УДК 004.056:004.738.5
DOI https://doi.org/10.32782/IT/2023-1-11

Вадим МЄШКОВ
аспірант кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005, mieshkov.v.i@nmu.one
***ORCID:** 0000-0001-9873-4712*

Бібліографічний опис статті: Мєшков, В. (2023). Аналіз систем інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 1, 85–92, doi: https://doi.org/10.32782/IT/2023-1-11

АНАЛІЗ СИСТЕМ ІНТЕЛЕКТУАЛЬНОГО МОНІТОРИНГУ ТРАФІКУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ АТАК

У статті розглянуто інформаційну технологію інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. В статті здійснено огляд сучасних систем моніторингу трафіку, виявлення аномалій та розпізнавання атак різного типу. Проаналізовано застосування машинного навчання для аналізу трафіку і розвиток сучасних алгоритмів.

Розглянуто класифікацію систем виявлення атак за основними параметрами та можливостями аналізу трафіку, а також наведено таблицю порівняння різних типів систем виявлення атак з указівкою їх переваг та недоліків.

Досліджено можливі мережеві загрози, які можна виявити за допомогою інтелектуального моніторингу трафіку комп'ютерної мережі, а також визначено перспективи застосування інтелектуального моніторингу для покращення систем виявлення атак.

***Ключові слова:** інтелектуальний моніторинг, мережевий трафік, система виявлення атак, кібербезпека, машинне навчання, аналіз трафіку, аномалії трафіку, класифікація систем виявлення атак, мережеві загрози.*

Vadym MIESHKOV
Postgraduate Student at the Department of Information Security and Telecommunications, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, mieshkov.v.i@nmu.one
***ORCID:** 0000-0001-9873-4712*

To cite this article: Mieshkov, V. (2023). Analiz system intelektualnoho monitorynhu trafiku komp'iuternoi merezhi dlia system vyiavlennia atak [Analysis of Intelligent Computer Network Traffic Monitoring Systems for Intrusion Detection Systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 1, 85–92, doi: https://doi.org/10.32782/IT/2023-1-11

ANALYSIS OF INTELLIGENT COMPUTER NETWORK TRAFFIC MONITORING SYSTEMS FOR INTRUSION DETECTION SYSTEMS

The article deals with the information technology of intelligent monitoring of computer network traffic for intrusion detection systems. The article provides an overview of modern systems for traffic monitoring, anomaly detection, and attack detection of various types. The use of machine learning for traffic analysis and the development of modern algorithms are analyzed.

The classification of intrusion detection systems by the main parameters and capabilities of traffic analysis is considered, and a table comparing different types of intrusion detection systems with their advantages and disadvantages is presented.

The possible network threats that can be detected by intelligent monitoring of computer network traffic are investigated, and the prospects for using intelligent monitoring to improve attack detection systems are determined.

***Key words:** intelligent monitoring, network traffic, intrusion detection system, cybersecurity, machine learning, traffic analysis, traffic anomalies, intrusion detection system classification, network threats.*

Вступ. Комп'ютерні мережі відіграють важливу роль в сучасному світі, оскільки вони стали основою комунікації, бізнесу та особистих взаємин. Через це, захист комп'ютерних мереж від різноманітних загроз та атак стає все більш актуальним завданням.

Сучасні системи моніторингу трафіку мають на меті аналізувати трафік, що передається через мережі, для виявлення аномалій та розпізнавання можливих атак різного типу. Відповідно до різних сценаріїв, ці системи можуть ідентифікувати атаки, засновані на відомих сигнатурах, а також виявляти нові атаки, що базуються на аномальній поведінці трафіку.

Останнім часом, застосування машинного навчання та інтелектуальних методів аналізу даних стало ключовим інструментом для покращення ефективності систем моніторингу трафіку. Використання алгоритмів машинного навчання дозволяє автоматично адаптуватись до змін у поведінці мережі, визначати нові шаблони атак та надавати більш точні результати виявлення аномалій.

У статті розглянуто сучасні підходи до моніторингу трафіку комп'ютерних мереж, методи виявлення аномалій та розпізнавання атак, а також роль машинного навчання у підвищенні ефективності таких систем.

Літературний огляд. Протягом останніх років багато авторів працювали над різними аспектами аналізу мережевого трафіку та розпізнавання атак.

Автор Vern Paxson «Bro: A System for Detecting Network Intruders in Real-Time» (Vern Paxson, 1998) описує систему виявлення вторгнень в мережі, засновану на аналізі мережевого трафіку в режимі реального часу. Система, названа Bro, розроблена для виявлення атак та аномальних поведінок, що можуть свідчити про спробу вторгнення. Основною ідеєю Bro є використання моделей поведінки користувачів та служб для виявлення зловмисників на основі збігів та відхилень від норми. Bro аналізує різні аспекти мережевого трафіку, такі як пакети даних, з'єднання та сесії, та застосовує набір правил для визначення аномальних активностей та спроб вторгнень.

Автор зосереджується на декількох ключових аспектах системи Bro, таких як: модульна архітектура системи, використання мови опису політики безпеки, процес виявлення аномалій та вторгнень в режимі реального часу, журналювання та оповіщення адміністраторів мережі, розширення та інтеграція з іншими системами безпеки та моніторингу, адаптація до нових загроз.

Автор також наводить результати експериментів, проведених з використанням системи Bro, які показують, що система здатна виявляти різноманітні атаки, такі як сканування портів, атаки на служби та спроби вторгнень у системи.

Автор Dr. Alina Oprea «Detection of Early-Stage Enterprise Infection by Mining Large-Scale Log Data» (Dr. Alina Oprea, 2015) розглядає підхід до виявлення ранньої стадії інфекції корпоративних систем шляхом аналізу великомасштабних даних журналів. У роботі розроблена методологія, яка використовує аналіз мережевих та системних журналів для виявлення аномальної поведінки та підозрілих активностей, які можуть свідчити про початкову стадію інфекції.

Ключові аспекти статті включають: автори пропонують використовувати вже існуючі дані журналів, які збираються корпоративними системами, для аналізу поведінки користувачів та виявлення аномалій. Методологія розроблена з урахуванням масштабованості та ефективності, що дозволяє аналізувати великі обсяги даних журналів, зібраних з різних джерел. Застосовуючи різноманітні алгоритми машинного навчання та статистичний аналіз, автори ідентифікують аномалії та підозрілі активності в даних журналів, які можуть вказувати на ранню стадію інфекції. В своїй роботі автори наводять результати експериментів, проведених на реальних корпоративних даних, що підтверджують ефективність пропонованої методології в виявленні ранніх стадій інфекцій.

Автори Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A., 2018) – «Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection» розглядають новий підхід до виявлення вторгнень у мережі в режимі реального часу з використанням ансамблю автоенкодерів, які є моделями машинного навчання без вчителя.

Kitsune NIDS, який є Plug and Play системою на основі нейронних мереж для ефективного виявлення аномальних шаблонів мережевого трафіку. Він моніторить статистичні моделі трафіку та виявляє аномалії через ансамбль автокодерів. Кожен автокодер відповідає за виявлення аномалії, пов'язані з певним аспектом поведінки мережі. В роботі описані компоненти структури Kitsune, такі як захоплювач пакетів, парсер пакетів, екстрактор функцій та детектор аномалій, а також їх режими роботи. Kitsune розроблений для роботи в простій мережі маршрутизаторів та має низьку обчислювальну складність.

Автори Ida Seraphim, Shreya Palit, Kaustubh Srivastava, Poovammal Eswaran. «A Survey on Machine Learning Techniques in Network Intrusion Detection System» (Ida Seraphim, Shreya Palit, Kaustubh Srivastava, Poovammal Eswaran, 2018).

У своїй роботі автори представляють огляд методів машинного навчання, які застосовуються в системах виявлення атак у мережі (NIDS). Автори починають із короткого введення

в NIDS та їх необхідність для забезпечення безпеки в мережі. Вони розглядають різні алгоритми машинного навчання, які використовуються для виявлення аномалій та класифікації атак. Огляд включає методи навчання з учителем, навчання без учителя та напівнаглядованого навчання. Розглядаються алгоритми, такі як дерева рішень, опорні вектори, нейронні мережі, k-найближчих сусідів, наївний класифікатор Байєса та кластеризацію, і пояснює, як вони застосовуються для вирішення проблем NIDS. Автори також обговорюють виклики, пов'язані з використанням машинного навчання в NIDS, такі як вибір оптимальних алгоритмів та балансування точності та швидкості виявлення. Ця стаття надає корисний огляд та аналіз алгоритмів машинного навчання, які застосовуються в системах виявлення атак у мережі. Вона може бути корисною для дослідників, які прагнуть зрозуміти та впровадити різні методи машинного навчання для підвищення безпеки мережі.

Основна частина. Інформаційна технологія інтелектуального моніторингу трафіку (ІТІМТ) комп'ютерної мережі (КМ) для систем виявлення атак (СВА) дозволяє виявити різноманітні мережеві загрози, що включають: DoS (Denial of Service) та DDoS (Distributed Denial of Service) атаки, віруси, троянські коні та черв'яки, атаки на віддалене виконання коду, атаки на аутентифікацію та авторизацію, міжсайтовий скриптінг (XSS) та атаки SQL-ін'єкцій, прослуховування та перехоплення мережевого трафіку, атаки на бездротові мережі, внутрішній загрози, паралельні атаки (APT – Advanced Persistent Threats).

Застосування інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак, що базуються на методах машинного навчання та штучного інтелекту, може значно підвищити ефективність виявлення та реагування на різноманітні мережеві загрози. Оскільки кіберзлочинці постійно розвивають нові стратегії та використовують нові вектори атак, важливо застосовувати передові технології для захисту мережевої інфраструктури.

СВА, які використовують ІТІМТ, можуть автоматично виявляти та реагувати на загрози безпеці мережі, наприклад, вони можуть зупиняти або блокувати доступ до комп'ютерних ресурсів або генерувати попередження для адміністраторів мережі. Такі СВА є важливою складовою забезпечення безпеки мережі, оскільки дозволяють реагувати на потенційні загрози до її безпеки та зменшити ризик від вразливостей та атак.

ІТІМТ КМ для СВА може використовуватися в різних галузях, де потрібна безпека мережі. Наприклад, вона може бути застосована в корпоративних мережах, мережах телекомунікацій, системах керування промисловими процесами та інших галузях.

Однією з головних переваг ІТІМТ є можливість виявлення нових та раніше невідомих загроз безпеці мережі. Такі загрози можуть бути виявлені за допомогою аналізу незвичайного або нетипового мережевого трафіку.

Крім того, СВА, які використовують ІТІМТ, можуть бути налаштовані для роботи в реальному часі, що дозволяє оперативно реагувати на потенційні загрози та швидко вживати заходів для їх усунення.

Варто зазначити, що такі СВА можуть також викликати помилкові спрацювання, тому важливо налагоджувати їх належним чином та регулярно оновлювати їх алгоритми.

Узагалі, ІТІМТ КМ для СВА є важливою складовою заходів забезпечення безпеки мережі, яка допомагає захистити комп'ютерну мережу від шкідливих дій та атак.

Розробка ІТІМТ КМ для СВА є міждисциплінарним завданням, яке потребує знань з різних галузей, таких як інформаційні технології, кібербезпека, математика, статистика та інші.

У зв'язку з цим, вчені, які займаються розробкою ІТІМТ КМ для СВА, можуть мати різні фахові профілі. Деякі з них включають: вчені з області кібербезпеки, які вивчають різні типи кібератак та розробляють заходи для їх запобігання та виявлення; спеціалісти з мережевих технологій, які вивчають протоколи мережі та розробляють методи для аналізу мережевого трафіку; математики та статистики, які розробляють методи для аналізу даних, статистичного моделювання та машинного навчання для виявлення шаблонів та аномалій в мережевому трафіку; інженери з програмного забезпечення, які розробляють програмне забезпечення для моніторингу та аналізу мережевого трафіку; експерти з баз даних, які розробляють системи зберігання та обробки великих обсягів даних, які використовуються в системах виявлення атак; експерти з інтерфейсу користувача, які розробляють інтерфейси користувача для систем виявлення атак, що дозволяють адміністраторам мережі відстежувати та аналізувати мережевий трафік.

Ці спеціалісти часто співпрацюють між собою, щоб створити інтегровану систему виявлення атак, яка може ефективно виявляти шкідливу активність в комп'ютерній мережі та захищати її від потенційних загроз.

Деякі зі спеціалістів у цій галузі ведуть дослідження в університетах та наукових інститутах. Вони розробляють нові методи та алгоритми для виявлення атак та розробляють нові програмні засоби для моніторингу трафіку мережі. Деякі з них можуть працювати у відділах досліджень та розробок у технологічних компаніях, що спеціалізуються на кібербезпеці та розробці програмного забезпечення.

Оскільки кібербезпека є швидко розвиваючою сферою, вчені з цієї галузі повинні постійно вдосконалювати свої знання та навички, щоб відповідати на нові виклики та загрози в цій області. Також вони повинні бути знайомі зі стандартами та нормами з кібербезпеки, які розробляються різними урядовими органами та міжнародними організаціями.

Процес моніторингу мережевого трафіку у СВА – це складний процес, що передбачає збір, аналіз та інтерпретацію великої кількості даних, що надходять з мережі.

Основні етапи процесу моніторингу мережевого трафіку у СВА (рис.1):

1. Збір даних: на першому етапі система збирає дані про трафік, що надходить на мережу. Для збору даних можуть використовуватися різні засоби, наприклад, сенсори, вузли збору даних, проксі-сервери та інші.

2. Фільтрація трафіку: після збору даних, вони проходять через фільтр, який виключає непотрібний трафік (наприклад, трафік, що створюється системними процесами). Фільтрація може здійснюватися за допомогою різних параметрів, таких як порти, IP-адреси, протоколи та інші.

3. Аналіз трафіку: після фільтрації дані аналізуються для виявлення вразливостей та атак на мережу. Аналіз може включати в себе різні методи, такі як статистичний аналіз, аналіз змісту пакетів, виявлення змін у звичайному поведінці трафіку та інші.

4. Виявлення вразливостей та атак: після аналізу, система виявляє потенційні вразливості та атаки на мережу. Виявлені вразливості та атаки можуть бути класифіковані згідно з їх типом та рівнем небезпеки. Наприклад, система може виявити SQL-ін’єкцію або DDoS-атаку.

5. Попередження про вразливості та атаки: після виявлення потенційних вразливостей і атак на мережу, система повинна забезпечувати моніторинг та сповіщення про ці події. Попередження можуть бути реалізовані за допомогою різних методів, таких як електронні листи, SMS-повідомлення, показ повідомлень у спеціальному додатку та інші.

6. Реагування на вразливості та атаки: після виявлення вразливостей та атак на мережу, система повинна забезпечувати можливість реагування на ці події. Наприклад, система може автоматично заблокувати IP-адресу, з якої здійснюється атака, або надіслати повідомлення до відповідальної людини, яка вживе необхідні заходи щодо усунення вразливостей.

7. Аудит та звітність: після реагування на вразливості та атаки, система повинна забезпечувати аудит та звітність про ці події. Це дозволяє зберігати інформацію про події та використовувати її для аналізу та вдосконалення системи виявлення атак.

Узагальнюючи, процес моніторингу мережевого трафіку у системі виявлення атак включає в себе збір, фільтрацію, аналіз, виявлення, попередження, реагування та аудит даних. Кожен з цих етапів важливий для забезпечення безпеки мережі та захисту від потенційних загроз.

Існує багато програм для інтелектуального моніторингу мережевого трафіку в комп’ютерній

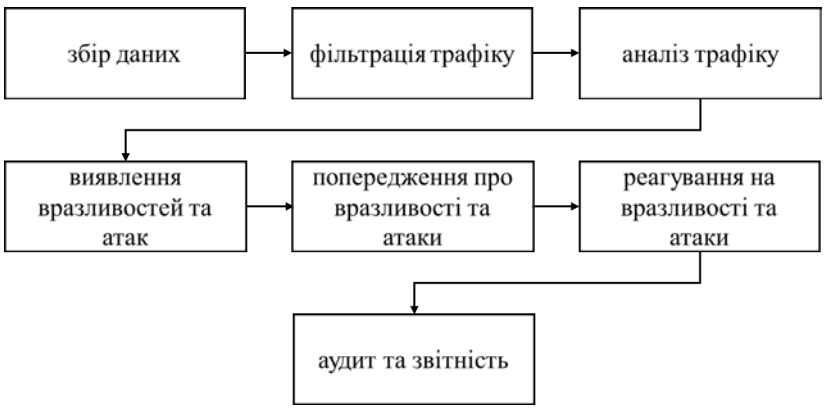

Рис. 1. Алгоритм аналізу мережевого трафіку та виявлення вразливостей/атак

мережі: Wireshark, Nagios, PRTG Network Monitor, SolarWinds Network Performance Monitor, Microsoft Network Monitor. Ці програми можуть допомогти в моніторингу мережі та виявленні проблем в мережевому трафіку.

СВА може аналізувати різні параметри мережевого трафіку залежно від типу сенсора та налаштувань. Деякі з найбільш поширених параметрів, що можуть бути аналізовані СВА, включають:

− IP-адресу відправника та отримувача пакетів. IP-адреса відправника та отримувача пакетів можуть бути аналізовані СВА для виявлення джерела атак або небезпек у мережі, а також для ідентифікації мережевих пристроїв, які залучені до атаки.

− порти відправника та отримувача пакетів. Аналіз портів може допомогти СВА визначити, які протоколи використовуються в пакетах, що може допомогти виявити атаки на конкретні служби або протоколи.

− протоколи, що використовуються в пакетах, наприклад TCP, UDP, ICMP тощо. Протоколи, що використовуються в пакетах, можуть бути аналізовані СВА для виявлення аномалій або шаблонів поведінки в мережі.

− розмір пакетів та їх фрагментація. Розмір пакетів та їх фрагментація можуть бути аналізовані СВА для виявлення атак, які використовують пакети незвичайних розмірів або фрагментовані пакети.

− структуру та заголовки пакетів, такі як заголовок Ethernet, заголовок IP, заголовок TCP/UDP/ICMP тощо. Заголовки та структура пакетів можуть бути аналізовані СВА для виявлення аномалій у протоколах мережі, включаючи відповідність заголовків та контрольні суми.

− заголовки та тіло повідомлень у різних протоколах, наприклад HTTP, DNS, FTP тощо. Аналіз повідомлень у різних протоколах може допомогти СВА виявити шкідливі відповіді від серверів, використання зловмисного коду у тілах повідомлень або небезпечні параметри запитів.

− шаблони, що вказують на конкретні типи атак, такі як відомі значення даних пакетів або шаблони поведінки в мережі. Використання шаблонів даних пакетів або поведінки в мережі може допомогти СВА виявляти відомі типи атак, такі як DDoS або SQL-ін'єкції, а також визначати нові атаки на основі виявлених шаблонів.

Ці параметри можуть бути використані СВА для виявлення аномалій, порівняння з відомими шаблонами атак, використання методів машинного навчання тощо.

СВА можна класифікувати за різними критеріями, наприклад за місцем встановлення, способом аналізу даних та метою використання. Розглянемо декілька загальних категорій, в які можна поділити СВА:

− за місцем встановлення: системи виявлення мережевих вторгнень (NIDS) – аналізують мережевий трафік на рівні мережевого протоколу; системи виявлення хост-вторгнень (HIDS) – аналізують активність на окремому комп'ютері або сервері, зокрема встановлені програми, файли, реєстрацію подій тощо.

− за способом аналізу даних: системи виявлення аномальної поведінки (англ. anomaly-based IDS) – аналізують активність на основі попередньо визначених параметрів та порівнюють їх з нормальною поведінкою; системи виявлення відомих вторгнень (англ. signature-based IDS) – аналізують активність на основі заздалегідь побудованих правил, які вказують на конкретні зразки відомих вторгнень.

− за метою використання: системи, що використовуються для виявлення атак (англ. intrusion detection systems, IDS) – зазвичай зосереджені на зборі та аналізі даних про можливі вторгнення; системи, що використовуються для запобігання атак (англ. intrusion prevention systems, IPS) – крім збору та аналізу даних, можуть приймати активні заходи для запобігання вторгненням.

− за способом реагування на вторгнення: системи, що дозволяють виявляти атаки та повідомляти про них (англ. passive IDS) – не втручаються у роботу системи, а лише сповіщають про можливе вторгнення; системи, що можуть виявляти атаки та приймати активні заходи для їх запобігання (англ. active IDS) – можуть втручатися у роботу системи, наприклад, блокувати підозрілі мережеві з'єднання або процеси.

− за обсягом зберігання даних: системи зберігання даних локально (англ. on-premise IDS) – зберігають та оброблюють дані на місці встановлення системи; системи зберігання даних у хмарі (англ. cloud-based IDS) – зберігають та оброблюють дані у хмарних сервісах, що дозволяє отримувати доступ до даних з різних місць та знижувати вартість обслуговування.

− за типом вторгнень, які вони виявляють: системи виявлення спроб вторгнення з зовнішньої мережі (англ. external IDS) – спрямовані на виявлення вторгнень з зовнішніх джерел, наприклад, з Інтернету; системи виявлення внутрішніх вторгнень (англ. internal IDS) – спрямовані на виявлення вторгнень з внутрішньої мережі, наприклад, зі сторони співробітників.

Ці класифікації можуть перетинатися та доповнюватися іншими категоріями, що залежать від конкретних потреб та вимог користувачів.

Таблиця 1

Аналіз різних типів СВА

Тип СВА	Опис сенсора СВА	Переваги	Недоліки
СВА на основі моніторингу протоколів мережі	Сенсор протоколів аналізує протоколи мережі та метадані, такі як IP-адреси, порти та часові мітки, для виявлення аномальної активності та атак.	Швидкість та масштабованість	Обмежений аналіз змісту пакетів
СВА на основі аналізу вмісту пакетів	Сенсор вмісту пакетів аналізує дані в мережевих пакетах, включаючи заголовки та корисне навантаження, для виявлення відомих підписів атак та аномалій.	Точне виявлення відомих атак	Високі вимоги до ресурсів, можливі помилкові спрацьовування
СВА на основі аналізу вмісту файлів	Сенсор вмісту файлів аналізує вміст файлів, що передаються через мережу, для виявлення зловмисних файлів, вірусів та іншої шкідливої програми.	Виявлення шкідливого програмного забезпечення	Обмежена швидкість та масштабованість
СВА на основі аналізу журналів	Сенсор журналів збирає та аналізує журнали подій системи та застосунків, такі як аудит безпеки, журнали доступу та журнали помилок, для виявлення аномальної активності та атак.	Аналіз багатьох джерел даних	Високі вимоги до ресурсів, можливі помилкові спрацьовування
СВА на основі аналізу поведінки системи	Сенсор поведінки аналізує поведінку системи, процесів та користувачів для виявлення аномальних відхилень, які можуть свідчити про атаки. Зазвичай використовують машинне навчання для розпізнавання патернів поведінки.	Виявлення нових та невідомих атак	Високі вимоги до ресурсів, можливі помилкові спрацьовування
СВА на основі аналізу використання ресурсів	Сенсор використання ресурсів моніторить показники використання ресурсів, такі як використання процесора, пам'яті, дискового простору та мережевого трафіку, для виявлення аномалій та атак, пов'язаних з неналежним або несанкціонованим використанням ресурсів.	Адаптація до змінних умов мережі	Висока кількість помилкових спрацьовувань, обмеженість виявлення атак

Інтелектуальний моніторинг трафіку комп'ютерної мережі для систем виявлення атак має великий потенціал та перспективи для подальшого розвитку та вдосконалення. Основні перспективи включають: застосування розширеного машинного навчання та штучного інтелекту, проактивне виявлення атак, адаптивність та масштабованість, застосування в Інтернеті речей (IoT) та промислових контрольних системах, автоматизація відповіді на інциденти, кіберстійкість та обмін інформацією про загрози, розробка нових стандартів та підходів.

Висновок. У сучасному світі зростає значення кібербезпеки через збільшення кількості інформаційних активів та залежності організацій від інформаційних технологій. Відповідно, важливістю набуває розробка та впровадження ефективних систем виявлення атак, здатних відстежувати та аналізувати трафік комп'ютерної мережі для захисту від кіберзлочинів.

Огляд сучасних досліджень та тенденцій в галузі інтелектуального моніторингу трафіку комп'ютерної мережі демонструє активний розвиток технологій машинного навчання та штучного інтелекту, які можуть значно підвищити ефективність систем виявлення атак.

Аналіз мережевих загроз, які можна виявити за допомогою інформаційної технології інтелектуального моніторингу трафіку, вказує на можливість виявлення різноманітних атак, таких як DoS-атаки, віруси, троянці, шпигунське ПЗ та інші. Класифікація систем виявлення атак за основними параметрами та можливостями аналізу трафіку дозволяє вибрати оптимальний варіант для конкретної організації та її специфіки.

Перспективи застосування ІТІМТ КМ для СВА включають розвиток нових алгоритмів та технологій, підвищення швидкодії та точності виявлення, забезпечення приватності та захисту даних, розробку нових стандартів та підходів.

ЛІТЕРАТУРА:

1. Vern Paxson. "Bro: A System for Detecting Network Intruders in Real-Time." Proceedings of the 7th USENIX Security Symposium San Antonio, Texas, January 26-29, 1998. doi: 10.1016/S1389-1286(99)00112-7

2. Leyla Bilge, Engin Kirda, Christopher Kruegel, Marco Balduzzi. "EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis." Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, San Diego, California, USA, 6th February - 9th February 2011.

3. Alina Oprea, Zhou Li, Ting-Fang Yen, Sang Chin, Sumayah Alrwais. "Detection of Early-Stage Enterprise Infection by Mining Large-Scale Log Data." Conference: 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). doi: 10.1109/DSN.2015.14

4. Yisroel Mirsky, Tomer Doitshman, Yuval Elovici, Asaf Shabtai. "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection." Conference: Network and Distributed System Security Symposium. January 2018. doi: 10.14722/ndss.2018.23211

5. N. Šrndić and P. Laskov, "Practical Evasion of a Learning-Based Classifier: A Case Study," 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2014, pp. 197-211, doi: 10.1109/SP.2014.20.

6. Ida Seraphim, Shreya Palit, Kaustubh Srivastava, Poovammal Eswaran. A Survey on Machine Learning Techniques in Network Intrusion Detection System, Conference: 2018 4th International Conference on Computing Communication and Automation (ICCCA), doi: 10.1109/CCAA.2018.8777596.

7. G. Shang-fu and Z. Chun-lan, "Intrusion detection system based on classification," 2012 IEEE International Conference on Intelligent Control, Automatic Detection and High-End Equipment, Beijing, China, 2012, pp. 78-83, doi: 10.1109/ICADE.2012.6330103.

8. M. O. Miah, S. Shahriar Khan, S. Shatabda and D. M. Farid, "Improving Detection Accuracy for Imbalanced Network Intrusion Classification using Cluster-based Under-sampling with Random Forests," 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka, Bangladesh, 2019, pp. 1-5, doi: 10.1109/ICASERT.2019.8934495.

9. N. S. Bhati and M. Khari, "Comparative Analysis of Classification Based Intrusion Detection Techniques," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-6, doi: 10.1109/ISCON52037.2021.9702411.

10. G. Sah and S. Banerjee, "Feature Reduction and Classifications Techniques for Intrusion Detection System," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 1543-1547, doi: 10.1109/ICCSP48568.2020.9182216.

11. A. S. Subaira and P. Anitha, "Efficient classification mechanism for network intrusion detection system based on data mining techniques: A survey," 2014 IEEE 8th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2014, pp. 274-280, doi: 10.1109/ISCO.2014.7103959.

12. R. Samrin and D. Vasumathi, "Review on anomaly based network intrusion detection system," 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Mysuru, India, 2017, pp. 141-147, doi: 10.1109/ICEECCOT.2017.8284655.

13. Rushendra, K. Ramli, N. Hayati, E. Ihsanto, T. S. Gunawan and A. H. Halbouni, "Development of Intrusion Detection System using Residual Feedforward Neural Network Algorithm," 2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 2021, pp. 539-543, doi: 10.1109/ISRITI54043.2021.9702773.

REFERENCES:

1. Vern Paxson. "Bro: A System for Detecting Network Intruders in Real-Time." Proceedings of the 7th USENIX Security Symposium San Antonio, Texas, January 26-29, 1998. doi: 10.1016/S1389-1286(99)00112-7

2. Leyla Bilge, Engin Kirda, Christopher Kruegel, Marco Balduzzi. "EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis." Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, San Diego, California, USA, 6th February - 9th February 2011.

3. Alina Oprea, Zhou Li, Ting-Fang Yen, Sang Chin, Sumayah Alrwais. "Detection of Early-Stage Enterprise Infection by Mining Large-Scale Log Data." Conference: 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). doi: 10.1109/DSN.2015.14

4. Yisroel Mirsky, Tomer Doitshman, Yuval Elovici, Asaf Shabtai. "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection." Conference: Network and Distributed System Security Symposium. January 2018. doi: 10.14722/ndss.2018.23211

5. N. Šrndić and P. Laskov, "Practical Evasion of a Learning-Based Classifier: A Case Study," 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2014, pp. 197-211, doi: 10.1109/SP.2014.20.

6. Ida Seraphim, Shreya Palit, Kaustubh Srivastava, Poovammal Eswaran. A Survey on Machine Learning Techniques in Network Intrusion Detection System, Conference: 2018 4th International Conference on Computing Communication and Automation (ICCCA), doi: 10.1109/CCAA.2018.8777596.

7. G. Shang-fu and Z. Chun-lan, "Intrusion detection system based on classification," 2012 IEEE International Conference on Intelligent Control, Automatic Detection and High-End Equipment, Beijing, China, 2012, pp. 78-83, doi: 10.1109/ICADE.2012.6330103.

8. M. O. Miah, S. Shahriar Khan, S. Shatabda and D. M. Farid, "Improving Detection Accuracy for Imbalanced Network Intrusion Classification using Cluster-based Under-sampling with Random Forests," 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka, Bangladesh, 2019, pp. 1-5, doi: 10.1109/ICASERT.2019.8934495.

9. N. S. Bhati and M. Khari, "Comparative Analysis of Classification Based Intrusion Detection Techniques," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-6, doi: 10.1109/ISCON52037.2021.9702411.

10. G. Sah and S. Banerjee, "Feature Reduction and Classifications Techniques for Intrusion Detection System," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 1543-1547, doi: 10.1109/ICCSP48568.2020.9182216.

11. A. S. Subaira and P. Anitha, "Efficient classification mechanism for network intrusion detection system based on data mining techniques: A survey," 2014 IEEE 8th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2014, pp. 274-280, doi: 10.1109/ISCO.2014.7103959.

12. R. Samrin and D. Vasumathi, "Review on anomaly based network intrusion detection system," 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Mysuru, India, 2017, pp. 141-147, doi: 10.1109/ICEECCOT.2017.8284655.

13. Rushendra, K. Ramli, N. Hayati, E. Ihsanto, T. S. Gunawan and A. H. Halbouni, "Development of Intrusion Detection System using Residual Feedforward Neural Network Algorithm," 2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 2021, pp. 539-543, doi: 10.1109/ISRITI54043.2021.9702773.