УДК 004.056

М. М. Маркевич
Ю. В. Баришев

АНАЛІЗ ЗАСОБІВ IDS ТА IPS

Вінницький національний технічний університет

Анотація

У тезах розглянуто системи виявлення (IDS) та запобігання вторгнень (IPS), основні методи виявлення загроз цими системами та їхню класифікацію. Також зроблено порівняльний аналіз IDS та IPS. Проаналізовано основні інструменти IDS/IPS. На основі виконаного аналізу обґрунтовано доцільність розроблення спеціалізованих рішень для об'єктів критичної інфраструктури попри наявність флагманських рішень.

Ключові слова: IDS, IPS, захист мереж, критичні системи, кібербезпека.

Abstract

This paper examines intrusion detection systems (IDS) and intrusion prevention systems (IPS), the main methods these systems use to detect threats, and their classification. It also provides a comparative analysis of IDS and IPS. The main IDS/IPS tools are analyzed. The topicality of specialized means development for the objects of critical infrastructure is substantiated in the spite of flagship solutions' presence.

Keywords: IDS, IPS, network protection, critical systems, cyber security.

Вступ

Інформаційні системи часто піддаються різним кіберзагрозам, серед яких, зокрема, є атаки на відмову в обслуговуванні (DDoS-атаки), несанкціонований доступ до даних, програми-вимагачі, фішинг, соціальна інженерія. З розвитком інформаційних технологій масштабність та наслідки атак стають з кожним роком серйознішими, тому питання про захист об'єктів набуває все більшого значення. Для того щоб виявити загрози та запобігти їх появі використовуються системи IDS (Intrusion Detection System – Система виявлення вторгнень) та IPS (Intrusion Prevention System – Система запобігання вторгненням). Ці системи підвищують рівень захисту та дозволяють своєчасно реагувати на кіберінциденти, зменшуючи наслідки атак.

Метою цього дослідження є покращення захисту мереж від вторгнень шляхом порівняльного аналізу можливостей систем IPS та IDS.

Результати дослідження

IDS (Intrusion Detection System) – це інструмент мережевої безпеки, який контролює мережевий трафік і пристрої на наявність відомої шкідливої активності, підозрілої активності або порушень політики безпеки. IDS допомагає пришвидшити та автоматизувати виявлення мережевих загроз, попереджаючи адміністраторів безпеки (зазвичай через SIEM систему) про відомі або потенційні загрози або надсилаючи сповіщення до централізованого засобу безпеки. Система виявлення вторгнень не може самостійно зупинити загрози безпеці, тому сьогодні її можливості зазвичай інтегровані або включені до систем запобігання вторгненням (IPS), які можуть виявляти загрози безпеці та автоматично діяти для їх запобігання [1].

Основними методами виявлення загроз IDS є сигнатурний та поведінковий аналіз (виявлення аномалій). Виявлення на основі сигнатур аналізує мережеві пакети на наявність сигнатур атак, унікальних характеристик або поведінки, пов'язаних з певною загрозою. Методи виявлення аномалій використовують машинне навчання для створення та постійного вдосконалення базової моделі нормальної мережевої активності [1].

Системи виявлення вторгнень поділяються на HIDS (Host-based IDS), NIDS (Network-based IDS), PIDS (Protocol-based IDS) та APIDS (Application protocol-based IDS) [1]:

– HIDS встановлюються безпосередньо на кінцевих пристроях, таких як сервери або комп'ютери. Вони відстежують лише активність на цьому пристрої, включаючи трафік до нього та з нього. HIDS, зазвичай працюють, періодично створюючи знімки критично важливих файлів

операційної системи та порівнюючи ці знімки з часом, якщо виявляють зміни, то повідомляють про це користувача.

– NIDS відстежують мережевий трафік у реальному часі. Вони аналізують пакети даних, що проходять через мережу, з метою виявлення ознак мережевих атак, таких як сканування портів, DoS-атаки (атаки на відмову в обслуговуванні) або зловмисні з'єднання. NIDS зазвичай розташовуються в стратегічних точках мережі для забезпечення максимальної ефективності моніторингу.
– PIDS контролюють протоколи з'єднання між серверами та пристроями, розміщуючись на веб-серверах для моніторингу HTTP або HTTPS-з'єднань.
– APIDS працюють на прикладному рівні, аналізуючи специфічні протоколи. Ці системи розгортаються між веб-сервером і базою даних SQL для виявлення SQL-ін'єкцій.

Перевагами IDS є своєчасне виявлення загроз, моніторинг активності та захист від внутрішніх загроз, а недоліками — фальшиві спрацьовування, обмежена ефективність проти нових атак та потреба в постійному оновленні.

IPS (Intrusion Prevention System) відстежує мережевий трафік на наявність потенційних загроз і автоматично блокує їх, попереджаючи команду безпеки, розриваючи небезпечні з'єднання, видаляючи шкідливий контент або активуючи інші пристрої безпеки. Ці системи розвинулися з IDS, які виявляють загрози та повідомляють про них команді безпеки. IPS має ті ж функції виявлення та звітування про загрози, що й IDS, а також автоматизовані можливості запобігання загрозам, тому їх іноді називають «системами виявлення та запобігання вторгненням» (IDPS) [2].

Основними методами виявлення загроз IPS є також сигнатурний та поведінковий аналіз, але система запобігання вторгненням включає ще й методи виявлення на основі політик, що базуються на політиках безпеки, встановлених командою безпеки [2].

IPS поділяються на NIPS (Network-based Intrusion Prevention System), HIPS (Host-based Intrusion Prevention System), WIPS (Wireless Intrusion Prevention System) та NBA (Network Behavior Analysis) [2]. NIPS контролює вхідний та вихідний трафік до пристроїв у мережі, перевіряючи окремі пакети на наявність підозрілої активності. HIPS встановлюється на певній кінцевій точці, такій як ноутбук або сервер, і контролює лише трафік, що надходить до цього пристрою та з нього. WIPS контролює протоколи бездротових мереж на наявність підозрілої активності, як-от неавторизованих користувачів та пристроїв, що підключаються до Wi-Fi компанії. NBA контролюють потоки мережевого трафіку, можуть перевіряти пакети, як і інші IPS, але багато NBA зосереджуються на деталях сеансів зв'язку вищого рівня, таких як IP-адреси джерела та призначення, використані порти та кількість переданих пакетів.

Переваги та недоліки IPS можна оформити у вигляді порівняльної таблиці з IDS (табл. 1).

Таблиця 1 – Порівняльна таблиця IDS та IPS

Особливість	IDS	IPS
Основна функція	Виявляти загрози та повідомляти про них.	Виявляти загрози та автоматично блокувати їх.
Механізм реагування	Виявлення загроз.	Блокування загроз.
Режим роботи	Пасивний (працює поза мережевим трафіком).	Активний (працює в режимі реального часу).
Вплив на мережевий трафік	Не впливає.	Можуть бути затримки.
Ціль	Повідомити про загрозу.	Запобігти загрозі.

Отже, система виявлення вторгнень базується на виявленні загроз та сповіщенні про них адміністратору, а система попередження — на виявленні та блокуванні загроз до того, як вони можуть завдати шкоди.

Основними інструментами IDS/IPS є Snort [3], Suricata [3], Fail2Ban [6], Zeek [7].

Snort — це система виявлення мережевих вторгнень та запобігання їм з відкритим кодом, розроблена вперше у 1999 році. Snort фіксує та аналізує мережевий трафік у режимі реального часу, виявляє потенційні загрози та сповіщає системних адміністраторів, використовуючи комбінацію виявлення на основі сигнатур, аналізу протоколів та виявлення аномалій [4].

Suricata — це засіб виявлення мережевих загроз та моніторингу мережевої безпеки з відкритим кодом, розроблений Фондом відкритої інформаційної безпеки (OISF) у 2009 році [5]. Він розроблений як надійний та високопродуктивний інструмент для виявлення вторгнень/загроз і моніторингу мережевої безпеки. Suricata використовує сучасні апаратні можливості, включаючи багатопотоковість, прискорення графічного процесора та розширене виявлення протоколів, що робить його надійним та масштабованим рішенням для виявлення мережевих загроз.

Відмінність між цими двома інструментами полягає у призначенні розробки, оскільки Snort був розроблений як однопотоковий механізм, а Suricata – як багатопотоковий, що дозволяє ефективно використовувати всі ядра сучасних процесорів для аналізу великих потоків даних.

Fail2Ban – це інструмент для запобігання вторгненням, який захищає сервери Linux від brute-force атак. Його особливістю є відстеження файлів журналів на наявність шкідливої активності та автоматичного блокування IP-адреси, які мають ознаки атаки, оновлюючи правила брандмауера.

Zeek – це інструмент з відкритим кодом для аналізу мережевого трафіку та моніторингу безпеки, який дозволяє досліджувати мережеву активність без активного втручання у трафік.

Таким чином, основні інструменти відрізняються режимом роботи (активний, пасивний), типом виявлення загроз (сигнатурний, поведінковий, аналіз протоколів) та основним призначенням (захист від атак грубої сили, пасивний аналіз мережевого трафіку, комплексна система для виявлення та запобігання вторгненням).

Висновки

Отже, IDS спеціалізується на виявленні загроз та повідомленні про них, а IPS – на виявленні та блокуванні загроз. Ці системи забезпечують своєчасне реагування на кіберінциденти та запобігання їм. На сьогодні, зазвичай, інструменти IDS поєднують можливості IPS. З виконаного в роботі аналізу засобів випливає, що окрім багатофункціональних засобів як-то Snort чи Suricata наявні більш вузькоспеціалізовані засоби як Fail2Ban, які, попри менші функціональні можливості, можуть розв’язувати практичні задачі для захисту мережевих вузлів спеціального призначення. Це демонструє, що актуальним залишається розроблення нішових рішень, які використовуючи меншу кількість ресурсів, виконуватимуть спеціалізовані завдання. Зокрема цей підхід є актуальних для захисту засобів IoT на об’єктах критичної інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is an intrusion detection system (IDS)? IBM. URL: https://www.ibm.com/think/topics/intrusion-detection-system (last accessed: 21.03.2026)
2. What is an intrusion prevention system (IPS)? IBM. URL: https://www.ibm.com/think/topics/intrusion-prevention-system (last accessed: 21.03.2026)
3. M. H. Qutqut et al A Comparative Evaluation of Snort and Suricata for Detecting Data Exfiltration Tunnels in Cloud Environments . *Journal of Cybersecurity and Privacy*. 2026. Vol. 6, no. 1. 17 p, URL: https://doi.org/10.3390/jcp6010017 (last accessed: 21.03.2026)
4. Croos J. Introduction to Snort. October 26, 2022. URL: https://jaycroos.com/introduction-to-snort/ (last accessed: 21.03.2026)
5. What is Suricata. URL: https://docs.suricata.io/en/latest/what-is-suricata.html (last accessed: 21.03.2026)
6. Installing and Configuring Fail2Ban – RamNode Cloud VPS Documentation. URL: https://ramnode.com/support/documentation/cloud-vps/fail2ban (last accessed: 21.03.2026)
7. Zeek: About. Zeek. URL: https://zeek.org/about/ (last accessed: 21.03.2026)

Маркевич Мар’яна Михайлівна – студентка групи 1БКС-23б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: 7mariaanaa@gmail.com

Баришев Юрій Володимирович – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua

Mariana Markevych – student of group 1BKS-23b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: 7mariaanaa@gmail.com

Yurii Baryshev – PhD, associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua