КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.889
УДК 004.056

Полотай Орест Іванович
кандидат технічних наук, доцент,
доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID ID: 0000-0003-4593-8601
orest.polotaj@gmail.com

Брич Тарас Богданович
кандидат технічних наук, доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID ID: 0000-0001-6853-1981
taras_brych@hotmail.com

Кухарська Наталія Павлівна
кандидат фізико-математичних наук, доцент,
доцент кафедри безпеки інформаційних технологій
Національний університет Львівська Політехніка, Львів, Україна
ORCID ID: 0000-0002-0896-8361
kukharska.n@gmail.com

Ящук Валентина Ігорівна
кандидат економічних наук, доцент,
доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID ID: 0000-0003-2651-4918
valentina.lender@gmail.com

Ткаченко Артур Мар'янович
викладач кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID ID: 0009-0009-6830-4741
tkachenko.am14@gmail.com

ІНТЕГРАЦІЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ У СТРУКТУРУ КОРПОРАТИВНОЇ МЕРЕЖІ: ПІДХОДИ, ВИКЛИКИ ТА ЕФЕКТИВНІСТЬ РЕАГУВАННЯ НА ІНЦИДЕНТИ

Анотація. У статті здійснено комплексне дослідження інтеграції систем виявлення вторгнень (IDS/IPS) у структуру корпоративної мережі з урахуванням вимог сучасної кібербезпеки, актуальних ризиків та управлінських підходів згідно з міжнародними стандартами. Розглянуто актуальні виклики, пов'язані зі зростанням складності мережевих інфраструктур, розвитком цільових атак і підвищеними вимогами до швидкості реагування на інциденти інформаційної безпеки. Запропоновано системний підхід, який передбачає поетапне впровадження IDS/IPS-рішень на основі попереднього аналізу мережевої архітектури, класифікації активів, виявлення вразливостей та оцінки ризиків. Побудовано модель загроз корпоративної мережі, яка охоплює основні типи активів (сервери, робочі станції, маршрутизатори, точки доступу, сервіси аутентифікації) та типові вектори атак (SQL-ін'єкції, DDoS, фішинг, брутфорс, шкідливе ПЗ тощо). Окрему увагу приділено реалізації процесів реагування відповідно до вимог стандарту ISO/IEC 27001:2017. В межах дослідження змодельовано інцидент інформаційної безпеки у вигляді атаки типу SQL-ін'єкція на веб-додаток корпоративної мережі. Інцидент виявлено за допомогою сигнатурної

NIDS, після чого активовано спеціалізований Playbook, який передбачав автоматизовані дії з локалізації загрози, відключення підозрілого трафіку, логування подій та інформування персоналу. Додатково проведено forensic-аналіз, який дозволив реконструювати хронологію атаки, виявити слабкі місця в конфігурації веб-сервера та сформувати аналітичний звіт для подальшого оновлення політик безпеки. Всі дії узгоджувалися з попередньо встановленими процедурами в межах системи менеджменту інформаційної безпеки (СМІБ), що підтверджує практичну застосовність та ефективність ризик-орієнтованого підходу. Стаття також пропонує алгоритм інтеграції IDS/IPS у корпоративну мережу, який охоплює аналіз існуючої архітектури, вибір типу системи, налаштування правил виявлення загроз, інтеграцію з SIEM-системами та організацію навчання персоналу. Обґрунтовано, що інтеграція технічних засобів захисту з управлінськими політиками та механізмами реагування дозволяє досягти вищого рівня адаптивності, зменшити час між виявленням та реагуванням, а також забезпечити доказову базу для подальших розслідувань. У висновках підкреслено переваги інтегрованого підходу до кіберзахисту, зокрема його здатність масштабуватись, адаптуватись до нових загроз та сприяти безперервному вдосконаленню інформаційної безпеки. Запропоновано напрями для майбутніх досліджень, серед яких автоматизація реагування з використанням штучного інтелекту, впровадження концепцій Zero Trust, розвиток поведінкових моделей аналізу загроз і побудова навчальних кіберполігонів для перевірки ефективності playbooks.

Ключові слова: інформаційна безпека; кіберзагрози; системи виявлення вторгнень; корпоративна мережа; реагування на інциденти; цифрова криміналістика; forensic-аналіз; playbook; SIEM; SQL-ін’єкція; оцінка ризиків.

ВСТУП

У сучасному цифровому середовищі, де інформація виступає ключовим ресурсом, питання забезпечення безпеки комп’ютерних мереж стає надзвичайно актуальним. З кожним роком кількість кібератак, спрямованих на корпоративні інфраструктури, неухильно зростає, при цьому зловмисники застосовують усе складніші методи обходу традиційних засобів захисту. В умовах високої вартості втрат, пов’язаних із витоком даних, компрометацією систем чи порушенням доступності сервісів, організації змушені інвестувати у комплексні рішення з інформаційної безпеки.

Одним із ключових компонентів сучасної системи захисту корпоративної мережі є системи виявлення вторгнень (IDS — Intrusion Detection Systems), які дозволяють оперативно виявляти ознаки несанкціонованого доступу, зловмисної активності або порушення політик безпеки. У поєднанні з системами запобігання вторгненням (IPS — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп’ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет) вони формують основу для побудови активної оборони, здатної не лише фіксувати інциденти, а й реагувати на них у реальному часі.

Інтеграція IDS/IPS у загальну інфраструктуру мережі потребує глибокого розуміння архітектурних особливостей мереж, знання сучасних загроз, а також дотримання принципів управління інформаційною безпекою відповідно до міжнародних стандартів (зокрема ISO/IEC 27001) [6]. Важливою складовою також виступають технології розслідування інцидентів, що включають аналіз логів, використання SIEM-систем, інструментів цифрової криміналістики [8] та автоматизованих процедур реагування.

Постановка проблеми. Попри наявність широкого спектра технічних засобів захисту інформаційних систем, більшість організацій продовжують стикатися з численними викликами у сфері кібербезпеки. Це пояснюється тим, що сучасні загрози постійно еволюціонують, а традиційні методи захисту (наприклад, фаєрволи та антивіруси) дедалі частіше виявляються недостатніми для своєчасного виявлення складних, прихованих або таргетованих атак.

Системи виявлення та запобігання вторгнень (IDS/IPS) надають розширені можливості для аналізу мережевого трафіку й виявлення підозрілої активності. Проте в умовах зростання обсягів даних, розподіленої структури мереж і збільшення кількості IoT-пристроїв, ефективність таких систем значною мірою залежить від:

- коректної інтеграції в інфраструктуру мережі;
- грамотного налаштування механізмів реагування;
- узгодженості з політиками інформаційної безпеки організації;
- наявності підготовленого персоналу для обробки інцидентів.

Крім того, часто спостерігається низький рівень координації між технічними засобами виявлення загроз і процесами менеджменту інформаційної безпеки, що унеможливлює цілісне реагування на інциденти. У результаті організації отримують численні попередження про потенційні загрози, але не мають чітких інструкцій або ресурсів для ефективного реагування, розслідування та усунення наслідків.

Таким чином, постає комплексна проблема: як забезпечити ефективне функціонування систем IDS/IPS у реальному середовищі корпоративної мережі, не лише з технічної точки зору, а й в контексті організаційного управління безпекою. Особливої уваги потребує питання інтеграції технологічних і управлінських підходів, що дозволяє оперативно виявляти інциденти, аналізувати причини їх виникнення та впроваджувати заходи з мінімізації ризиків у майбутньому.

У межах цієї статті розглядаються:

- сучасні підходи до побудови систем виявлення та реагування на кіберзагрози;
- виклики, що виникають при інтеграції таких систем у корпоративне середовище;
- приклади ефективного реагування на інциденти інформаційної безпеки;
- взаємозв’язок між технічними засобами захисту та організаційним управлінням інформаційною безпекою.

Метою дослідження є аналіз ефективності використання IDS/IPS у контексті побудови стійких до загроз інформаційних систем, а також розробка рекомендацій для підвищення рівня захисту комп’ютерних мереж з урахуванням сучасних викликів.

Аналіз останніх досліджень і публікацій. Проблематика виявлення та запобігання кіберзагрозам у корпоративних мережах широко висвітлюється в наукових і технічних публікаціях. Дослідженню методиці виявлення вторгнень присвячені роботи [7], [9], [5], в яких розглянуто принципи побудови систем IDS/IPS, методи аналізу трафіку, алгоритми машинного навчання для виявлення аномалій та концепції глибокого інспектування пакетів (DPI). Проте, попри глибину технічного аналізу, більшість наукових публікацій фокусуються або на ізольованому розгляді окремих компонентів (наприклад, IDS-алгоритмів), або на теоретичних аспектах управління інформаційною

безпекою, не приділяючи достатньої уваги практичному узгодженню технічної інфраструктури з організаційними процедурами реагування на інциденти.

Крім того, брак емпіричних досліджень, що демонструють інтеграцію IDS/IPS у реальному корпоративному середовищі з конкретними сценаріями інцидентів, обмежує застосовність існуючих підходів у практиці кіберзахисту. У багатьох роботах недостатньо враховано виклики, пов'язані з масштабованістю, складністю мереж, автоматизацією розслідувань і впливом людського фактора на ефективність реагування.

Мета статті. Метою дослідження є аналіз ефективності використання IDS/IPS у контексті побудови стійких до загроз інформаційних систем, а також розробка рекомендацій для підвищення рівня захисту комп'ютерних мереж з урахуванням сучасних викликів.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Система забезпечення кібербезпеки корпоративної мережі є складною сукупністю технічних, організаційних та процедурних компонентів, основною метою яких є захист конфіденційності, цілісності та доступності інформації. Теоретичний фундамент цього дослідження базується на поєднанні концепцій із таких галузей, як інформаційна безпека, мережеві технології, управління ризиками, а також технології розслідування кіберінцидентів.

Однією з базових передумов побудови ефективної системи виявлення вторгнень є чітке розуміння моделі загроз, що характерна для конкретної організації або галузі. Згідно з принципами ризик-менеджменту, що закріплені у міжнародному стандарті ISO/IEC 27005, ефективне реагування можливе лише за умови ідентифікації активів, вразливостей, загроз і потенційних наслідків. Тому інтеграція IDS/IPS повинна враховувати саме ті ризики, які мають найвищий пріоритет.

Існує кілька основних типів систем виявлення вторгнень [2]:

HIDS (Host-based Intrusion Detection Systems) — орієнтовані на моніторинг активності окремих хостів;

NIDS (Network-based Intrusion Detection Systems) — аналізують мережевий трафік у реальному часі;

Hybrid IDS — комбінують обидва підходи для досягнення більш повного охоплення.

Системи можуть бути пасивними (реєструють події) або активними/превентивними (IPS — запобігають загрозам шляхом блокування або ізоляції трафіку). Основні методи, які використовуються в IDS [10]:

Сигнатурний аналіз — порівняння з базою відомих атак;

Аналіз аномалій — виявлення відхилень від «нормальної» поведінки;

Гібридні моделі — поєднання сигнатур і поведінкових патернів.

Ефективність виявлення загроз залежить від архітектурних особливостей мережі: наявності демілітаризованих зон (DMZ), сегментації мережі, побудови маршрутів та точок моніторингу трафіку. IDS/IPS мають бути правильно позиціоновані у мережі для того, щоб забезпечити повне охоплення трафіку та уникнути сліпих зон [1].

Організаційний аспект кібербезпеки передбачає розробку політик, планів реагування, протоколів оповіщення та систем логування. Згідно з ISO/IEC 27001, важливими компонентами системи управління безпекою є:

- оцінка ризиків;
- контроль доступу;
- моніторинг інцидентів;
- безперервне покращення.

Інтеграція IDS/IPS повинна здійснюватися з урахуванням політик ІБ і бути частиною цілісного циклу PDCA (Plan-Do-Check-Act).

Процеси реагування на інциденти включають:

- виявлення та класифікацію інциденту;
- збереження доказової бази;
- аналіз логів;
- вжиття відповідних заходів (ізоляція, блокування, усунення вразливостей).

Сучасні SIEM-системи (Security Information and Event Management) забезпечують централізований збір, кореляцію та аналіз подій, що значно підвищує ефективність розслідування.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Побудуємо модель загроз інформації корпоративної мережі, використовуючи ризик-орієнтований підхід. Для цього визначимо найбільш значущі активи (Asset Inventory), ідентифікуємо ризики (Threat Modeling), визначимо вразливості (Vulnerabilities) та проведемо оцінку ризиків (Risk Assessment).

До найбільш значущих активів віднесемо:

- Сервери баз даних.
- Робочі станції.
- Маршрутизатори та точки доступу.
- Сховища резервних копій.
- Портали для співробітників.

Серед небезпечних ризиків, які притаманні активам варто виділити:

- Несанкціонований доступ.
- DDoS-атаки.
- Встановлення бекдорів.
- Витік облікових даних.
- Мережеве сканування.

Вразливості, які притаманні нашим активам такі:

- Відкриті порти на серверах.
- Використання застарілого ПЗ.
- Відсутність мережевої сегментації.
- Слабкі паролі.

Для оцінки ризиків використаємо матрицю оцінки ризику:

- Ймовірність (Low/Medium/High)
- Наслідки (Low/Medium/High)

ISSN 2663 - 4023

Таблиця 1

Модель загроз

#	Актив	Загроза	Вразливість	Ймовірність	Наслідки	Рівень ризику	Рекомендації / Роль IDS/IPS
1	Сервер бази даних	SQL-ін’єкція	Вразливий веб-інтерфейс	Висока	Витік даних, порушення цілісності	**Критичний**	IPS з сигнатурним аналізом, контроль доступу до запитів, сегментація мережі
2	Веб-сервер	DDoS-атака	Відсутність засобів фільтрації	Середня	Втрата доступності	**Високий**	NIDS з механізмами виявлення аномалій, автоматичне блокування надмірного трафіку
3	Робочі станції персоналу	Інфікування шкідливим ПЗ	Відсутність антивірусу, відкриті порти	Висока	Компрометація мережі, розповсюдження атаки	**Високий**	HIDS для моніторингу поведінки, політика мінімальних прав
4	Система електронної пошти	Фішинг	Низький рівень обізнаності користувачів	Висока	Викрадення облікових даних	**Високий**	Моніторинг вхідної пошти, SIEM для кореляції підозрілих входів, навчання персоналу
5	Wi-Fi точка доступу	Несанкціонований доступ	Слабке шифрування, спільні паролі	Середня	Прослуховування трафіку, проникнення в мережу	**Середній**	IDS для виявлення сторонніх пристроїв, WPA3, сегментація гостьової мережі
6	Система резервного копіювання	Внутрішня атака	Відсутність шифрування та логування	Низька	Порушення відновлення після інциденту	**Середній**	Контроль доступу, аудит подій, HIDS на серверах бекапів
7	Система управління доменом (Active Directory)	Зловмисний доступ	Відсутність контролю привілеїв	Середня	Повна компрометація домену	**Критичний**	SIEM для виявлення спроб ескалації привілеїв, HIDS на контролерах домену
8	Сервіс VPN	Брутфорс-атаки	Прості або спільні паролі	Середня	Несанкціонований доступ	**Високий**	IDS із правилами виявлення брутфорсу, MFA, обмеження IP

На основі побудованої моделі загроз встановлено, що найбільшу небезпеку для корпоративної мережі становлять:

– складні атаки типу SQL-ін’єкцій, брутфорсу, розповсюдження шкідливого ПЗ;
– вразливості, пов’язані з людським фактором, слабкими конфігураціями та браком моніторингу;
– недостатність контролю над критичними активами, такими як сервери баз даних, точки доступу, служби аутентифікації.

Це потребує цілісного підходу до моніторингу подій у мережі та на кінцевих пристроях, що забезпечується шляхом інтеграції систем IDS/IPS як ключових елементів архітектури захисту.

Доцільним буде запропонувати алгоритм інтеграції IDS/IPS у корпоративну мережу, який можна представити у такому вигляді (рис. 1):

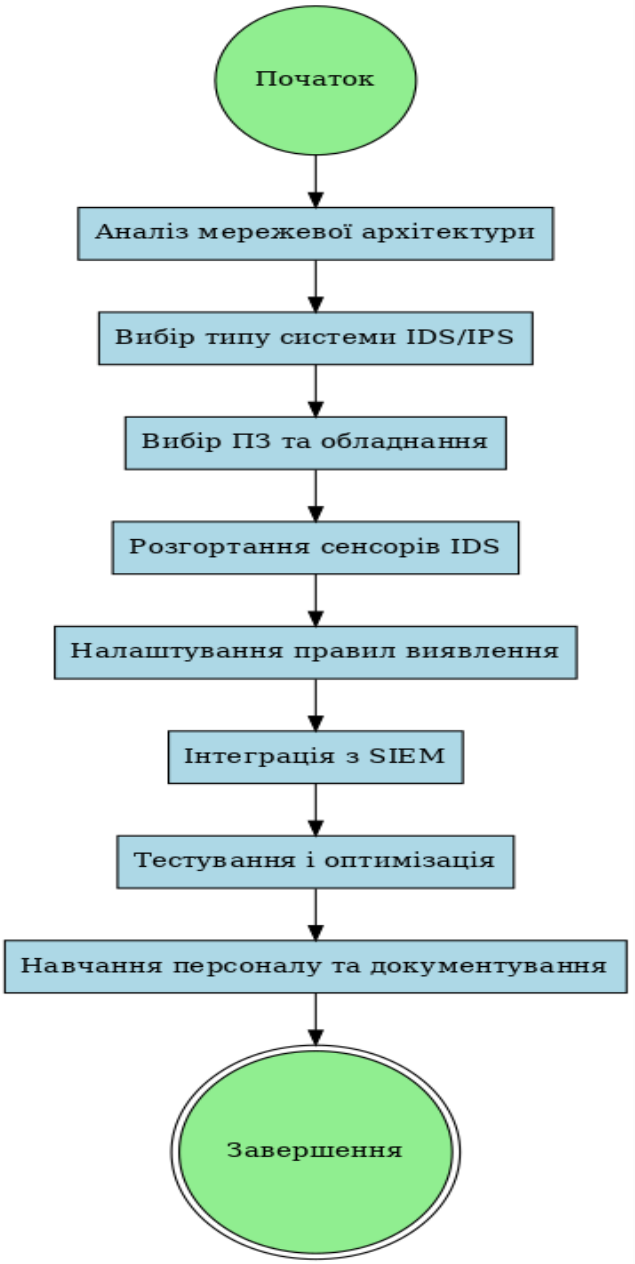

Рис. 1. Алгоритм інтеграції IDS/IPS у корпоративну мережу

Алгоритм, який представлений на рисунку, повинен складатись з таких кроків:

Крок 1. Аналіз мережевої архітектури:

Ідентифікувати логічну й фізичну структуру мережі.

Виділити критичні вузли: сервери, шлюзи, DMZ-зону, точки підключення користувачів.

Визначити обсяги трафіку та точки, де доцільно розміщувати сенсори IDS.

Крок 2. Вибір типу системи:

NIDS (мережева) — для аналізу зовнішнього й внутрішнього трафіку.

HIDS (хостова) — для моніторингу серверів та робочих станцій.

Гібридна — об'єднання NIDS та HIDS для повного покриття.

Крок 3. Вибір програмного забезпечення / апаратних рішень:

Комерційні: Cisco Secure IPS, Fortinet FortiGate, Palo Alto.

Відкриті: Snort, Suricata, OSSEC, Zeek (ex-Bro).

Врахувати сумісність з SIEM-системами та вимоги до продуктивності.

Крок 4. Розгортання сенсорів IDS:

На ключових точках доступу: між інтернетом і внутрішньою мережею, у DMZ, біля серверів.

На окремих вузлах (для HIDS): файрволи, контролери домену, веб-сервери.

Враховувати обхідні маршрути, щоб уникнути «сліпих зон».

Крок 5. Налаштування правил виявлення та фільтрації:

Використовувати оновлювані сигнатури для виявлення відомих атак.

Впровадити евристичні й аномальні модулі для виявлення нових загроз.

Встановити політики реагування: блокування, сповіщення, логування.

Крок 6. Інтеграція з SIEM:

Об'єднати дані з IDS/IPS, логів серверів, фаєрволів у централізовану систему.

Впровадити кореляційні правила для виявлення складних атак.

Автоматизувати генерацію інцидентів та створення звітів.

Крок 7. Тестування і оптимізація:

Провести пентест або контрольоване моделювання атак.

Виміряти кількість хибних спрацювань (false positives) і реальних виявлень.

Налаштувати винятки, відфільтрувати фоновий шум.

Крок 8. Навчання персоналу та документування:

Провести тренінги для адміністраторів SOC.

Розробити процедури реагування на події.

Документувати політики, конфігурації та сценарії дій.

Інтеграція IDS/IPS — це не лише технічне рішення, а частина комплексної стратегії безпеки, яка забезпечує:

- своєчасне виявлення атак;
- реагування на інциденти з урахуванням ризиків;
- скорочення часу між атакою та відповіддю;
- доказову базу для подальшого розслідування.

Для розслідування виявлених інцидентів інформаційної безпеки корпоративної мережі, враховуючи наведену модель загроз, використаємо метод Playbooks та forensic-аналіз.

Playbook — це структурований набір дій та сценаріїв реагування на конкретні типи інцидентів інформаційної безпеки. Playbooks застосовуються в рамках роботи Security Operations Center (SOC) та є основою для швидкого, уніфікованого і повторюваного реагування на кіберзагрози. У контексті відповіді на інцидент інформаційної безпеки, playbook забезпечує чітку послідовність кроків, які включають:

- класифікацію інциденту;
- збір артефактів;
- аналіз загроз;
- ескалацію при потребі;
- нейтралізацію атаки;
- відновлення;
- пост-інцидентний аналіз.

Forensic-аналіз (цифрова криміналістика) — це процес збору, збереження, аналізу та інтерпретації цифрових доказів, що мають відношення до інциденту інформаційної безпеки. Мета forensic-аналізу полягає в ідентифікації природи атаки, визначенні її наслідків, джерела та шляху проникнення, а також в отриманні доказів, які можуть бути використані в юридичному процесі.

Основні етапи цифрової криміналістики:

– Ідентифікація інциденту та підозрілих систем.
– Збір цифрових артефактів:
– Збереження цілісності доказів (chain of custody).
– Аналіз цифрових слідів:
– Формування звіту з висновками та доказами.

Поєднання методу playbooks та forensic-аналізу забезпечує як оперативне реагування, так і глибоке розслідування інцидентів. У той час як playbook регламентує послідовність дій, forensic-аналіз дозволяє:

– підтвердити або спростувати факт компрометації,
– виявити залишкові загрози,
– надати докази для кримінального переслідування або аудиту.

У рамках дослідження практичних аспектів реагування на інциденти інформаційної безпеки, було змодельовано реальний сценарій атаки типу SQL-ін’єкції на сервер бази даних корпоративного середовища. Інцидент проаналізовано відповідно до моделі загроз, із застосуванням методології цифрової криміналістики (forensics) та сценаріїв реагування (playbooks).

Опишемо випадок реального інциденту інформаційної безпеки з використанням Playbooks, forensic-аналізу та з урахуванням поданої моделі загроз (таблиця 1). Інформаційна система виявила потенційну загрозу після спрацювання сигнатурної системи виявлення вторгнень (IPS), яка зафіксувала SQL-запити з підозрілими параметрами. Запити були надіслані через веб-інтерфейс, що має прямий доступ до сервера бази даних. Первинний аналіз вказував на спробу SQL-ін’єкції з використанням типових шаблонів OR ‘1’=‘1’, яка загрожує серверу бази даних (актив №1). В даної загрози є висока ймовірність виникнення, рівень ризику критичний а наслідком є витік даних та втрата конфіденційності. Рекомендовано використовувати IPS з сигнатурним аналізом, сегментацію та списки контролю доступу ACL.

Опишемо кроки методу Playbook та представимо ц вигляді табл. 2.

Таблиця 2

Playbook: Реагування на SQL-ін’єкцію

Крок 1. Виявлення інциденту			
Джерело: Система IPS (наприклад, Snort) спрацювала за сигнатурою sql-injection-attempt	Місце спрацювання: DMZ-зона, веб-сервер 192.168.1.10.	Аномалія: HTTP-запит типу GET /product?id=1’ OR ‘1’=‘1’— викликає спрацювання сигнатури атаки на рівні веб-додатку.	
Крок 2. Класифікація та оцінка			
Тип інциденту: Використання SQL-ін’єкції	Потенційний ризик: Компрометація БД на 192.168.1.15	Пріоритет: Критичний	Вжиті автоматичні дії IPS: блокування IP-адреси зловмисника
Крок 3. Ізоляція та обмеження доступу			
Тимчасове обмеження запитів до веб-серверу.	Встановлення ACL на міжмережевому екрані для фільтрації трафіку	Аналіз живих з’єднань до БД — примусове завершення невідомих сесій.	

	з підозрілих підмереж.		
Крок 4. Ліквідація та відновлення			
Видалено зловмисний обліковий запис.	Відновлено структуру БД з останнього бекапу (24 години до атаки).	Посилено WAF з правилами на блокування ін'єкцій.	Застосовано оновлення CMS із патчем до вразливого параметра.
Крок 5. Пост-інцидентний звіт			
Ідентифікатор	INCIDENT-20250806-SQL01		
Тип атаки	SQL Injection		
Джерело атаки	91.203.45.182		
Ціль	Веб-сервер → Сервер БД		
Наслідки	Створення фальшивого користувача, витік клієнтів		
Рівень ризику	Критичний		

Аналогічно представимо Forensic-аналіз інциденту (табл. 3).

Таблиця 3

Forensic: Реагування на SQL-ін'єкцію

Кроки	Характеристики
1. Збір артефактів:	Логи веб-сервера (access.log, error.log) Логи БД (mysql.log) PCAP-запис мережевого трафіку за останні 12 годин Знімок файлової системи для аналізу змін
2. Аналіз веб-логів:	Виявлено серію запитів із payload на кшталт: sql Копировать Редактировать ‘ OR 1=1-- ‘ UNION SELECT ... Запити з IP: 91.203.45.182, 91.203.45.183
3. Аналіз трафіку:	POST-запити до /search.php SQL-результати повертались у відповіді HTTP 200 — потенційний витік даних клієнтів.
4. Аналіз бази даних:	Зіставлення хешів таблиць і дампу — виявлено змінену структуру таблиці users. Додано новий обліковий запис із правами адміністратора (user_hack, role=admin).

Отже, для оперативного реагування було застосовано попередньо визначений playbook, який передбачав такі кроки:

- Класифікація події як критичної (висока ймовірність + високі наслідки).
- Ізоляція джерела загрози шляхом блокування IP-адреси.
- Збір артефактів: журнали веб-сервера, дампи трафіку та даних БД.
- Forensic аналіз:
- Виявлено факт несанкціонованого доступу до таблиці users.
- Встановлено, що зловмисник створив нового адміністративного користувача.
- Ліквідація наслідків — видалення зловмисних облікових записів, відновлення БД з резервної копії.
- Післяінцидентна звітність — створення звіту, оновлення playbook, ревізія сигнатур IPS.

Даний випадок демонструє важливість поєднання технологічних засобів (IDS/IPS, SIEM) із формалізованими методиками (playbooks, forensic analysis). Інцидент також підкреслює необхідність регулярного оновлення сигнатур, застосування засобів

сегментації, а також навчання персоналу із безпеки веб-додатків.

Використання плейбуків (Playbooks) та інструментів цифрової криміналістики (forensic-аналізу) дозволяє формалізувати та автоматизувати процес реагування на інциденти. Це особливо важливо в умовах, коли швидкість та узгодженість дій є вирішальними для зменшення впливу загроз.

Після виявлення загрози за допомогою IDS/IPS:

- Playbook активується автоматично або вручну оператором SOC.
- Forensic дозволяє встановити ланцюг подій (від джерела атаки до її наслідків).
- Звіти інтегруються до системи ризик-менеджменту, оновлюється база ризиків.
- На основі отриманих результатів актуалізуються політики безпеки.

Однак ефективність таких дій можлива лише за умови їх інтеграції в загальну систему управління інформаційною безпекою, яка регламентується стандартом ISO/IEC 27001. Цей міжнародний стандарт визначає вимоги до побудови, впровадження, підтримання та постійного вдосконалення системи менеджменту інформаційної безпеки (СМІБ).

Ключові пункти взаємозв’язку:

Playbook повинні розроблятись на основі політик та процедур, закладених у СМІБ. Вони конкретизують, що саме робити при певному типі інциденту, відповідно до контексту ризику.

Forensic-аналіз виконує роль інструмента для збереження доказової бази, що є обов’язковою частиною розслідування інцидентів згідно з вимогами ISO/IEC 27035 (супутній стандарт до ISO/IEC 27001).

Оцінка ризиків (Risk Assessment), що є фундаментом ISO/IEC 27001, визначає пріоритети для створення плейбуків: для яких активів і загроз створювати сценарії реагування в першу чергу.

Політики інформаційної безпеки, згідно з ISO/IEC 27002, зобов’язують організацію:

- забезпечити реєстрацію інцидентів;
- розслідувати події;
- зберігати логи;
- вживати заходів для попередження повторень.

Такий підхід забезпечує не лише технічну, а й організаційну зрілість системи реагування.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Результати проведеного дослідження засвідчили, що ефективне забезпечення кібербезпеки корпоративної мережі можливе лише за умов впровадження інтегрованого підходу, що поєднує технічні, організаційні та управлінські аспекти. Системи виявлення вторгнень (IDS/IPS), у поєднанні з централізованими платформами обробки подій (SIEM), playbooks для сценарного реагування та інструментами цифрової криміналістики, дозволяють формувати багаторівневу оборону, здатну виявляти та нейтралізовувати широкий спектр загроз — від стандартних мережевих атак до складних цільових вторгнень.

Особливо важливо, що реагування на інциденти в межах такого підходу не здійснюється ізольовано, а базується на попередньо визначених політиках інформаційної безпеки, результатах оцінки ризиків і принципах стандарту ISO/IEC 27001. Це дозволяє організаціям реагувати на загрози з урахуванням бізнес-контексту, критичності активів і потенційного впливу на безперервність діяльності. Такий підхід також сприяє досягненню високого рівня узгодженості між технічними діями фахівців з безпеки та стратегічними цілями IT-менеджменту, що позитивно впливає на загальну інформаційну зрілість організації.

Інтегрований підхід демонструє адаптивність до змін у мережевій інфраструктурі та загрозовому середовищі, дозволяє масштабувати систему безпеки відповідно до зростання бізнесу, а також знижує ймовірність людських помилок за рахунок стандартизованих процедур реагування. Він формує передумови для побудови повноцінної системи кіберстійкості, яка базується на принципі безперервного вдосконалення згідно з циклом PDCA (Plan–Do–Check–Act).

У межах подальших досліджень перспективним є напрям автоматизації реагування з використанням технологій штучного інтелекту та SOAR-платформ, а також побудова адаптивних моделей виявлення загроз на основі поведінкового аналізу. Важливо також дослідити можливості інтеграції IDS/IPS у концепцію Zero Trust, оцінити економічну ефективність впроваджених рішень та розробити стандартизовані підходи до навчання персоналу через моделювання сценаріїв інцидентів у кіберлабораторіях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Damasevicius, R., Venckauskas, A., Grigaliunas, S., Toldinas, J., Morkevicius, N., Aleliunas, T., & Smuikys, P. (2020). LITNET-2020: An annotated real-world network flow dataset for network intrusion detection. *Electronics, 9*(5), 800. https://doi.org/10.3390/electronics9050800
2. Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *Journal of Big Data, 7*(1). https://doi.org/10.1186/s40537-020-00346-6
3. Osanaiye, O., Cai, H., Choo, K.-K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking, 2016*(1), 1–10. https://doi.org/10.1186/s13638-016-0623-3
4. Shushura, O. M., Asieieva, L. A., Nedashkivskiy, O. L., Havrylko, Y. V., Moroz, Y. O., Smailova, S. S., & Sarsembayev, M. (2022). Simulation of information security risks of availability of project documents based on fuzzy logic. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 12*(3), 64–68. https://doi.org/10.35784/iapgos.3033
5. Zavada, A. A., Samchyshyn, O. V., & Ohrimchuk, V. V. (2012). Analysis of modern attack detection and intrusion prevention systems. *Information Systems. Collection of Scientific Papers of ZhVINAU, 6*(12), 97–106.
6. Kukharska, N. P., Semenuk, S. A., & Polotai, O. I. (2025). Key aspects of the updated standard ISO/IEC 27002:2022. *Modern Information Protection, 2,* 76–87.
7. Lukyanenko, T. Yu., Ponochovny, P. M., & Legominova, S. V. (2022). Methodology for detecting network intrusions and signs of computer attacks based on an empirical approach. *Modern Information Protection, 2*(50), 15–21.
8. Polotai, O. I. (2023). Using computer forensics to ensure effective investigation of information and cybersecurity incidents. *Bulletin of the LDUBZHD, 28,* 73–80.
9. Tolyupa, S., Plyushch, O. G., & Parkhomenko, I. I. (2020). Building attack detection systems in information networks based on neural network structures. *Cybersecurity: Education, Science, Technology, 2*(10), 169–181.
10. Chichkarev, E., Zinchenko, O., Bondarchuk, A., & Aseeva, L. (2023). Feature selection method for intrusion detection system using ensemble approach and fuzzy logic. *Cybersecurity: Education, Science, Technology, 1*(21), 234–251.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

O. Polotai
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID: 0000-0003-4593-8601
orest.polotaj@gmail.com

T. Brych
Candidate of Technical Sciences,
Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID: 0000-0001-6853-1981
taras_brych@hotmail.com

N. Kukharska
Candidate of Physical and Mathematical Sciences,
Associate Professor, Associate Professor of the Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-0896-8361
kukharska.n@gmail.com

V. Yashchuk
Candidate of Economic Sciences, Associate Professor,
Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID: 0000-0003-2651-4918
valentina.lender@gmail.com

A. Tkachenko
Lecturer of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID: 0009-0009-6830-4741
tkachenko.am14@gmail.com

INTEGRATION OF INTRUSION DETECTION SYSTEMS INTO THE CORPORATE NETWORK STRUCTURE: APPROACHES, CHALLENGES AND EFFICIENCY OF INCIDENT RESPONSE

Abstract. The article presents a comprehensive study of the integration of intrusion detection systems (IDS/IPS) into the structure of a corporate network, taking into account the requirements of modern cybersecurity, current risks and management approaches in accordance with international standards. The current challenges associated with the growth of the complexity of network infrastructures, the development of targeted attacks and increased requirements for the speed of response to information security incidents are considered. A systematic approach is proposed, which involves the phased implementation of IDS/IPS solutions based on a preliminary analysis of the network architecture, asset classification, vulnerability detection and risk assessment. A corporate network threat model is built, which covers the main types of assets (servers, workstations, routers, access points, authentication services) and typical attack vectors (SQL injections, DDoS, phishing, brute force, malware, etc.). Special attention was paid to the implementation of response processes in accordance with the requirements of the ISO/IEC 27001:2017 standard. The study simulated an information security incident in the form of an SQL injection attack on a corporate network web application. The incident was detected using a signature-based NIDS, after which a specialized Playbook was activated, which provided for automated actions to localize the threat, disable suspicious traffic, log events, and inform personnel. Additionally, a forensic analysis was conducted, which allowed reconstructing the attack chronology, identifying weaknesses in the web server configuration, and generating an analytical report for further updating security policies. All actions were consistent with pre-established procedures within the information security management system (ISMS), which confirms the practical applicability and effectiveness of the risk-based approach. The

article also proposes an algorithm for integrating IDS/IPS into a corporate network, which includes analyzing the existing architecture, selecting the type of system, configuring threat detection rules, integrating with SIEM systems, and organizing personnel training. It is substantiated that integrating technical protection with management policies and response mechanisms allows for a higher level of adaptability, reducing the time between detection and response, and providing an evidentiary base for further investigations. The conclusions emphasize the advantages of an integrated approach to cyber protection, in particular its ability to scale, adapt to new threats, and contribute to continuous improvement of information security. Directions for future research are proposed, including automation of response using artificial intelligence, implementation of Zero Trust concepts, development of behavioral models of threat analysis, and construction of training cyber polygons to test the effectiveness of playbooks.

Keywords: information security; cyber threats; intrusion detection systems; corporate network; incident response; digital forensics; forensic analysis; playbook; SIEM; SQL injection; risk assessment.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Damasevicius, R., Venckauskas, A., Grigaliunas, S., Toldinas, J., Morkevicius, N., Aleliunas, T., & Smuikys, P. (2020). LITNET-2020: An annotated real-world network flow dataset for network intrusion detection. *Electronics, 9*(5), 800. https://doi.org/10.3390/electronics9050800
2. Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *Journal of Big Data, 7*(1). https://doi.org/10.1186/s40537-020-00346-6
3. Osanaiye, O., Cai, H., Choo, K.-K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking, 2016*(1), 1–10. https://doi.org/10.1186/s13638-016-0623-3
4. Shushura, O. M., Asieieva, L. A., Nedashkivskiy, O. L., Havrylko, Y. V., Moroz, Y. O., Smailova, S. S., & Sarsembayev, M. (2022). Simulation of information security risks of availability of project documents based on fuzzy logic. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 12*(3), 64–68. https://doi.org/10.35784/iapgos.3033
5. Zavada, A. A., Samchyshyn, O. V., & Ohrimchuk, V. V. (2012). Analysis of modern attack detection and intrusion prevention systems. *Information Systems. Collection of Scientific Papers of ZhVINAU, 6*(12), 97–106.
6. Kukharska, N. P., Semenuk, S. A., & Polotai, O. I. (2025). Key aspects of the updated standard ISO/IEC 27002:2022. *Modern Information Protection, 2,* 76–87.
7. Lukyanenko, T. Yu., Ponochovny, P. M., & Legominova, S. V. (2022). Methodology for detecting network intrusions and signs of computer attacks based on an empirical approach. *Modern Information Protection, 2*(50), 15–21.
8. Polotai, O. I. (2023). Using computer forensics to ensure effective investigation of information and cybersecurity incidents. *Bulletin of the LDUBZHD, 28,* 73–80.
9. Tolyupa, S., Plyushch, O. G., & Parkhomenko, I. I. (2020). Building attack detection systems in information networks based on neural network structures. *Cybersecurity: Education, Science, Technology, 2*(10), 169–181.
10. Chichkarev, E., Zinchenko, O., Bondarchuk, A., & Aseeva, L. (2023). Feature selection method for intrusion detection system using ensemble approach and fuzzy logic. *Cybersecurity: Education, Science, Technology, 1*(21), 234–251.