УДК 004.056.53
DOI: 10.31673/2409-7292.2024.040007

Котляров О. Ю., Бортнік Л. Л.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ СИСТЕМ ЗАХИСТУ ВІРТУАЛЬНИХ МЕРЕЖ ТА ЇХ МЕТОДОЛОГІЇ

Стаття є дослідженням сучасних систем захисту віртуальних мереж і їх методологій, зокрема SIEM, IDS / IPS, NGFW, EDR, CASB та CWPP. У роботі обґрунтовано актуальність інтеграції цих рішень у єдину екосистему безпеки в умовах зростаючої складності багатовекторних кіберзагроз. Проведено порівняльний аналіз систем захисту за критеріями функціональності, продуктивності, інтеграції, масштабованості та вартості. Особливу увагу приділено ролі інноваційних підходів, таких як поведінковий аналіз, машинне навчання та автоматизація, які забезпечують швидке виявлення та реагування на загрози в реальному часі. У статті висвітлено ключові переваги сучасних рішень. NGFW забезпечують розширену перевірку трафіку та інтеграцію функцій IPS, тоді як EDR орієнтовані на глибокий аналіз поведінкових аномалій. CASB та CWPP демонструють ефективність у захисті хмарних середовищ, забезпечуючи контроль доступу та захист робочих навантажень. Виявлено, що поєднання цих технологій створює комплексну архітектуру, здатну адаптуватися до мінливих загроз. Дослідження також підкреслює важливість вибору між платними та безкоштовними рішеннями залежно від фінансових можливостей організацій. Системи з відкритим кодом, такі як Wazuh, забезпечують базовий рівень захисту, тоді як преміальні рішення, як-от Splunk, пропонують розширені функції для великих корпоративних мереж. Наукова новизна полягає у систематизованому підході до порівняння сучасних систем захисту, який враховує їхню функціональність, вартість та інтеграцію в СУІБ. Отримані результати сприяють кращому розумінню ефективності різних технологій у протидії сучасним кіберзагрозам і можуть бути використані для розробки рекомендацій щодо впровадження багаторівневої стратегії кібербезпеки в організаціях.

Ключові слова: фаєрвол, антивірус, трафік, віртуальні мережі, кіберзахист, хмірні технології.

Вступ і формулювання проблеми

В умовах стрімкого розвитку інформаційних технологій та цифровізації економіки питання забезпечення захисту віртуальних мереж набуває особливого значення. Віртуальні мережі, що є основою сучасних інформаційних систем, одночасно стають привабливими цілями для кібератак, які завдають дедалі більшої шкоди компаніям, організаціям та їхній інфраструктурі. Зростання складності та кількості атак вимагає ефективних рішень, спрямованих на захист даних, цілісності інформації та мінімізацію ризиків.

Проблематика захисту віртуальних мереж у сучасних умовах охоплює не лише питання ефективності засобів моніторингу та реагування, але й інтеграції різних технологій у єдину екосистему безпеки. Зокрема, традиційні засоби, такі як антивірусне програмне забезпечення та базові фаєрволи, вже не забезпечують належного рівня захисту від багатовекторних загроз. Натомість, новітні системи, такі як EDR (Endpoint Detection and Response), NGFW (Next-Generation Firewall) та XDR (Extended Detection and Response), пропонують інноваційні підходи, які потребують детального дослідження та оцінки ефективності.

Сьогодні на ринку представлено широкий спектр систем захисту, що включають як платні, так і безкоштовні рішення з відкритим кодом. Проте їх вибір часто обмежується бюджетними або часовими ресурсами організацій. Відтак виникає необхідність у проведенні всебічного порівняльного аналізу цих систем із метою визначення оптимального рішення, яке б відповідало потребам організацій з урахуванням їхніх можливостей. Крім того, ефективне застосування систем захисту неможливе без інтеграції з комплексною системою управління інформаційною безпекою (СУІБ), що забезпечує загальну координацію заходів безпеки. Таким чином, дослідження також розглядає, як різні системи захисту доповнюють і підсилюють функціональність СУІБ, створюючи єдину екосистему безпеки.

Аналіз літератури

Робота ґрунтується на аналізі науково-методичної літератури, методичних посібників, наукових статей, періодичних видань та напрацювань сучасних вчених, серед них: А. В. Жилін, Т. І. Коробейнікова, К. Шуліка, A. L. DeCarlo, S. Akhtar, L. Kharb та багато інших.

Аналіз літератури свідчить про багатогранний підхід до вивчення сучасних систем захисту віртуальних мереж і їх методологій. У працях дослідників акцентовано увагу на

ключових аспектах, таких як ефективність NGFW у моніторингу та аналізі трафіку [1], роль EDR у забезпеченні захисту кінцевих точок від складних атак [12], а також важливість CASB і CWPP у хмарних середовищах [16]. Порівняльний аналіз традиційних та інноваційних рішень, представлений у роботах [14] та [15], підкреслює зростаючу потребу в інтеграції функціональних можливостей різних систем у межах єдиної екосистеми безпеки. Таким чином, літературний огляд підтверджує актуальність теми й обґрунтовує необхідність розробки рекомендацій щодо інтеграції систем безпеки для протидії багатовекторним загрозам.

Метою дослідження є проведення порівняльного аналізу сучасних систем захисту віртуальних мереж з обґрунтуванням їхньої ефективності, функціональності, продуктивності, інтеграції та масштабованості.

Завдання дослідження:

1. Проаналізувати сучасні виклики у сфері забезпечення безпеки віртуальних мереж.
2. Провести порівняльний аналіз основних систем захисту за критеріями функціональності, швидкості реагування, продуктивності, масштабованості та інтеграції.
3. Вивчити особливості впровадження та використання інноваційних рішень, таких як NGFW, EDR та XDR, у сучасних інформаційних середовищах.
4. Дослідити ефективність CASB та CWPP у захисті хмарних середовищ, забезпеченні контролю доступу та моніторингу робочих навантажень.
5. Оцінити економічні аспекти вибору між платними та безкоштовними системами захисту, враховуючи можливості організацій.
6. Розробити рекомендації щодо інтеграції систем захисту в єдину екосистему безпеки під управлінням СУІБ.

Основна частина. Забезпечення безпеки віртуальних мереж є критично важливим аспектом інформаційної безпеки в умовах сучасної кіберзагрозової екосистеми. Віртуалізоване середовище не лише створює нові можливості для масштабування, ефективності та оптимізації ресурсів, але й стає вразливим до складних і багатовекторних атак. Це вимагає комплексного підходу до формування багаторівневої системи захисту, яка враховує специфіку динамічних інфраструктур, інтегрує інноваційні технології та орієнтується на адаптивність до нових викликів.

Традиційні підходи базуються на застосуванні сигнатурного аналізу, який використовується антивірусним програмним забезпеченням для ідентифікації відомих загроз. Незважаючи на свою ефективність у боротьбі зі стандартними атаками, такі рішення мають обмежену здатність до виявлення невідомих загроз (zero-day attacks) та складних методів маскування.

Фаєрволи першого покоління, які функціонують на рівні транспортного протоколу (OSI Layer 4), забезпечують базову фільтрацію трафіку за IP-адресами та портами. Їхня обмеженість у контексті аналізу прикладного рівня знижує здатність виявляти складні атаки, що обходять стандартні механізми фільтрації.

Сегментація мережі є однією з основних стратегій мінімізації ризиків шляхом ізоляції критично важливих компонентів системи. Використання VLAN, DMZ (демілітаризованих зон) та інших методів ізоляції дозволяє локалізувати вплив потенційної атаки. Проте сегментація вимагає значних інвестицій у правильне проектування та управління мережею.

IDS та IPS є ключовими елементами адаптивної безпеки. IDS аналізує мережевий трафік для виявлення аномалій і потенційних атак, використовуючи методи сигнатурного та поведінкового аналізу. IPS, у свою чергу, забезпечує активне втручання для нейтралізації виявлених загроз [1, с. 1030].

Сучасні IDS / IPS використовують методи глибокого навчання для аналізу мережевих шаблонів і автоматичної ідентифікації загроз у реальному часі. Недоліками є необхідність налаштування для мінімізації помилкових позитивів (false positives) та високі вимоги до обчислювальних ресурсів.

SIEM (Security Information and Event Management) платформи об’єднують дані з IDS, IPS, фаєрволів та інших джерел, забезпечуючи кореляцію подій для виявлення складних атак. Це дозволяє отримати глобальне уявлення про безпекову ситуацію та запроваджувати проактивні заходи.

В теорії принцип роботи SIEM рішення заключається у наступному: система збирає інформацію, аналізує “на льоту” (генеруючи попередження), складає аналізовані події в бази даних, перевіряє поведінку на підставі попередніх спостережень. На рис. 1 представлена узагальнена схема роботи SIEM системи [2, с. 146].

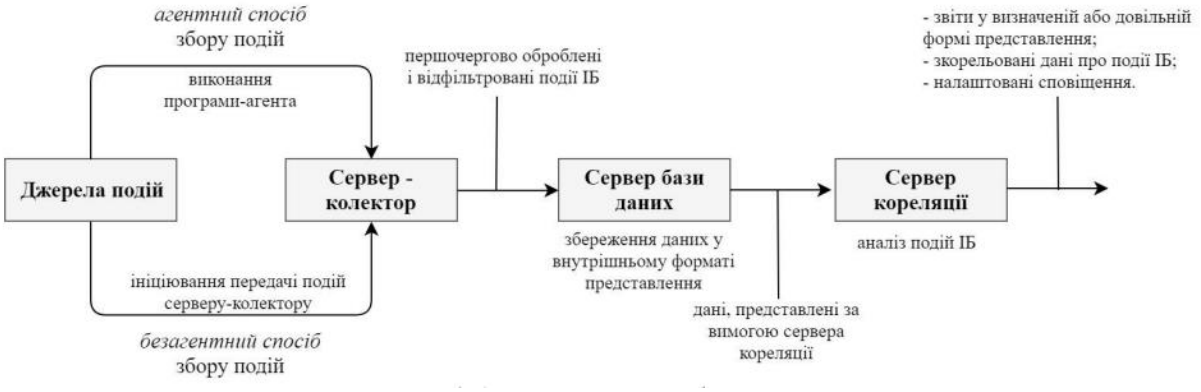

Рис. 1 Схема роботи SIEM системи [2, с. 146]

Шифрування є базовим, але необхідним елементом адаптивної безпеки віртуальних мереж. Протоколи IPsec і TLS забезпечують шифрування даних на мережевому та транспортному рівнях відповідно, що захищає інформацію від несанкціонованого доступу під час передачі.

Нині системи нового покоління, такі як NGFW (Next-Generation Firewall), EDR (Endpoint Detection and Response) та XDR (Extended Detection and Response), стають основними елементами стратегії кіберзахисту, забезпечуючи більш глибокий рівень моніторингу, виявлення та реагування на загрози. Ці інноваційні технології дозволяють не лише інтегрувати захист на різних рівнях інфраструктури, але й пропонують динамічний та комплексний підхід до управління кібербезпекою.

NGFW (Next-Generation Firewall) інтегрує функціонал класичних фаєрволів із можливостями аналізу прикладного рівня (Layer 7), контролю додатків, перевірки SSL-трафіку та функціями IPS. Це забезпечує кращу видимість та контроль над мережевою активністю.

EDR (Endpoint Detection and Response) спрямований на виявлення та реагування на загрози, що орієнтовані на кінцеві точки. Інтеграція поведінкових аналітичних алгоритмів дозволяє виявляти атаки, що обходять традиційні засоби захисту.

XDR (Extended Detection and Response) розширює EDR шляхом аналізу подій із різних джерел, таких як мережеві пристрої, хмарні сервіси та кінцеві точки. Цей підхід забезпечує комплексну координацію реагування на загрози [3].

Слід зазначити, що застосування штучного інтелекту та машинного навчання (ML) стає невід’ємною частиною інноваційних підходів до безпеки. Ці технології забезпечують прогнозування загроз на основі аналізу поведінкових моделей та ідентифікації аномалій. Наприклад, алгоритми ML використовуються для динамічного оновлення сигнатур загроз без втручання людини.

CASB (Cloud Access Security Broker) та CWPP (Cloud Workload Protection Platform) стають важливими для захисту гібридних інфраструктур. Вони дозволяють контролювати

доступ до хмарних ресурсів, виявляти загрози та забезпечувати відповідність регуляторним вимогам.

Ефективність усіх розглянутих підходів значною мірою залежить від їхньої інтеграції у систему управління інформаційною безпекою (СУІБ). СУІБ є оркестратором, що координує роботу різних компонентів захисту, забезпечуючи їхню взаємодію та адаптацію до нових загроз. Інтеграція рішень SIEM, NGFW, EDR та інших компонентів у СУІБ створює цілісну екосистему безпеки [4].

Тож, ефективне забезпечення безпеки віртуальних мереж вимагає впровадження багаторівневих підходів, які охоплюють традиційні, адаптивні та інноваційні стратегії. Поєднання технологій, таких як NGFW, XDR, SIEM, та використання алгоритмів ШІ створює комплексну систему захисту, яка відповідає викликам сучасного кіберсередовища. Впровадження цих підходів у рамках СУІБ забезпечує не лише поточний захист, але й здатність до адаптації у швидкозмінному технологічному ландшафті.

Для проведення порівняльного аналізу сучасних систем захисту віртуальних мереж доцільно використовувати ключові критерії, які охоплюють технічні та економічні аспекти: *вартість, функціональність, інтеграцію та продуктивність.* Оцінка вартості включає ліцензійні платежі, витрати на впровадження, супутні витрати, такі як навчання персоналу й технічна підтримка, а також загальну вартість володіння (TCO), яка враховує витрати протягом усього життєвого циклу рішення. Бюджетні обмеження часто визначають вибір між платними та безкоштовними системами, однак варто враховувати довгострокове співвідношення ціни й якості. Щодо функціональності, вона оцінюється через здатність системи виявляти загрози, запобігати вторгненням, проводити моніторинг і аналітику, підтримувати автоматизацію та забезпечувати гнучкість налаштувань.

Інтеграція системи захисту в існуючу інфраструктуру передбачає сумісність із іншими платформами (SIEM, ERP, CRM), наявність API для розширення функціональності, централізоване управління та масштабованість для адаптації до змін у мережі. Відсутність належної інтеграції може призвести до прогалин у безпеці та конфліктів між компонентами. Продуктивність системи визначається її пропускною здатністю, швидкістю реакції на загрози, оптимальним використанням обчислювальних ресурсів і стійкістю до високих навантажень. Чітке врахування цих критеріїв дозволяє організаціям вибирати рішення, що відповідають їхнім технічним і фінансовим потребам, забезпечуючи при цьому максимальну ефективність у протидії сучасним кіберзагрозам [5, с. 12–13].

Як вже було зазначено, одним із основних інструментів для моніторингу та захисту даних є система управління інформацією та подіями безпеки (SIEM). Це рішення дозволяє здійснювати централізований збір, аналіз і кореляцію подій з різних джерел інформації про безпеку, таких як системи мережевого моніторингу, журнали доступу, та інші лог-файли, що створюються в процесі роботи IT-інфраструктури [6, с. 84].

Одним із найбільш відомих комерційних рішень у сфері SIEM є система ***Splunk.*** Ця система надає потужні можливості для збору та аналізу даних у реальному часі, що дозволяє швидко виявляти аномалії, атакуючі дії та інші інциденти безпеки. Splunk забезпечує високий рівень масштабованості, що дозволяє ефективно працювати як у малих компаніях, так і в великих корпораціях з розподіленими мережами. Однією з головних особливостей Splunk є її здатність до глибокої кастомізації, що дозволяє налаштувати систему під специфічні вимоги організації. Проте варто зазначити, що комерційне використання Splunk має певні фінансові обмеження, оскільки ліцензії на використання цієї системи зазвичай розраховуються на обсяг оброблюваних даних, що значно збільшує загальні витрати на її впровадження та обслуговування. Крім того, Splunk потребує певних ресурсів для забезпечення своєї безперебійної роботи, зокрема, для зберігання великих обсягів даних та проведення складного аналізу [7, с. 66].

На противагу цьому, *Wazuh* є безкоштовною системою SIEM з відкритим кодом, яка є популярним вибором серед організацій з обмеженим бюджетом. Вона забезпечує базовий

набір функцій для моніторингу безпеки, виявлення аномалій і управління відповідністю. Побудована на основі Elastic Stack, Wazuh інтегрується з такими інструментами, як Elasticsearch, Logstash і Kibana, що дозволяє здійснювати ефективний збір, зберігання та візуалізацію даних. Хоча Wazuh може бути менш функціональною в порівнянні з Splunk, вона дає можливість забезпечити базовий рівень захисту без великих фінансових витрат. Однак необхідно враховувати, що для досягнення максимальних результатів у великих організаціях ця система вимагає додаткових налаштувань і оптимізації, що може вимагати додаткових людських та технічних ресурсів.

Порівнюючи ці дві системи, можна зазначити кілька ключових відмінностей. Splunk пропонує значно більш широкі можливості для аналізу та інтеграції з іншими корпоративними рішеннями, що робить її ідеальним вибором для великих організацій з великими вимогами до безпеки та наявністю бюджету для таких інвестицій. У свою чергу, Wazuh є більш доступним варіантом для малих і середніх підприємств, які не мають змоги витрачати значні кошти на захист своїх мереж, але при цьому потребують належного рівня моніторингу і виявлення загроз [8].

Вибір між платними та безкоштовними рішеннями залежить від багатьох факторів, серед яких ключовими є: наявність фінансових ресурсів, рівень складності мережі, вимоги до масштабованості, а також рівень технічної підготовки персоналу. У цьому контексті варто зазначити, що хоча ***Splunk*** пропонує більш розширені функції та підтримку [7, с. 67], ***Wazuh*** здатен задовольнити базові вимоги до безпеки без великих витрат, що робить його привабливим для організацій з обмеженими бюджетами [8]. Тому, вибираючи між цими системами, організації повинні орієнтуватися на свої реальні потреби в контексті забезпечення безпеки, зокрема з урахуванням того, чи потрібна їм висока продуктивність і масштабованість, чи достатньо буде функціоналу базового рівня для їхнього середовища.

Системи виявлення та запобігання вторгненням (IDS / IPS) є ключовими компонентами захисту віртуальних мереж, що спрямовані на виявлення, аналіз і протидію несанкціонованим спробам доступу або атакам. IDS (Intrusion Detection System) виконує моніторинг мережі для виявлення аномальної активності чи підозрілих дій, сповіщаючи адміністраторів про потенційні загрози, але не має функції блокування. Вона працює за двома основними принципами: сигнатурним виявленням, що ідентифікує загрози за відомими шаблонами, та аномальним виявленням, яке виявляє відхилення від нормальної поведінки мережі. Водночас система запобігання вторгненням (IPS) інтегрує функції IDS із активним блокуванням шкідливого трафіку в режимі реального часу, перехоплюючи загрози та запобігаючи їх подальшому поширенню.

Основні відмінності між IDS та IPS полягають у підході до реагування: IDS пасивно аналізує мережевий трафік, сповіщаючи про загрози, тоді як IPS автоматично блокує їх у режимі реального часу. Це надає IPS перевагу в оперативності, однак збільшує ризик хибних спрацьовувань, які можуть впливати на легітимний трафік. Крім того, IPS більш вимоглива до ресурсів і може знижувати продуктивність мережі через обробку трафіку, тоді як IDS працює незалежно, не втручаючись у мережевий потік. Таким чином, вибір між IDS і IPS залежить від потреб організації в оперативності реагування та рівні прийнятного впливу на мережу [9].

Крім відмінності у способі реагування на атакуючий або підозрілий трафік, IPS та IDS відрізняються способом встановлення в інфраструктурі мережі та по відношенню до мережевого трафіку. Якщо, як правило, IDS системи встановлюються “збоку” від мережевих потоків, обробляючи копію трафіку, що проходить через мережу, то IPS зазвичай встановлюються “в розрив” і стоять на проході трафіку через активне мережеве обладнання. На рис. 2 детально зображено відмінності у встановлені IPS та IDS систем.

У цьому випадку перевага IDS полягає у такому. При вичерпанні ресурсів, які є у засоби захисту для обробки трафіку, IDS не впливатиме на пропуск трафіку через мережу. IPS встановлений на проході оброблюваного трафіку, є вузьким місцем системи захисту. Як додатковий модуль у складі міжмережевого екрану, IPS дає додаткове навантаження на

обладнання міжмережевого екрану і здебільшого є частиною міжмережевого екрану нового покоління (Next Generation Firewall, NGFW) [10, с. 318–319].

Рис. 2 Різниця між встановленням IDS та IPS систем [10, с. 318–319]

Один із найбільш відомих інструментів для реалізації IDS / IPS – це **Snort.** Це система з відкритим кодом, яка надає можливості як для виявлення вторгнень, так і для запобігання. Snort використовує сигнатурне та аномальне виявлення і є популярним рішенням завдяки своїй гнучкості і можливості інтеграції з іншими компонентами мережевої безпеки. Однак Snort може мати проблеми з обробкою великих обсягів трафіку, що обмежує його ефективність у великих мережах.

Suricata – це ще один популярний інструмент з відкритим кодом для реалізації IDS / IPS, який є більш масштабованим і оптимізованим для обробки великих потоків даних. Suricata підтримує мульти-ядрову обробку та високопродуктивні функції для виявлення загроз. Вона також підтримує додаткові функції, такі як аналіз трафіку на рівні додатків та автоматичне визначення загроз на основі контексту. Це дозволяє Suricata бути більш ефективною в умовах високої пропускної здатності мережі [11, с. 237].

Порівняння між Snort і Suricata демонструє різницю в ефективності та масштабованості двох рішень. Snort більше орієнтований на невеликі мережі з помірним трафіком, в той час як Suricata є оптимальним вибором для великих корпоративних мереж з високими вимогами до пропускної здатності та швидкості обробки даних.

Вибір між системою виявлення та запобігання вторгнень залежить від потреб організації. Якщо компанія потребує більш гнучкого підходу до моніторингу безпеки, здатного реагувати на нові або невідомі загрози, система IDS може бути достатньою. Однак для організацій, що мають високі вимоги до безпеки та швидкої реакції на атаки, система IPS є більш підходящою, оскільки вона дозволяє автоматично запобігти атакам без участі адміністратора.

Таким чином, обрання між IDS і IPS повинно базуватись на критеріях, таких як розмір і складність мережі, вимоги до безпеки, наявність людських ресурсів для реагування на інциденти та бюджетні обмеження організації [9].

Системи IDS / IPS, хоча й відіграють ключову роль у виявленні та запобіганні мережевим загрозам, є лише частиною загальної екосистеми безпеки. У сучасних умовах, коли кібератаки стають дедалі складнішими та багатовекторними, необхідно зосередитися не лише на захисті мережевої інфраструктури, а й на кінцевих точках (endpoints), які часто стають основними векторами компрометації. У цій площині особливу увагу привертають рішення для захисту кінцевих пристроїв, такі як антивірусні програми (Antivirus) та системи розширеного виявлення та реагування (EDR).

Антивірусні програми є найбільш традиційним підходом до забезпечення безпеки кінцевих точок. Їхні основні функції зосереджені на виявленні, блокуванні та видаленні

відомого шкідливого програмного забезпечення. Антивірусні рішення працюють за принципом порівняння файлів і процесів із базою сигнатур, яка містить відомі зразки шкідливих програм. Деякі сучасні антивіруси також використовують евристичний аналіз, що дозволяє виявляти нові загрози на основі поведінкових шаблонів.

Попри свою поширеність, антивірусні рішення мають низку обмежень:

о**бмежена ефективність проти невідомих загроз.** Традиційні антивіруси залежать від оновлення бази сигнатур, що залишає прогалини для "нульових днів";

в**ідсутність активного моніторингу.** Більшість антивірусів функціонує у форматі "після виявлення", тобто реагує на загрозу лише після її ідентифікації [12, с. 187–188].

Endpoint Detection and Response (EDR) представляє нове покоління систем захисту кінцевих точок, які виходять за рамки традиційного підходу антивірусів. EDR фокусується на виявленні загроз у реальному часі, аналізі поведінкових аномалій та наданні глибокого огляду інцидентів безпеки. Це досягається завдяки використанню таких компонентів:

1. Моніторинг активності. EDR безперервно аналізує події на кінцевих точках, включаючи виконання програм, зміни файлів та мережеві підключення.
2. Поведінковий аналіз. Використання штучного інтелекту (AI) та машинного навчання (ML) дозволяє виявляти складні атаки, які не мають сигнатур.
3. Інтеграція з іншими системами. EDR рішення часто інтегруються з SIEM для кореляції даних між мережевими та кінцевими точками.

Серед переваг EDR варто виділити:

реагування в реальному часі. EDR автоматично блокує або ізолює кінцеву точку під час виявлення загрози;

прозорість і деталізація. Глибокий аналіз інцидентів дозволяє адміністраторам розслідувати та запобігати подібним атакам у майбутньому.

Таблиця 1 нижче демонструє ключові відмінності між традиційними антивірусами та сучасними EDR-системами.

Таблиця 1

Відмінності між традиційними антивірусами та сучасними EDR-системами

Критерій	**Antivirus**	**EDR**
Підхід	Сигнатурне виявлення, евристика	Поведінковий аналіз, AI, ML
Моніторинг	Локальний, пасивний	Безперервний, активний
Реагування	Видалення шкідливого ПЗ після виявлення	Автоматичне ізолювання, запобігання в реальному часі
Прогалини	Уразливість до атак "нульового дня"	Мінімізація невідомих загроз
Інтеграція	Обмежена	Інтегрується з SIEM, SOC

Джерело: авторська розробка

Антивіруси забезпечують мінімальний рівень захисту і підходять для невеликих організацій із обмеженими ресурсами. У той же час EDR орієнтовані на корпоративний сектор та організації, які потребують комплексного, проактивного підходу до безпеки.

На рис. 3 зображено радарна діаграма, яка порівнює антивірусні системи та EDR за такими параметрами: здатність до виявлення загроз, швидкість реагування, продуктивність, масштабованість та інтеграція. Графік демонструє дані, де EDR має перевагу в більшості категорій, особливо в швидкості реагування та масштабованості [13].

На радарній діаграмі порівнюються антивірусні системи та системи розширеного виявлення і реагування (EDR) за п'ятьма ключовими критеріями: здатність до виявлення загроз, швидкість реагування, продуктивність, масштабованість та інтеграція. Дані для діаграми є концептуальними та базуються на теоретичних оцінках, сформованих шляхом аналізу наукової літератури та практичних кейсів, опублікованих у відкритих джерелах. Ці

оцінки відображають загальні тенденції у використанні антивірусів та EDR і не претендують на абсолютну точність, оскільки реальна ефективність залежить від конкретної реалізації кожної системи, інфраструктури, що захищається, і контексту використання.

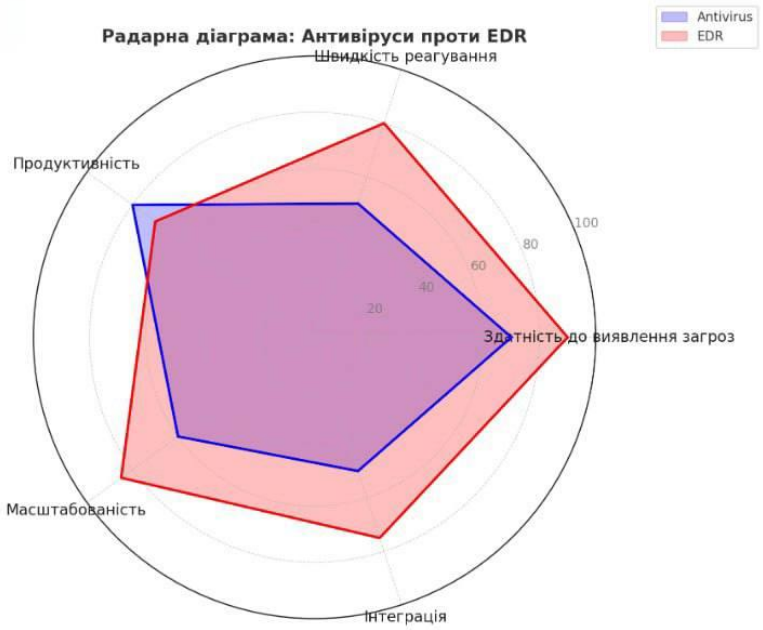

Рис. 3 Порівняння Антивірусу та EDR [13]

Аналіз показує, що EDR має значно вищу ефективність у виявленні сучасних загроз завдяки використанню алгоритмів поведінкового аналізу та інтеграції з іншими системами безпеки. Ці системи забезпечують швидке реагування і краще масштабуються для великих корпоративних мереж, але вимагають більше ресурсів. Натомість антивірусні рішення залишаються оптимальними для базового рівня захисту завдяки простоті використання, невисоким вимогам до продуктивності та нижчим витратам.

Перехід від традиційних антивірусів до EDR є еволюційною необхідністю в умовах сучасного кіберзагрозового середовища. У той час як антивіруси залишаються важливим компонентом безпеки, їх роль зводиться до базового рівня. Натомість EDR забезпечує інтегрований та аналітичний підхід, що дозволяє компаніям залишатися на крок попереду зловмисників [12, с. 189].

Еволюція захисту кінцевих точок, яка втілюється у переході від антивірусних програм до комплексних рішень EDR, є лише одним із аспектів загальної стратегії кіберзахисту. Іншою важливою складовою є захист на рівні мережевої інфраструктури, де основну роль відіграють фаєрволи (firewall). З моменту своєї появи традиційні фаєрволи стали базовим елементом безпеки мережі, але зі зростанням складності атак і використанням багатовекторних методів зловмисниками виникла потреба в удосконаленні цих рішень. Це призвело до розробки фаєрволів нового покоління (Next-Generation Firewall, NGFW), які інтегрують сучасні технології аналізу та забезпечення безпеки.

Традиційні фаєрволи функціонують на основі принципу фільтрації трафіку за IP-адресами, портами та протоколами. Вони створюють бар'єр між внутрішньою мережею організації та зовнішнім світом, використовуючи правила доступу (Access Control Lists, ACL). Основним завданням є запобігання несанкціонованому доступу до ресурсів мережі та блокування відомих загроз.

Однак їх ефективність обмежена кількома факторами:

відсутність глибокого аналізу**.** Традиційні фаєрволи не аналізують вміст пакетів, що дозволяє зловмисникам маскувати шкідливий трафік під легітимний;

нездатність протистояти сучасним загрозам. Більшість традиційних рішень безпорадні проти атак на рівні додатків, таких як SQL-ін'єкції або XSS.

Фаєрволи нового покоління (NGFW) розширюють функціональність традиційних рішень за рахунок інтеграції додаткових модулів аналізу та контролю. Вони дозволяють аналізувати трафік на рівні додатків (Layer 7 OSI), виявляти складні загрози та забезпечувати вищий рівень захисту.

Основні характеристики NGFW включають:

1. Детекція та блокування загроз. Використання баз сигнатур шкідливих програм і поведінкових шаблонів для виявлення аномалій.
2. Інтеграція функцій IPS. NGFW містить вбудовані системи запобігання вторгнень, що дозволяє їм оперативно реагувати на відомі загрози.
3. Контроль додатків. NGFW здатні ідентифікувати конкретні програми у мережевому трафіку, дозволяючи чи забороняючи їх використання залежно від політик.

Порівняння традиційних фаєрволів і NGFW [14, с. 30–31]

Для детального аналізу різниць між традиційними фаєрволами та NGFW наведемо порівняння за ключовими критеріями (Табл. 2).

Таблиця 2

Порівняння традиційних фаєрволів та NGFW за ключовими критеріями

Критерій	**Традиційні фаєрволи**	**NGFW**
Рівень аналізу		Рівень додатків (Layer 7 OSI)
Аналіз трафіку	Фільтрація IP, портів та протоколів	Глибокий аналіз вмісту пакетів
Захист від загроз	Обмежений, сигнатурний	Розширений, включаючи поведінковий аналіз
Інтеграція	Відсутність додаткових функцій	IPS, контроль додатків, SSL-інспекція
Гнучкість політик	Прості правила доступу	Комплексні політики з урахуванням додатків та користувачів
Продуктивність	Вища через меншу кількість обробки трафіку	Вимагає більше ресурсів для глибокого аналізу

Джерело: авторська розробка

Традиційні фаєрволи залишаються ефективними для базових потреб і забезпечують мінімальний рівень безпеки в мережах із низьким ризиком. Проте для сучасних організацій, які працюють у динамічному середовищі та піддаються багатовекторним атакам, NGFW стають обов'язковим компонентом. Їхня здатність інтегрувати контроль додатків, аналіз шифрованого трафіку (SSL Inspection) та виявлення загроз робить їх надзвичайно ефективними для захисту критично важливих інфраструктур.

Впровадження NGFW забезпечує глибоку інтеграцію з іншими елементами систем управління інформаційною безпекою (наприклад, SIEM), що дозволяє створити єдину екосистему безпеки з розширеними можливостями моніторингу та реагування. Традиційні фаєрволи, у свою чергу, залишаються релевантними для сегментованих мереж або систем, де складність атак є мінімальною. У цьому контексті порівняльний аналіз традиційного фаєрвола та NGFW дає змогу оцінити їхню ефективність за ключовими параметрами: пропускною здатністю та часом обробки (рис. 4) [15, с. 149].

Графік порівняння традиційного фаєрвола та NGFW демонструє пропускну здатність (у Gbps) та час обробки (у мс) при однакових навантаженнях. Пропускна здатність NGFW значно вища, досягаючи 8.2 Gbps у порівнянні з 3.5 Gbps у традиційного фаєрвола. Це свідчить про здатність NGFW обробляти більший обсяг трафіку без значної втрати ефективності. Також NGFW має значно нижчий час обробки запитів (40 мс проти 120 мс у традиційного фаєрвола), що підтверджує його перевагу в швидкості реакції.

Ці результати базуються на концептуальних даних, що відображають загальні технічні тенденції у використанні цих систем. Реальні параметри залежать від конкретних моделей, конфігурації мережі та типу навантаження. Графік демонструє, що NGFW забезпечує більш високий рівень продуктивності та ефективності в умовах сучасних багатовекторних загроз. Таким чином, вибір між традиційним фаєрволом і NGFW залежить від специфіки організації, її бюджету, ризиків і вимог до безпеки [15, с. 152].

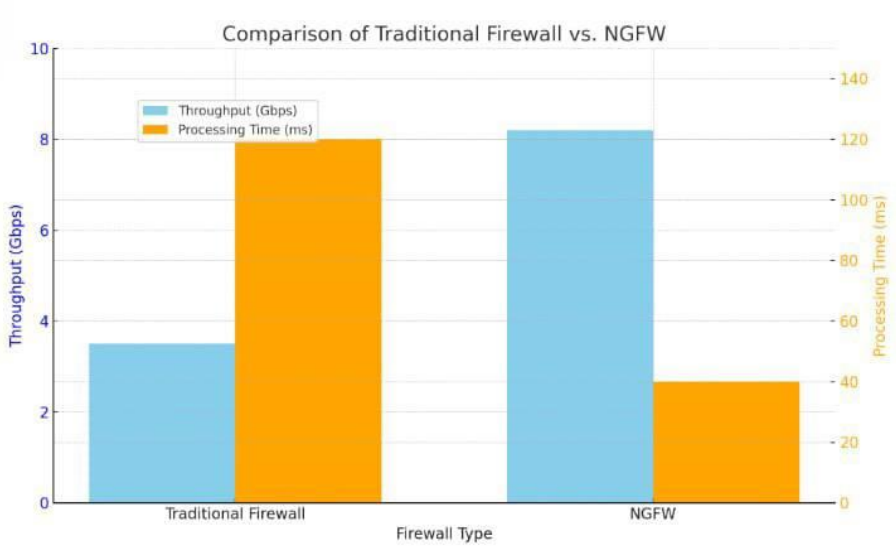

Рис. 4 Порівняльний аналіз традиційного фаєрвола та NGFW [15, с. 149].

Сучасний розвиток хмарних технологій та масове перенесення організаційних даних до хмарних середовищ створили унікальні виклики для забезпечення інформаційної безпеки. Традиційні інструменти захисту не здатні ефективно справлятися з багаторівневими загрозами, характерними для динамічних хмарних екосистем. У зв'язку з цим з'явилися спеціалізовані рішення, зокрема Cloud Access Security Broker (CASB) та Cloud Workload Protection Platform (CWPP), які відповідають потребам контролю доступу та захисту робочих навантажень відповідно. Їхнє впровадження дозволяє забезпечити всебічний моніторинг, управління ризиками та миттєву реакцію на інциденти безпеки.

CASB функціонує як посередник між користувачами та постачальниками хмарних послуг, забезпечуючи політики доступу, шифрування даних, контроль дій користувачів і захист від загроз, які виникають під час використання хмарних сервісів. Одним із ключових завдань CASB є забезпечення багатоетапної аутентифікації, що ускладнює несанкціонований доступ до даних. Крім того, CASB інтегрує механізми запобігання втраті даних (DLP), які моніторять пересування конфіденційної інформації та запобігають її витоку, навіть у разі компрометації облікових записів. CASB також шифрує дані перед їх передачею у хмару, зберігаючи конфіденційність навіть у випадку атак на сервери провайдера. Основним викликом для CASB залишається необхідність підтримки інтеграції з різноманітними хмарними платформами, зберігаючи при цьому високу продуктивність і мінімальну затримку [16, с. 642].

На відміну від CASB, яке орієнтоване на контроль доступу до хмарних сервісів, CWPP призначене для забезпечення безпеки на рівні робочих навантажень, таких як контейнери, віртуальні машини та безсерверні обчислення. Ця платформа забезпечує управління вразливостями через постійний аудит ресурсів і автоматизоване виявлення невідповідностей безпековим стандартам. CWPP також використовує поведінковий аналіз із застосуванням алгоритмів машинного навчання для розпізнавання аномалій, що можуть свідчити про внутрішні чи зовнішні загрози. Завдяки автоматизації реагування CWPP дозволяє ізолювати

небезпечні контейнери чи завершувати шкідливі процеси, мінімізуючи ризик поширення загрози [17].

CASB та CWPP відрізняються не лише своєю спрямованістю, а й способами інтеграції в загальну систему захисту. CASB ефективно вирішує завдання на рівні доступу до SaaS-додатків, у той час як CWPP зосереджується на захисті внутрішніх компонентів хмарної інфраструктури. У хмарному середовищі, де вразливості можуть виникати як на рівні користувацьких дій, так і на рівні внутрішніх ресурсів, часто доцільно використовувати обидва рішення в комплексі. Це забезпечує багаторівневий підхід до безпеки, при якому CASB захищає зовнішній периметр і контролює доступ, а CWPP гарантує захист критичних компонентів інфраструктури, створюючи єдину інтегровану екосистему кібербезпеки.

Еволюція хмарних рішень у контексті інформаційної безпеки підкреслює нагальну потребу в створенні комплексних архітектур, які інтегрують різнорівневі інструменти захисту. Зокрема, інтеграція таких рішень, як CASB і CWPP, демонструє здатність сучасних систем протидіяти багатовекторним загрозам, зберігаючи ефективність у розподілених і динамічних середовищах. Однак ці системи не є автономними; їхня повна функціональність розкривається лише в рамках інтегрованих підходів до управління інформаційною безпекою (СУІБ). Саме роль СУІБ як базової архітектури для систем захисту потребує глибокого технічного аналізу [18].

Система управління інформаційною безпекою (СУІБ), побудована відповідно до міжнародного стандарту ISO / IEC 27001, є основою для побудови цілісної екосистеми безпеки. Інтеграція сучасних засобів захисту з СУІБ дозволяє забезпечити централізоване управління всіма аспектами безпеки, від моніторингу до реагування на інциденти. Така інтеграція вимагає суворого узгодження політик доступу, моніторингу загроз, а також їхньої відповідності нормативним та бізнес-вимогам.

Реалізація інтеграції передбачає створення єдиного інформаційного простору, в якому дані з таких систем, як SIEM, IDS / IPS, EDR, NGFW, CASB та CWPP, консолідуються в реальному часі. Цей підхід дозволяє знизити ймовірність помилкових спрацьовувань завдяки кореляції подій і автоматизації процесів аналізу загроз. Наприклад, CASB, інтегрований із СУІБ, може надати додатковий контекст для політик доступу, в той час як CWPP забезпечує відповідність робочих навантажень стандартам безпеки, визначеним у рамках СУІБ.

Інтеграція також вимагає тісної взаємодії з системами управління ідентифікацією та доступом (IAM) для забезпечення чіткої сегментації прав доступу. Це дозволяє мінімізувати ризики, пов’язані з людським фактором, і підвищити прозорість доступу до критичних активів. Крім того, у випадку багатофакторної автентифікації (MFA) інтеграція CASB з IAM і СУІБ гарантує виконання корпоративних політик навіть у віддалених хмарних середовищах [19, с. 16–17].

Створення єдиної екосистеми безпеки передбачає не лише технічну інтеграцію, але й координацію процесів управління ризиками, відповідності регуляторним вимогам та інцидент-менеджменту. Єдина екосистема безпеки повинна поєднувати в собі такі елементи, як:

централізована аналітика. SIEM-системи виступають ядром екосистеми, консолідуючи дані з різних джерел і забезпечуючи швидке виявлення аномалій;

інтеграція поведінкового аналізу. EDR і CWPP можуть застосовувати алгоритми машинного навчання для ідентифікації нових загроз, забезпечуючи динамічну адаптацію політик захисту;

безшовний контроль доступу. CASB у поєднанні з NGFW гарантують, що зовнішній периметр залишається захищеним, а доступ до хмарних сервісів суворо регламентований;

масштабована автоматизація. Використання оркестрації, автоматизації та реакції на інциденти (SOAR) дозволяє мінімізувати час реагування та підвищити ефективність роботи персоналу.

Забезпечення єдиної екосистеми безпеки також сприяє підвищенню стійкості організації до кібератак завдяки динамічному обміну даними між системами. У рамках такого підходу рішення, що працюють окремо, перетворюються на єдиний організм, здатний адаптуватися до мінливого середовища загроз.

Інтеграція сучасних систем захисту з СУІБ та формування єдиної екосистеми безпеки забезпечують не лише технічну ефективність, але й відповідність стратегіям організаційного розвитку, сприяючи довгостроковій кіберстійкості [20].

Результати

Результати проведеного дослідження показали, що сучасні системи захисту віртуальних мереж мають різноманітні функціональні можливості, які забезпечують комплексну безпеку інформаційних інфраструктур. Аналіз показав, що IDS ефективно виявляє складні загрози через пасивний моніторинг і інтеграцію з SIEM для подальшого аналізу, тоді як IPS забезпечує проактивний захист, автоматично блокуючи шкідливий трафік у реальному часі. Однак IPS вимагає значних ресурсів і точного налаштування, що робить його більш придатним для середовищ із високими вимогами до швидкості реагування.

Дослідження порівняло традиційні фаєрволи та NGFW, де останні виявилися значно ефективнішими завдяки функціям перевірки трафіку на рівні додатків, SSL-декрипції та інтеграції IPS. Незважаючи на високу вартість і ресурсомісткість, NGFW стали ключовим елементом сучасної системи безпеки, особливо для складних загрозових середовищ. Аналогічно, аналіз антивірусів і EDR продемонстрував, що антивіруси ефективні для базових завдань, але обмежені у виявленні сучасних атак. EDR, завдяки поведінковому аналізу та проактивному моніторингу, є кращим вибором для протидії складним загрозам, хоча їхня реалізація потребує значних фінансових і технічних ресурсів.

У хмарних середовищах рішення CASB та CWPP довели свою ефективність. CASB зосереджений на контролі доступу, запобіганні витокам даних і відповідності нормативним вимогам, тоді як CWPP забезпечує захист робочих навантажень, зокрема контейнерів і серверів. Їхнє комбіноване використання дозволяє створити високий рівень безпеки для гібридних і мультихмарних інфраструктур. Інтеграція цих систем із SIEM, NGFW та EDR у рамках СУІБ створює єдину екосистему безпеки, яка забезпечує як проактивний захист, так і відповідність регуляторним вимогам.

Висновки і рекомендації

Отже, узагальнюючи результати дослідження, можна констатувати, що сучасні системи захисту віртуальних мереж, такі як SIEM, IDS / IPS, NGFW, EDR, CASB і CWPP, є критично важливими для забезпечення кібербезпеки в умовах зростаючих загроз. Максимальна ефективність цих технологій досягається через їх інтеграцію в єдину екосистему безпеки під управлінням СУІБ, що дозволяє забезпечити централізований моніторинг, мінімізувати дублювання функцій і підвищити адаптивність до загроз. При цьому сучасні підходи, засновані на поведінковому аналізі та реальному реагуванні, стають ключовими в боротьбі з динамічними кіберзагрозами, включаючи APT-атаки та zero-day уразливості.

Зростання використання хмарних технологій вимагає спеціалізованих рішень, таких як CASB і CWPP, що забезпечують контроль доступу та захист робочих навантажень. Крім того, автоматизація процесів кіберзахисту та впровадження технологій штучного інтелекту дозволяють значно скоротити час реагування на загрози й підвищити ефективність роботи персоналу. Для організацій із обмеженим бюджетом важливо враховувати баланс між вартістю рішень і їхньою функціональністю, зокрема, шляхом впровадження систем з відкритим кодом за наявності технічної експертизи.

Ефективність систем кіберзахисту значною мірою залежить від інтеграції рішень у бізнес-процеси організації, регулярного аудиту та дотримання принципів багаторівневого захисту. Збалансований підхід до вибору й впровадження інструментів кібербезпеки, що враховує технічні, фінансові й регуляторні аспекти, є ключем до створення стійкої й

ефективної системи протидії кіберзагрозам. Особливу увагу варто приділити інтеграції хмарних рішень для уникнення розривів у безпеці між локальними й хмарними середовищами.

Перелік посилань

1. Lamdakkar O., Ameur I., Mbarek Eleyatt M., Carlier F., Ait Ibourek L. Toward a modern secure network based on next-generation firewalls: recommendations and best practices. Procedia Computer Science. Vol. 238. 2024. Pp. 1029–1035. DOI: https: // doi. org / 10.1016 / j. procs. 2024.06.130.
2. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, Вид-во "Політехніка", 2021. 213 с.
3. What is a Next-Generation Firewall?: веб-сайт. URL: https: // www. coro. net / glossary / next-generation-firewall (дата звернення: 16.11.2024).
4. DeCarlo A. L. CASB vs. CSPM vs. CWPP: Comparing cloud security tool types: веб-сайт. URL: https: // www. techtarget. com / searchsecurity / feature / CASB-CSPM-CWPP-emerge-as-future-of-cloud-security (дата звернення: 16.11.2024).
5. Технології забезпечення безпеки мережевої інфраструктури: підручник / В. Л. Бурячок та ін. К.: КУБГ, 2019. 218 с.
6. Akhtar S., Sheorey P. A., Bhattacharya S. Cyber Security Solutions for Businesses in Financial Services: Challenges, Opportunities, and the Way Forward. International Journal of Business Intelligence Research (IJBIR). 2021. №12 (1). Pp. 82–97. DOI: https: // doi. org / 10.4018 / IJBIR. 20210101. oa5
7. Малькевич Р., Балацька В. Використання SPLUNK для захисту інформації в організаціях. Інформаційна безпека та інформаційні технології: зб. тез доповідей V Всеукр. наук. – практ. конф. молодих учених, студентів і курсантів. С. 66–68.
8. Brandstaetter S. Understanding Wazuh: The Free, Open Source Security Platform for XDR & SIEM: веб-сайт. URL: https: // osintph. medium. com / understanding-wazuh-the-free-open-source-security-platform-for-xdr-siem – 48b3c3dfba9d (дата звернення: 15.11.2024).
9. IDS vs. IPS: Definitions, Comparisons & Why You Need Both: веб-сайт. URL: https: // www. okta. com / identity – 101 / ids-vs-ips/ (дата звернення: 17.11.2024).
10. Коробейнікова Т. І., Цар О. О. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. Грааль науки. 2023. № 27. С. 317–325. DOI: https: // doi. org / 10.36074 / grail-of-science. 12.05.2023.050.
11. Очеретний С. О. Крижановський В. Г. Системи виявлення та запобігання вторгнень, найбільш успішні практики. Прикладні аспекти сучасних міждисциплінарних досліджень. 2024. 236–238. URL: https: // jpasmd. donnu. edu. ua / article / view / 14833 (дата звернення: 16.11.2024).
12. Шуліка К., Балагура Д., Смірнов А., Непокритов Д., Литвин А. Метод використання сучасних систем захисту кінцевих точок (EDR) для убезпечення від комплексних атак». Сучасний стан наукових досліджень та технологій в промисловості. 2024. №2 (28). С. 182–195. DOI: https: // doi. org / 10.30837 / 2522–9818.2024.2.182.
13. Traditional Antivirus vs. EDR (Endpoint Detection and Response): веб-сайт. URL: https: // cybriant. com / 2019 / 07 / 16 / antivirus-vs-edr/ (дата звернення: 17.11.2024).
14. Sichkar M., Pavlova L. A short survey of the capabilities of Next Generation firewalls. Computer Science and Cybersecurity. 2023. №1. С. 28–33. DOI: https: // doi. org / 10.26565 / 2519–2310–2023–1-02.
15. Patel U. The role of next-generation firewalls in modern network security: a comprehensive analysis. International Journal of Advanced Research in Engineering and Technology (IJARET). 2024. Vol. 15, Issue 4. Pp. 135–154. DOI: https: // doi. org / 10.5281 / zenodo. 13643404.
16. Kharb L., Chahal D. Cloud access security brokers: strengthening cloud security. International journal of research publication and reviews. 2023. Vol 4. №8. Pp 642–644. DOI: https: // doi. org / 10.55248 / gengpi. 4.823.50412.
17. What is a cloud workload protection platform (CWPP)?: веб-сайт. URL: https: // www. paloaltonetworks. com / cyberpedia / what-is-cwpp-cloud-workload-protection-platform (дата звернення: 17.11.2024).
18. Varghese Sh. J. Differences Between CSPM, CASB, CWPP & CNAPP in Cloud Security: веб-сайт. URL: https: // www. gsoftcomm. net / blogs / difference-between-cspm-casb-cwpp-cnapp-in-cloud-security/ (дата звернення: 17.11.2024).
19. Скіцько О. Ширшов Р. Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об'єктів критичної інфраструктури. International Science Journal of Engineering & Agriculture. 2023. Vol. 2. No. 6. Pp. 12–22. DOI: https: // doi. org / 10.46299 / j. isjea. 20230206.02.
20. Brandenburg G. The role and implementation of an information security management system in modern enterprises: веб-сайт. URL: https: // ctrl-disrupt. nl / en/-insights-news / the-role-and-implementation-of-an-information-security-management-system-in-modern-enterprises (дата звернення: 17.11.2024).

Надійшла 17.11.2024