика сравнительного анализа

Методика сравнительного анализа строится как последовательность взаимосвязанных этапов: формирование семейства доменов эксплуатации, подготовка размеченных данных, выполнение сравниваемых методов в базовом и целевых доменах, анализ устойчивости к маскировке и сдвигу распределений, а также итоговое синтезирование профиля метода. На первом этапе фиксируются сравниваемые методы, тип доступных входных данных и допустимые условия

их применения: для rule-based и DPI-ориентированных подходов задаются анализируемые поля протокольного стека и доступность служебной информации, а для ML-подходов — схема формирования признаков, объем наблюдаемого окна, правила разбиения данных и требования к вычислительным ресурсам. Общая схема методики представлена на рис. 1.

На втором этапе формируется набор доменов эксплуатации: базовый домен ξ_0 используется для получения in-domain оценки, а множество Ξ_{tar} задает целевые сценарии, на которых измеряется переносимость метода. В него включаются изменения платформы клиента, маршрута, сетевой среды, протокола и режима маскировки, что позволяет сравнивать методы не по одному значению качества, а по поведению на семействе контролируемых сценариев. В качестве основного интегрального показателя принимается F1-мера, чувствительная к дисбалансу классов и учитывающая полноту и точность; AUPRC используется для оценки устойчивости при изменении порога решения, а Ассигасу приводится только как вспомогательная характеристика и не применяется как главный критерий ранжирования.

$$Q(m, \xi) = F1(m; D_\xi) \quad (4)$$

Для интерпретации результатов важна не только абсолютная величина $Q(m, \xi)$, но и ее изменение относительно базового домена. Поэтому в методике вводится относительная деградация качества и индекс переносимости. Первый показатель отражает локальное снижение качества при переходе к конкретному домену, а второй показывает, насколько хорошо метод в среднем сохраняет свойства на множестве эксплуатационных сценариев.

$$G(m, \xi) = 1 - \frac{Q(m, \xi)}{(Q(m, \xi_0) + \varepsilon)}, \quad (5)$$

$$T(m) = \frac{1}{|\Xi_{tar}|} \sum_{\xi \in \Xi_{tar}} \frac{Q(m, \xi)}{(Q(m, \xi_0) + \varepsilon)} \quad (6)$$

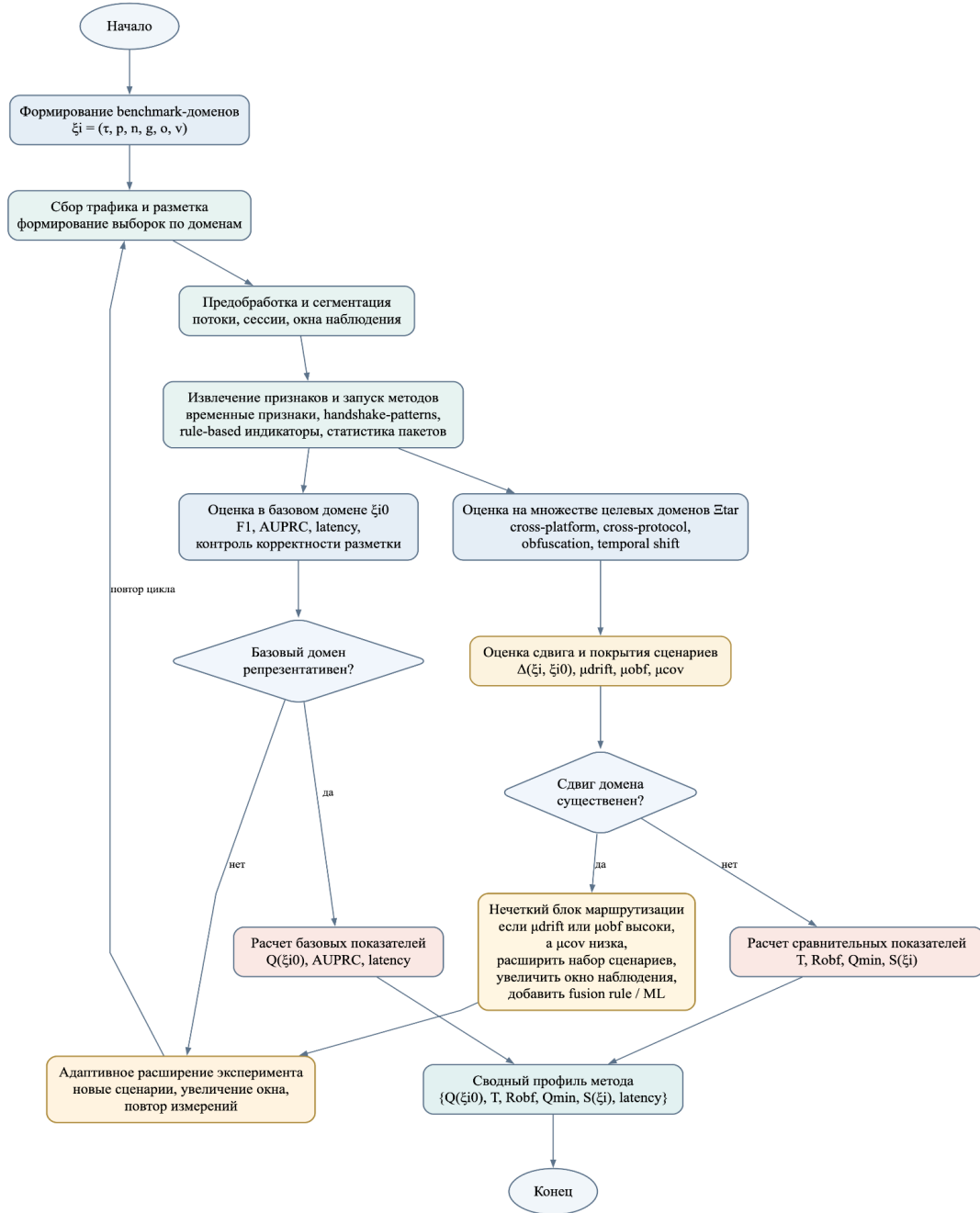


Рис. 1. Блок-схема методики оценки методов обнаружения VPN с адаптивной нечеткой маршрутизацией

Отдельно оценивается устойчивость к маскировке. Для этого из множества целевых доменов выделяются сценарии, в которых изменяется только режим обфускации, а остальные условия эксперимента удерживаются максимально близкими к базовому. Интегральная устойчивость к маскировке задается усреднением по набору таких сценариев с учетом их относительной значимости.

$$Robf(m) = \sum_{k=1}^K w_k \frac{Q(m, \xi_{obf, k})}{(Q(m, \xi_0) + \varepsilon)}, \quad \sum_{k=1}^K w_k = 1 \quad (7)$$

Для анализа причин деградации вводится оценка сдвига между базовым и целевым доменами. Сдвиг вычисляется на едином признаковом представлении $\varphi(X)$, выбранном одинаково для всех сравниваемых методов. В зависимости от природы данных в качестве меры расстояния между распределениями могут использоваться Jensen-Shannon divergence, MMD или иные статистические критерии. Чувствительность метода к drift определяется как отношение относительной деградации качества к величине измеренного сдвига.

$$\Delta(\xi, \xi_0) = D(P_{\xi}(\varphi(X)), P_{\xi_0}(\varphi(X))), \quad S(m, \xi) = \frac{G(m, \xi)}{(\Delta(\xi, \xi_0) + \varepsilon)} \quad (8)$$

Наряду с качеством классификации в методике фиксируется вычислительная цена. Она включает время обработки, требуемый объем наблюдения и устойчивость результата при ограниченном окне данных. Такие характеристики особенно важны для сравнения легковесных эвристических подходов и более тяжелых ML-моделей. Итогом эксперимента является профиль метода, который объединяет in-domain качество, переносимость, устойчивость к маскировке, чувствительность к drift, worst-case результат и вычислительную цену.

Для корректного применения методики benchmark-матрица должна включать следующие оси сравнения:

- 1) In-domain – оценка метода в базовом домене ξ_0 ;
- 2) Temporal shift – переносимость между временными срезами наблюдения.
- 3) Cross-platform shift – изменение клиента, платформы или операционной системы;
- 4) Cross-protocol shift – переход между VPN-протоколами и реализациями;
- 5) Obfuscation shift – устойчивость к различным режимам маскировки;
- 6) Worst-case performance – минимальное качество на множестве целевых доменов.

При практическом применении методики необходимо соблюдать несколько базовых требований. Все сравниваемые решения должны оцениваться строго в бинарной постановке VPN/non-VPN; задачи определения конкретного протокола, приложения внутри туннеля или типа сервиса не должны смешиваться с основной задачей обнаружения.

In-domain, temporal shift, cross-platform shift, cross-protocol shift и obfuscation shift необходимо измерять раздельно. Усреднение этих сценариев без явной фиксации доменных факторов делает результаты методологически неинтерпретируемыми. Для всех методов должна использоваться единая процедура оценки величины $\Delta(\xi, \xi_0)$, иначе чувствительность к drift перестает быть сопоставимой.

Для всех методов также должны использоваться единые правила формирования обучающей, валидационной и тестовой выборок, чтобы различия в результатах определялись свойствами метода, а не особенностями экспериментального протокола. В отчетах об экспериментах необходимо фиксировать значения всех координат $\xi = (\tau, p, n, g, o, v)$, используемое признаковое пространство, правила предобработки данных и вычислительные ограничения.

Итоговое сравнение методов должно проводиться не по одному агрегированному числу, а по профилю, включающему in-domain качество, индекс переносимости, устойчивость к маскировке, показатель worst-case качества, чувствительность к drift и вычислительную цену. На практике это означает следующую процедуру: сначала для каждого метода вычисляются показатели в базовом домене ξ_0 , затем анализируется изменение качества на множестве Ξ_{tar} , после чего выполняется сопоставление методов по совокупности критериев. Предпочтение должно отдаваться тем методам, которые обеспечивают приемлемое базовое качество и одновременно сохраняют устойчивость при смене домена, а не только демонстрируют высокий результат в одном лабораторном сценарии.

Заключение

Предложенная методика задает целостную схему сравнительного анализа методов обнаружения VPN на семействе эксплуатационных доменов. Научная новизна методики состоит в совместном использовании доменной постановки, интегральных показателей качества, индекса переносимости, интегральной устойчивости к маскировке, оценки worst-case качества и анализа чувствительности к domain shift.

Ключевой результат методики состоит в переходе от оценки метода в одном статическом сценарии к анализу его поведения на семействе контролируемых доменов эксплуатации. Такой подход позволяет выявлять случаи, когда методы с близкими значениями F1 в базовом домене существенно различаются по переносимости, устойчивости к маскировке и чувствительности к изменению сетевой среды.

Практическая значимость методики заключается в том, что она задает воспроизводимый протокол сравнения существующих решений и позволяет формировать более обоснованные требования к разрабатываемым системам обнаружения VPN. Применение данной методики дает возможность выбирать методы не по разовому максимуму качества, а по совокупности свойств, критически важных для эксплуатации в корпоративных сетях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Universal Encryptor: The number of cyberattacks in Russia increased by 140% in 2023 // F.A.C.C.T. URL: <https://www.facct.ru/media-center/press-releases/cyberattacks-2023/> (accessed: 21.04.2024).
2. Wu H. et al. Real-time identification of VPN traffic based on counting Bloom filter and chained hash table from sampled data in high-speed networks // ICC 2022-IEEE International Conference on Communications. IEEE, 2022. P. 5070-5075.
3. Wu H. et al. RT-CBCH: Real-time VPN Traffic Service Identification based on Sampled Data in High-speed Networks // IEEE Transactions on Network and Service Management. 2023.
4. Обзор методов обнаружения VPN и DNS-анализ для классификации на примере Hotspot Shield Free / К. Н. Канатъев, С. Р. Шишкин, И. И. Басыров [и др.] // Инновации и инвестиции. 2023. № 10. С. 215-219.
5. Передовые методы обнаружения и обфускации VPN-трафика: углубленный анализ OpenVPN и его уязвимостей в современную цифровую эпоху / К. Н. Канатъев, М. Д. Нурмагомедов, А. А. Гребенщиков [и др.] // Инновации и инвестиции. 2023. № 10. С. 211-214.

6. Басыня Е. А. Система самоорганизующегося виртуального защищенного канала связи / Е. А. Басыня // Защита информации. Инсайд. 2018. № 5 (83). С. 10-15.
7. System of a self-organizing virtual secure communication channel based on stochastic multi-layer encryption and overlay technologies / E. A. Basinya, Z. B. Akhayeva, D. H. Omarkhanova, G. B. Tolegenova [et al.] // Journal of Theoretical and Applied Information Technology. 2022. Vol. 100, iss. 16. P. 4918-4927.
8. Басыня Е. А. Программная реализация и исследование системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Е. А. Басыня // Вестник Самарского государственного технического университета. Серия: Технические науки. 2020. Т. 28, № 1 (65). С. 6-21.
9. Akbari I., Salahuddin M. A., Aniva L. [et al.]. A Look Behind the Curtain: Traffic Classification in an Increasingly Encrypted Web // Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2021. Vol. 5, No. 1. Article 4. DOI: 10.1145/3447382.
10. Xue D., Ramesh R., Jain A. [et al.]. OpenVPN Is Open to VPN Fingerprinting // 31st USENIX Security Symposium (USENIX Security 22). 2022. P. 483-500.
11. Xue D., Kallitsis M., Houmansadr A., Ensafi R. Fingerprinting Obfuscated Proxy Traffic with Encapsulated TLS Handshakes // 33rd USENIX Security Symposium (USENIX Security 24). 2024. P. 2689-2706.
12. Malekghaini N., Akbari E., Salahuddin M. A. [et al.]. Deep Learning for Encrypted Traffic Classification in the Face of Data Drift: An Empirical Study // Computer Networks. 2023. Vol. 225. Article 109648. DOI: 10.1016/j.comnet.2023.109648.
13. Lv S., Wang C., Wang Z. [et al.]. AAE-DSVDD: A One-Class Classification Model for VPN Traffic Identification // Computer Networks. 2023. Vol. 236. Article 109990. DOI: 10.1016/j.comnet.2023.109990.
14. Hanlon M., Wan G., Ascherman A., Durumeric Z. Detecting VPN Traffic through Encapsulated TCP Behavior // Free and Open Communications on the Internet. 2024. P. 77-82.
15. Razooqi Y. S., Pekar A. VPN Traffic Analysis: A Survey on Detection and Application Identification // IEEE Access. 2025. DOI: 10.1109/ACCESS.2025.3592152.
16. Guerra-Manzanares A., Caprolu M., Di Pietro R. A Comprehensive Review on Machine Learning-Based VPN Detection: Scenarios, Methods, and Open Challenges // Computer Science Review. 2025. Vol. 58. Article 100781. DOI: 10.1016/j.cosrev.2025.100781.
17. Arp D., Quiring E., Pendlebury F. [et al.]. Dos and Don'ts of Machine Learning in Computer Security // 31st USENIX Security Symposium (USENIX Security 22). 2022.
18. О внесении изменений в Критерии оценки материалов и информации для включения интернет-ресурсов в единый реестр запрещенной информации: Приказ Роскомнадзора от 8 нояб. 2023 г. № 168 // Собрание законодательства Рос. Федерации. – 2023. – 1 дек.

© Е. А. Басыня, В. Ю. Сапегин, 2026