https://doi.org/10.31891/2307-5732-2025-355-64
УДК 004.056.52

ПЕДЯШ ВОЛОДИМИР
Міжнародний гуманітарний університет
https://orcid.org/0000-0002-4071-357X
e-mail: vpedyash@gmail.com
ЛЕДОВСЬКИЙ ЄВГЕН
Міжнародний гуманітарний університет
https://orcid.org/0009-0003-2176-9265
e-mail: ledovskyi_yevhen@ukr.net
ТКАЧ ВОЛОДИМИР
Міжнародний гуманітарний університет
https://orcid.org/0009-0003-0517-6355
e-mail: tkach_volodym@ukr.net
НОВОЧИНСЬКИЙ ЄВГЕН
Міжнародний гуманітарний університет
https://orcid.org/0009-0007-2884-6103
e-mail: novochynskyiievgen@gmail.com

АНАЛІЗ ЕТАПІВ РОЗВИТКУ АПАРАТНИХ ФАЄРВОЛІВ ДЛЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

У статті проаналізовано еволюцію апаратних фаєрволів для телекомунікаційних мереж від їх зародження у 1980-х роках минулого століття до сучасних багатофункціональних систем із елементами штучного інтелекту. Детально розглянуто шість послідовних поколінь фаєрволів, вказано їхні функціональні особливості, архітектурні рішення, типові представники та обмеження, що стимулювали подальший розвиток технологій. Особлива увага приділяється сучасним фаєрволам нового покоління (NGFW), їхній архітектурі та функціональним можливостям, інтеграцію широкого спектру функцій безпеки. Досліджено також новітній напрямок розвитку — фаєрволи з елементами штучного інтелекту, що здатні автономно аналізувати великі обсяги трафіку, виявляти приховані закономірності та адаптуватися до нових типів атак. На основі проведеного аналізу визначено перспективи подальшого розвитку апаратних фаєрволів у напрямку посилення інтеграції технологій штучного інтелекту та створення єдиної екосистеми захисту даних.

***Ключові слова**: інформаційна безпека, фаєрволи, еволюція, NGFW, штучний інтелект, мережний захист*

PEDYASH VOLODYMYR
LEDOVSKYI YEVHEN
TKACH VOLODYMYR
NOVOCHYNSKYI YEVHEN
International Humanitarian University

ANALYSIS OF THE STAGES IN THE DEVELOPMENT OF HARDWARE FIREWALLS FOR TELECOMMUNICATIONS NETWORKS

This paper analyzes the evolution of hardware firewalls for telecommunication networks from simple packet filters of the 1980s to contemporary systems with artificial intelligence capabilities. The research examines six generations of firewalls, each representing a significant advancement in network security technology responding to emerging threats. First-generation firewalls implemented basic packet filtering based on IP addresses and ports but offered limited protection against complex attacks. Second-generation devices introduced stateful inspection, enhancing security by monitoring active network connections. The third generation, application-level gateways, expanded analysis to the application layer, enabling deeper traffic inspection and more granular security policies. Fourth-generation firewalls integrated intrusion detection and prevention systems (IDS/IPS), allowing identification and blocking of attack patterns in real-time. Next-Generation Firewalls (NGFW), representing the fifth generation, revolutionized network security with deep packet inspection, application identification regardless of ports used, and integration of multiple security functions including traditional packet filtering, intrusion prevention, antivirus protection, URL filtering, and user identification. The paper details the architecture and capabilities of NGFWs, which currently dominate the enterprise segment. The newest sixth generation incorporating artificial intelligence is also examined, highlighting its ability to autonomously analyze traffic, detect hidden patterns, and adapt to new attacks without manual updates. The authors discuss hardware implementation challenges for each generation, from general-purpose processors to specialized systems with multi-level architectures incorporating ASIC circuits, network processors, and specialized machine learning modules. The research concludes by identifying trends pointing toward enhanced AI technologies and stronger integration with other security systems to create a unified ecosystem for data protection.

***Keywords**: information security, firewalls, evolution, NGFW, artificial intelligence, network protection*

Стаття надійшла до редакції / Received 19.05.2025
Прийнята до друку / Accepted 26.06.2025

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Сьогодні повсякденне життя та бізнес-процеси включають в себе обмін цифровими даними, тому завдання по організації інформаційної безпеки є досить актуальним. Сучасні методи організації кібератак на інформаційні системи стали досить досконалими та масштабними. Також змінилася їх мета - спочатку вони були спрямовані в сторону банківського сектору для організації фінансових злочинів. Зараз сфера їх

застосування суттєво розширилася і включає атаки на критичну інфраструктуру та внутрішні мережі організацій, оскільки сьогодні автоматизуються все більше технологічних процесів. Інфраструктура сучасної організації включає в себе комп'ютерні системи, роботизовані комплекси та системи управління з хмарних сервісів. Одним із основних елементів організації системи інформаційної безпеки є фаєрволи (брандмауери), що представляють собою спеціалізовані комп'ютерні системи системи для аналізу та обробки мережного трафіку [1]. За кілька десятиліть свого існування вони пройшли шлях від простих фільтрів пакетів до складних систем, що виконують аналіз пакетів на прикладному рівні, включають функції захисту мережі від вторгнень та використовують штучний інтелект (ШІ) для виявлення аномалій [2, 3]. Фаєрволи можна розділити на дві основні групи: апаратні (фізично реалізовано у вигляді окремих пристроїв) та програмні (віртуальні), що реалізуються у вигляді спеціалізованих віртуальних машин.

Аналіз досліджень та публікацій

Еволюція фаєрволів та алгоритмів їх функціонування досліджувалася багатьма науковцями. Однією з перших робіт, де були закладені теоретичні основи побудови фаєрволів та базові алгоритми їх функціонування були дослідження Чесвіка та Белловіна [4]. В подальшому їх робота була продовжена групами інших дослідників [5], які систематизували підходи до архітектури та використання фаєрволів різних поколінь.

Сучасні дослідження в даній галузі сфокусовано на інтегруванні фаєрволів з комплексними системами інформаційної безпеки безпеки, зокрема з системами виявлення (Intrusion Detection System, IDS) та запобігання (Intrusion Prevention System, IPS) вторгнень. В більш пізніх роботах сформульовано вимоги до сучасних фаєрволів та методи їх тестування [6]. З розвитком хмарних обчислень стали актуальними питання безпеки у віртуалізованих середовищах, тому сформувався відповідний напрям досліджень по захисту інформації. Однак незважаючи на значну кількість публікацій, присвяченим фаєрволам, питання щодо узагальнення напрямів їх розвитку та принципів побудови залишається розкритим недостатньо.

Формулювання цілей статті

Метою дослідження даної роботи є аналіз етапів еволюції апаратних фаєрволів, включаючи дослідження їх функціональних можливостей, архітектурних особливостей та перспектив подальшого розвитку.

Виклад основного матеріалу

Розвиток фаєрволів для телекомунікаційних мереж відбувався послідовно, паралельно з розвитком комп'ютерних мереж, мікропроцесорної техніки та сфери її застосування. Кожне нове покоління пристроїв радикально змінювало підходи до забезпечення мережної безпеки, а не було розширеним варіантом попередників. Результати проведеного авторами аналізу, що наведено в таблиці 1, включають всі етапи еволюції апаратних фаєрволів. Слід зазначити, що хронологічні межі вказано досить умовно, оскільки на практиці завжди є певне відставання у фізичному впроваджені запропонованих дослідниками теоретичних розробок (алгоритми та архітектура пристроїв). Також слід мати на увазі, що з кожним новим поколінням змінювалося коло виробників обладнання, що сприяло посиленню конкуренції на ринку, швидшому розвитку технологій та їх впровадження. Далі в тексті роботи розглянуто кожне з вказаних поколінь пристроїв, проаналізовано їх функціонал, особливості реалізації та типових представників.

Таблиця 1

Етапи еволюції апаратних фаєрволів для телекомунікаційних мереж

Покоління	Період	Основні характеристики та типові представники
1. Пакетні фільтри (Packet Filters)	Кінець 1980-х - початок 1990-х	Фільтрація на основі IP-адрес та портів (Cisco PIX, Checkpoint FireWall-1)
2. Шлюзи стану (Stateful Inspection Firewalls)	Середина 1990-х - початок 2000-х	Відстеження стану з'єднань, контроль сесій (NetScreen-5GT та NetScreen-100)
3. Шлюзи прикладного рівня (Application Level Gateways)	Кінець 1990-х - середина 2000-х	Аналіз на прикладному рівні, проксі-функціональність (Cisco Secure PIX, Check Point FireWall-1)
4. Системи запобігання вторгнень (IPS)	Початок 2000-х - 2010	Виявлення та блокування атак на основі сигнатур та аналізу поведінки (Cisco IPS 4200 Series, Juniper IDP)
5. Фаєрволи нового покоління (NGFW)	2010 - теперішній час	Глибокий аналіз пакетів, ідентифікація додатків, інтеграція з системами безпеки (Palo Alto Networks PA Series, Fortinet FortiGate, Cisco Firepower, Check Point R80)
6. Фаєрволи з елементами штучного інтелекту	2018 - теперішній час	Машинне навчання для виявлення загроз, автоматична адаптація правил (Palo Alto Networks з Cortex XDR, Fortinet FortiGuard AI)

Перші зразки фаєрволів першого покоління були запропоновані наприкінці 1980-х років і являли собою прості фільтри мережного трафіку. Вони працювали на мережному та транспортному рівнях моделі OSI [7, 8]. Їх функціонал полягав у аналізі заголовків пакетів та застосуванні певного набору правил, в яких вказувалася політика безпеки. В правилах можна було вказувати IP адреси вузлів відправника та призначення,

номери портів та типи протоколів. Кожен пакет даних аналізувався окремо, без урахування змісту області корисного навантаження чи стану з'єднання, що призводило до неможливості захисту від складних атак. Простота реалізації та висока швидкодія сприяли швидкому впровадженню пристроїв в комп'ютерні мережі на ранніх етапах їх розвитку.

Одним із перших комерційних апаратних фаєрволів був пристрій PIX Firewall (Private Internet eXchange), розроблений і представлений компанією Network Translation, Inc. (NTI) в 1994 році. Цей пристрій підтримував фільтрацію пакетів на основі IP адрес та портів, а також технологію трансляції мережних адрес (NAT), яка почала впроваджуватися на мережах в той час. Згодом відома фірма Cisco викупила NTI і в 1999 році представила модель фаєрволу Cisco PIX 515, яка обробляла до 130000 одночасних з'єднань зі швидкістю до 190 Мбіт/с, що для того часу було значним досягненням. Іншим відомим представником фаєрволів першого покоління був Check Point FireWall-1. Його суттєвою перевагою була наявність графічного інтерфейсу у вигляді окремого додатку на ОС Windows, що дозволяв інтуїтивно (візуально шляхом перетягування об'єктів) створювати політики доступу, VPN, NAT, тощо. Для досягнення високої продуктивності в реальному часі, операції пакетної фільтрації виконувалися апаратно на спеціалізованих ASIC-мікросхемах.

Суттєвим обмеженням першого покоління фаєрволів був низький коефіцієнт захисту від атак, що використовували фрагментацію пакетів або дії над TCP-заголовками. Також ці пристрої не мали можливості аналізувати пакети на прикладному рівні. Налаштування правил фільтрації вимагало залучення адміністраторів високої кваліфікації, що глибоко розуміли мережні протоколи та конкретні топології мережі. Ці обмеження стали рушієм для подальшого розвитку технологій захисту мереж.

Друге покоління фаєрволів, відоме під назвою шлюзи стану, з'явилося в середині 1990-х років минулого століття та врахувало обмежені можливості пакетних фільтрів. Суттєвою відмінністю пристроїв цього покоління була їх здатність проводити моніторинг стану активних мережних з'єднань [9, 10]. Для зберігання цієї інформації в пам'яті пристрою створювалась спеціальна таблиця станів. Це дозволило аналізувати послідовності пакетів, що значно підвищило рівень безпеки системи. Ці пристрої могли встановлювати належність пакету до вже встановленого з'єднання, що надавало можливість блокувати несанкціоновані спроби встановлення нових з'єднань та захищатися від багатьох видів нових атак, включаючи спуфінг та деякі різновиди DoS-атак.

Одним із лідерів у виробництві апаратних фаєрволів другого покоління була компанія NetScreen, що була пізніше придбана Juniper Networks в 2004 році. Типовими представниками пристроїв цього покоління були моделі серій NetScreen-5GT та NetScreen-100, які підтримували відстеження стану з'єднань, інтегровані функції VPN та систему попередження вторгнень IPS. Зрозуміло, що для виконання всіх функцій в режимі реального часу, всі операції над трафіком виконувалися в спеціалізованих ASIC інтегральних мікросхемах.

Незважаючи на суттєвий прогрес функціональності порівняно з пакетними фільтрами, фаєрволи другого покоління мали обмежені можливості по аналізу трафіку на рівні додатків. Вони не могли ефективно протидіяти атакам, що використовували вразливості в протоколах прикладного рівня або замасковані атаки. Окрім цього, розвиток веб-технологій призвів до появи розподілених додатків, які використовували динамічний розподіл портів або тунелювання через стандартні порти HTTP/HTTPS. В результаті це призвело до появи наступного покоління фаєрволів.

Третє покоління фаєрволів, відоме як шлюзи прикладного рівня або проксі-фаєрволи, з'явилося наприкінці 1990-х років. На відміну від пристроїв попередніх поколінь, ці фаєрволи опрацьовували заголовки та вміст пакетів на всіх рівнях моделі OSI, включаючи прикладний. Принцип роботи шлюзів прикладного рівня полягав у переході від прямого з'єднання клієнт – сервер до двох окремих з'єднань: від клієнта до фаєрволу та від фаєрволу до сервера [11]. Це дозволяло організувати більш глибокий аналіз трафіку та блокувати потенційно небезпечні пакети від їх потрапляння до захищеного сегменту мережі. Одним із перших фаєрволів, що реалізував функції шлюзу прикладного рівня була модель Cisco PIX 525, яка могла обробляти до 280 000 одночасних з'єднань на швидкості до 330 Мбіт/с та підтримувала аналіз протоколів прикладного рівня (HTTP, FTP, SMTP та ряду інших). В схожій за функціоналом моделі Check Point FireWall-1 була реалізована нова технологія Application Intelligence, яка дозволяла аналізувати понад 600 різних додатків та протоколів. Зазвичай ці пристрої інтегрувалися з серверами автентифікації та системами управління політиками безпеки, що дозволяло реалізувати гнучкі та зрозумілі політики контролю доступу.

Побудова апаратних шлюзів прикладного рівня вимагала значно більших обчислювальних ресурсів порівняно з попередніми поколіннями пристроїв. Особливість цього покоління фаєрволів полягала у впровадженні модульної архітектури, яка дозволяла додавати нові функції безпеки шляхом встановлення додаткових модулів для аналізу SSL/TLS-трафіку, виявлення шкідливого програмного забезпечення або фільтрації URL. Але шлюзи прикладного рівня мали і недоліки, головний з яких полягав у внесенні суттєвих затримок в мережний трафік, що негативно впливало на продуктивність мережі в цілому. Для ефективного виявлення нових загроз вимагалося регулярне оновлення сигнатур та правил, що збільшувало витрати на експлуатацію мережі. Ці обмеження, а також поява нових типів загроз стимулювали подальший розвиток технологій фаєрволів та перехід до наступного покоління.

Четверте покоління фаєрволів, яке з'явилося на початку 2000-х років, включало інтеграцію до фаєрволів функцій систем виявлення та запобігання вторгнень (IDS/IPS). Характерною інновацією пристроїв цього покоління була здатність пошуку в трафіку відомих шаблонів атак (сигнатур) та аномальної поведінки,

що вказувало про ризики потенційного вторгнення [12]. Одним із перших представників фаєрволів цього покоління були пристрої Cisco серії IPS 4200. Так, модель IPS 4260 забезпечувала пропускну здатність до 2 Гбіт/с та підтримувала до 4000 сигнатур атак, що оновлювалися через службу Cisco Security Intelligence. Інша компанія Juniper Networks також активно розвивала цей напрямок, представивши серію пристроїв Juniper IDP. Ці пристрої мали удосконалені механізми виявлення атак на основі аналізу аномалій, поведінкових шаблонів та інтегрувалися з централізованими системами управління безпекою.

Апаратна реалізація фаєрволів четвертого покоління вимагала значних обчислювальних ресурсів для забезпечення глибокого аналізу пакетів та порівняння їх з базою сигнатур в реальному часі. Для вирішення цієї проблеми виробники ввели до складу пристроїв спеціалізовані процесори обробки мережного трафіку (Network Processing Unit, NPU) та багатоядерні процесори із залученням механізмів паралельних обчислень. Наприклад, згадана вище архітектура Cisco IPS 4200 включала спеціалізовані чіпи ASIC для прискорення обробки трафіку та виділені блоки пам'яті для зберігання бази сигнатур.

Незважаючи на суттєвий прогрес в порівнянні з попередніми поколіннями, фаєрволи з інтегрованими функціями IPS стикалися з рядом проблем. По-перше, вони були дорогими, складними в налаштуванні та експлуатації. По-друге, завжди існував ризик помилкових спрацьовувань через схожість поточного трафіку із відомими шаблонами атак. По-третє, ці системи не завжди могли ефективно протидіяти новим загрозам (zero-day attacks), для яких ще не існувало сигнатур. Окрім того, традиційні методи виявлення вторгнень показували свою обмеженість при роботі із зашифрованим трафіком та багаторівневими атаками. Ці проблеми, а також стрімкий розвиток хмарних технологій та мобільних пристроїв, призвели до створення наступного покоління фаєрволів.

П'яте покоління фаєрволів, відоме як фаєрволи нового покоління (Next-Generation Firewalls, NGFW), з'явилося близько 2010 року. Основною відмінністю NGFW є здатність до глибокої інспекції пакетів та ідентифікації додатків незалежно від портів чи протоколів, які вони використовують. Окрім цього, NGFW інтегрують в собі широкий спектр функцій безпеки: традиційну фільтрацію пакетів, відстеження стану з'єднань, запобігання вторгненням, антивірусний захист, фільтрацію URL, контроль додатків та ідентифікацію користувачів [13]. Одним із родоначальників у сфері NGFW була компанія Palo Alto Networks, яка представила свого часу серію пристроїв PA. Топові пристрої серії PA-5000 мали змогу обробляти трафік обсягом до 20 Гбіт/с з всіма задіяними функціями безпеки та підтримували ідентифікацію понад 3000 програмних застосунків. Згодом конкуруючі фірми (Fortinet, Cisco, Check Point) також представили свої апаратні рішення для даного покоління.

На даний час пристрої цього покоління є найбільш масовими та затребуваними в корпоративному сегменті мереж. Зважаючи на це, слід розглянути типову схему пристрою NGFW (рис. 1), що демонструє основні компоненти та їх взаємодію в процесі обробки мережного трафіку. Ця архітектура представляє собою складну багаторівневу систему, яка містить кілька взаємопов'язаних функціональних блоків, кожен з яких відповідає за певну функцію захисту. Вхідний трафік спочатку обробляється на рівні мережного процесора, який виконує початкову фільтрацію та класифікацію пакетів. Далі пакети передаються до модуля глибокої інспекції, що складається з кількох спеціалізованих блоків: аналізу протоколів, ідентифікації додатків, сигнатурного аналізу, поведінкового аналізу, виявлення аномалій та запобігання вторгненням. Центральний процесорний блок слугує для виконання функцій операційної системи та обробляє складні випадки, які вимагають додаткового аналізу. Пам'ять пристрою складається з наступних частин:

- надшвидка кеш-пам'ять для зберігання таблиць станів активних з'єднань;
- оперативна пам'ять для роботи програмних модулів;
- енергонезалежна пам'ять для зберігання конфігурацій та журналів подій.

Окремий криптографічний модуль відповідає за дешифрування та аналіз захищеного трафіку протоколів SSH/TLS, використовуючи спеціалізовані алгоритми та апаратне прискорення. Модуль управління політиками застосовує налаштовані адміністратором правила до обробленого трафіку. Всі компоненти пристрою з'єднані високошвидкісними внутрішніми шинами даних для забезпечення максимальної продуктивності при обробці трафіку. Вся система працює під керуванням спеціалізованої операційної системи реального часу, оптимізованої для обробки мережного трафіку з мінімальними затримками.

Незважаючи на значний прогрес у порівнянні з попередніми поколіннями, NGFW все ще стикаються з певними проблемами. Зокрема, зростання обсягів зашифрованого трафіку ускладнює його аналіз без значного зниження продуктивності. Окрім того, постійно зростаюча кількість додатків та їх короткий життєвий цикл вимагають регулярного оновлення відповідних баз даних. Також виникають питання щодо приватності при обробці зашифрованого трафіку, зважаючи на зміну вимог чинного законодавства про захист персональних даних в багатьох країнах. Ці виклики, а також поява нових типів загроз, пов'язаних з використанням технологій штучного інтелекту для планування та проведення атак, стимулюють подальший розвиток технологій фаєрволів.

Шосте покоління фаєрволів, яке почало формуватися приблизно з 2018 року, характеризується активним впровадженням технологій ШІ для боротьби із загрозами [14]. Ці пристрої здатні автономно аналізувати великі обсяги трафіку, виявляти приховані закономірності та адаптуватися до нових типів атак без необхідності ручного оновлення правил. Наприклад, платформа Cortex XDR, представлена Palo Alto Networks, використовує алгоритми ШІ для аналізу поведінки користувачів, додатків та пристроїв.

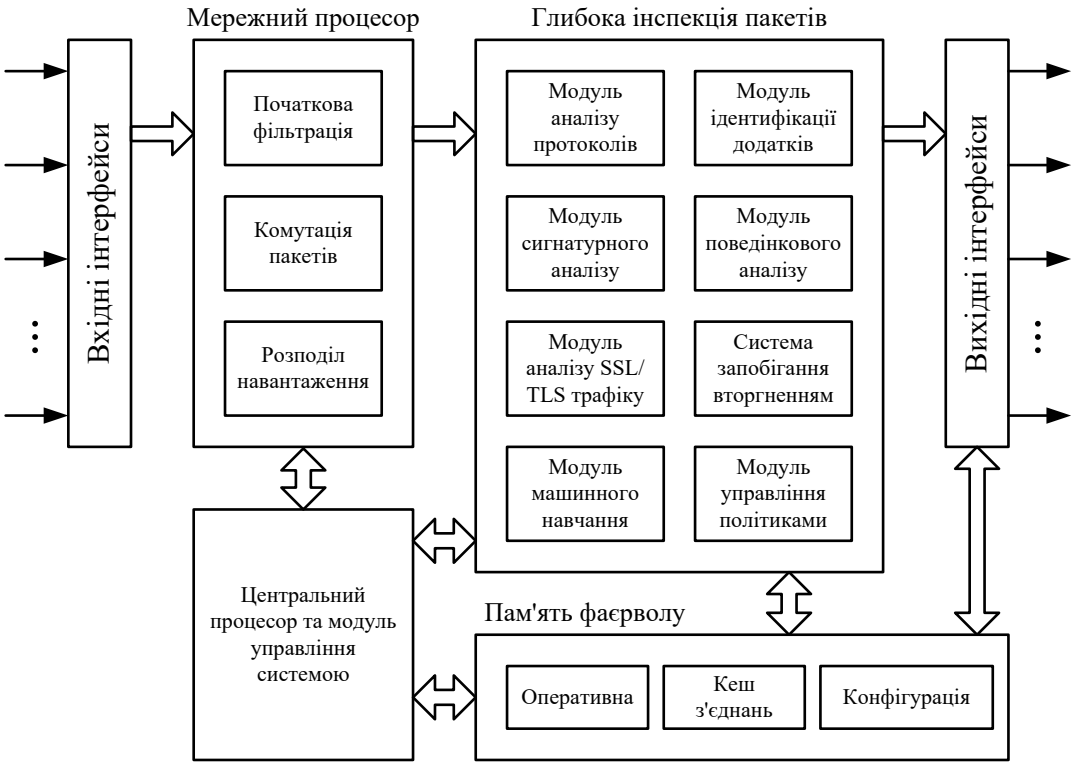

Рис. 1. Архітектура апаратного фаєрволу нового покоління NGFW

Апаратна реалізація фаєрволів з елементами ШІ вимагає значних обчислювальних ресурсів, тому пристрої цього типу зазвичай оснащуються спеціалізованими процесорами (GPU, TPU або FPGA) для прискорення операцій машинного навчання. Важливою особливістю цих пристроїв є наявність великого обсягу оперативної та енергонезалежної пам'яті для роботи моделей нейронних мереж.

Незважаючи на перспективність цього напряму розвитку, фаєрволи з елементами ШІ все ще стикаються з певними проблемами. По-перше, для ефективного навчання моделей машинного навчання потрібні великі обсяги достовірних даних. По-друге, існує ризик помилкових спрацьовувань або пропуску загроз через недостатню точність алгоритмів. По-третє, алгоритми машинного навчання можуть самі стати об'єктом атак, коли зловмисники навмисно маніпулюють вхідними даними для обходу захисту. Однак, незважаючи на ці виклики, розвиток технологій ШІ та їх інтеграція у фаєрволи є одним із найбільш перспективних напрямків еволюції засобів мережної безпеки.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Проведений в роботі аналіз еволюції апаратних фаєрволів для телекомунікаційних мереж демонструє чіткий їх розвиток в напрямі формування комплексних інтелектуальних систем, що здатні аналізувати трафік на всіх рівнях моделі OSI та адаптуватися до нових типів загроз. Кожне нове покоління пристроїв не лише розширювало функціональність, але й усувало обмеження попередників. Паралельно еволюціонувала і апаратна платформа — від загальнодоступних компонентів мікропроцесорних систем до спеціалізованих систем з багаторівневою архітектурою, що включає схеми ASIC, мережеві процесори, криптографічні акселератори та спеціалізовані модулі для машинного навчання. Сучасні тенденції розвитку цих пристроїв вказують на подальший розвиток технологій штучного інтелекту, посилення інтеграції з іншими системами безпеки для створення єдиної екосистеми для вирішення завдань по захисту даних.

Література

1. Смірнов О. А. Інформаційна безпека в комп’ютерних мережах : навч. посіб. / О. А. Смірнов, О. К. Конопліцька-Слободенюк, С. А. Смірнов, К. О. Буравченко, Т. В. Смірнова, Л. І. Поліщук. — Кропивницький : Видавець Лисенко В. Ф., 2020. — 295 с.

2. Комплексна безпека інформаційних мережевих систем : навч. посіб. для студентів спец. 174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка» / уклад.: А. Г. Микитишин, М. М. Митник, О. С. Голотенко, В. В. Карташов. — Тернопіль : ФОП Паляниця В. А., 2023. — 324 с.

3. Яцюк С. Використання фаєрволів як важливих компонентів системи безпеки вебсайтів та додатків / С. Яцюк, В. Юнчик, А. Яцюк, В. Муляр // Herald of Khmelnytskyi National University. Technical Sciences. — 2025. — № 349(2). — С. 500–504.

4. Cheswick W. R. Firewalls and Internet Security: Repelling the Wily Hacker / W. R. Cheswick, S. M. Bellovin. — Boston : Addison-Wesley, 1994. — 320 p.

5. Zwicky E. D. Building Internet Firewalls / E. D. Zwicky, S. Cooper, D. B. Chapman. — Sebastopol : O'Reilly Media, 1999. — 894 p.

6. Scarfone K. Guide to Firewalls and Firewall Policy / K. Scarfone, P. Mell. — Gaithersburg, MD : National Institute of Standards and Technology, 2009. — 54 p.

7. Goncalves M. Firewalls Complete / M. Goncalves. — New York : McGraw-Hill Osborne Media, 1998. — 632 p.

8. Deal R. A. Cisco Router Firewall Security / R. A. Deal. — Indianapolis : Cisco Press, 2005. — 456 p.

9. Whitman M. E. Guide to Firewalls and Network Security / M. E. Whitman, H. J. Mattord, R. Austin, G. Holden. — 2nd ed. — Boston : Cengage Learning, 2008. — 528 p.

10. Oppenheimer P. Top-Down Network Design / P. Oppenheimer. — 3rd ed. — Indianapolis : Cisco Press, 2010. — 528 p.

11. Suehring S. Linux Firewalls / S. Suehring, R. L. Ziegler. — 3rd ed. — Indianapolis : Novell Press, 2005. — 533 p.

12. Scarfone K. Guide to Intrusion Detection and Prevention Systems (IDPS) / K. Scarfone, P. Mell. — Gaithersburg, MD : National Institute of Standards and Technology, 2007. — 127 p.

13. Stallings W. Network Security Essentials: Applications and Standards / W. Stallings. — 6th ed. — Boston : Pearson, 2016. — 432 p.

14. Rais R. Zero Trust Networks: Building Secure Systems in Untrusted Networks / R. Rais, C. Morillo, E. Gilman, D. Barth. — 2nd ed. — Sebastopol : O'Reilly Media, 2024. — 332 p.

References

1. Smirnov O. A. Informatsiina bezpeka v kompiuternykh merezhakh : navch. posib. / O. A. Smirnov, O. K. Konoplitska-Slobodeniuk, S. A. Smirnov, K. O. Buravchenko, T. V. Smirnova, L. I. Polishchuk. — Kropyvnytskyi : Vydavets Lysenko V. F., 2020. — 295 s.

2. Kompleksna bezpeka informatsiinykh merezhevykh system : navch. posib. dlia studentiv spets. 174 «Avtomatyzatsiia, kompiuterno-intehrovani tekhnolohii ta robototekhnika» / uklad.: A. H. Mykytyshyn, M. M. Mytnyk, O. S. Holotenko, V. V. Kartashov. — Ternopil : FOP Palianytsia V. A., 2023. — 324 s.

3. Iatsiuk S. Vykorystannia faiervoliv yak vazhlyvykh komponentiv systemy bezpeky vebsaitiv ta dodatkiv / S. Yatsiuk, V. Yunchyk, A. Yatsiuk, V. Muliar // Herald of Khmelnytskyi National University. Technical Sciences. — 2025. — № 349(2). — S. 500–504.

4. Cheswick W. R. Firewalls and Internet Security: Repelling the Wily Hacker / W. R. Cheswick, S. M. Bellovin. — Boston : Addison-Wesley, 1994. — 320 p.

5. Zwicky E. D. Building Internet Firewalls / E. D. Zwicky, S. Cooper, D. B. Chapman. — Sebastopol : O'Reilly Media, 1999. — 894 p.

6. Scarfone K. Guide to Firewalls and Firewall Policy / K. Scarfone, P. Mell. — Gaithersburg, MD : National Institute of Standards and Technology, 2009. — 54 p.

7. Goncalves M. Firewalls Complete / M. Goncalves. — New York : McGraw-Hill Osborne Media, 1998. — 632 p.

8. Deal R. A. Cisco Router Firewall Security / R. A. Deal. — Indianapolis : Cisco Press, 2005. — 456 p.

9. Whitman M. E. Guide to Firewalls and Network Security / M. E. Whitman, H. J. Mattord, R. Austin, G. Holden. — 2nd ed. — Boston : Cengage Learning, 2008. — 528 p.

10. Oppenheimer P. Top-Down Network Design / P. Oppenheimer. — 3rd ed. — Indianapolis : Cisco Press, 2010. — 528 p.

11. Suehring S. Linux Firewalls / S. Suehring, R. L. Ziegler. — 3rd ed. — Indianapolis : Novell Press, 2005. — 533 p.

12. Scarfone K. Guide to Intrusion Detection and Prevention Systems (IDPS) / K. Scarfone, P. Mell. — Gaithersburg, MD : National Institute of Standards and Technology, 2007. — 127 p.

13. Stallings W. Network Security Essentials: Applications and Standards / W. Stallings. — 6th ed. — Boston : Pearson, 2016. — 432 p.

14. Rais R. Zero Trust Networks: Building Secure Systems in Untrusted Networks / R. Rais, C. Morillo, E. Gilman, D. Barth. — 2nd ed. — Sebastopol : O'Reilly Media, 2024. — 332 p.