https://doi.org/10.31891/2219-9365-2026-86-22
УДК 004.724.4

ТІТОВА Віра
Хмельницький національний університет
https://orcid.org/0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ Юрій
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
БЕРЧУК Валентин
Хмельницький національний університет
https://orcid.org/0009-0009-9414-6580
e-mail: bervalenchuk@gmail.com

МЕТОД ВИЯВЛЕННЯ ШКІДЛИВОЇ АКТИВНОСТІ В IPSEC-КАНАЛАХ БЕЗ ДЕШИФРУВАННЯ ТРАФІКУ

У статті розглянуто підхід до виявлення шкідливої активності в шифрованих каналах зв'язку без дешифрування вмісту трафіку. Проведено огляд існуючих підходів до аналізу шифрованого трафіку, зокрема методів TLS-фінгерпринтингу, класифікації трафіку за розподілом довжин пакетів і сучасних систем мережевого моніторингу. Запропоновано метод визначення типів трафіку в IPsec-каналах на основі аналізу розподілу довжин пакетів, параметрів інкапсуляції та оцінювання допустимих діапазонів довжин вкладеного навантаження. Окремо розглянуто підхід до побудови еталонних розподілів для конкретних конфігурацій шифрованих каналів, аналіз змішаного трафіку із застосуванням предиктивного віднімання внеску окремих протоколів, а також варіант практичної реалізації у вигляді системи сенсорів і модуля-оркестратора. Показано, що запропонований підхід може бути використаний для практичного виявлення підозрілої активності в шифрованих каналах зв'язку за низької обчислювальної складності.

Ключові слова: шифрований трафік, IPsec, ESP-пакет, аналіз трафіку, виявлення шкідливої активності, розподіл довжин пакетів, TLS-фінгерпринтинг, VPN-канал, пасивний моніторинг, захист інформації.

TITOVA Vira, KLOTS Yurii, BERCHUK Valentyn
Khmelnitskyi National University

METHOD FOR DETECTING MALICIOUS ACTIVITY IN IPSEC CHANNELS WITHOUT TRAFFIC DECRYPTION

The paper addresses the problem of detecting malicious activity in encrypted communication channels without decrypting traffic contents. The relevance of the study is determined by the rapid growth of encrypted traffic in modern networks, where protocols such as HTTPS, QUIC, and VPN-based communication significantly reduce the applicability of traditional payload-based inspection and signature matching. Under such conditions, passive monitoring methods must rely on observable indirect features rather than packet contents.

The paper reviews current approaches to encrypted traffic analysis, including TLS fingerprinting methods, traffic classification based on packet length distributions, and practical monitoring solutions used in modern network security systems. It is shown that existing approaches achieve promising results in identifying traffic types in TLS sessions and VPN channels, but many of them depend on machine learning or deep learning models, exact fingerprint matching, or computationally expensive analysis pipelines. As a result, the problem of combining low computational complexity, real-time applicability, and sufficient detection capability remains open.

To address this issue, the paper proposes a method for identifying traffic types in encrypted IPsec channels based on the analysis of packet length distributions over short time intervals. For each interval, packet lengths observed in both transmission directions are aggregated and analyzed as a normalized distribution. Characteristic patterns are considered informative, including stable packet lengths in one direction, paired response/request patterns, multiple persistent packet-length lines, upper bounds of packet size, and wide packet-length spectra typical of file transfer. A schematic comparison of such patterns is provided for VoIP, FTP, and RDP traffic.

A key contribution of the paper is the use of the formal relationship between the observed ESP packet length and the length of the encapsulated payload. The total ESP packet length is represented as a sum of the payload size, service headers, encapsulation parameters, and padding. This makes it possible, for a known or estimated IPsec configuration, to calculate admissible ranges of encapsulated payload lengths and to use them during traffic classification. On this basis, an algorithm for determining traffic types inside an IPsec channel is proposed. The algorithm includes estimation of channel parameters, construction of packet-length distributions for both directions, calculation of admissible payload ranges, comparison with characteristic protocol patterns, and formation of a conclusion about the presence of particular traffic types.

The paper also considers practical issues of applying the proposed method. It is shown that the effectiveness of detection strongly depends on the configuration of the encrypted channel; therefore, partial models and reference distributions tailored to specific encapsulation settings are preferable to universal models. To reduce the cost of dataset preparation, the paper suggests constructing reference packet-length distributions from unencrypted traffic samples with subsequent adjustment for encapsulation headers and tunnel parameters. Another important aspect is the analysis of mixed traffic. Since multiple traffic types may coexist in the same encrypted channel, the paper proposes iterative analysis with predictive subtraction of already identified traffic patterns, especially for periodic traffic such as voice or video streams. This facilitates the detection of additional protocols that are initially masked by dominant flows.

Finally, a practical implementation concept is outlined in the form of multiple traffic sensors coordinated by a central orchestrator. Each sensor is responsible for detecting a specific class of traffic within a time window, while the orchestrator estimates and refines encrypted channel parameters and distributes them across the analysis modules. The proposed approach does not require payload decryption or neural networks, which reduces computational costs and makes it suitable for deployment in passive real-time traffic monitoring systems.

Keywords: encrypted traffic, IPsec, ESP packet, traffic analysis, malicious activity detection, packet length distribution, TLS fingerprinting, VPN channel, passive monitoring, information security.

Стаття надійшла до редакції / Received 11.03.2026
Прийнята до друку / Accepted 16.04.2026
Опубліковано / Published 31.05.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Частка шифрованого трафіку в сучасних мережах постійно зростає. Протоколи HTTPS і QUIC майже повністю витіснили незахищений HTTP, а для інших сервісів дедалі частіше застосовують механізми шифрування або VPN. Це підвищує конфіденційність передавання даних, але одночасно ускладнює виявлення шкідливої мережевої активності. Зокрема, шкідливий трафік може маскуватися під легітимний і приховувати взаємодію з керувальними серверами.

Наявні системи виявлення та запобігання вторгненням здатні фіксувати підозрілу активність у мережі, однак їхня ефективність істотно знижується в умовах поширення шифрованого трафіку. Традиційні підходи, засновані на аналізі вмісту пакетів або сигнатурах відомих загроз, не забезпечують належного рівня виявлення прихованих або нових типів атак.

Отже, актуальною є задача розроблення методів виявлення шкідливої активності в шифрованих каналах зв'язку без дешифрування вмісту, на основі аналізу доступних пасивному спостерігачу ознак, зокрема розподілу довжин пакетів, напрямків передавання та параметрів тунелю.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У сучасних дослідженнях шифрованого трафіку важливе місце посідають підходи, засновані на аналізі мережевих і протокольних відбитків. Зокрема, визначення реалізації клієнтського TLS-протоколу за ознаками TLS-рукостискання стало основою для розвитку методів TLS-фінгерпринтингу. Такі підходи застосовуються для виявлення аномалій, підозрілих реалізацій протоколів і потенційно шкідливої мережевої активності [1-3].

Проблематиці класифікації трафіку, що передається в шифрованих мережах зв'язку, присвячено значну кількість сучасних робіт [2,4]. Ці підходи демонструють добрі результати у визначенні типу трафіку за розподілом довжин пакетів як для окремих TLS-сеансів, так і для трафіку, переданого всередині VPN-каналів. У багатьох дослідженнях для аналізу використовуються моделі машинного навчання або глибокого навчання, а одним з основних інформативних наборів ознак виступає нормалізований у часі та за розміром розподіл довжин пакетів.

Однією з близьких за призначенням систем аналізу трафіку для виявлення атак є клас NDR/NTA-рішень, що здійснюють поведінковий аналіз мережевого трафіку, виявлення прихованих загроз і дослідження підозрілої активності, зокрема також у шифрованому трафіку [5]. Такі системи можуть працювати на різних ділянках мережі: до міжмережевого екрана, після нього або на дзеркалі трафіку комутаторів, залежно від архітектури розгортання та джерела телеметрії.

Для високошвидкісного захоплення трафіку в сучасних системах мережевого моніторингу можуть застосовуватися такі механізми, як DPDK, PACKET_MMAP / AF_PACKET та PF_RING [6,7]. Їх використання дає змогу підвищити продуктивність захоплення пакетів і зменшити накладні витрати під час аналізу трафіку в реальному часі.

У сучасних засобах аналізу шифрованого трафіку широко застосовуються TLS-відбитки у форматах JA3/JA3S, а також новіші підходи на кшталт JA4 [8, 9]. Такі засоби ефективні для задач точного зіставлення відомих реалізацій, однак вони гірше враховують ступінь подібності між близькими реалізаціями протоколів. Крім того, використання лише хешованого представлення відбитка спрощує зіставлення, але обмежує можливості змістовного аналізу його структури.

Отже, попри розвиток методів аналізу шифрованого трафіку, задача виявлення шкідливої активності всередині VPN-каналів без дешифрування вмісту залишається актуальною. Особливої уваги потребують підходи, що поєднують низьку обчислювальну складність, придатність до роботи в реальному часі та використання ознак, доступних пасивному спостерігачу, зокрема розподілу довжин пакетів і параметрів шифрованого каналу.

ВИЯВЛЕННЯ ШКІДЛИВОЇ АКТИВНОСТІ В ШИФРОВАНИХ КАНАЛАХ ЗВ'ЯЗКУ

Для визначення складу протоколів, що використовуються в шифрованому каналі, пропонується розбити сеанс на невеликі часові інтервали Δt. Для кожного такого інтервалу формується перелік довжин

пакетів, зафіксованих у відповідний проміжок часу. На основі цього будується розподіл нормалізованих довжин пакетів, тобто довжин, поділених на розмір блока шифрування. Аналіз такого розподілу дає змогу виявляти характерні закономірності, притаманні окремим типам трафіку.

До інформативних ознак належать:

– серії сталих значень довжин пакетів в одному з напрямків у суміжних часових інтервалах; це характерно, зокрема, для VoIP-сеансів, де довжина пакета визначається використовуваним аудіокодеком;

– сталі значення довжин пакетів, за якими слідує серія інших сталих значень; така картина типова для протоколів із запитами фіксованого розміру та відповідями на них;

– утворення пар серій сталих значень в одному напрямку, причому одна з них часто близька до максимальної можливої довжини пакета; подібна ознака спостерігається, наприклад, під час роботи протоколу віддаленого робочого столу Windows;

– наявність верхньої межі довжин пакетів для певного напрямку передавання;

– поява в короткому часовому інтервалі широкого спектра довжин пакетів за відсутності активності або за значно вужчого спектра в сусідніх інтервалах; така картина характерна для передавання файлів.

Характерні відмінності між такими ознаками розподілу довжин пакетів для VoIP-, FTP- та RDP-трафіку схематично показано на рис. 1.

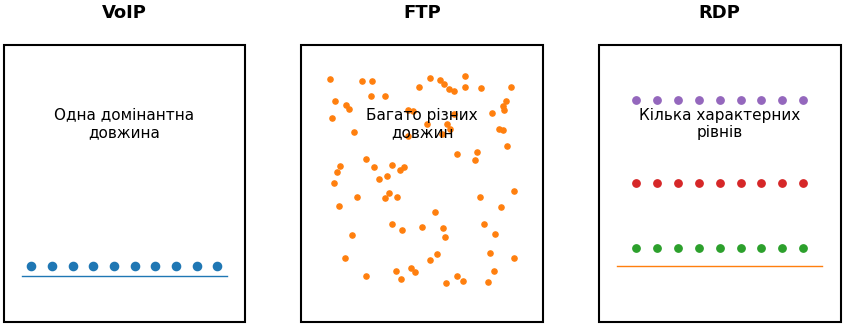

Рис.1 Схематичне порівняння характерних ознак трафіку в шифрованому каналі

Абсолютні значення довжин пакетів залежать від параметрів шифрування і конфігурації VPN-каналу. Якщо конфігурація каналу відома, ці значення можуть бути оцінені. Зокрема, максимальна довжина спостережуваних пакетів визначається як MTU (максимальний розмір пакета без фрагментації) каналу зв'язку, а MTU всередині тунелю додатково зменшується на розмір службових заголовків інкапсуляції.

OpenVPN підтримує різні режими роботи та може використовувати як TCP-, так і UDP-транспорт. Частина службових ознак OpenVPN-пакетів, зокрема тип повідомлення, залишається доступною пасивному спостерігачу, що робить можливим частковий аналіз такого трафіку без дешифрування. Водночас для задачі визначення типів трафіку за розподілом довжин пакетів більш придатним є IPsec, оскільки в ньому зв'язок між довжиною зовнішнього пакета та структурою вкладеного навантаження є стабільнішим.

У IPsec транспортом захищених даних є ESP (Encapsulating Security Payload), який може передаватися безпосередньо після IP-заголовка як протокол із кодом 50 або всередині UDP-пакета. IPsec підтримує два основні режими роботи:

– транспортний режим, у якому шифрується лише корисне навантаження IP-пакета, а початковий IP-заголовок зберігається;

– тунельний режим, у якому весь вихідний IP-пакет, включно з адресною інформацією, поміщається всередину нового зашифрованого пакета. На практиці цей режим часто використовується разом із L2TP.

Залежно від обраної конфігурації, вміст корисного навантаження ESP-пакета містить сталу складову, довжина якої визначається режимом роботи тунелю. Для транспортного режиму така складова відсутня, для тунельного режиму вона включає щонайменше вкладений IP-заголовок, а у випадку використання L2TP – ще й службові поля відповідного протокольного стеку. Це означає, що навіть без дешифрування вмісту довжина пакета частково визначається не лише даними, що передаються, а й конфігурацією самого каналу.

Для пасивного спостерігача це має принципове значення: розмір ESP-пакета формується як сума корисного навантаження та службових заголовків, розміри яких у межах конкретної конфігурації є передбачуваними. Саме тому параметри IPsec-каналу можна враховувати під час аналізу розподілу довжин пакетів і використовувати для оцінювання типу трафіку, що передається всередині шифрованого каналу. Ця властивість робить IPsec зручнішим для побудови методу пасивного аналізу, ніж ті VPN-рішення, у яких довжини пакетів менш стабільно пов'язані зі структурою вкладених даних.

Для IPsec-каналів довжина ESP-пакета визначається не лише обсягом корисного навантаження, а й сукупністю службових полів, параметрами вкладеного стеку та паддінгом. Завдяки цьому між довжиною

спостережуваного ESP-пакета та довжиною переданих усередині даних існує формалізований зв'язок. Це дає змогу перейти від емпіричного аналізу розподілу довжин до моделі, що враховує параметри конкретного шифрованого каналу.

У загальному випадку довжина ESP-пакета визначається як:

$$S_{ESP} = H_{ESP} + TR_{ESP} + IV_{ESP} + AUT_{ESP} + L_D + L_{STACK} + PAD_{ESP}, \quad (1)$$

де S_{ESP} – довжина ESP-пакета; H_{ESP} – довжина заголовка ESP; TR_{ESP} – довжина трейлера ESP; IV_{ESP} – довжина вектора ініціалізації; AUT_{ESP} – довжина поля автентифікації; L_D – довжина вкладеного корисного навантаження; L_{STACK} – довжина вкладеного службового стеку протоколів; PAD_{ESP} – довжина паддінгу.

Величина паддінгу визначається розміром блока шифрування та обчислюється за формулою

$$PAD_{ESP} = (BL - ((L_D + L_{STACK} + TR_{ESP}) mod\ BL)) \,\&\, (BL - 1), \quad (2)$$

де BL – розмір блока алгоритму шифрування. З формули (2) випливає, що сума $PAD_{ESP} + L_D + L_{STACK} + TR_{ESP}$ завжди є кратною BL, а отже, за відомих або оцінених параметрів каналу можна визначати допустимі діапазони довжин вкладених даних за спостережуваною довжиною зовнішнього ESP-пакета.

Таким чином, формули (1)-(2) дають змогу пов'язати спостережувані характеристики шифрованого трафіку з параметрами вкладеного навантаження. Це особливо важливо в тих випадках, коли в розподілі одночасно з'являються кілька характерних ліній, пов'язаних з одним типом трафіку. Наприклад, під час передавання великих порцій даних одночасно можуть проявлятися лінії, що відповідають максимальному розміру пакета та залишку порції. У такому разі для класифікації доцільно враховувати не лише абсолютні довжини пакетів, а і їх відносні значення, а також допустимі діапазони розмірів вихідних, ще не зашифрованих даних, визначені на основі формул (1)-(2).

На основі описаної моделі пропонується такий порядок визначення типів трафіку всередині IPsec-каналу (рис.2):

- визначення або уточнення параметрів шифрованого каналу;
- побудова часового розподілу довжин пакетів для двох напрямків передавання;
- обчислення допустимих діапазонів довжин вкладеного навантаження за формулами (1)-(2);
- зіставлення отриманих розподілів із характерними шаблонами типових протоколів;
- формування висновку щодо наявності певних типів трафіку в шифрованому каналі.

Для практичного застосування запропонованого алгоритму недостатньо лише побудови розподілу довжин пакетів і його зіставлення з типовими шаблонами. Точність визначення типів трафіку істотно залежить від параметрів конкретного шифрованого каналу, тому наступним етапом є формування еталонних розподілів для заданої конфігурації інкапсуляції.

Ефективність визначення типів трафіку в шифрованому каналі істотно залежить від параметрів конкретної конфігурації каналу. За коректного врахування параметрів шифрованих каналів одночасно зменшується кількість помилок першого і другого роду. З цієї причини часткова модель, побудована для конкретної конфігурації шифрованого каналу, є ефективнішою за універсальну модель, орієнтовану на всі можливі конфігурації.

Водночас формування повноцінних наборів даних для кожної можливої конфігурації шифрованого каналу на основі реального зашифрованого трафіку є трудомістким і пов'язане з ризиком потрапляння до вибірки сторонніх типів трафіку. Тому доцільним є підхід, за якого еталонні розподіли довжин пакетів будуються на основі незашифрованих зразків трафіку з подальшим урахуванням розмірів службових заголовків і параметрів інкапсуляції конкретного шифрованого каналу.

Такий підхід дає змогу, маючи еталонний трафік відомого типу, змоделювати, як саме він виглядатиме після інкапсуляції та шифрування в заданій конфігурації шифрованого каналу. У результаті можна сформувати набір очікуваних розподілів довжин пакетів без необхідності окремого запису трафіку для кожної комбінації параметрів каналу.

Істотним обмеженням багатьох підходів до класифікації шифрованого трафіку є те, що вони демонструють добрі результати переважно тоді, коли в каналі присутній лише один тип трафіку. У реальних шифрованих каналах зв'язку, навпаки, зазвичай одночасно передається кілька типів трафіку, і їхні характеристики накладаються одна на одну в сумарному розподілі довжин пакетів.

Додаткову складність становить те, що звичайний розподіл довжин пакетів не дає змоги безпосередньо визначити, скільки одночасних сесій одного й того самого типу наклалося в межах одного часового інтервалу. Найбільш придатними для такого аналізу є протоколи з чіткою періодичністю передавання пакетів, зокрема мовні та відеопотоки. Розподіли довжин для таких сеансів є достатньо прогнозованими, що дає змогу після ідентифікації одного з типів трафіку предиктивно відняти його внесок із сумарного розподілу довжин пакетів. Після такого віднімання полегшується виявлення інших протоколів, які

до цього маскувалися домінантним або регулярним трафіком. Схематично цей ефект показано на рис. 3.

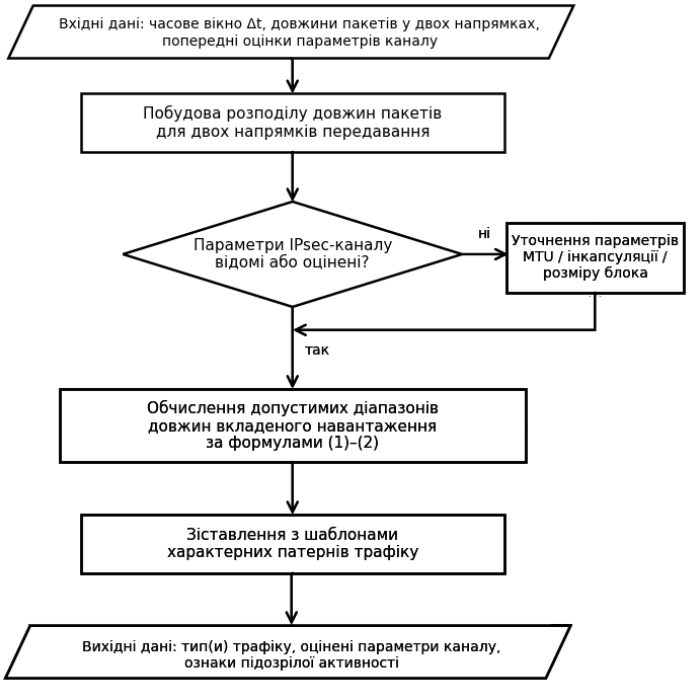

Рис. 2. Блок-схема визначення типів трафіку в IPsec-каналі за розподілом довжин пакетів

З практичного погляду це означає, що аналіз трафіку в шифрованих каналах може виконуватися ітеративно: спочатку виявляються найбільш стабільні та добре прогнозовані типи трафіку, після чого їхній внесок виключається із сумарного розподілу. Такий підхід дає змогу перейти від аналізу “одного домінантного патерна” до послідовного розпізнавання кількох типів трафіку в одному шифрованому каналі.

Практична реалізація запропонованого підходу може бути побудована у вигляді набору програмних модулів-сенсорів і центрального модуля-оркестратора. Кожен сенсор орієнтований на виявлення одного конкретного класу трафіку у заданому часовому вікні на основі аналізу розподілу довжин пакетів, сформованого сукупністю одночасно передаваних протоколів.

Важливою умовою такої реалізації є можливість використовувати достовірно визначені параметри конкретного шифрованого каналу одним сенсором під час аналізу іншими сенсорами. Це дає змогу враховувати специфіку конфігурації шифрованих каналів не ізольовано, а на рівні всієї системи аналізу. При цьому не можна спиратися лише на одне абсолютне значення MTU, оскільки воно може відрізнятися навіть для різних сесій одного й того самого протоколу. Також необхідно враховувати можливу фрагментацію пакетів, за якої великі пакети розбиваються на кілька фрагментів і формують окремий характерний патерн у розподілі довжин.

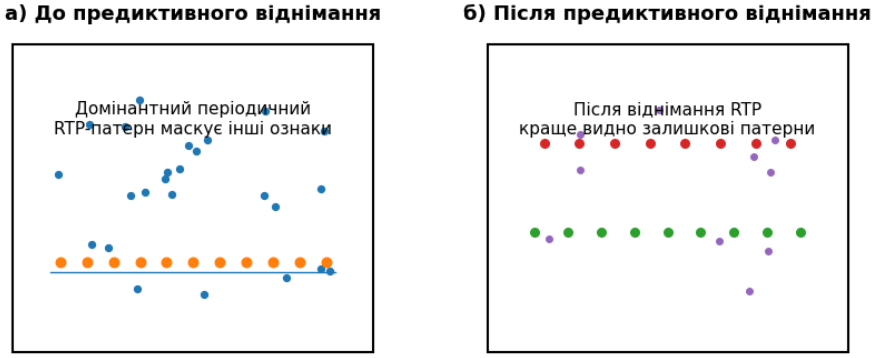

Рис.3. Схематичне порівняння розподілу довжин пакетів до та після предиктивного віднімання внеску RTP-пакетів у VoIP-трафіку

Центральний модуль-оркестратор виконує визначення типу та можливих параметрів шифрованого каналу, передає ці параметри сенсорам разом із вхідними даними – розподілом довжин пакетів для поточного часового вікна – і надалі уточнює параметри шифрованих каналів на основі відповідей окремих сенсорів. Така архітектура дає змогу поєднати аналіз різних класів трафіку в межах єдиної системи й послідовно уточнювати гіпотези щодо складу трафіку та параметрів каналу.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШОГО РОЗВИТКУ У ДАНОМУ НАПРЯМІ

У статті розглянуто підхід до виявлення шкідливої активності в шифрованих каналах зв'язку без дешифрування вмісту трафіку. Показано, що для пасивного спостерігача інформативними залишаються розподіл довжин пакетів у часі, напрямки передавання та параметри інкапсуляції шифрованого каналу. Це дає змогу визначати характерні ознаки окремих типів трафіку навіть за відсутності доступу до корисного навантаження.

Обґрунтовано доцільність використання IPsec як основного об'єкта аналізу, оскільки для нього існує формалізований зв'язок між довжиною зовнішнього ESP-пакета та параметрами вкладеного навантаження. На цій основі подано модель визначення допустимих діапазонів довжин вкладених даних і запропоновано алгоритм визначення типів трафіку в IPsec-каналі за розподілом довжин пакетів.

Показано, що ефективність аналізу істотно залежить від параметрів конкретної конфігурації шифрованого каналу. Тому для практичного застосування доцільно використовувати часткові моделі й еталонні розподіли, побудовані для конкретних параметрів інкапсуляції, а не універсальні схеми, орієнтовані на всі можливі конфігурації.

Окремо розглянуто задачу аналізу змішаного трафіку в шифрованому каналі. Показано, що для протоколів із добре прогнозованими патернами, зокрема для мовних і відеопотоків, доцільним є предиктивне віднімання вже ідентифікованого трафіку із сумарного розподілу довжин пакетів, що полегшує подальше виявлення інших типів трафіку.

Запропонований підхід не потребує дешифрування вмісту та використання нейронних мереж, що зменшує обчислювальні витрати і робить його придатним для практичної реалізації в системах мережевого моніторингу. Перспективою подальших досліджень є експериментальна оцінка точності методу для різних конфігурацій шифрованих каналів, а також розширення набору шаблонів для виявлення інших типів підозрілої активності.

References

1. Alwhbi, I.A.; Zou, C.C.; Alharbi, R.N. Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning. Sensors 2024, 24, 3509. https://doi.org/10.3390/s24113509

2. Wireshark Foundation. Transport Layer Security (TLS) field reference. URL: wireshark.org/docs/dfref/t/tls.html

3. Cisco. Mercury: Network metadata capture and analysis. GitHub repository. URL: github.com/cisco/mercury

4. Sharma A. A survey on encrypted network traffic: A comprehensive review of machine learning and deep learning approaches // Computer Networks. 2025. URL: https://doi.org//10.1016/j.comnet.2024.110984

5. Fortinet. What Is Network Detection and Response (NDR)? URL: fortinet.com/resources/cyberglossary/what-is-ndr

6. Larin D. V., Get'man A. I. Tools for Capturing and Processing High-Speed Network Traffic // Programming and Computer Software. 2022. Vol. 48. P. 756–769. DOI: https://doi.org/10.1134/S0361768822080011

7. Emmerich P., Pudelko M., Gallenmüller S., Carle G. FlowScope: Efficient Packet Capture and Storage in 100 Gbit/s Networks // 2017 IFIP Networking Conference (IFIP Networking). 2017. DOI: https://doi.org/10.23919/IFIPNetworking.2017.8264852

8. Heino J., Hakkala A., Virtanen S. Categorizing TLS Traffic Based on JA3 Pre-Hash Values // Procedia Computer Science. 2023. Vol. 220. P. 94–101. DOI: https://doi.org/10.1016/j.procs.2023.03.015

9. Matoušek P., Ryšavý O., Burgetová I. Experience Report: Using JA4+ Fingerprints for Malware Detection in Encrypted Traffic // Proceedings of the 20th International Conference on Network and Service Management (CNSM). 2024. P. 1–5. DOI: https://doi.org/10.23919/CNSM62983.2024.10814358