isu-conference.com

ISU

INTERNATIONAL SCIENTIFIC UNITY

COLLECTION OF SCIENTIFIC PAPERS

ISSUE №49

5TH INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

RESEARCH IN SCIENCE, TECHNOLOGY AND ECONOMICS

DECEMBER 10-12, 2025
LUXEMBOURG, LUXEMBOURG

UDC 001(08)

Research in Science, Technology and Economics: Collection of Scientific Papers with Proceedings of the 5th International Scientific and Practical Conference. International Scientific Unity. December 10-12, 2025. Luxembourg, Luxembourg. 735 p.

ISBN 979-8-89704-985-1 (series)
DOI 10.70286/ISU-10.12.2025

The conference is included in the Academic Research Index ReserchBib International catalog of scientific conferences.

The collection of scientific papers presents the materials of the participants of the 5th International Scientific and Practical Conference "Research in Science, Technology and Economics" (December 10-12, 2025. Luxembourg, Luxembourg).

The materials of the collection are presented in the author's edition and printed in the original language. The authors of the published materials bear full responsibility for the authenticity of the given facts, proper names, geographical names, quotations, economic and statistical data, industry terminology, and other information.

ISBN 979-8-89704-985-1

ISU
INTERNATIONAL SCIENTIFIC UNITY

Official site: https://isu-conference.com/

на Полтавщині відбулася зустріч з поліцейськими [Електронний ресурс] / ГУНП в Полтавській області // Офіційний вебсайт ГУНП в Полтавській області. – 2025. – Режим доступу: https://pl.npu.gov.ua/news/yak-ditei-verbuiut-cherez-telegram-i-shcho-robyty-iakshcho-pobachyv-pidozrilyi-pakunok-u-litsei-na-poltavshchyni-vidbulasia-zustrich-z-politseiskymy
(дата звернення: 07.12.2025).
4. Шепелева А., Чайковська В. Буданов: Telegram – палка з двома кінцями [Електронний ресурс] / А. Шепелева, В. Чайковська // DW. – 2024. – Режим доступу: https://www.dw.com/uk/budanov-telegram-palka-z-dvoma-kincami/a-68688211
(дата звернення: 07.12.2025).
5. Мельник Р. Telegram усе ж пішов на співпрацю з поліцією Франції та передав необхідні дані — Libération [Електронний ресурс] / Р. Мельник // Hromadske. – 2024. – Режим доступу: https://hromadske.ua/svit/231150-telegram-use-z-pishov-na-spivpratsiu-z-politsiyeiu-frantsiyi-ta-peredav-neobkhidni-dani-liberation
(дата звернення: 07.12.2025)

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ БАГАТОРІВНЕВОГО КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Деркач Тетяна
к.т.н., доцент
Приходько Роман
здобувач вищої освіти
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна

Розвиток цифрових технологій та зростання залежності суспільства від комп'ютерних мереж призводить до істотного збільшення кількості кібератак, які стають дедалі складнішими та масштабнішими. Відтак питання забезпечення кібербезпеки є одним із пріоритетних для сучасних організацій, незалежно від їхнього профілю діяльності. Одним з основних інструментів протидії несанкціонованому доступу є системи виявлення вторгнень (Intrusion Detection Systems, IDS), що забезпечують оперативне виявлення аномальних дій у мережах та на окремих хостах.

Метою дослідження є аналіз принципів роботи IDS, їх видів, практичних можливостей та обмежень, а також значення таких систем у побудові комплексного механізму кіберзахисту.

1. Призначення та роль IDS у забезпеченні кібербезпеки

Система виявлення вторгнень виконує функцію безперервного моніторингу активності у мережі або на окремому пристрої з метою виявлення підозрілих дій, що можуть свідчити про можливу атаку. IDS аналізує мережевий трафік, зміни у файловій системі, доступ до системних ресурсів, активність користувачів та інші показники.

Основними завданнями IDS є:

- виявлення аномальних і шкідливих дій;
- формування сповіщень про інциденти безпеки;
- підтримка аналізу журналів подій;
- зменшення ризику та масштабів збитків від кібератак.

Завдяки використанню IDS організації отримують змогу оперативно реагувати на загрози та підвищують рівень мережевої прозорості.

2. Класифікація IDS та особливості їх роботи

Системи виявлення вторгнень традиційно поділяють на два основні типи:

2.1. Мережева система виявлення вторгнень (NIDS)

NIDS здійснює аналіз мережевого трафіку, що проходить через контрольні точки мережі. Такий підхід дозволяє виявити спроби проникнення ще до того, як вони вплинуть на окремі хости. NIDS є ефективним засобом контролю глобальної мережевої активності.

2.2. Хостова система виявлення вторгнень (HIDS)

HIDS встановлюється безпосередньо на кінцевому пристрої та контролює локальні процеси, зміни файлів, доступ до ресурсів та спроби ескалації привілеїв. Завдяки цьому HIDS є незамінним інструментом контролю над станом окремих серверів та робочих станцій.

Оптимальним рішенням є комбінування NIDS і HIDS, що забезпечує багаторівневий захист інформаційного середовища.

3. Методи виявлення атак

Існує два основних підходи до виявлення вторгнень:

3.1. Сигнатурний метод

Цей метод ґрунтується на використанні сигнатур – відомих шаблонів атак. Система порівнює мережеву та системну активність із попередньо визначеними ознаками шкідливих дій. Перевагою є висока точність, недоліком – неможливість виявлення нових атак.

3.2. Метод аналізу аномалій

IDS формує модель «нормальної» поведінки системи, а відхилення від неї інтерпретує як потенційну атаку. Це дозволяє фіксувати нові та нетипові загрози, однак збільшує ризик хибнопозитивних спрацювань.

У сучасних рішеннях часто поєднуються обидва методи, що підвищує надійність системи.

4. Практичні аспекти роботи IDS та приклади використання

Ілюстративним прикладом роботи IDS є виявлення сканування портів, яке часто передує спробі проникнення. Мережева IDS може розпізнати характерні патерни трафіку, що відповідають скануванню Nmap, і сформувати сповіщення

про інцидент. Водночас хостова система зафіксує спроби модифікації системних файлів або несанкціонований доступ до ресурсів сервера.

Популярні рішення IDS:

– Snort – розповсюджена система з відкритим кодом, орієнтована на сигнатурний аналіз.

– Suricata – високопродуктивна IDS/IPS, оптимізована для багатоядерних систем.

– OSSEC – HIDS, що забезпечує контроль цілісності файлів та аналіз журналів подій.

5. Переваги та обмеження систем виявлення вторгнень

Переваги IDS включають:

– оперативність виявлення інцидентів;
– підвищення рівня мережевої прозорості;
– підтримку розслідування кібератак;
– зменшення ризиків компрометації мережевих ресурсів.

Серед недоліків виокремлюють:

– можливість значної кількості хибнопозитивних спрацювань;
– обмеженість функцій активного захисту (на відміну від IPS);
– необхідність професійного налаштування та підтримки.

6. Типові атаки, що виявляються IDS

IDS ефективно ідентифікує такі типи атак:

– підбір облікових даних (Brute Force);
– DDoS-атаки;
– сканування портів;
– розповсюдження шкідливих програм;
– зміни конфігурацій та спроби ескалації привілеїв.

Це робить IDS універсальним інструментом для виявлення різноманітних загроз.

Висновки

Системи виявлення вторгнень є важливим елементом сучасних кіберзахисних механізмів. IDS забезпечує вчасне сповіщення про підозрілі дії, підвищує загальну захищеність мережі та підтримує розслідування інцидентів. Поєднання мережевих і хостових рішень формує багаторівневу інфраструктуру протидії кібератакам. Використання IDS у навчальних і реальних середовищах підкреслює важливість безперервного моніторингу та превентивного реагування на загрози.

Список використаних джерел

1. Beale J., Baker A., Esler J., Northcutt S. Snort Intrusion Detection and Prevention Toolkit. Burlington: Syngress Publishing, 2007. 448 p.
2. Northcutt S., Novak J. Network Intrusion Detection. Indianapolis: New Riders Publishing, 2002. 672 p.
3. Roesch M. Snort – Lightweight Intrusion Detection for Networks // Proceedings of the 13th USENIX Conference on System Administration. Seattle: USENIX Association, 1999. P. 229–238.

4. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). Gaithersburg: NIST, 2007. 127 p.
5. The Suricata Project. Suricata Documentation. The Open Information Security Foundation, 2023.
6. Деркач Т.М., Данилко В.О. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби // Тези 75-ї наукової конференції професорів, викладачів, наукових працівників, аспірантів та студентів Національного університету «Полтавська політехніка імені Юрія Кондратюка». Т. 1. (Полтава, 02 травня – 25 травня 2023 року). Полтава: Національний університет імені Юрія Кондратюка, 2023. С. 446–448.
7. Деркач Т.М., Лавренко М. Кіберпростір: аналіз загроз та методи захисту // L International scientific and practical conference «Innovative Education: Problems and Prospects of Scientific Research» (December 4–6, 2024). Stuttgart, Germany: International Scientific Unity, 2024. P. 112–115.

МОДЕЛЮВАННЯ ТА ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ АВТОМАТИЗАЦІЇ РЕКРУТИНГОВИХ ПРОЦЕСІВ В IT-КОМПАНІЇ

Пилип Даніела
здобувачка вищої освіти магістерського рівня
Спеціальність «Управління ІТ проєктами»
Пасічник Володимир
д.т.н., професор
Кафедра інформаційних систем та мереж
Ужгородський національний університет, Україна

Цифровізація HR-процесів є одним із ключових напрямів розвитку сучасних IT-компаній, оскільки швидкість та якість рекрутингу безпосередньо впливають на стабільність бізнесу, динаміку масштабування команд і рівень конкурентоспроможності на ринку технологій. В умовах високої конкуренції за кваліфікованих фахівців компанії вимушені переглядати свої підходи до організації рекрутингу, впроваджуючи системи, що забезпечують прозорість, керованість і безперервність процесів [4]. Ці зміни є критично важливими також через зростання обсягів даних, які обробляються в рекрутингу, та необхідність швидкої реакції на зміни ринку праці.

Попри це, значна частина українських компаній досі використовує ручні або частково автоматизовані методи обробки кандидатських даних, ведення вакансій та комунікації між учасниками процесу. Такий підхід часто призводить до дублювання інформації, втрати важливих даних і зниження точності кадрової аналітики. Розрізненість каналів комунікації, відсутність централізованого зберігання інформації та складність у відстеженні статусів кандидатів