УДК 004.032.24:004.272.2

ІМІТАЦІЙНА МОДЕЛЬ СИСТЕМИ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК

Лабжинський В. А., к. т. н., доцент,
labzhynskyi.volodymyr@lll.kpi.ua, ORCID: 0000-0003-0970-770X
Снігур В. В., студентка, НН ІАТЕ
Національний технічний університет України
«Київський політехнічний інститут ім. І. Сікорського» (Україна, м. Київ)

Анотація *– у статті розглянуті питання запобігання кібератакам та аналізу їх наслідків на мережеву інфраструктуру. Метою роботи є розроблення імітаційної моделі, що дозволить протестувати вплив поширених типів атак на мережу та оцінити ефективність впроваджених механізмів захисту. Для досягнення мети було використано Cisco Packet Tracer – середовище, що дозволить налаштувати мережу, реалізовувати політики безпеки та здійснювати імітаційне моделювання атак. У ході дослідження була створена імітаційна модель, що дає можливість здійснити оцінку ефективності захисних механізмів. Отримані результати показали, що застосування комбінованого підходу, що включає в себе ACL, VPN та фаєрволи, значно знижує шанс успішної атаки. Було також встановлено, що використання Syslog та NetFlow дозволяє своєчасно ідентифікувати аномальну активність у мережі.*

Ключові слова *– кіберзахист, DDoS, MITM, SQL Injection.*

Постановка проблеми. Перехід від індустріального суспільства до інформаційного, що відбувається в теперішній час, поряд з безсумнівними перевагами несе з собою й негативні фактори, обумовлені можливістю завдання збитків з використанням дистанційного доступу до інформаційних і автоматизованих систем. На сьогоднішній день відсутня необхідність безпосереднього фізичного впливу на технічну систему з метою порушення її нормального функціонування. Набагато простіше, дешевше й безпечніше порушити керування такою системою, що й здійснюється шляхом деструктивного інформаційного впливу на об'єкти критичної інформаційної інфраструктури. Численні приклади свідчать про зростання частоти випадків комп'ютерних атак на вищезгадані об’єкти, що здійснюють керування різними технічними системами забезпечення життєдіяльності держави й суспільства. Більше того, останнім часом відзначається тенденція на підвищення вибірковості таких впливів. Очевидним є той факт, що розроблення систем виявлення кібератак пов’язана з численними викликами, які вимагають від дослідників пошуку оптимальних підходів для забезпечення високого рівня захисту мережевих середовищ.

З кожним роком кількість кібератак на мережеву інфраструктуру зростає, що вимагає створення більш ефективних механізмів захисту. Атаки типу DDoS, MITM та SQL Injection можуть нашкодити роботі інформаційних систем або спричинити витік конфіденційної інформації. Власне крім перерахованих втрат, фінансові є найбільш непередбачуваними та їх дуже складно прорахувати, а їх вартість з кожним роком прогнозовано зростає, що продемонстровано на рисунку 1.

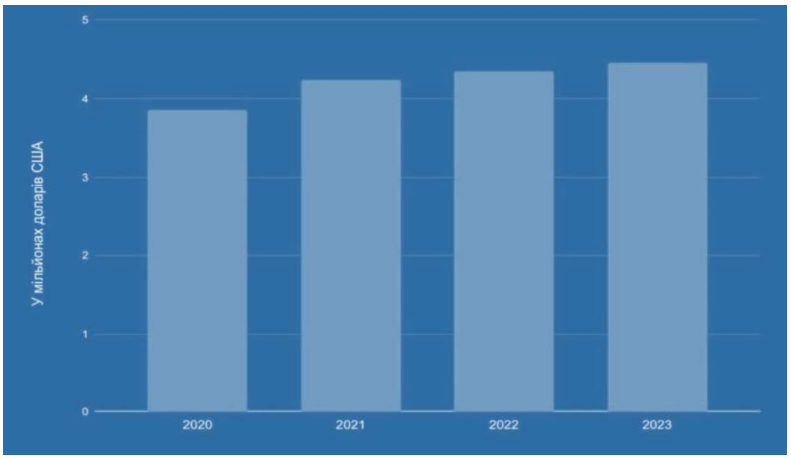

Рис. 1. Середня вартість збитків від одного витоку даних [1]

Формулювання цілей (Постановка завдання). Метою дослідження є розроблення імітаційної моделі, що дозволить протестувати вплив поширених типів атак на мережу та оцінити ефективність впроваджених механізмів захисту. Для цього буде використано Cisco Packet Tracer – середовище, що дозволить налаштувати мережу, реалізовувати політики безпеки та здійснювати симуляції атак.

Аналіз останніх досліджень. У сучасних дослідженнях значну увагу приділено методам запобігання атакам та аналізу їх наслідків. Наприклад, системи виявлення вторгнень, що аналізують поведінку мережевого трафіку та дозволяють виявляти аномалії [2]. Такі системи формують профіль нормальної активності та фіксують відхилення, які можуть вказувати на ймовірні атаки, несанкціонований доступ чи зловмисне програмне забезпечення. Вони використовують методи машинного навчання, статистичного аналізу та евристичних підходів для виявлення незвичних явищ у мережевій активності.

В теперішній час користувачі часто здійснюють підключення до інтернету через загальнодоступні Wi-Fi мережі, які більш вразливі до атак перехоплення даних (Packet Sniffing). VPN є вдалим працюючим рішенням захисту трафіку завдяки шифруванню з’єднання між клієнтом і віддаленим сервером. VPN створює захищений тунель між ними, використовуючи протоколи шифрування, що унеможливлює перехоплення даних третіми особами. Дослідження ефективності VPN для захисту конфіденційних даних у публічних мережах [3] виявили ряд переваг, проте виявлено деякі обмеження та ризики.

Деякі роботи пропонують використання штучного інтелекту для прогнозування атак [4]. Цей метод має великий потенціал, однак багато досліджень не враховують тестування за реальних умов, що може призвести до хибних спрацьовувань. Крім того, подібні системи передбачувано матимуть обмежену ефективність реагування на нові або комбіновані види атак, що не входять до навчального набору моделі.

Основна частина. Наслідки кібератак на об'єкти критичної інфраструктури порівняно з традиційними галузями застосування інформаційних технологій можуть бути набагато важчими, навіть катастрофічними. Ефективна протидія атакам, що здійснюються зловмисниками на автоматизовані систем управління технологічними процесами, неможлива без врахування особливостей та відмінностей кіберзахисту таких систем від захисту традиційних інформаційно-комунікаційних об'єктів та ресурсів.

Серед сучасних підходів до протистояння інформаційним загрозам є системи виявлення вторгнень (IDS/IPS), фаєрволи та VPN, проте у конкретних сценаріях їх ефективність є недостатньо вивченою.

За даними McAfee та Cybersecurity Ventures збитки від кіберзлочинності уряду та бізнесу обчислюються трильйонами доларів, що ускладнює можливість їх передбачити та є важчим завданням порівняно з традиційними, що викликають фінансові втрати, наприклад стихійні лиха чи класична, фізична злочинна діяльність. На рисунку 2 зображена діаграма кіберзлочинів, здійснених у 2022-2023 роках.

Оскільки більшість досліджень аналізують атаки теоретично або надають методи захисту без їх використання та тестування у мережі призначення, що не дає можливості проведення більш "чутливих" налаштувань – це все ще залишається проблемою. Саме точу необхідність створення середовища для імітації атаки та застосування захисних механізмів у відповідь є актуальною, а також це дасть змогу краще оцінити ефективність цих механізмів захисту максимально наближено до цільових систем.

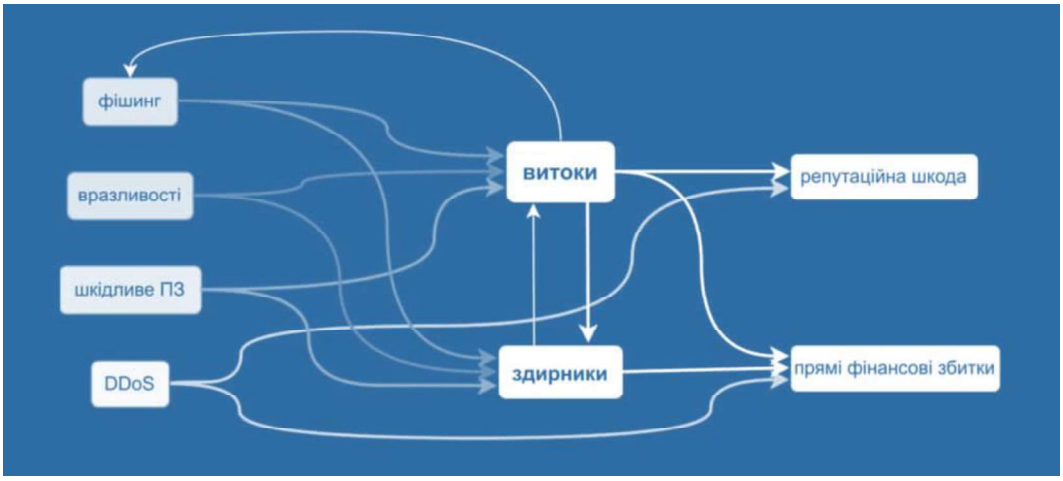

Рис. 2. Діаграма кіберзлочинів за 2022-2023 роки [5]

Основними методами дослідження є аналіз наукових публікацій у сфері кібербезпеки, налаштування тестового середовища, моделювання атак та оцінка ефективності застосованих механізмів захисту. Зокрема, у роботі буде використано механізми ACL, фаєрволи, VPN, VLAN, NetFlow та Syslog з метою контролю мережевого трафіку та виявлення атак.

У ході дослідження була створена імітаційна модель, що дає можливість здійснити оцінку ефективності застосованих захисних механізмів. Було налаштовано мережу з клієнтами, серверами та точками доступу, після чого змодельовано кілька типових атак, зокрема DDoS, MITM та спроби несанкціонованого доступу. Отримані результати показали, що застосування комбінованого підходу, що включає в себе ACL, VPN та фаєрволи, значно знижує шанс успішної атаки. Було також встановлено, що використання Syslog та NetFlow дозволяє своєчасно ідентифікувати аномальну активність у мережі.

Висновки. Запропонована модель дозволяє тестувати та аналізувати кіберзагрози в безпечних, ізольованих та контрольованих умовах, що може бути важливим для навчання фахівців з кібербезпеки та покращити показники мережевої безпеки у корпоративних системах. Наукова новизна полягає у практичному дослідженні відпрацювання захисних механізмів на атаки у єдиному середовищі та у розробленні алгоритму з метою автоматизації блокування атак. Результати роботи можуть бути використані у навчальних закладах для підготовки фахівців з кібербезпеки, а також у реальних організаціях для тестування мережевих політик безпеки. Шляхом їх оптимізації буде знижено ризики на всіх етапах взаємодії з мережею. Такий підхід зменшить час реакції на атаки, надаючи можливість зосередитись на вдосконаленні стратегій безпеки.

Бібліографічний список

1. Середня вартість збитків від витоку даних. URL: https://www.h-x.technology/wp-content/uploads/2023/12/The-average-cost-of-damages-from-data-breach-ua-1024x678.jpeg (дата звернення: 24.02.2025).
2. Parhizkari S. Anomaly Detection in Intrusion Detection Systems. IntechOpen, 2023. URL: https://doi.org/10.5772/intechopen.112733 (дата звернення: 24.02.2025).
3. Sharma Y. K., Kaur C. The vital role of VPN in making secure connection over internet world. International Journal of Recent Technology and Engineering (IJRTE). 2020. V. 8, № 6. P. 2336–2339.
URL: https://doi.org/10.35940/ijrte.F8335.038620 (дата звернення: 24.02.2025).
4. Ahmed T., Kim D. AI-Based Anomaly Detection in Cybersecurity. IEEE Transactions on Network Security. 2023. V. 19, № 1. P. 1–14.
5. Статистика кіберзлочинності 2022-2023. URL: https://www.h-x.technology/wp-content/uploads/2023/12/cybercrime-2022-2023-diagram-ua-min-1024x534.jpg (дата звернення: 24.02.2025).