НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**22 листопада 2024 року**


# КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

**МАТЕРІАЛИ**
**V МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Національний університет «Одеська юридична академія»**
**Факультет кібербезпеки та інформаційних технологій**
**Кафедра кібербезпеки**

# КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

**МАТЕРІАЛИ V МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

**22 листопада 2024 року, м. Одеса**

Одеса, 2024

**УДК 340.12:316.3**

## Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 25.11.2024 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 22 листопада 2024 р.). Одеса, 2024. 289 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

**V Міжнародна науково-практична конференція**

# «Кібербезпека в сучасному світі: актуальні виклики»

**22 листопада 2024 року**

**ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:**

**Секція 1. Алгоритмічні та технічні аспекти кібербезпеки**

**Секція 2. Штучний інтелект та інформаційні технології в задачах кібербезпеки**

**Секція 3. Управлінські, соціальні та психологічні аспекти кібербезпеки**

**Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації**

## СКЛАД ПРОГРАМНОГО КОМІТЕТУ КОНФЕРЕНЦІЇ:

Доц. **Дикий О.В.**, НУ “Одеська юридична академія”, Україна
Проф. **Горбаченко С.А.**, НУ “Одеська юридична академія”, Україна
Проф. **Казакова Н.Ф.**, НУ “Одеська юридична академія”, Україна
Доц. **Соколов А.В.**, НУ “Одеська юридична академія”, Україна
Проф. **Евсеев С.П.**, НТУ «Харківський політехнічний інститут», Україна
Проф. **Ткач Ю.М.**, НУ “Чернігівська політехніка”, Україна
Проф. **Опірський І.Р.**, НУ “Львівська Політехніка”, Україна
Проф. **Шелест М.Є.**, НУ “Чернігівська політехніка”, Україна
Проф. **Mikolaj Karpinski,** University of the National Education Commission, Польща
Проф. **Нємкова О.А.**, НУ “Львівська Політехніка”, Україна

**E-mail: kiberprostirconf@gmail.com (Для питань та тез)**

# АПАРАТНИЙ ЗАХИСТ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ NGFW МЕРЕЖЕВИХ ЕКРАНІВ

***Задерейко Олександр***
*доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент*

Модель OSI (Open Systems Interconnection) є стандартом взаємодії між мережевими пристроями, що описує 7 рівнів абстракції. Ці рівні виконують різні функції: перший — фізичний, другий — канальний, третій — мережевий, четвертий — транспортний, п'ятий — сесійний, шостий — рівень уявлення даних, і сьомий — прикладний рівень, який взаємодіє з програмним забезпеченням користувача (рис. 1).

| Рівні моделі OSI ISO | Приклади протоколів |
|---|---|
| 7. Прикладний | HTTP, FTP, SMTP, DNS |
| 6. Представлення | ASII, MPEG, JPEG |
| 5. Сеансовий | |
| 4. Транспортний | TCP, UDP |
| 3. Мережений | IP, IPS, RIP, OSF |
| 2. Канальний | Ethernet |
| 1. Фізичний | |

*Рис. 1. Мережева семирівнева модель OSI ISO.*

Кожен мережевий пристрій функціонує на своєму конкретному рівні абстракції: веб-сервер та веб-браузер взаємодіють на рівні додатків (рівень 7 або L7), тоді як маршрутизатори обмінюються інформацією на канальному (L2) та мережевому (L3) рівнях, передаючи кадри та пакети [1].

Міжмережевий екран (брандмауер, firewall) також є мережевим пристроєм, який може виконувати функції свічу, маршрутизатора або навіть виступати як

«віртуальний кабель» у мережевій топології, залежно від свого типу. Однак на ці пристрої лягає додаткове навантаження, оскільки вони повинні аналізувати вміст пакетів, що ускладнює їх роботу [2].

Глибина аналізу мережевих пакетів може варіюватися, і важливою відмінністю є те, чи здійснюється аналіз на рівнях L4 або L7. Це визначає рівень деталізації перевірки та функціональність пристрою.

Брандмауер (firewall) сам собою не є частиною рівнів моделі OSI. Натомість він має додаткові правила, доданими до функціональності різних рівнів OSI.

Найбільш типовий брандмауер працює на рівнях L3 та L4 (IP обох типів та TCP/UDP). У його функції входить можливість блокувати чи дозволяти комунікацію через різні порти, вхідні і вихідні. Брандмауери можуть бути структуровані по-різному, але насправді тісно пов'язані з мережевою реалізацією самого пристрою (особливо з його операційною системою).

Іноді брандмауер може мати додаткову логіку розуміння деяких протоколів прикладного рівня та брандмауера з їхньої основі.

L4 брандмауер — це міжмережевий екран, який пропускає мережевий трафік і перевіряє заголовки протоколів 4-го рівня: TCP, UDP, ICMP. Основними критеріями для фільтрації трафіку є IP-адреси, порти TCP/UDP та сервіси ICMP.

Сучасні L4 брандмауери зберігають стан як TCP, UDP і ICMP, а й відстежують взаємодія всього прикладного ПЗ лише на рівні L7. Наприклад, стан FTP, HTTP, SIP та іншого прикладного ПЗ, що вже залежить від конкретної реалізації firewall.

L7 брандмауери — це міжмережеві екрани, які пропускають IP-трафік і аналізують не лише заголовки 4-го рівня, але й сегмент даних кожного IP-пакета. Вони здатні розпізнавати трафік на рівні прикладного ПЗ (L7), зокрема визначати, які файли передаються і в якому напрямку. Оскільки аналізується більше даних, правила L7 брандмауера мають значно більше критеріїв перевірки, таких як ім’я користувача, тип прикладного ПЗ, категорія URL і стан ПЗ на комп’ютері користувача.

Навантаження на L7 брандмауер значно вищі, оскільки його процесор повинен постійно аналізувати великі обсяги даних, які передаються прикладними програмами. Це включає мегабайти полів даних, в той час як L4 брандмауер перевіряє лише кілька байт заголовка IP-пакета, зокрема адреси джерела та призначення, а також порти. Для зберігання стану кожного прикладного ПЗ на L7 потрібен набагато більший буфер, оскільки обсяг передаваних даних на цьому рівні значно більший, ніж у заголовку TCP/IP. Через це, при однаковому обсязі пам'яті, L7 брандмауер може одночасно зберігати менше сесій, ніж L4. Оскільки L7 брандмауер може ідентифікувати, яке прикладне ПЗ використовує мережу, правила фільтрації можуть бути сформульовані за ім'ям ПЗ, а не за номером порту, як у L4. Крім того, сучасне прикладне ПО генерує безліч з'єднань і всі вони є його частиною. Цей вид брандмауера дозволяє повернути контроль за сучасним динамічним при-

кладним програмним забезпеченням, що працює по будь-якому порту, наприклад, teamviewer, bittorent, tor, про «поведінку» яких L4 firewall фактично нічого не знає. Тобто L7 firewall у сучасних реаліях потрібен, якщо необхідно забезпечити високий рівень безпеки у мережі.

Тобто L7 брандмауер отримав у мережному профільному середовищі назву Next-Generation Firewall (NGFW). Усередині цього мережевого пристрою, реалізованого L7 брандмауері основним кваліфікатором стає ім'я програми L7, то правила пишуться за новими критеріями. У NGFW завжди працює динамічне зіставлення IP адрес користувачів у мережі, тому ім'я користувача теж стає кваліфікатором (критерієм). NGFW включає функції роз- шифровки SSL/TLS і SSH для розпізнавання додатків і атак всередині них, IPS, антивіруса, URL фільтрації і т.д. [3].

Термін NGFW спочатку був вигаданий маркетингом компанії Palo Alto Networks. Але поступово зміцнився на мережевому ринку, і всі виробники UTM зараз теж називають себе NGFW. NGFW теж виконує кілька функцій одночасно. Відмінність NGFW від UTM важливо знати та розуміти. Воно полягає в тому, що NGFW функції безпеки додатків (IPS, антивірус, URL фільтрація) прискорені апаратно. Існують спеціалізовані апаратні чіпи: IPS перевіряє атаки на своєму чіпі, антивірус сигнатури на своєму, розшифровка SSL - на своєму і таке інше. Поділ функцій з різних процесорів дає можливість запускати захисні функції паралельно і чекати, коли закінчить працювати попередня функція, як і UTM. Наприклад, в апаратних міжмережевих екранах компанії Palo Alto Networks встановлено до 60 спеціалізованих процесорів, що виконують прискорення функцій безпеки, мережевих функцій та їх керування. Важливо, що NGFW містять єдиний програмний інтерфейс керування всіма функціями одночасно.

Ідея функціонування NGFW на відміну від UTM - реалізувати кожну функцію на окремому процесорі, який спеціалізований під необхідний функціонал.

Подібно до того, як виробники комп'ютерів колись винесли функції математичних обчислень та графіки в окремі співпроцесори, сучасні NGFW (нові покоління міжмережевих екранів) оснащуються спеціалізованими процесорами для розпізнавання прикладного ПЗ на рівні L7, для розшифрування SSL/SSH, перевірки антивірусних сигнатур, аналізу IPS-сигнатур тощо. Це дозволяє виконувати всі ці функції одночасно, без зниження швидкості або затримок у передачі трафіку під час перевірки.

Саме тому міжмережеві екрани без прискорення купують, оскільки прискорення не потрібно на невеликих швидкостях, але коли швидкості аналізу трафіку виходять за 1-5 Гігабіт — реалізувати всі функції безпеки вже неможливо без апаратного прискорення.

Мета пристрою NGFW: дати можливість безпечно працювати кінцевому користувачеві не уповільнюючи мережевий трафік. Це дозволяє постійно перевіряти, що прикладне ПЗ передає потрібний користувачеві безпечний контент, і

паралельна робота рушіїв захисту з одним потоком мережного трафіку гарантує задану продуктивність при всіх включених функціях безпеки і мінімальну затримку мережевого трафіку.

**Список використаних джерел:**

1. Задерейко О. В., Логінова Н. І., Толокнов А. А. Комп'ютерні мережі : навчальний посібник [Електронне видання ], Одеса : Фенікс, 2022, 249 с. ISBN 978-966-928-828-8. URL: https://dspace.onua.edu.ua/handle/11300/19423.
2. Ільге, І. Г., Ільге, О. І., & Запорожцев, С. Ю. (2021). Особливості вибору міжмере- жевих екранів для захисту комп'ютерної мережі організації. URL: https:// api.dspace.khadi.kharkov.ua/server/api/core/bitstreams/c3b62d41-3c08-4307-b0e9-ddd2d08d8ad0/content.
3. Brar, M. K., Kaur, B., Singh, G., Jindal, P K., & Sood, S. (2024, July). Traditional firewall vs. next-generation firewall: A review. In AIP Conference Proceedings (Vol. 3121, No. 1). AIP Publishing.

**Ключові слова:** NGFW, UTM, мережева інфраструктура, мережевий пристрій, фільтрація трафіка, перевірка сигнатур, розшифровка SSL/TLS
**Keywords:** NGFW, UTM, network infrastructure, network device, traffic filtering, signature checking, SSL/TLS decryption

# КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ ТА ПРАКТИКА

**МАТЕРІАЛИ**
**V МІЖНАРОДНОЇ**
**НАУКОВО-ПРАКТИЧНОЇ**
**КОНФЕРЕНЦІЇ**

*22 листопада 2024 року*
*м. Одеса*

**Відповідальній редактор: О.В. Дикий**

Дизайн та верстка:
М.Ю. Овчинников