МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Новосьолов Дмитро Сергійович

УДК 004.056:519.87

КВАЛІФІКАЦІЙНА РОБОТА

ПОБУДОВА ЕФЕКТИВНИХ МОДЕЛЕЙ РЕАГУВАННЯ НА ІНЦИДЕНТИ В КІБЕРПРОСТОРІ.

125 «Кібербезпека та захист інформації»

Подається на здобуття освітнього ступеня магістр

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи:
Веретюк Сергій Михайлович,
кандидат технічних наук, доцент

Житомир – 2024

Висновок кафедри_____

за результатами попереднього захисту:_____

Протокол засідання кафедри_____

№ ____ від «_____» _____ 20____ р.

Завідувач кафедри_____

_____ _____ _____

(науковій ступінь, вчене звання) (підпис) (прізвище, ім’я, по батькові)

«_____» _____ 20____ р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти _____ захистив (ла)

(прізвище ,ім’я, по батькові)

кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____

за шкалою ECT8 _____

за національною шкалою _____

Секретар ЕК

_____ _____ _____

(науковій ступінь, вчене звання) (підпис) (прізвище, ім’я, по батькові)

АНОТАЦІЯ

Новосьолов. Д.С. Побудова ефективних моделей реагування на інциденти в кіберпросторі. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 – Кібербезпека. – Поліський національний університет, Житомир, 2024.

У роботі досліджено вплив кіберінцидентів на інформаційні системи та запропоновано новий підхід до моделювання процесів їхнього реагування. Основою моделі є інформаційно-ентропійний підхід, який дозволяє оцінити рівень порушення системи за допомогою дивергенції Кульбака-Лейблера. Такий підхід надає можливість кількісно вимірювати ступінь відхилення системи від нормального стану, враховуючи динаміку атак та відновлювальних процесів.

Розроблена адаптивна модель реагування на кіберінциденти охоплює моніторинг, оцінку стану системи, динамічне управління швидкістю відновлення та заходи з превенції. Проведено імітаційне моделювання, яке підтвердило, що швидкість відновлення є ключовим фактором мінімізації шкоди та часу простою системи після інцидентів. Запропонована модель забезпечує стійкість інформаційних систем до нових викликів у сфері кібербезпеки.

Отримані результати мають практичну цінність для підвищення ефективності кіберзахисту в корпоративних та державних структурах, дозволяючи не лише мінімізувати наслідки інцидентів, але й вдосконалювати механізми превентивної протидії.

Робота містить 42 сторінки, 4 рисунка, 6 таблиць, 32 літературних джерел.

Ключові слова: кіберінциденти, кібербезпека, інформаційна ентропія, математичне моделювання, адаптивна модель, стійкість систем, дивергенція Кульбака-Лейблера.

SUMMARY

Novosiolov, D.S. Development of Effective Response Models to Cyber Incidents. – Qualification thesis manuscript.

Qualification work for obtaining a master's degree in specialty 125 – Cybersecurity. – Polissya National University, Zhytomyr, 2024.

This study examines the impact of cyber incidents on information systems and proposes a novel approach to modeling response processes. The core of the model is an information-entropy-based method utilizing the Kullback-Leibler divergence to evaluate the extent of system disruption. This approach enables the quantitative assessment of a system's deviation from its normal state, considering the dynamics of attacks and recovery processes.

The developed adaptive response model includes system monitoring, state assessment, dynamic recovery management, and preventive measures. Simulation modeling confirmed that the recovery speed is a critical factor in minimizing system damage and downtime following incidents. The proposed model enhances the resilience of information systems against emerging cybersecurity challenges.

The findings have practical value for improving cybersecurity efficiency in corporate and governmental structures. They not only help minimize the impact of incidents but also advance mechanisms for preventive countermeasures.

The work contains 42 pages, 4 figures, 6 tables, 32 literary sources.

Key words: cyber incidents, cybersecurity, information entropy, mathematical modeling, adaptive model, system resilience, Kullback-Leibler divergence.

ЗМІСТ

ВСТУП

Стрімкий розвиток цифрових технологій та зростання обсягів інформації, що обробляється й передається через мережі, супроводжується суттєвим підвищенням ризиків кіберінцидентів. Кіберзагрози, що раніше були переважно локальними та відносно передбачуваними, нині набули глобального характеру та динамічності. Кібератаки стають дедалі витонченішими, спрямованими на обходження традиційних захисних механізмів, що ставить під загрозу не лише окремі інформаційні системи, а й критично важливу інфраструктуру держав та корпорацій.

У цьому контексті перед дослідниками постає завдання пошуку нових підходів, які враховують динамічний характер кіберінцидентів, а також складність їхнього прогнозування. Одним із перспективних напрямів є використання інформаційно-ентропійного підходу, що дозволяє кількісно оцінити ступінь хаосу й невизначеності, які виникають у системі під час атак, що надає можлливість удосконалювати механізми реагування та подолання наслідків кіберінциндентів. Інформаційна ентропія забезпечує глибоке розуміння деструктивного впливу загроз на цілісність, доступність і конфіденційність даних, а також відкриває можливості для аналізу динаміки відновлення систем після атак.

Існуючі підходи до реагування на кіберзагрози — проактивний, реактивний та їх інтегративні модифікації — хоча й забезпечують певний рівень безпеки, часто виявляються недостатніми для ефективного подолання сучасних викликів. Проактивні моделі, спрямовані на передбачення й запобігання атакам, не завжди здатні впоратися з новими або раніше невідомими загрозами. Натомість реактивні моделі, хоча й забезпечують швидке усунення наслідків інцидентів, не дозволяють системі підготуватися до атак заздалегідь. Інтегративні моделі, які поєднують обидва підходи, мають потенціал для забезпечення комплексного захисту, проте їхня реалізація вимагає значних ресурсів та ретельного налаштування.

Наукова новизна отриманих результатів:

Розроблено інформаційно-ентропійну модель для оцінки впливу кіберінцидентів, що використовує дивергенцію Кульбака-Лейблера як метрику порушення стану системи.

Уперше проведено моделювання взаємозв'язку між швидкістю відновлення та рівнем стабільності інформаційної системи після кіберінцидентів.

Запропоновано адаптивну модель реагування, яка враховує динаміку відновлювальних процесів та впроваджує механізми адаптації до змін у середовищі загроз.

Така модель буде не лише ефективним інструментом для оцінки впливу загроз, а й базисом для оптимізації процесів відновлення інформаційних систем. Вона враховуватиме як характерні параметри кіберзагроз (інтенсивність атак, тип загроз, цілісність системи), так і динаміку адаптації системи до змін.

Таким чином, дослідження спрямоване на вирішення таких завдань кібербезпеки: підвищення адаптивності систем до нових викликів, забезпечення ефективного реагування на кіберзагрози та вдосконалення механізмів їхнього подолання.

Мета роботи: розроблення та обґрунтування інформаційно-ентропійної моделі, яка підвищує ефективність оцінки динаміки кіберінцидентів та сприяє вдосконаленню механізмів захисту й відновлення інформаційних систем. Для досягнення мети були поставлені такі завдання:

1. Проаналізувати підходи, методи та моделі реагування на кіберінциденти.
2. Дослідити інформаційні процеси в системах під впливом кіберінцидентів.
3. Розробити математичну модель реагування на основі інформаційно-ентропійного підходу для аналізу та прогнозування впливу кіберзагроз.
4. Провести оцінку моделі, її ефективності та розробити рекомендації для впровадження моделі в практику реагування на кіберінциденти.

Об'єкт дослідження: процеси реагування на кіберінциденти в інформаційних системах.

Предмет дослідження: інформаційно-ентропійні моделі оцінки впливу кіберзагроз і механізмів відновлення систем.

За темою кваліфікаційної роботи опубліковано наукові публікації, а саме:

- Новосьолов Д. С. Моделювання кіберінцидентів в мультиагентному середовищі NetLogo. Моделювання, керування та інформаційні технології (*MCIT*–2024) : збірник праць учасників Міжнародної науково-практичної конференції, 2024. 367 с.

- Новосьолов Д. С. Математична модель еволюції кіберінцинденту. *Litteris et Artibus*: Нові горизонти : збірник матеріалів Всеукраїнської науково-практичної конференції. Випуск IX / за заг. ред. О. В. Тригуби. Кременець : ВЦ КОГПА ім. Тараса Шевченка, 2024. 358 с.

- - Новосьолов Д. С . Ентропійно-інформаційна модель кіберінциндентів: збірник праць учасників міжфакультетської науково-практичної інтернет-конференції здобувачів вищої освіти і молодих вчених, 12 листопада 2024 р. Житомир : Поліський національний університет, 2024. 102 с

Структура та обсяг роботи. Дипломна робота складається зі вступу, трьох розділів основної частини, висновків та списку використаних джерел

Розділ 1. АНАЛІЗ МОДЕЛЕЙ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

1.1 Класифікація моделей реагування на кіберінциденти

Кіберзагроза — це серйозний виклик для інформаційної системи, яка функціонує у мережевому середовищі, тому розробка ефективних моделей реагування є ключовим аспектом забезпечення кібербезпеки. Такі моделі покликані не лише виявляти та нейтралізувати загрози, а й мінімізувати їхній вплив на систему, забезпечуючи її швидке відновлення після інциденту. Завдяки різноманітності кіберзагроз та їхньої динамічності, створення і застосування адаптивних моделей реагування дозволяє оптимально використовувати наявні ресурси, водночас враховуючи специфіку конкретного середовища.

Моделі реагування на кіберінциденти поділяються на: математичні, імітаційні, тренувальні, експертні, наочні, символьні, кібернетичні[2]. Математичні моделі використовують алгоритми для аналізу й прогнозування інцидентів, що зручно для автоматизованого моніторингу. Імітаційні моделі створюють віртуальні сценарії для тестування без ризику для реальних даних. Тренувальні моделі готують фахівців через симуляції реальних атак. Експертні моделі базуються на знаннях спеціалістів для вирішення нестандартних загроз.

Для глибокого розуміння моделей реагування на кіберзагрози необхідно провести їх систематичну класифікацію та аналіз. Однією з ключових концепцій у цій галузі є проактивна модель реагування, яка базується на принципі передбачення. Її головна ідея полягає в підготовці системи до протидії потенційним ризикам ще до їхньої реалізації. Використання проактивного підходу дозволяє завчасно виявляти загрози та пом'якшувати їхній вплив, що суттєво знижує ризик порушення стабільності системи. Водночас проактивна модель має свої обмеження, зокрема щодо ефективності у випадках нових і невідомих загроз. Її впровадження потребує глибокого розуміння існуючих векторів атак, на основі яких формуються захисні механізми. Це вимагає

постійного оновлення даних та адаптації до нових викликів, що створює певні труднощі при реалізації.

Окрім того, значну роль у сучасних системах відіграє реактивна модель реагування, яка спрямована на оперативне виявлення та усунення наслідків атак, що вже відбулися. Такий підхід є особливо важливим у ситуаціях, коли атака залишається непередбачуваною або неможливою для попередження. Реактивна модель дозволяє швидко мінімізувати шкоду за рахунок впровадження відповідних заходів, проте її недоліком є відсутність механізмів запобігання. Ефективність цього підходу безпосередньо залежить від швидкості реагування, оперативного аналізу інциденту та коректності зібраної інформації.

Особливу увагу привертає інтегративна модель реагування, яка поєднує переваги як проактивного, так і реактивного підходів. Завдяки такій синергії вона дозволяє системі передбачати можливі загрози, швидко реагувати на реалізовані атаки та адаптуватися до нових викликів, використовуючи отриманий досвід для вдосконалення захисних механізмів. Інтегративна модель забезпечує збалансований рівень захисту, що є критично важливим для сучасних кіберсистем, які стикаються з багатовимірними та динамічними загрозами. Водночас її впровадження є складним процесом, який вимагає значних ресурсів та ретельного налаштування системи.

Серед математичних основ аналізу кіберзагроз вирізняється модель Лотки-Вольтерри, що відображає взаємодію "хижака" та "жертви". У контексті кібербезпеки ця модель ілюструє протистояння між кіберзлочинцями (агресорами) та оборонними механізмами системи. Вона дозволяє наочно змоделювати базові взаємодії між сторонами (“зловмисник”-”система”). Однак ця модель не враховує багатовимірність і складність реальних кіберсистем, що складаються з численних векторів атак і захисних механізмів. Крім того, її застосування потребує надійних і достовірних даних, доступ до яких часто є обмеженим у сфері кібербезпеки.

Не менш важливим підходом є імітаційне моделювання, яке базується на створенні моделей реальних систем для проведення експериментів та отримання релевантної інформації. Такий підхід дозволяє аналізувати складні явища без прямої взаємодії з реальними об’єктами, що знижує ризик експериментів та сприяє виявленню слабких місць у захисних механізмах. Імітаційне моделювання має кілька різновидів, таких як метод Монте-Карло, статистичне моделювання, ігрові та агентні моделі. Вони надають можливість адаптувати системи до змін, проте вимагають значних ресурсів і спеціалізованих знань[1].

1.2 Аналіз існуючих моделей

Результати порівняльного аналізу на основі вивчення джерел [12,14,6,12,14,29,28] представлено в табл.1.

Таблиця 1 – аналіз моделей реагування

Модель	Переваги	Недоліки
Проактивна	Завчасне виявлення та пом’якшення загроз до їх реалізації.[28]	Менш ефективна проти нових або невідомих загроз.[14]
	Зниження ризику порушення стабільності системи.[12]	Потребує глибокого розуміння існуючих векторів атак.
	Підготовка систем до можливих ризиків.	Вимагає адаптивного підходу для виявлення нових загроз.
Реактивна	Швидке реагування на вже реалізовані атаки.[12]	Ефективність залежить від оперативності аналізу та реагування.[14]

	Зменшення шкоди за рахунок негайного впровадження заходів.	Не працює на попередження, лише на усунення наслідків.
	Незамінна при непередбачуваних інцидентах.	Висока залежність від точності та швидкості збору даних.
Інтегративна	Поєднує сильні сторони проактивного та реактивного підходів.[6]	Складність у налаштуванні та інтеграції.[12]
	Забезпечує баланс між передбаченням загроз та оперативним реагуванням.	Потребує регулярного аналізу та вдосконалення механізмів.
Лотки-Вольтерри	Відображає базові взаємодії "хижак-жертва", що спрощує аналіз кіберзагроз.[29]	Не враховує багатовимірну природу реальних кіберсистем.[14]
	Застосовується для базового аналізу загроз та протидії їм.	Складно адаптувати до систем із великою кількістю механізмів захисту та різноманітними загрозами.

Конкретні моделі наведено в табл.2

Таблиця 2 – приклади моделей

Модель	Опис	Приклади застосування	Джерела
Модель Марковських процесів	Використовує ймовірності переходів між станами системи	Визначення ймовірності успішного відновлення	[18] NIST SP 800-30,

	для аналізу та прогнозування розвитку кіберінцидентів.	системи після інциденту або переходу в критичний стан.	ResearchGate
Ігрові моделі	Використовує теорію ігор для аналізу взаємодій між атакуючими (хакерами) і захисниками (адміністраторами).	Розробка оптимальних стратегій захисту з урахуванням дій атакуючих, наприклад, мінімізація втрат від DDoS-атак.	[15] Lye & Wing, Game Theory for Cyber Security
Системи масового обслуговування	Моделює потоки запитів у системі для аналізу її продуктивності під час кібератак.	Аналіз перевантаження серверів у випадку DDoS-атак і визначення моменту, коли система стане недоступною.	[11] Kleinrock, Queueing Systems
Епідеміологічні моделі	Використовує аналогії з поширенням інфекцій для моделювання розповсюдження шкідливого програмного	Прогноз поширення вірусів або черв'яків у корпоративних мережах, розробка стратегій ізоляції заражених вузлів.	[20] Pastor-Satorras & Vespignani, Epidemic Spreading in Networks

	забезпечення у мережах.		
Баєсові мережі	Використовує графічну модель залежностей для оцінки ризиків імовірностей кіберінцидентів.	Прогноз імовірності інциденту залежно від певних умов (наприклад, наявності вразливостей або загроз).	[10] Jensen & Nielsen, Bayesian Networks and Decision Graphs
Моделі відновлення (Resilience Models)	Використовує диференціальні рівняння для опису процесу відновлення після кібератаки.	Аналіз часу відновлення після атак, моделювання впливу різних стратегій реагування на загальну функціональність системи.	[8] Hollnagel, Resilience Engineering
Лінійне та нелінійне програмування	Використовує математичну оптимізацію для розподілу ресурсів під час реагування на інциденти.	Розробка оптимальних планів дій для мінімізації втрат і витрат на відновлення після кіберінцидентів.	[19] Operations Research in Cybersecurity

Стохастичні моделі ризиків	Використовує імовірнісний підхід для оцінки фінансових втрат та часу простою систем через кіберінциденти.	Оцінка ймовірності виникнення інцидентів і їхніх наслідків для бізнесу, наприклад, у кіберстрахуванні.	[7] FAIR: Factor Analysis of Information Risk
Агентно-орієнтовані моделі	Моделює поведінку окремих агентів (користувачів, атакуючих, систем) для аналізу динаміки кіберінцидентів.	Аналіз впливу поведінки користувачів на поширення атак, наприклад, відкриття шкідливих вкладень або порушення політик безпеки.	[16] Macal & North, Agent-based Modeling and Simulation
Моделі на основі теорії катастроф	Використовують математичний апарат для аналізу різких змін стану системи під впливом невеликих факторів.	Ідентифікація точок, де невеликі зміни (наприклад, додаткові запити) можуть спричинити катастрофічні збої в роботі системи.	Poston & Stewart, Catastrophe Theory and Its Applications

Інша класифікація моделей передбачає розгляд моделей в площині експертні-тренувальні, що особливо актуально в контексті поставленого завдання, а саме аналіз підходів до реагування.

Експертні моделі реагування є важливим інструментом у кібербезпеці, який дозволяє імітувати або перевершувати рішення людини-експерта [28]. Вони використовують методи штучного інтелекту та логічного висновку для аналізу шаблонів атак і прогнозування потенційних загроз. Завдяки цьому ці моделі допомагають формалізувати складні системи й розробляти рекомендації для підвищення захищеності інформаційних систем. Їхньою перевагою є універсальність, яка дозволяє адаптувати їх до різних наукових сфер, але в кібербезпеці вони потребують значних ресурсів та висококваліфікованих фахівців. Регулярне оновлення таких моделей є критичним для їхньої ефективності у виявленні нових загроз. Переваги та недоліки цієї моделі наведено в Таблиці 3 для детальнішого аналізу.

Тренувальні моделі реагування на кіберінциденти є ключовим елементом сучасної кібербезпеки, що дозволяє підвищити готовність системи та персоналу до деяких загроз. Вони забезпечують можливість моделювання реальних сценаріїв атак, аналізу їх впливу на інфраструктуру та оптимізацію стратегій реагування [29]. Такий підхід дозволяє тестувати захисні механізми в контрольованих умовах, що сприяє виявленню слабких місць до реалізації реальних загроз. Крім того, моделі сприяють підвищенню кваліфікації персоналу, надаючи йому практичний досвід у боротьбі з кіберзагрозами. Однак їх впровадження потребує значних ресурсів, включаючи фінансові витрати та постійне оновлення сценаріїв відповідно до нових викликів. на ці складнощі, поточні моделі залишаються ефективним інструментом для підготовки до протидії кіберзагрозам. Аспекти даної моделі систематизовано у таблиці 3.

Таблиця 3 – аналіз моделей реагування

Модель	Переваги	Недоліки
Тренувальна	Можливість симуляції реальних сценаріїв атак.	Висока ресурсоємність і потреба у значних фінансових вкладеннях.

	Тестування захисних механізмів у контрольованих умовах.	Залежність ефективності від якості та реалістичності сценаріїв.
	Виявлення слабких місць у системі до виникнення реальних загроз.	Постійна необхідність оновлення сценаріїв відповідно до нових типів загроз.
Експертна	Використання знань і досвіду фахівців для аналізу попередніх кіберінцидентів.	Залежність від доступності висококваліфікованих спеціалістів.
	Ідентифікація шаблонів атак та розробка рекомендацій для захисту	Висока вартість впровадження та утримання.
	Точна адаптація до специфічних потреб організації.	Значні ресурси для збору, зберігання та обробки даних.

Таблиця 4 – тепловий-порівняльний аналіз моделей реагування (авторська доробка)

Таблиця 5 – приклади моделей

Моделі	Приклади моделей
Реактивна	OODA Loop [24], SANS Incident Response Model
Проактивна	Kill Chain Model [27], MITRE ATT&CK Framework [31], Lockheed Martin Cyber Kill Chain ()
Інтегративна	NIST Cybersecurity Framework (CSF) [30], MITRE ATT&CK Framework [23]
Лотки-Вольтера	Підходи, що моделюють динаміку кіберзагроз через математичні рівняння [32])
Тренувальна	SANS Incident Response Model [26], навчальні симуляції інцидентів
Експертна	Моделі з використанням ручного аналізу експертів, комбіновані з автоматичними системами [25]

Інтегративна модель є найкращим підходом до кібербезпеки завдяки поєднанню різних методів, що забезпечує високу адаптивність, продуктивність та масштабованість. Вона ефективно справляється з багатовекторними атаками й відповідає вимогам сучасних інформаційних систем. Натомість модель Лотки-Вольтерри має низьку адаптивність і продуктивність у реальному часі, оскільки зосереджена на прогнозуванні, а не на оперативному захисті, що обмежує її застосування у складних умовах.

1.3 В1иклики та обмеження сучасних моделей

Розробка та впровадження моделей реагування на кіберінциденти стикаються з низкою викликів, які обмежують їхню ефективність у сучасному динамічному кіберсередовищі. Однією з ключових проблем є недостатня адаптивність до нових і нестандартних загроз. З огляду на швидкий розвиток технік кіберзлочинців, існуючі моделі часто виявляються неготовими до сценаріїв атак, які виходять за межі передбачених алгоритмів. Ще одним значним бар’єром є висока ресурсоємність таких систем. Впровадження, налаштування та підтримка моделей вимагають великих фінансових, технічних та людських ресурсів, що ускладнює їх використання в умовах обмеженого бюджету або слабкої технічної інфраструктури.

Додатковим обмеженням є складність інтеграції різних моделей у єдину систему. Використання комбінованих підходів потребує злагодженої роботи алгоритмів, узгодження протоколів обробки даних і вирішення конфліктів між моделями. Це часто призводить до зниження ефективності або додаткових витрат ресурсів. Також актуальною залишається проблема хибних спрацювань: навіть найкращі моделі іноді генерують помилкові сигнали, що відволікає ресурси й сповільнює реакцію на реальні загрози.

Окремої уваги потребує питання етичності та конфіденційності, адже більшість моделей вимагають обробки великих обсягів даних, що може створити

ризик порушення приватності користувачів або організацій. Крім того, швидкий темп змін у кіберпросторі ускладнює регулярне оновлення та підтримку моделей, що знижує їхню актуальність і стійкість до нових типів атак.

Висновок першого розділу

Аналіз існуючих моделей реагування на кіберінциденти (проактивних, реактивних, інтегративних) показав їх переваги та недоліки. Виявлено, що сучасні підходи недостатньо адаптовані до динамічних та складних загроз. Найперспективнішим визнано інтегративний підхід із комбінуванням проактивного прогнозування та реактивного реагування.

Розділ 2. РОЗРОБЛЕННЯ ІНФОРМАЦІЙНО-ЕНТРОПІЙНОЇ МОДЕЛІ ЕВОЛЮЦІЇ КІБЕРІНЦИНДЕНТУ

2.1 Інформаційно-ентропійні процеси в системі

Ентропія є універсальним поняттям, яке описує міру невпорядкованості або хаосу у системі. У контексті інформаційних систем вона застосовується для кількісної оцінки невизначеності стану даних або подій, які впливають на роботу системи. Це поняття було введене в інформаційну теорію Клодом Шенноном і є базисом для оцінки складності інформаційних процесів.

Математично рівень ентропії у системі визначається формулою:

$$H(X) = \sum_{i=1}^{n} P(x_i) log_2 P(x_i)$$

$H(X)$ – ентропія системи X, $P(x_i)$ – ймовірність настання конкретної події x, n — загальна кількість можливих станів системи.

Ентропія відображає ступінь невизначеності у системі: чим більш рівномірний розподіл ймовірностей, тим вищий рівень ентропії. У інформаційній системі це означає максимальну непередбачуваність поведінки даних. Протилежним процесом до ентропії є антиентропія — здатність системи до відновлення порядку та зменшення рівня хаотичності. В інформаційних системах антиентропія реалізується через дії, спрямовані на підтримання стабільності, наприклад:

1. Впровадження резервного копіювання даних.
2. Використання алгоритмів виявлення аномалій.
3. Захист інформації за допомогою шифрування.
4. Проведення організаційних заходів.

5. Навчання персоналу.

Та всі інші, які спрямовані на підвищення дисципліни, порядку та передбачуваності.

Антиентропійні механізми дозволяють зберігати контроль над системою, навіть у випадку значного зовнішнього чи внутрішнього впливу. Наприклад, при спробах вторгнення у систему або втраті даних через апаратний збій, резервні копії дозволяють зменшити ризики втрати інформації, а автоматизовані алгоритми ідентифікують потенційні загрози.

Таким чином, ентропія та антиентропія знаходяться у динамічному балансі, що є важливим для забезпечення стабільності системи. З одного боку, ентропія вказує на ризики хаосу, а з іншого — антиентропія забезпечує заходи для його усунення.

Інформаційні системи функціонують у середовищі, яке постійно змінюється через зовнішні впливи. Ці впливи можуть бути позитивними, сприяючи покращенню роботи системи (наприклад, впровадження оновлень безпеки), або негативними, що призводять до зростання ентропії. Аналіз таких впливів дозволяє ефективно управляти інформаційними ресурсами, прогнозувати ризики та мінімізувати втрати.

Розглянемо основні типи зовнішніх впливів:

1. Кібератаки та зловмисні дії

Кібератаки є одним із найпоширеніших джерел зростання ентропії в інформаційних системах. Зловмисні дії, такі як спроби отримати несанкціонований доступ, шкідливе програмне забезпечення або атаки типу DDoS, порушують нормальний функціонал системи. Наприклад:

a. DDoS-атаки генерують аномальний трафік, що спричиняє перевантаження мережі та підвищення рівня ентропії.
b. Фішинг та соціальна інженерія впливають на довіру користувачів, вводячи їх в оману та викрадаючи облікові дані.

Наслідком таких дій є не лише порушення цілісності даних, але й значні збої у роботі системи.

2. Технічні збої та відмови обладнання

Технічні збої, такі як пошкодження серверів, відмова мережевого обладнання чи перебої в електропостачанні, створюють хаос в обробці та зберіганні даних. Зменшення ентропії в таких ситуаціях можливе завдяки впровадженню резервування (дублювання системних ресурсів) та автоматизованих механізмів відновлення.

3. Природні катастрофи та форс-мажорні обставини

Землетруси, повені чи інші природні явища можуть фізично знищити інформаційні носії. Такі події підвищують ентропію до критичних рівнів, оскільки можуть бути втрачені як дані, так і апаратні ресурси. Для зменшення ризиків важливо використовувати хмарні технології, які забезпечують зберігання інформації незалежно від фізичної інфраструктури.

4. Соціальні та економічні чинники

Збільшення кількості кіберзлочинів, економічні кризи або недостатнє фінансування кібербезпеки також впливають на рівень ентропії в системах. Наприклад, низький рівень інвестицій у безпеку підвищує вразливість системи до зовнішніх атак.

5. Легітимні процеси

Певні зовнішні впливи, такі як впровадження оновлень програмного забезпечення чи інтеграція нових компонентів, тимчасово підвищують ентропію через перебудову системи. Однак згодом вони сприяють стабілізації та покращенню роботи інформаційних систем.

Ключовим джерелом зростання ентропії в сучасних інформаційних системах є саме кіберінциденти. Ці події мають комплексний вплив, який охоплює не лише окремі компоненти системи, але й взаємозв’язки між ними. Кіберінциденти є потужним тригером для зміни інформаційно-ентропійного стану системи, що робить їх об’єктом детального аналізу.

1. Під час кіберінциденту хаотизація в системі досягає високого рівня, оскільки:

- Порушується передбачуваність обробки даних.
- Змінюється структура інформаційних потоків.

- Виникає загроза для конфіденційності, цілісності та доступності інформації.

2.2 Кіберінцидент як джерело ентропії

Кіберінциденти виступають джерелом ентропії в інформаційних системах, оскільки їхній вплив безпосередньо спричиняє зростання невизначеності, дезорганізації та нестабільності. У межах інформаційно-ентропійного підходу ці події можуть бути описані через показники, що характеризують міру хаосу ентропією системи. Такі методи дозволяють не лише оцінювати вплив атак, але й моделювати загальну поведінку системи під їхнім впливом, включаючи відновлення після інцидентів [4, 9].

Кіберінциденти, такі як DDoS-атаки, витоки даних чи проникнення шкідливого програмного забезпечення, є подіями з високим рівнем ентропії. Це пояснюється їхньою непередбачуваністю, випадковим характером і здатністю до масштабного деструктивного впливу [22]. Зокрема, випадковість і нерегулярність таких інцидентів можна ефективно описувати через пуассонівські процеси, які моделюють потоки подій у системі. Якщо припустити, що атаки трапляються з середньою інтенсивністю λ, ймовірність виникнення k атак за час t визначається формулою:

$$P(k,t) = \frac{(\lambda t)^2 e^{-\lambda t}}{k!}$$

де λ відображає частоту атак за одиницю часу, а k — кількість атак за період t. Ця модель дозволяє аналізувати поведінку системи в умовах різної

інтенсивності атак, від низько інтенсивних загроз до сценаріїв масштабних атак, характерних для складних мережевих середовищ [21].

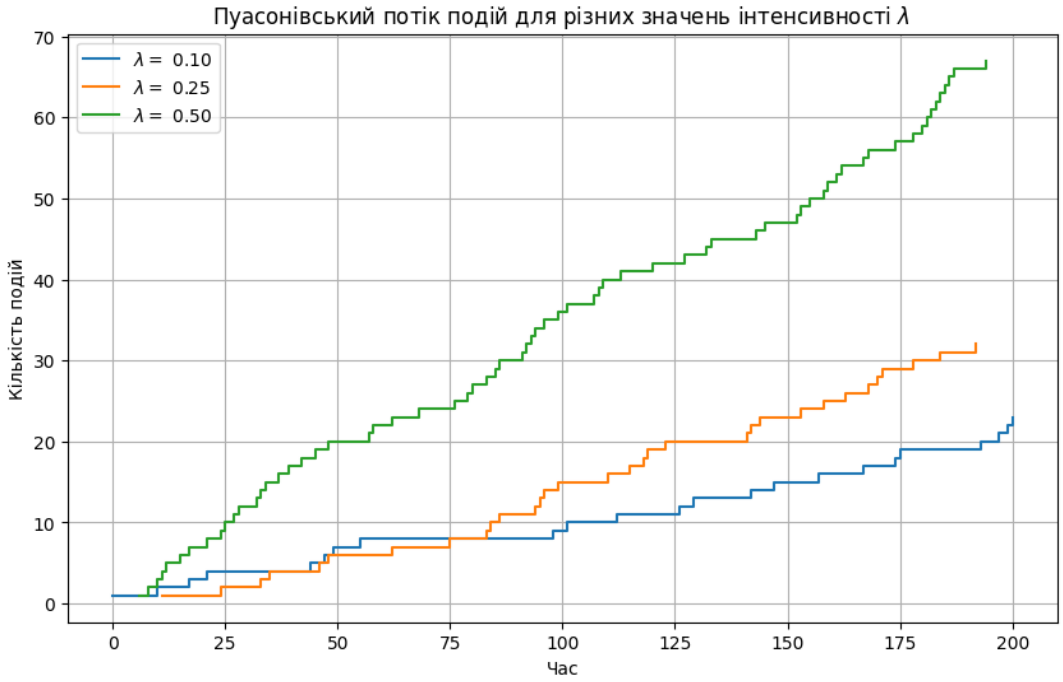

Рисунок 1 – Пуасонівський потік подій

Особливістю кіберінцидентів є те, що кожна атака створює змінну за інтенсивністю деструктивність. Для оцінки цього ефекту введено так званий імпакт-фактор (Ii)який визначає рівень шкоди від і-ї атаки. Імпакт-фактор моделюється як випадкова величина, що підпорядковується або рівномірному розподілу ($I_i \sim U(I_{min}, I_{max})$), або нормальному закону (Ii~N(μ,σ2)) [17]. У рівняннях моделювання враховується як початковий вплив атаки (I_0), так і її затухання в часі через експоненційний процес:

$$I(t) = I_0 e^{-at} + \xi(t)$$

де α — параметр затухання, I_0 — початкова сила впливу .а ξ(t)— стохастичний шум, що враховує випадкові флуктуації. Таким чином, модель дозволяє врахувати як швидкість, із якою система піддається деструктивним змінам, так і варіативність цих змін у часі [5].

У реальних умовах кіберінциденти не лише змінюють поточний стан системи, але й змінюють розподіл ймовірностей її станів. Якщо початковий стан системи описується вектором $P0 = \{P0_1, P0_2, \dots, P0_n\}$ то під впливом і-ї атаки розподіл станів системи змінюється на P_i, а потім поступово повертається до початкового базового стану P_i . Це відновлення відбувається за рахунок антиентропійного процесу (процесів відновлення), швидкість якого залежить від параметрів внутрішньої стабільності системи. Однак інтенсивні атаки (λ>10) можуть створювати настільки значні відхилення, що система не встигає адаптуватися.

2.2 Метрика для оцінки відхилення системи від базового стану

Як метрику, в роботі використано дивергенцію Кульбака-Лейблера. Дивергенція Кульбака-Лейблера (D_{KL}) є ключовим інструментом для оцінки впливу кіберінцидентів на системи[**Error! Reference source not found.**]. Вона дозволяє кількісно визначити відхилення поточного стану системи від стабільного стану:

$$D_{KL}(P||P_0) = \sum_i P_i \; log \; log \; \frac{P_i}{P_{0i}}$$

Де P_i — ймовірність і-го стану після впливу атаки, а P_{0i} — ймовірність цього ж стану у початковій системі. Значення D_{KL} дозволяє не лише кількісно оцінити ефективність атак, але й визначити ефективність процесів відновлення. Наприклад, при моделюванні DDoS-атак було виявлено, що зі зростанням інтенсивності λ значення D_{KL} зростає експоненційно, сигналізуючи про втрату

стабільності системи [власна теза автора].Іншим важливим показником є ентропія Шеннона:

$$H(P) = -\sum_i P_i log P_i$$

Котра відображає загальний рівень невизначеності в системі. Зростання H(P) під впливом кіберінцидентів демонструє підвищення ентропійного рівня, що ускладнює функціонування системи та її відновлення. Системи з низьким рівнем внутрішньої адаптивності можуть досягати критичних значень H(P), що потребує негайного втручання.

Застосування інформаційно-ентропійних методів у реальних умовах дозволяє не лише моніторити поточний стан системи, а й прогнозувати її реакцію на майбутні атаки. Наприклад, використання пуассонівської моделі для аналізу атак на телекомунікаційні мережі демонструє, що збільшення інтенсивності $\lambda = 20$ подій на годину призводить до стрімкого зростання значення H(P) та D_{KL}, яке сигналізує про необхідність перегляду механізмів безпеки .

2.3 Математична модель еволюції кіберінцинденту

Модель системи (об'єкт кібератаки):

Система має початковий базовий стан із розподілом P, під впливом атаки, система набуває розподілу Q. Після події і-ої атаки стан системи змінюється відповідно до:

$Q_{t+1} = Q_t + I_i * noise$, де noise~N(0,1) — випадковий шум.

Між подіями система намагається відновитись до базового стабільного стану P із швидкістю α:

$$\frac{dQ}{dt} = -a(Q - P)$$

Позначимо $Q(t) = [q_1(t), q_2(t), \dots, q_t(t)]$ як вектор ймовірностей станів у час t, де $\sum \quad q_i(t) = 1$. Деструктивні події з інтенсивністю λ впливають на кожен елемент $q_i(t)$, змінюючи ймовірність певного стану. Антиентропійний (recovery) процес відновлює кожен компонент q_i у напрямку базового розподілу $P = [p_1, p_2, \dots, p_n]$.

Тоді загальну динаміку системи у векторній формі можна описати як:

$$\frac{dQ(t)}{dt} = \lambda I(t) * w(t) - \lambda(Q(t) - P),$$

де: λ(t)·noise — деструктивний вплив на систему з випадковим шумом, який моделює силу атаки або зовнішніх подій; α(Q(t)−P) — антиентропійний компонент, що відповідає за повернення системи до стабільного стану P, w(t) - шум та/або випадкові флуктуації.

Розподіл Q(t) відхиляється від початкового стабільного стану P у процесі еволюції системи внаслідок дії зовнішнього впливу. Як міру оцінки цього відхилення вибрано дивергенцію Кульбака Лейблера, яка дозволяє кількісно оцінити ефект деструктивного впливу та антиентропійного відновлення[3]:

$$D_{KL}(Q(t)||P) = \sum_{i=1}^{n} q_i(t) log(\frac{q_i(t)}{p_i})$$

Висновок до другого розділу

Розроблено інформаційно-ентропійну модель, яка враховує рівень хаосу в системі через ентропію та відхилення стану за допомогою дивергенції Кульбака-Лейблера. Доведено, що під час кіберінцидентів ентропія різко зростає, однак відновлювальні механізми здатні повернути систему до стабільності за умов правильного управління швидкістю відновлення.

Розділ 3.МОДЕЛЮВАННЯ ПРОЦЕСУ РЕАГУВАННЯ НА КІБЕРІНЦИНДЕНТ

3.1 Визначення екстремальних режимів та стану динамічної рівноваги

Екстремальні режими кіберсистеми характеризуються станами, у яких її функціонування перебуває на межі критичного руйнування через значне відхилення від динамічної рівноваги. У таких режимах система досягає максимальної ентропії, що свідчить про високий ступінь невизначеності та втрату стійкості. Для аналізу цих явищ важливо розробити математичний апарат, який дозволить кількісно оцінювати рівень відхилення поточного стану системи від її рівноважного розподілу. Таким підходом стала використана в дослідженні KL-дивергенція (D_{KL})

KL-дивергенція є мірою відстані між двома ймовірнісними розподілами:

$$D_{KL}(P\|Q) = \int_{-\infty}^{\infty} P(x) \log \frac{P(x)}{Q(x)}\, dx$$

Дивергенція Кульбака-Лейблера (D_{KL}) досягає максимального значення, коли два порівнювані розподіли $P(x)$ і $Q(x)$ є максимально "віддаленими" один від одного, тобто коли вони мають мінімальну схожість.

У випадку нормального і рівномірного розподілів:

1. Рівномірний розподіл ($Q(x)$): має фіксовані границі $[a, b]$.

2. Нормальний розподіл ($P(x)$): є необмеженим, але його щільність значно концентрується в межах $[\mu - 3\sigma, \mu + 3\sigma]$.

Дивергенція сягає максимуму за умов:

- Середнє (μ) нормального розподілу виходить за межі рівномірного інтервалу $[a, b$, що призводить до мінімального перетину між щільностями $P(x)$ і $Q(x)$.

- Стандартне відхилення (σ) набуває малих значень, тобто розподіл $P(x)$ стає схожим на дельта-функцію, що суттєво відрізняється від рівномірного.

Для вказаного випадку можна записати:

$$D_{KL}(\mathcal{N}(\mu,\sigma^2)\|\mathcal{U}[a,b]) \approx \frac{1}{2}\log\left(\frac{2\pi e\sigma^2}{(b-a)^2}\right) + \frac{1}{2\sigma^2}\int_a^b (x-\mu)^2\,dx$$

- Коли μ поза межами $[a,b]$, значення $(x-\mu)^2$ стає значним.
- Якщо σ^2 набуває малих значень, перший логарифмічний член також зростає.

Отже:

1. Максимальна дивергенція спостерігається, коли:
   - $\mu \ll a$ або $\mu \gg b$ (нормальний розподіл повністю поза межами рівномірного).
   - $\sigma \to 0$(нормальний розподіл стає надзвичайно вузьким).
2. Якщо нормальний розподіл "вписується" в межі рівномірного розподілу $[a,b]$, дивергенція зменшується.

На рис. 2 представлено залежність дивергенції Кульбака-Лейблера від показників нормального та рівномірного розподілу.

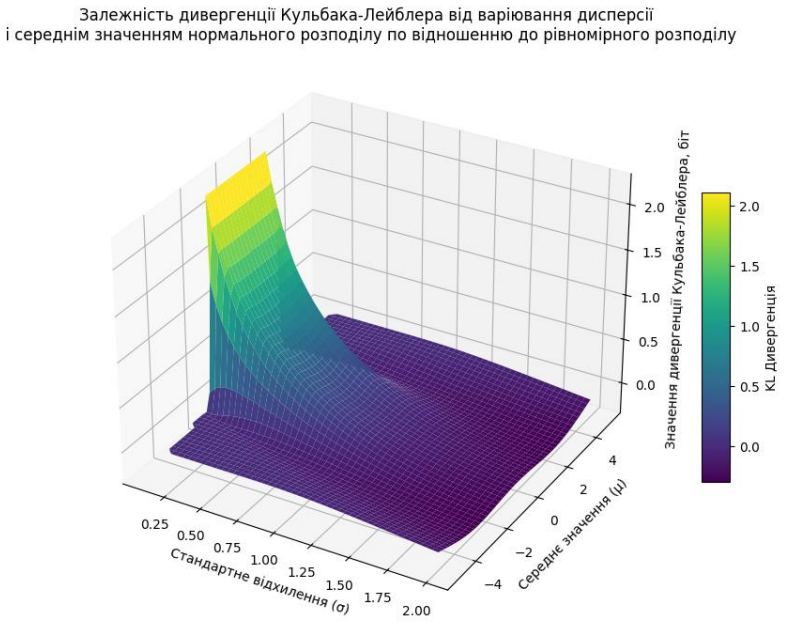

Рисунок 2 – залежність дивергенції Кульбака-Лейблера від показників нормального та рівномірного розподілу

Екстремальний режим відповідає максимальному значенню ентропії системи, яке має місце за умови переходу розподілу щільності ймовірності в рівномірний розподіл - тобто система переходить в стан максимальної невизначеності.

3.2 Імітаційне моделювання еволюції кіберінциденту

В ході роботи було проведено імітацію поведінки системи за різних значень показника швидкості відновлення (ефективності реагування). Результати моделювання наведено на рис. 3

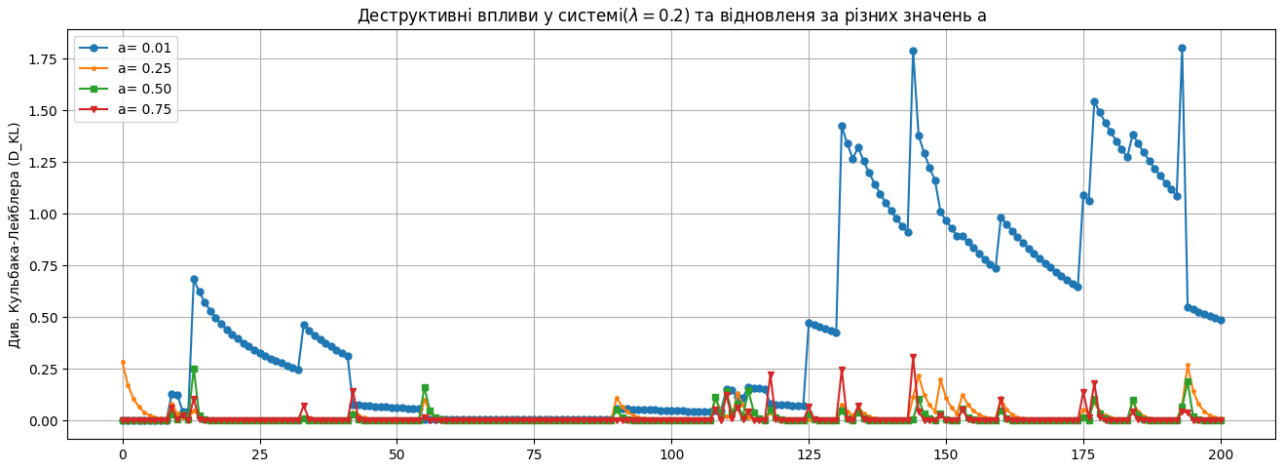

Рисунок 3 – Результати моделювання

Інтерпретація отриманих результатів:

1. Залежність між швидкістю відновлення та дивергенцією: для малих значень a (повільна швидкість відновлення) дивергенція D_{KL} досягає високих значень, що свідчить про сильну відмінність між станами системи "до" і "після" впливу. Це означає, що система довше перебуває у стані порушення, накопичуючи більшу різницю між розподілами. Для великих значень a (висока швидкість відновлення) дивергенція D_{KL} значно нижча, а максимуми стають менш вираженими. Це свідчить про те, що система швидше відновлюється після деструктивних впливів, зменшуючи розрив між розподілами "до" і "після".

2. Максимуми: періодичні піки для всіх значень а вказують на повторювані деструктивні впливи (наприклад, атаки або системні збої). Для повільної швидкості відновлення ($a = 0.01$), система довше "затримується" в стані порушення. При швидшому відновленні ($a = 0.75$), амплітуда максимумів значно нижча, що свідчить про швидке усунення наслідків впливу.

3. Значення для стабільності системи: малі значення a означають слабку здатність системи до відновлення після атак чи збоїв. Це призводить до тривалого дисбалансу і накопичення відмінностей між станами. Великі значення a свідчать про високу ефективність механізмів відновлення, що робить систему більш стійкою до деструктивних впливів.

4. Розподіли у контексті швидкості відновлення: графік підтверджує, що максимальна дивергенція досягається, коли швидкість відновлення низька ($a \to 0$), оскільки система довго перебуває у стані значних змін. При високих швидкостях відновлення (a ближче до 1), система швидко повертається до рівноваги, тому D_{KL} значно нижча.

Додатково в роботі досліджено залежність часу відновлення від умовної швидкості відновлення. Для цього було розглянуто сценарії зміни а від 0 до 1, результати моделювання представлено на рис. 4

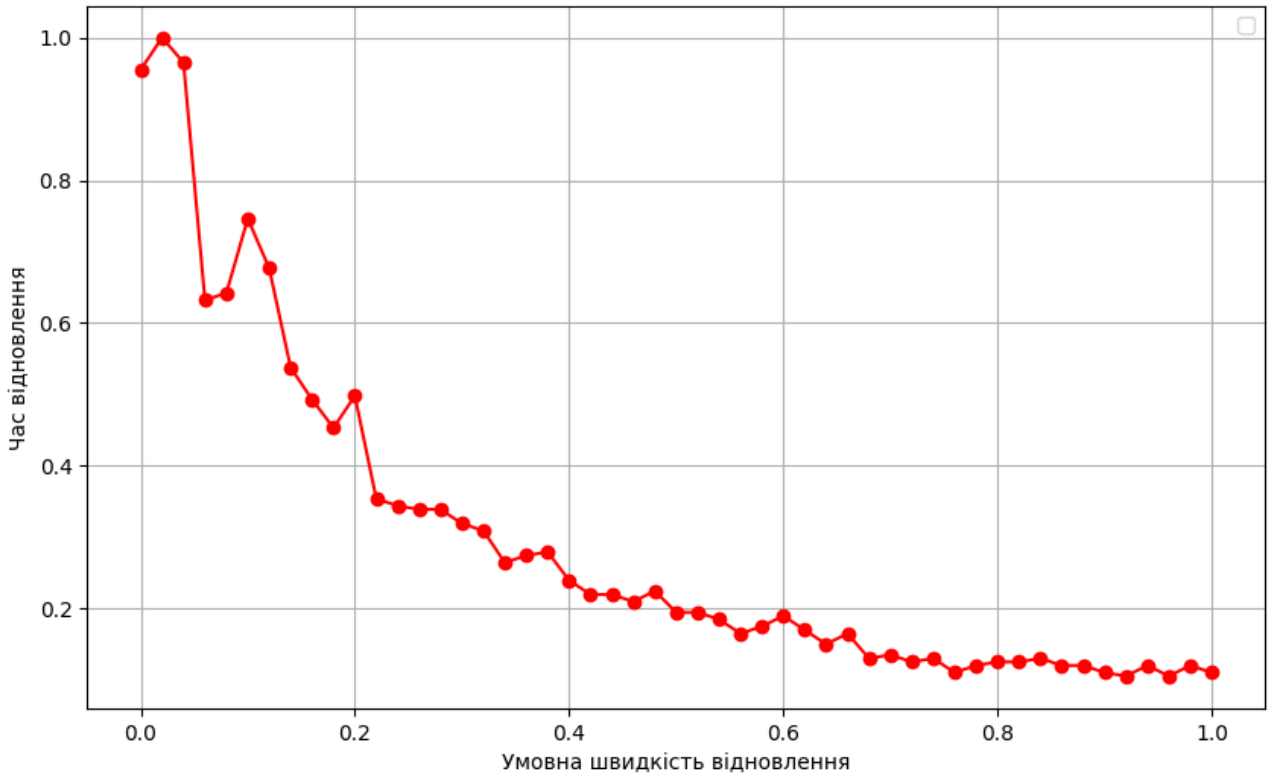

Рисунок 4 – Залежність часу від швидкості

За умови низьких α — час відновлення тривалий, за високих α— час відновлення швидко зменшується і стабілізується. Висока швидкість ($\alpha > 0.6$) забезпечує мінімальний час відновлення.

3.3. Синтез моделі реагування на кіберінциденти

На основі аналізу моделі еволюції кіберінциденту, а також оцінки впливу швидкості відновлення (a) на дивергенцію Кульбака-Лейблера (D_{KL}) та час вілновлення, можна запропонувати адаптивну модель реагування, що враховує поточний стан системи, інтенсивність впливу і швидкість відновлення. Модель базується на ключових етапах: виявлення, оцінка, адаптація, відновлення та превенція (фази відповідають працям Linkov)

Компоненти моделі

1. Виявлення

- Постійний моніторинг стану системи для виявлення аномалій у реальному часі.
- Використання метрик, схожих на D_{KL}, щоб оцінити відмінність між поточним

$$D_{KL} = \int P(x) \log \frac{P(x)}{Q(x)} dx$$

$P(x)$ станом системи та її нормальним функціонуванням: — реальний стан системи (розподіл метрик), $Q(x)$ — еталонний стан (наприклад, нормальний розподіл).

Інструменти, які дозволяють оцінити стани системи:системи SIEM (Security Information and Event Management, байєсові мережі та алгоритми виявлення аномалій, втоматичне обчислення дивергенцій для раннього попередження.

2. Оцінка впливу

- Визначення інтенсивності впливу на систему через:
  - Швидкість зміни стану системи (ааа).
  - Час перебування у порушеному стані (тривалість, коли D_{KL} перевищує певний поріг).
  - Здатність системи відновлюватися (швидкість зменшення D_{KL}).

Методи:

- Побудова моделі для аналізу стану системи:

$$\frac{dS(t)}{dt} = -\alpha S(t) + \beta I(t) dt,$$

де $S(t)$) — стан системи, α— швидкість відновлення , β — інтенсивність атаки ($I(t)$).

3. Адаптація та відновлення

- Динамічне управління параметром α (швидкістю відновлення) залежно від рівня пошкоджень, втрат та наявних ресурсів
- Застосування механізмів адаптивного відновлення:
  - Збільшення відновлювальних ресурсів (перерозподіл обчислювальної потужності).
  - Ізоляція пошкоджених частин системи (мережеве сегментування).
  - Пріоритетне відновлення критичних компонентів.

Умови:

- Якщо $D_{KL} > D_{threshold}$ (висока відмінність від нормального стану або перетин встновленого порогового значення), то підвищити α: прискорити відновлення через автоматизацію процесів та задіяння антиентропійних чинників (табл.6). Якщо D_{KL} поступово знижується, то перейти в режим стабілізації, де ресурси економляться для подальшого відновлення.

Таблиця 6 – чинники ентропії та антиентропії

Ентропійні чинники	Антиентропійні чинники
Поширення шкідливого програмного збезпечення	Кібергігієна співробітників
Людські помилки	Резервні копії
Відсутність актуальних оновлень	Оновлення обладнання
Відсутність плану реагування	Шифрування даних

4. Оновлення бази знань та превенція

- Використання отриманих даних для модифікації захисної стратегії системи.

- Зниження базової вразливості системи, що включає регулярне оновлення програмного забезпечення, вдосконалення механізмів розподілу навантаження, поглиблене навчання персоналу, забезпечення обміну інформацією між відповідальними підрозділами, аналіз та розслідування інциденту.

Прогнозування нових атак:

- Побудова моделей на основі машинного навчання для оцінки майбутніх ризиків.
- Симуляція потенційних кіберзагроз, в тому числі їх параметрів в контексті розробленої інформаційно-ентропійної моделі

Етапи реалізації моделі на практиці

1. Фаза підготовки:
   - Встановити базову швидкість відновлення α для нормального стану.
   - Визначити порогові значення $D_{threshold}$ для реакції системи.
2. Фаза реагування:
   - У момент інциденту оцінити значення та забезпечити постійний моніторинг D_{KL}.
   - Якщо $D_{KL} > D_{threshold}$, негайно підвищити α (наприклад, за рахунок перерозподілу ресурсів).
3. Фаза стабілізації:
   - Після досягнення стабільності (низьке D_{KL}) повернутися до базового стану α_0.
4. Фаза вдосконалення:
   - Аналізувати поведінку системи під час інциденту для оптимізації параметрів α та механізмів відновлення.

Математична формалізація моделі

Для опису зміни стану системи $S(t)$ під час інциденту:

$$\frac{dS(t)}{dt} = -\lambda(t)S(t) + \beta I(t)t,$$

де:

- $\alpha(t) = f(D_{KL}, \alpha)$— динамічна швидкість відновлення, залежить від D_{KL}.
- $I(t)$ — інтенсивність атаки.
- α — параметр адаптації, який змінюється для максимізації швидкості відновлення.

Очікувані результати

1. Зменшення тривалості впливу інцидентів:
   - Швидке реагування через адаптивне підвищення швидкості відновлення ааа.
2. Зниження загальної шкоди системі:
3. Покращення стійкості системи:
   - Оптимізована стратегія превенції для мінімізації майбутніх інцидентів.

Висновки до третього розділу

Синтезовано адаптивну модель реагування на кіберінциденти, яка базується на моніторингу, оцінці впливу, адаптації швидкості відновлення та превентивних заходах. Проведено імітаційне моделювання, яке підтвердило ефективність запропонованої моделі для мінімізації тривалості та впливу інцидентів.

ВИСНОВОК

Запропоновано новий підхід до аналізу кіберінцидентів, що базується на використанні інформаційної ентропії та дивергенції Кульбака-Лейблера для оцінки деструктивного впливу на інформаційні системи.

Розроблено математичну модель еволюції кіберінцидентів, яка враховує інтенсивність атак, швидкість відновлення та стан системи.

Синтезовано адаптивну модель реагування, яка забезпечує швидке повернення системи до рівноважного стану після атак.

Результати дослідження підтвердили можливість мінімізації шкоди від кіберінцидентів шляхом адаптації відновлювальних процесів та превентивних заходів.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. "Content." ELA.KPI.ua: веб-сайт. URL: http://surl.li/abikww. Accessed 24 Nov. 2024. (дата звернення: 14.10.2024)

2. "Класифікація моделей та вимоги до них." Wiki.cusu.edu.ua. веб-сайт. URL: http://surl.li/uadtes. Accessed 24 Nov. 2024. (дата звернення: 14.10.2024)

3. Новосьолов Д.С. Ентропійно-інформаційна модель кіберінциндентів. Моделювання, керування та інформаційні технології (MCIT–2024) : збірник праць учасників Міжнародної науково-практичної конференції, 2024. 367 с. (дата звернення: 15.10.2024)

4. Bianconi, G. (2009). Entropy of network ensembles. Physical Review E, 79(3), 036114. (дата звернення: 18.10.2024)

5. Cover, T. M., & Thomas, J. A. (2006). Elements of Information Theory (2nd ed.). Wiley-Interscience. (дата звернення: 16.10.2024)

6. EY. "Information Security Risk Management." EY: веб-сайт. URL: https://www.ey.com/en_gl/consulting/how-we-help-clients-protect-against-cyber-threats. (дата звернення: 14.10.2024).

7. FAIR: Factor Analysis of Information Risk – Модель аналізу ризиків: веб-сайт FAIR Institute(дата звернення: 20.10.2024)

8. Hollnagel, Resilience Engineering – Праця про стійкість систем: Resilience Engineering(дата звернення: 21.10.2024)

9. Iturriza, M., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2018). Modelling methodologies for analysing critical infrastructures. Journal of Simulation, 0, 1–16. (дата звернення: 14.10.2024)

10. Jensen & Nielsen, Bayesian Networks and Decision Graphs – Книга про байєсові мережі: веб-сайт. URL: Bayesian Networks and Decision Graphs(дата звернення: 25.11.2024)

11. Kleinrock, Queueing Systems – Класична робота про теорію масового обслуговування: веб-сайт. URL: Queueing Systems(дата звернення: 20.11.2024)

12. KPMG Ukraine. "How Businesses Can Protect Themselves Against Cyberattacks." KPMG: веб-сайт URL : https://home.kpmg/xx/en/home/insights/2020/10/cyber-security-protection.html. (дата звернення: 25.10.2024)

13. Lazarus Alliance. "Reactive vs. Proactive Cybersecurity: Benefits and Challenges." Lazarus Alliance: веб-сайт. URL: https://lazarusalliance.com/proactive-vs-reactive-security. (дата звернення: 29.10.2024).

14. Lemon School. "Cybersecurity: Current Threats and Protection Methods." Lemon School: веб-сайт. URL: https://lemon.school/blog/cybersecurity-current-threats-and-protection-methods. (дата звернення: 15.11.2024).

15. Lye & Wing, Game Theory for Cyber Security – Дослідження з теорії ігор у кібербезпеці: веб-сайт. URL: Game Theory for Cyber Security(дата звернення: 19.11.2024)

16. Macal & North, Agent-based Modeling and Simulation – Агентно-орієнтоване моделювання: веб-сайт. URL: Agent-based Modeling and Simulation(дата звернення: 25.11.2024)

17. Mitzenmacher, M., & Upfal, E. (2005). Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge University Press. (дата звернення: 17.11.2024)

18. NIST SP 800-30 – Національний інститут стандартів і технологій (NIST): веб-сайт. URL: NIST SP 800-30. (дата звернення: 17.10.2024)

19. Operations Research in Cybersecurity – Огляд застосування операційних досліджень у кібербезпеці: веб-сайт. URL: Operations Research in Cybersecurity. (дата звернення: 24.10.2024)

20. Pastor-Satorras & Vespignani, Epidemic Spreading in Networks – Дослідження поширення епідемій у мережах: веб-сайт. URL: Epidemic Spreading in Networks(дата звернення: 21.10.2024)

21. Ross, S. M. (2014). Introduction to Probability Models (11th ed.). Academic Press. (дата звернення: 26.11.2024)

22. Shannon, C. E. (1948). A mathematical theory of communication. Bell System Technical Journal, 27, 379–423. (дата звернення: 1.11.2024)

23. "Comparing the MITRE ATT&CK and NIST Cybersecurity Frameworks." ISACA: веб-сайт. URL: https://www.isaca.org/resources/news-and-trends/industry-news/2024/comparing-the-mitre-attck-and-nist-cybersecurity-frameworks. (дата звернення: 9.11.2024)

24. "CPS-VO: Cyber-Physical Systems Virtual Organization." CPS-VO: веб-сайт. URL: htt28ps://cps-vo.org/node/48788. (дата звернення: 6.11.2024).

25. "FLAIRS 2011 Conference Paper." AAAI: веб-сайт. URL: https://aaai.org/papers/flairs-2011-2532/. (дата звернення: 11.12.2024).

26. "SANS Institute: Information Security Training and Certification." SANS: веб-сайт. URL: https://www.sans.org/emea/. (дата звернення: 12.12.2024)

27. Amritraj, Manju. "IT Now: Technological Trends in Modern IT." Oxford Academic, 2023: веб-сайт. URL: https://academic.oup.com/itnow/article-abstract/64/2/38/6585369?redirectedFrom=fulltext&login=false. (дата звернення: 7.12.2024)

28. Makarov, Sergey, et al. "Expert modelling." ResearchGate: веб-сайт. URL: https://www.researchgate.net/publication/356601534_Expert_modelling. (дата звернення: 1.12.2024)

29. Mamun, M. A., et al. "Psychological Studies and Expert Modelling." Frontiers in Psychology, 2018: веб-сайт. URL: https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2018.00691/full. (дата звернення: 14.11.2024).

30. Park, Jisoo, et al. "Quantum Computing in Cybersecurity." IEEE Xplore: веб-сайт. URL: https://ieeexplore.ieee.org/document/9119914. (дата звернення: 28.10.2024).

31. Zhang, Hao. "A Study of Quantum Computing." arXiv, 2023: веб-сайт. URL: https://arxiv.org/abs/2308.14016. (дата звернення: 29.11.2024)

32. Zhang, Xian. "Study of Computational Algorithms." arXiv, 2023: веб-сайт. URL: https://arxiv.org/abs/2302.04413. (дата звернення: 30.11.2024)

Збірники тез	Моделювання, керування та інформаційні технології (*МСІТ*–2024) : збірник праць учасників Міжнародної науково-практичної конференції, 2024.
	Нові горизонти : збірник матеріалів Всеукраїнської науково-практичної конференції. Випуск IX / за заг. ред. О. В. Тригуби. Кременець : ВЦ КОГПА ім. Тараса Шевченка, 2024.
	Безпека, технології, інновації: нові горизонти: збірник праць учасників міжфакультетської науково-практичної інтернет-конференції здобувачів вищої освіти і молодих вчених, 12 листопада 2024 р. Житомир : Поліський національний університет, 2024.