ISSN 2519-2310 (Online)

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2025, № 2 (28)

COMPUTER SCIENCE AND CYBERSECURITY, 2025, Iss. 2 (28)

https://doi.org/10.26565/2519-2310-2025-2-04
УДК 004.056:004.7:004.89

АНАЛІЗ МЕТАДАНИХ ШИФРОВАНОГО ТРАФІКУ ДЛЯ УСУНЕННЯ «СЛІПИХ ЗОН» БЕЗПЕКИ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Максим Горелько[1], студент (бакалаврат, спеціальність F5), кафедра кібербезпеки інформаційних систем, мереж і технологій, e-mail: maksym.horelko@student.karazin.ua,
Сергій Малахов[1], к.т.н., ст. науковий співробітник, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, e-mail: malakhov@karazin.ua,
ORCID: https://orcid.org/0000-0001-8826-1616
[1]*Харківський національний університет імені В.Н. Каразіна, 61022, проспект Свободи, 4, Харків, Україна*

Рукопис надійшов 1 вересня 2025 р. Отримано після рецензування 1 жовтня 2025 р.
Прийнято 2 листопада 2025 р. Опубліковано 30.12.2025 р.

Анотація: Запропоновано огляд останніх напрацювань в межах проблематики комплексного аналізу зашифрованого мережевого трафіку в сучасних інформаційних системах. Основними методами досліджень є: - аналіз, узагальнення та порівняння. Розглянуті питання пошуку можливих шляхів забезпечення компромісу в умовному трикутнику «факторів впливу» при вирішенні завдань оперативного виявлення небезпек в структурі даних зашифрованого трафіку. В якості «факторів впливу» розглянута комбінація наступних чинників: - необхідність забезпечення потрібного рівня інформаційної безпеки (ІБ); - підтримка права користувачів на їх конфіденційність; - ресурсний консенсус впроваджуваних програмно-апаратних рішень. Звернено увагу, що інтеграція технологій штучного інтелекту і машинного навчання (AI/ML) до структури алгоритмів контролю трафіку, є ключовим важелем впливу на кінцевий результат. Підкреслено, що протидіюча сторона, також буде використовувати ці технології для маскування своєї діяльності. Зроблено висновок, що впровадження процедур аналізу метаданих мережевого трафіку, є компромісним рішенням. Реалізація такого підходу дозволяє покращити «прозорість» поточної мережевої активності для завчасного виявлення загроз безпеки, безпосередньо не вдаючись до процедур дешифрування трафіку. Акцентовано увагу, що впровадження парадигми «Cyber Deception» та комплексний аналіз метаданих циркулюючого шифрованого трафіку, є перспективним вектором зусиль для завчасного нівелювання фактору утворення «сліпих зон» безпеки сучасних IT систем.

Ключові слова: *трафік, фільтрація, відбитки трафіку, патерн, інформаційна безпека, VPN, Tor, Cyber Deception*

Як цитувати: Горелько М., Малахов С., Аналіз метаданих шифрованого трафіку для усунення «сліпих зон» безпеки сучасних інформаційних систем. *Комп'ютерні науки та кібербезпека*. 2025; № 2(28): С. 40–50. https://doi.org/10.26565/2519-2310-2025-2-04

In cites: Horelko M., Malakhov S. (2025). Metadata analysis of encrypted traffic to eliminate security «Blind Spots» of modern information systems. *Computer Science and Cybersecurity.* 2(28): 40–50. https://doi.org/ 10.26565/2519- 2310-2025-2-04 (in Ukrainian)

1. Вступ

В сучасному світі телекомунікацій, технології шифрування трафіку VPN та Tor [1-2], де-факто стали стандартом для захисту чутливих даних користувачів в корпоративному та приватному сегментах ринку інформаційних послуг. Однак, на шляху практичної імплементації відповідних рішень існують певні труднощі, що обумовлені «подвійною» природою процесу шифрування. Так, з одного боку, воно є необхідним для забезпечення конфіденційності і цілісності даних, де відмова від процедур шифрування трафіку або його «ослаблення» є неприйнятним (з різних причин). З іншої сторони, впровадження процедур шифрування створює «великий» бар'єр для традиційних систем моніторингу поточного стану інформаційної безпеки (ІБ), які покладаються на перевірку вмісту пакетів даних, що циркулюють в межах умовного периметру безпеки. Така інженерна дилема не є проблемою, яку можна «вирішити» в один крок – «раз і назавжди», що зумовлено неперервною ґенезою IT-технологій. Інакше кажучи, така суперпозиція умов роботи сучасних інформаційно-комунікаційних систем (ІКС), є новою реальністю, до якої системи безпеки повинні швидко адаптуватися.

Метою роботи є стислий огляд і узагальнення сучасного досвіду в галузі створення інтелектуальних систем реального часу для цілей аналізу метаданих шифрованого трафіку, що базуються на широкої імплементації можливостей технологій AI/ML.

Ключовими питаннями, що розглядаються є: - передумови утворення «сліпих зон» безпеки в структурі сучасних ІКС, котрі зумовлені присутністю (циркуляцією) шифрованого трафіку; - можливі напрями зусиль для вирішення завдань комплексного аналізу метаданих шифрованого трафіку з метою завчасного виявлення загроз безпеки, без виконання ресурсоємних (умовно «важких») процедур дешифрування.

2. Основна частина

2.1 Технологічний контекст й обмеження «традиційного» моніторингу та вплив новітніх стандартів шифрування

Розглянемо обидва підходи шифрування трафіку, VPN та Tor. Технологія VPN (Virtual Private Network) створює зашифрований «тунель» поверх публічної мережі і виступає, як умовний проксі-сервер, що приховує IP-адресу відправника даних та шифрує трафік [1]. Tor (*The Onion Router*) – це децентралізована мережа, що забезпечує анонімність користувача шляхом маршрутизації його трафіку через ланцюжок випадкових мережевих вузлів [2]. В цьому разі багатошарове шифрування гарантує, що кожен вузол знає лише попередній й наступний елементи ланцюжка, що робить відстеження вихідного джерела надзвичайно складним. Кіберзлочинці активно використовують обидві технології для приховування власної інфраструктури, управління ботнетами, проведення атак, поширення шкідливого програмного забезпечення (ПЗ) та непомітного витоку конфіденційних даних. При цьому традиційні системи безпеки, такі як системи виявлення вторгнень (IDS) чи глибокого аналізу пакетів (DPI), стають менш ефективні, оскільки не можуть аналізувати вміст зашифрованих пакетів.

Окремим викликом для сучасних систем моніторингу трафіку, став перехід мережі Інтернет на протокол TLS 1.3. В минулих версіях протоколу процедура «рукостискання» передавалася у відкритому вигляді, проте в TLS 1.3 шифрується вже більшість параметрів узгодження, включаючи серверний сертифікат. Це робить традиційні методи перевірки валідності сертифікатів без дешифрування (пасивний SSL/TLS аналіз) неможливими. Більш того, впровадження розширення ECH (*Encrypted Client Hello*) [3] закриває останню вразливість в приватності – поле SNI (Server Name Indication), яке раніше дозволяло ідентифікувати доменне ім'я цільового ресурсу. В умовах використання протоколу TLS 1.3 з ECH, пасивний

спостерігач «бачить» лише факт встановлення з'єднання з певною IP-адресою, але не може визначити конкретний сервіс чи хост. Саме це нівелює ефективність сигнатурних методів, таких як JA3/JA3S, змушуючи системи безпеки остаточно змістити фокус зі звичайного/традиційного аналізу заголовків на поведінковий аналіз часових рядів та статистичних характеристик потоку (*Deep Packet Dynamics*).

2.2 Методологія «Traffic Fingerprinting» та її особливості

Як було зазначено вище, в умовах, коли безпосередній аналіз вмісту є неможливий або обтяжливим (*перш за все, з точки зору балансу прикладених зусиль та отримуваного ефекту*), фокус зусиль поступово зміщується на процес аналізу метадані. Цей підхід базується на концепції т.з. «відбитків трафіку» (*Traffic Fingerprinting*), так як будь-яка діяльність в мережі практично завжди залишає унікальний та відтворювальний патерн відповідного мережевого трафіку, навіть якщо його вміст був зашифрован [4]. Ці патерни складаються з таких характеристик, як: - послідовність, розмір пакетів, часові інтервали між ними та напрямок передачі, періодичність й інтенсивність сеансів та ін. При цьому одним з найкращих векторів зусиль для класифікації є послідовність розмірів пакетів. Відомо, що різні програмні застосунки мають різні характерні патерни. Так наприклад, трафік VoIP (Voice over Internet Protocol) складається з великої кількості малих пакетів однакового розміру, що передаються через рівні проміжки часу. Веб-серфінг є асиметричним: - короткі запити від клієнта та значно більші відповіді від сервера. Водночас командно-керуючий (C&C) трафік ботнетів може проявлятися у вигляді дуже малих, періодичних «heartbeat» пакетів. Таким чином, всі ці патерни суттєво відрізняються, як від трафіку звичайного інтернет користувача, так і від передачі великих обсягів даних, що робить їх «помітними» для систем аналізу трафіку (звісно, в разі якщо це не є робота HoneyPot [5]). Часові характеристики трафіку, наприклад інтервали між послідовними пакетами (Inter-Arrival Times), надають цінну інформацію про «природу» даної комунікації. Цей вектор аналізу даних особливо ефективний для відокремлення антропогенної мережевої активності від трафіку породжуваного роботою автоматизованих процесів/систем. Класичним прикладом є аналіз трафіку сесії SSH (*Secure Shell*). Оскільки протокол SSH в інтерактивному режимі відправляє в окремому пакеті відомості про кожне натискання юзером умовних клавіш, то аналіз часових проміжків між цими пакетами дозволяє відтворити ритм набору символів, звичайно за умови якщо це не є наслідком навмисної роботи поведінкового аватару в рамках його сценарного полю [5]. На противагу цьому, технологічна C&C комунікація ботнету, часто відбувається через фіксовані, автоматично генеровані інтервали (тайм-слоти). Також, в межах дослідження «відбитків трафіку», використовується аналіз на рівні мережевих потоків (*Flows*) за допомогою протоколів NetFlow та IPFIX (*Internet Protocol Flow Information Export*) [6-7]. В цілому, ключові метадані Flows, що використовуються для аналізу «відбитків», включають:

- Ідентифікатори потоку: IP-адреси, порти джерела й призначення, протокол (TCP/UDP). Хоча мережі VPN та Tor маскують реальну IP-адресу, ця інформація залишається корисною для аналізу внутрішніх патернів та зв'язків з відомими «шкідливими» серверами;
- Статистика потоку: Тривалість сесії, загальна кількість переданих пакетів та байтів в обох напрямах (як є, тобто без урахування впливу поведінкових аватарів);
- Метадані TLS Handshake: Цінність аналізу TLS-рукостискання полягає в тому, що ще до початку будь-якого шифрування, можливо ідентифікувати ПЗ, що «виходить» в мережу. Те, як програма пропонує шифрувати дані, зумовлює її унікальний «відбиток» (JA3 FingerPrinting). Це дозволяє системам ІБ відрізнити, наприклад легітимний браузер від відомої сигнатури вірусу і заблокувати загрозу ще на етапі підключення [8].

- Сертифікати: Аналіз SSL/TLS сертифікатів (навіть без дешифрування) полягає у швидкій перевірці легітимності сервера. Зловмисники часто економлять на належній інфраструктурі чи цілісності заходів, тому використання ними підозрілих сертифікатів є поширеною практикою. В цьому разі, коли система ІБ «бачить» самопідписаний сертифікат, сертифікат від невідомого центру або з нештатними параметрами (наприклад, невідповідність домену) - це може свідчити, що сервер, ймовірно, є частиною шкідливої інфраструктури, наприклад, фішинговим сайтом, сервером управління ботнетом тощо [9].

2.3 Специфіка аналізу «анонімізуючих» мереж (на прикладі Tor)

Практичні підходи до аналізу трафіку Tor включають заходи на основі парсінгу т.з. «відбитків веб-сайтів» (*Website Fingerprinting, WF*). Відповідні зусилля полягають в спробі ідентифікації відвідуваних сайтів через унікальні патерни розмірів та часу пакетів. Так наприклад, автори роботи [10] свідчать, що хоча в контрольованих «лабораторних» умовах точність висока (95% для 5 сайтів), у реальних сценаріях подій вона стрімко падає (*до 60% при 100 сайтах*). Більш практичний підхід передбачає «онлайн навчання» з використанням справжнього трафіку. У цій парадигмі дій, зловмисник може збирати репрезентативні дані для навчання власної інфраструктури, наприклад, керуючи власним вихідним вузлом (*Exit Relay*) у легітимній мережі «Tor». Це потенційно дозволяє йому отримувати частину справжніх даних з DNS-запитів [11] до моменту встановлення TLS-з'єднання, і постійно оновлювати модель, враховуючи реальну поведінку легітимних користувачів. Проте даний шлях має суттєвий недолік: - результати WF аналізу суттєво залежать від масштабу здійснюваного моніторингу.

Узагальнюючи результати дослідження [12] можна констатувати, що більшою загрозою для Tor є атаки на основі кореляції потоків – «*Stream Correlation Attacks*». В межах цієї концепції подій, зловмисник, що спостерігає за Tor-трафіком на вході (*R1*) та виході (*R3*) ланцюга, може зіставити відповідні потоки (*див. Рис.1*).

$$Alice \xrightarrow{[M]_{K_{3,2,1}}} R_1 \xrightarrow{[M]_{K_{3,2}}} R_2 \xrightarrow{[M]_{K_3}} R_3 \xrightarrow{M} Bob$$

Рис. 1 – Умовний ланцюг TOR
Fig. 1 – Tor circuit [12]

В цьому разі, атака покладається не на вміст, а на аналіз патернів часу, що зумовлено тим що мережа «Tor» використовує комірки фіксованого розміру в 512 байт (*див. Рис.2*) [12].

В межах цієї концепції, атакуючий може приховано (сніфити) порівнювати затримки між різними комірками «Tor» або штучно створювати часові ряди (задаючи кількість комірок у N-секундному вікні) та, потім, статистично порівнювати параметри векторів R1 та R3 (рис. 1).

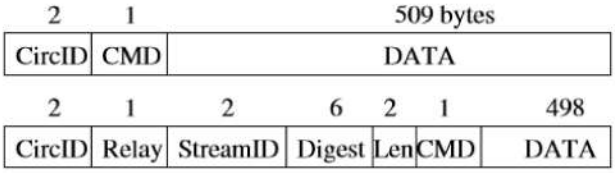

Рис. 2 – Структура комірки TOR
Fig. 2 – Tor cell structure

Відомі і активні атаки: - зловмисник на R1 навмисно вносить зміни в потік (затримка або відкидання комірок), таким чином створюючи власний «водяний знак», який можна ідентифікувати на R3. Такі атаки можуть досягати 99% точності [12]).

2.4 Ідентифікація та аналіз VPN-тунелів

Поряд з цим, VPN трафік, також, має певні вразливості. Оскільки VPN-протоколи, на відміну від Tor, не стандартизують розміри пакетів, вони є потенційно більш вразливими до аналізу. Автори дослідження [13] продемонстрували можливість ідентифікації сеансів OpenVPN з 85% ефективністю. Архітектура відповідної системи (див. Рис.3) передбачає двоетапний підхід. Спочатку мережевий трафік (1) перенаправлявся на відповідний «фільтр» (2), котрий резидентно аналізував весь обсяг даних (зі швидкістю близько 20 Гбіт/с), виявляючи IP-адреси, які поводилися, як VPN-сервери (точка 3, на рис. 3). На 2-му етапі всі «підозрілі» адреси (4) передавалися відповідним «тестувачам» для їх активної перевірки (точка 5 «Пробери»). Якщо за результатами перевірки, сервер підтверджував, що він є OpenVPN, то його додавали до бази даних (6) для подальшого аналізу.

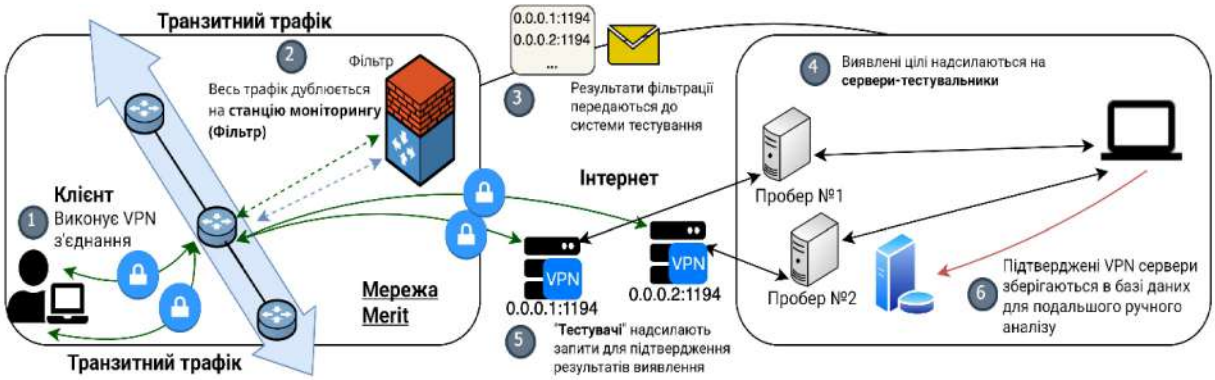

Рис. 3 – Спрощена архітектура системи пасивного моніторингу трафіку для ідентифікації роботи VPN-серверів

Fig. 3 – Simplified architecture of a passive traffic monitoring system for identifying the operation of VPN servers [13]

В цілому, запропонований авторами роботи [14], алгоритм ідентифікації роботи OpenVPN, базується на трьох характеристиках:

По-перше: - аналіз послідовності «*opcode*» (тобто, кодів операцій) у незашифрованих заголовках пакетів «*каналу управління*» під час процедури *TLS Handshake* (*див. Рис.4*) [13];

По-друге: - аналіз «унікальних» розмірів IP пакетів. Інфографіка на Рис.5 свідчить про те, що OpenVPN (*світло-сині стовпці*) демонструє надзвичайно високі «сплески» для певних довжин пакетів-відповідей (*Probe Length*), особливо в діапазоні 1400-1600 байт, на відміну від випадкового трафіку (*стовпці помаранчевого кольору*). Пунктирна темно-синя зростаюча крива (*легенда - OpenVPN CDF, де CDF (Cumulative Distribution Function) - Інтегральна функція розподілу*) стрімко зростає в цих точках, підтверджуючи, що більшість серверів системи OpenVPN відповідають пакетами передбачуваного розміру;

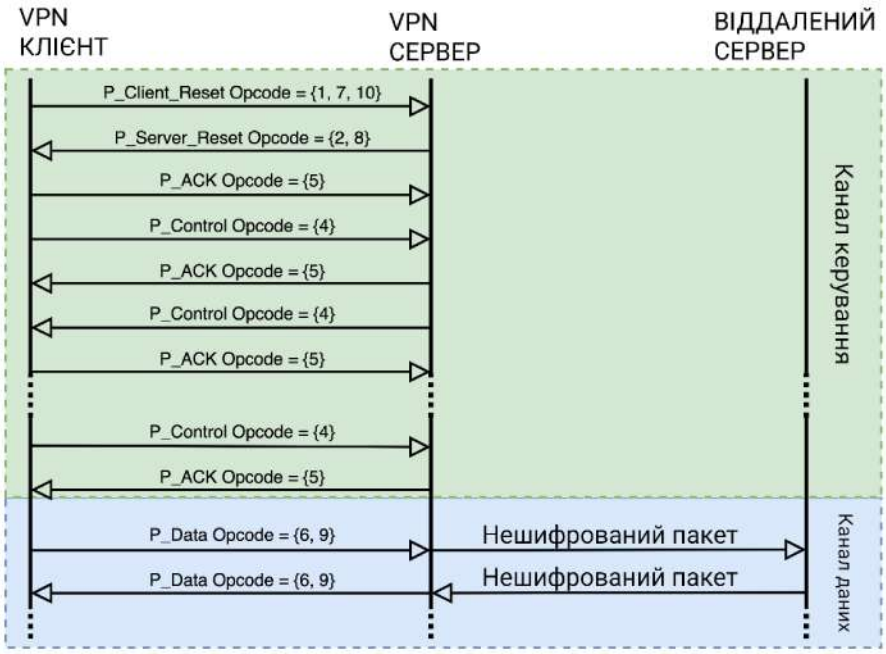

Рис. 4 – Послідовність обміну пакетами та їх «opcode» під час встановлення з'єднання OpenVPN
Fig. 4 – Packet exchange sequence and opcodes during OpenVPN connection establishment [13]

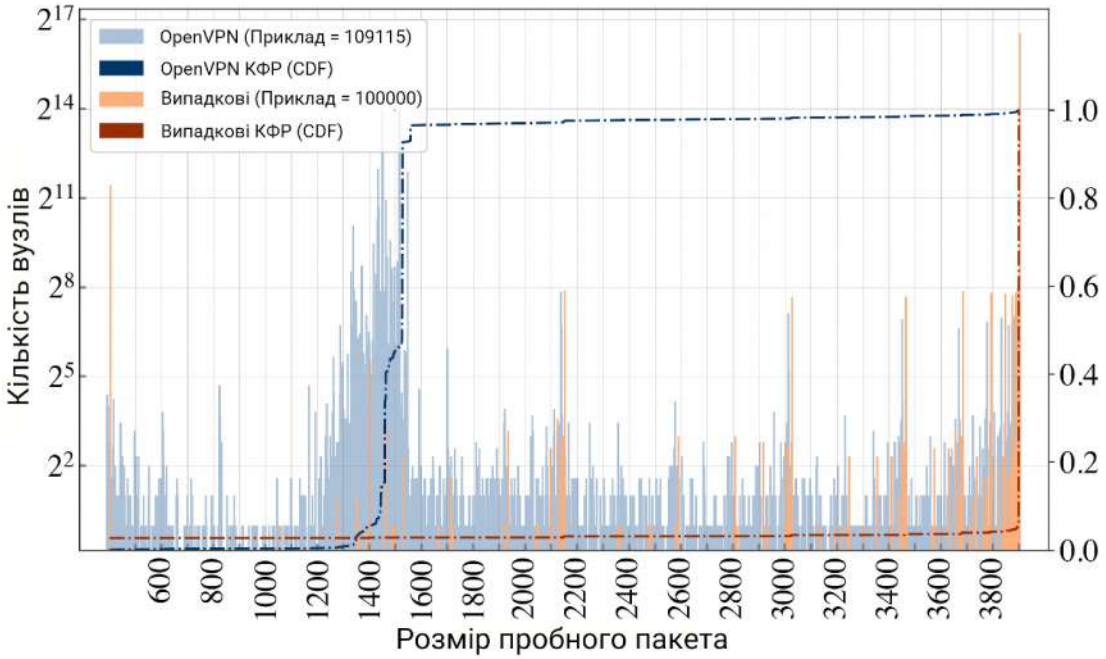

Рис. 5 - Розподіл довжин пакетів-відповідей для серверів OpenVPN, порівняно з іншими випадковими серверами *(згідно з даними [13])*
Fig. 5 - Distribution of response packet lengths for OpenVPN servers, compared to random servers [13]

По-третє: – проведення процедур активної перевірки (див. точка 5 - «*Пробери*», на рис.

3). «Тестувач» надсилає спеціальний запит, на який «справжній» сервер OpenVPN, відповідає характерним RST-пакетом. Однак цей метод має обмеження: - він не працює, якщо на сервері ввімкнено режим «*TLS-Auth*». Як показано на блок-схемі на Рис. 6, пакет тестувача не пройде перевірку «*Valid HMAC?*» та буде відкинутий/ідентифіковано, як «*Invalid HMAC*» (червона стрілка на рис.6) ще до того, як цільовий сервер згенерує відповідь.

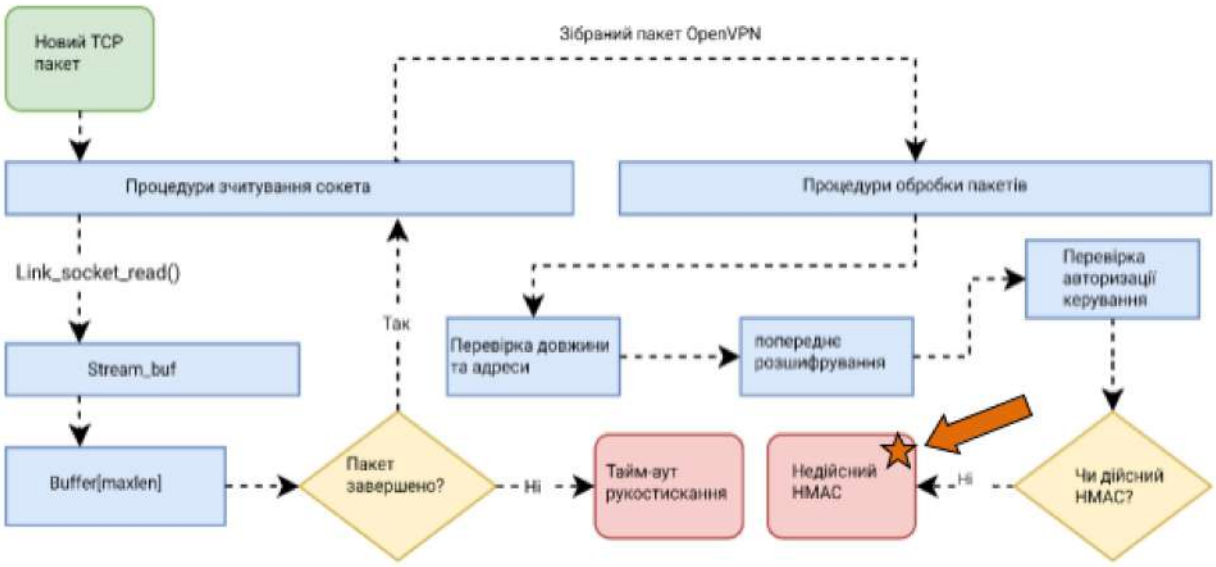

Рис. 6 – Внутрішня логіка обробки пакетів і валідації HMAC сервером OpenVPN [13]
Fig. 6 – Internal logic of packet processing and HMAC validation by the OpenVPN server [13]

Автори дослідження [14] проаналізували вплив «фонового» трафіку всередині VPN, як протидію WF-атакам. Отримані ними результати свідчать, що фоновий трафік дійсно знижує точність (з 95% до 70%). Однак, якщо атакуюча модель попередньо не навчалася на трафіку з «шумом», а потім має справу з ним, то її точність роботи значно погіршується (до 5-30%). При цьому, попередньо навчена система (наприклад, на трафіку Netflix), може «успішно» атакувати користувачів YouTube, підтверджуючи те, що фоновий трафік ускладнює, але не зупиняє атаки.

Виявлення зловмисної активності в зашифрованому трафіку, особливо роботи ботнетів у Tor, є найскладнішим завданням [12]. Зловмисники активно використовують мережу Tor для анонімізації активності C&C серверів, перетворюючи їх на приховані сервіси (.onion).

Концептуально, мережа Tor від самого початку була розроблена, щоб зробити її трафік невизначеним: - IP-адреси анонімні; - порти й протоколи уніфіковані (*все виглядає як звичайний HTTPS*); - вміст зашифрований; - пакети мають фіксований розмір 512 байт (*див. Рис.2*). Однак, незважаючи на це, автори роботи [3] вказують на те, що використання Tor може створювати помітні аномалії. Так, наприклад, сам факт завантаження клієнта Tor на комп'ютер потенційної жертви, опосередковано вже є передумовою, щоб ідентифікувати цей процес, як «підозріла дія». Централізований C&C сервер, навіть гарно прихований, збирає трафік від власної системи ботів, створюючи відповідну мережеву аномалію. В цьому сенсі, відомий приклад ботнету «*Mevade*» показав [15], що одночасне та масове приєднання мільйонів нових клієнтів до мережі «Tor», є сигналом загрози, яка потребує серйозної уваги (*можлива і навмисна імітація*).

Враховуючи все вище зазначене, цілком логічно очікувати, що нові підходи до виявлення зловмисної активності в мережі Tor [16], поступово зміщують увагу з питань контролю вмісту трафіку, на аналіз його поведінкових характеристик та властивостей. Вочевидь, що оскільки IP-адреси, порти та розміри пакетів даних уніфіковані, то очевидними

ознаками для аналізу є: - час (в т.ч., періодичність) та кількість комірок даних, що циркулюють в мережі. Більшість відомих ботнетів для забезпечення власної функціональності, використовують періодичний зв'язок «*heartbeat*». Ця поведінка характерна і для Tor. Хоча періодичність технологічних сеансів зв'язку притаманна і легітимним додаткам (наприклад, IRC), однак їх характеристики відрізняються.

Приклади досліджень реально діючих ботнетів (Win32/Atrax, [17]), підтверджують, що мережа Tor, хоч і приховує місцезнаходження власного «C&C», але при цьому, ніяк не приховує факт його періодичної активності (*збір телеметрії та видача команд управління*). Доречі, дослідники компанії ESETâ змогли ідентифікувати внутрішню .onion адресу ботнету «*Atrax*» [18] та проаналізувати протокол його взаємодії, який виявився звичайними HTTP-запитами. При цьому, хоча локалізувати фізичне місцезнаходження «C&C» ботнетів вкрай важко, проте відомі інструменти й технології аналізу поведінки і протоколів, залишаються актуальними для виявлення такого роду загроз.

3. Застосування методів ML для класифікації зашифрованого трафіку

Розвиток криптографічних протоколів створює умовний бар'єр для традиційних систем моніторингу. Одним із ефективних підходів є використання ансамблевих методів на основі дерев рішень, зокрема алгоритму «Random Forest». Так, згідно дослідження [19], «*TorBot Stalker*» показав себе як дуже результативний інструмент, що здатен легко деанонімізувати ботнети в мережі Tor. Специфіка трафіку Tor вимагає аналізу часових рядів та кількості комірок. *Random Forest* здатний класифікувати таку активність з точністю 99% [19], успішно відокремлюючи трафік ботнетів від легітимних додатків (*наприклад, IRC або Web*) навіть в умовах зашумлених каналів зв'язку (як вже говорилося, зашумлений канал не дуже сильно ускладнює деанонімізацію [12]).

Схема на Рис.7 демонструє етапи обробки даних [19]: - від перехоплення «сирих» комірок до етапу збору та групування за кількістю. Ключовим елементом є «Видобувач інтервалів», який виокремлює регулярні часові шаблони перед передачею їх на вхід «Класифікатора додатків» для верифікації трафіку.

Ключовими ознаками для цього алгоритму виступають інтервали між прибуттям пакетів (*Inter-Arrival Times*) та унікальні підрахунки комірок, що дозволяє ідентифікувати періодичні патерни зв'язку «C&C» серверів. Порівняльний аналіз показав перевагу Random Forest над алгоритмом J48 (C4.5 алгоритм) [20], забезпечуючи нижчий рівень помилкових спрацьовувань. Поряд з цим, для задач виявлення аномалій у шифрованому трафіку високу ефективність демонструє алгоритм XGBoost (*Extreme Gradient Boosting*) [21].

Недоліком ML-моделей залишається проблема існування т.з. «чорного ящика». Для вирішення цих труднощів можна використовувати алгоритми з методами *Explainable AI* (XAI), зокрема SHAP (*SHapley Additive exPlanations*) [22]. Використання SHAP дозволяє розкрити внутрішню логіку моделі, визначаючи вклад кожної ознаки у фінальне рішення блокування.

Впливовими ознаками є загальна кількість переданих пакетів, порт отримувача та початковий розмір вікна (від ініціатора з'єднання до отримувача). Такий підхід робить алгоритм зрозумілим і прозорим, де аналітик SOC (*Security Operations Center*) може бачити конкретні причини класифікації трафіку.

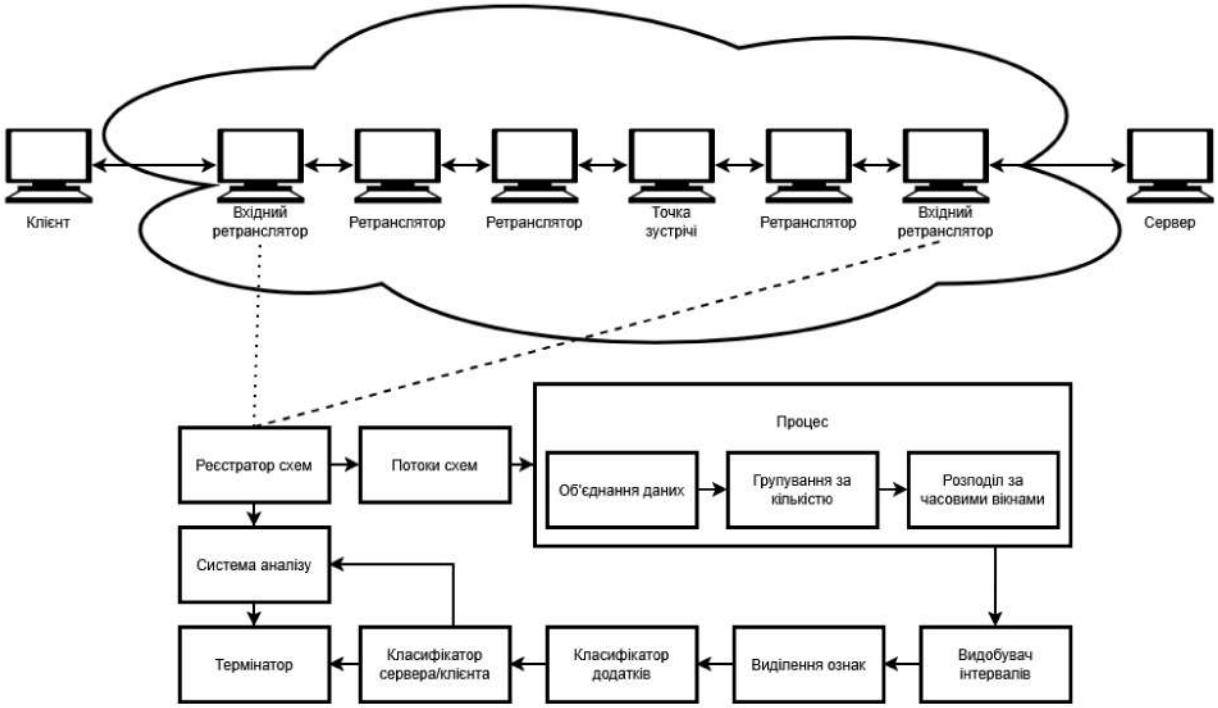

Рис. 7 – Схема роботи TorBot Stalker
Fig. 7 – TorBot Stalker operation scheme [19]

4. Висновки

1. Огляд відомих інцидентів ІБ та останніх напрацювань в галузі активної протидії складним – інтегрованим загрозам ІБ, дозволяє окреслити та конкретизувати можливі підходи до вирішення проблематики існування т.з. «сліпих зон» ІБ. В певному сенсі, процедури шифрування даних (трафіку) формують нову – «мережеву реальність», котра породжує формування відповідних «зон». Як наслідок - діючи системи ІБ вимушені швидко адаптуватися, змінюючи традиційні методики й засоби протидії новим викликам.

2. Аналіз метаданих трафіку є компромісним рішенням, що дозволяє покращити «прозорість» мережевої активності для завчасного виявлення загроз, не вдаючись до процедур дешифрування. Ключова перевага – збереження конфіденційності, оскільки аналізуються лише характеристики процесу передачі (сеансів/сесій), а не вміст пакетів трафіку. На відміну від ресурсномісткого дешифрування (*SSL/TLS*), аналіз метаданих є більш реалістичним сценарієм дій, що забезпечує високу масштабованість (*перш за все за рахунок віртуалізації процесів обробки та організації спеціалізованих хмарних систем*) відповідних реалізацій (рис. 3).

3. Узагальнення результатів сучасних досліджень [10, 12-14, 16, 19, 22] декількох незалежних груп фахівців з ІБ, дозволяє стверджувати, що перспективним напрямом зусиль є синтез інтегрованих систем, що здатні в реальному часі аналізувати метадані зашифрованого трафіку за допомогою широкої імплементації AI/ML. Такі функціональні платформи реалізують проактивний підхід (*Threat Hunting*). Вони базуються на зборі спеціалізованих метаданих (*IPFIX/NetFlow, JA3, дані сертифікатів*), що складає субстантивний фундамент аудиту аномальної мережевої активності. Т.ч. забезпечується еволюційний перехід від реактивної моделі ІБ до концепції проактивного захисту, що базується на розподіленому пошуку та систематизації опосередкованих індикативних ознак існування різного типу загроз.

4. Традиційні методи, що засновані на DPI, поступово втрачають ефективність. Натомість впровадження парадигми технології *Cyber Deception* та комплексний аналіз метаданих циркулюючого трафіку (*інтервалів та розмірів пакетів*) є найбільш перспективним вектором зусиль для цілей детектування і класифікації зашифрованого трафіку [13,19]. Таке поєднання в змозі забезпечити оперативне сепарування застосунків та виявлення непрямих ознак деструктивної дії ботнетів, навіть при роботі на вузлових мережевих шлюзах при гігабітних швидкостях транзитного трафіку (приклад, як в разі «*Merit Network*» на рис.3).

5. За сукупністю отримуваних властивостей зазначена вище стратегія дій, бачиться як практично можливий шлях для підтримки (принаймні на близьку перспективу) бажаного компромісу між: - необхідністю забезпечення потрібного рівня безпеки; - правом користувачів на їх конфіденційність; - можливостями ресурсної підтримки впроваджуваних програмно-апаратних реалізацій. На цьому шляху, глибока інтеграція технологій AI/ML є ключовим фактором впливу на кінцевий результат, оскільки зловмисники, у свою чергу, також будуть використовувати ці технології для маскування своєї діяльності.

Конфлікт інтересів

Автори повідомляють про відсутність конфлікту інтересів.

References

1. Cloudflare. *What is a VPN?* https://www.cloudflare.com/ru-ru/learning/access-management/whatisavpn/
2. Tor Project. *Tor: Overview* https://2019.www.torproject.org/about/overview.html.en
3. Cloudflare. *ECH Protocol* https://developers.cloudflare.com/ssl/edge-certificates/ech/
4. Multilogin. *What is Traffic Fingerprinting?* https://surl.lt/empsdf
5. Kokhanovska, T., Narezhnyi, O., & Diachenko, O. (2020). Exploring the possibilities of Honeypot technology. *Computer Science and Cybersecurity, 1(17)*, 33-42. https://doi.org/10.26565/2519-2310-2020-1-03 [in Ukrainian]
6. Softpiua. *What is NetFlow?* https://surl.li/dqzslu [in Ukrainian]
7. Pitutin V. Softpiua. *What is IP Flow Information Export?* https://surl.lu/cwmkud [in Ukrainian]
8. Peakhour. *What is JA3 Fingerprinting?* https://www.peakhour.io/learning/fingerprinting/what-is-ja3-fingerprinting/
9. Cloudflare. *What is an SSL certificate?* https://www.cloudflare.com/ru-ru/learning/ssl/what-is-an-ssl-certificate/
10. Cherubin, G., Jansen, R., & Troncoso, C. (2022, August 10-12). *Online Website Fingerprinting: Evaluating Website Fingerprinting Attacks on Tor in the Real World* https://www.usenix.org/system/files/sec22-cherubin.pdf
11. Chepel, D., & Malakhov, S. (2024). Summary of DNS traffic filtering trends as a component of modern information systems security. *Computer Science and Cybersecurity, 1(25)*, 6–21. https://doi.org/10.26565/2519-2310-2024-1-01 [in Ukrainian]
12. DeFabbia-Kane, S. (2011, April). *Analyzing the Effectiveness of Passive Correlation Attacks on the Tor Anonymity Network* https://surl.li/zghbyu
13. Xue, D., Ramesh, R., Jain, A., Kallitsis, M., Halderman, J. A., Crandall, J. R., & Ensafi, R. (2024, March 6). *OpenVPN is Open to VPN Fingerprinting* https://arxiv.org/html/2403.03998v1
14. DeFabbia-Kane, S. (2023, June 15). *The Effect Background Traffic in VPNs has on Website Fingerprinting* https://www.diva-portal.org/smash/get/diva2:1779408/FULLTEXT01.pdf
15. Tor Project. *Tor metrics. Directly connecting users* https://metrics.torproject.org/userstats-relay-country.png?start=2013-06-05&end=2013-11-02&country=all&events=off
16. Fajana, O. (2023, October). *Novel Techniques for Detecting Tor Botnets* https://pure.port.ac.uk/ws/portalfiles/portal/91457639/up797388-Oluwatobi-Fajana-Thesis-2023-final.pdf

17. Stormshield Customer Security Lab. (2014, August 20). *Win32/Atrax.A* https://www.stormshield.com/news/win32atrax-a/
18. Matrosov, A. (2013, July 24). *The rise of TOR-based botnets* https://www.welivesecurity.com/2013/07/24/the-rise-of-tor-based-botnets/
19. Fajana, O., Owenson, G., & Cocea, M. *TorBot Stalker: Detecting Tor Botnets through Intelligent Circuit Data Analysis* https://pure.port.ac.uk/ws/portalfiles/portal/12745078/TorBot_Stalker_new.pdf
20. Khanna, N. (2021, August 18). *J48 Classification (C4.5 Algorithm) in a Nutshell* https://medium.com/@nilimakhanna1/j48-classification-c4-5-algorithm-in-a-nutshell-24c50d20658e
21. Pawan Saxena. GeeksforGeeks. (2025, October 24). *XGBoost* https://www.geeksforgeeks.org/machine-learning/xgboost/
22. Sing, K., Kashyap, A., & Cherukuri, A. K. (2025, May). *Interpretable Anomaly Detection in Encrypted Traffic Using SHAP with Machine Learning Models* https://surl.lt/oidsuz

METADATA ANALYSIS OF ENCRYPTED TRAFFIC TO ELIMINATE SECURITY «BLIND SPOTS» OF MODERN INFORMATION SYSTEMS

Maksym Horelko[1], Student (Bachelor's degree, specialty F5) at the Department of Cybersecurity of Information Systems, Networks and Technologies; E-mail: maksym.horelko@student.karazin.ua;
Serhii Malakhov[1], Ph.D., Senior Researcher, Associate Professor of the Department of Cybersecurity of Information Systems, Networks and Technologies; e-mail: malakhov@karazin.ua; ORCID: https://orcid.org/0000-0001-8826-1616
[1]*V. N. Karazin Kharkiv National University, Ukraine*
Manuscript was received September 1, 2025; Received after review October 1, 2025;
Accepted November 2, 2025; Published December 30, 2025

Abstract. A review of recent developments is offered on the issues in the complex analysis of encrypted network traffic in modern information systems. The main research methods are: - analysis, generalization and comparison. The paper considers the issue of finding possible ways to ensure a compromise in the conditional triangle of «influence factors» when solving the tasks of operational detection of dangers in the data structure of encrypted traffic. As «influence factors» a combination of the following factors is considered: - the need to ensure the required level of Information Security (IS); - support for the right of users to their confidentiality; - resource consensus of the implemented software and hardware solutions. Attention is drawn to the fact that the integration of artificial intelligence and machine learning (AI/ML) technologies into the structure of network traffic control algorithms is a key lever for influencing the final result. It is emphasized that the opposing party will also use these technologies to mask its activities. It is concluded that the implementation of procedures for analyzing network traffic metadata is a compromise solution. The implementation of such an approach allows to improve the «transparency» of current network activity for early detection of security threats, without directly resorting to traffic decryption procedures. It is emphasized that the implementation of the «Cyber Deception» paradigm and a comprehensive analysis of the metadata of circulating encrypted traffic are a promising vector of efforts for preventive elimination of the prerequisites of the formation of "blind spots" in the security of modern IT systems.

Keywords: *traffic, Filtering, Traffic Fingerprinting, Pattern, Information Security (IS), VPN, Tor, Cyber Deception*

Conflicts of Interest: the authors declare no conflict of interest.