Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему
Метод захисту корпоративних інформаційних систем від комплексних деструктивних впливів

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.220180.22.01.08 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 Підпис Голота І.О.

Керівник доц., к.т.н, доцент Підпис Орленко В.С.

Нормоконтролер старший викладач Підпис Мостовий С.В.

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц Підпис Кльоц Ю.П.

20 грудня 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Магістр

Галузь знань 12 Інформаційних технологій

Спеціальність 125 Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Голоті Ірині Олександрівні

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод захисту корпоративних інформаційних систем від комплексних деструктивних впливів

Керівник роботи Орленко Вікторія Сергіївна .

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проєкту (роботи) на кафедру 01.12.2023

3. Вихідні дані до проекту (роботи) Розробити модель функціонування захищеної КІС у умовах комплексних деструктивних інформаційних загроз, алгоритм реконфігурації системи захисту в залежності від результатів її роботи, розробити архітектура програмної системи адаптивного захисту корпоративної інформаційної системи.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз відомих методів захисту корпоративних інформаційних систем. Постановка задачі. Розробка моделі функціонування захищеної корпоративної інформаційної системи. Розробка алгоритму адаптивного захисту корпоративної інформаційної системи від комплексних деструктивних впливів. Розробка архітектури системи адаптивного захисту. Формування рекомендацій щодо підвищення ефективності захисту корпоративних інформаційних систем до системи управління. Оцінка ефективності роботи системи. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)_____

_____

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

7. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – аналіз відомих методів захисту корпоративних інформаційних систем, постановка задачі	18.09.2023	
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	02.10.2023	
5	Робота над розділом 3 – розробка методу адаптивного захисту корпоративної інформаційної системи	16.10.2023	
6	Робота над розділом 4 – розробка системи адаптивного захисту корпоративної інформаційної системи	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	06.12.2023	

Студент _____ І.О. Голота
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ В.С. Орленко
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод керування безпекою мобільних пристроїв в корпоративних мережах.

Автор роботи: Голота Ірина Олександрівна

Керівник роботи: к.т.н., доц. Орленко Вікторія Сергіївна

Загальний обсяг роботи: 79 сторінок, 19 рисунків, 12 таблиць, 1 додаток, 51 посилання.

Ключові слова: корпоративна інформаційна система, комплексний деструктивний вплив, адаптивний захист, реконфігурація системи.

Для досягнення мети в роботі були сформульовані та вирішені наступні завдання: розроблено моделі функціонування захищеної корпоративної інформаційної системи, алгоритм адаптивного захисту корпоративної інформаційної системи від комплексних деструктивних впливів, архітектуру системи адаптивного захисту. Надано рекомендації щодо підвищення ефективності захисту корпоративних інформаційних систем до системи управління.

Здобуті результати мають практичне значення в контексті побудови захисту корпоративних інформаційних систем.

19.12.23

ANNOTATION

Theme of qualification work: Method of managing the security of mobile devices in corporate networks.

Author of the work: Golota Iryna Oleksandrivna

Mentor: Ph.D., Assoc. Orlenko Viktoriya Serhiyivna

Total volume of work: 79 pages, 19 figures, 12 tables, 1 appendix, 51 references.

Keywords: corporate information system, complex destructive influence, adaptive protection, system reconfiguration.

To achieve the goal, the following tasks were formulated and solved in the work: models of functioning of the protected corporate information system, algorithm of adaptive protection of the corporate information system from complex destructive influences, architecture of the adaptive protection system were developed. Recommendations are given to increase the effectiveness of the protection of corporate information systems to the management system.

The obtained results are of practical importance in the context of building the protection of corporate information systems.

19.12.23

ЗМІСТ

ВСТУП

Один із найважливіших класів інформаційних систем, які підлягають захисту від комплексних деструктивних впливів, - це корпоративні інформаційні системи (КІС). Ефективність багатьох сучасних підприємств і організацій в значній мірі залежить від їх успішної функціонування. Ці масштабовані системи призначені для комплексної автоматизації всіх видів господарської діяльності компаній та корпорацій, які вимагають єдиної управлінської системи. Такі системи часто базуються на глибокому аналізі даних, широкому використанні систем підтримки прийняття рішень, електронному обігу документів та діловодства. Вони мають певну специфіку як об'єкти захисту від комплексних деструктивних інформаційних впливів, які постійно вдосконалюються.

Масштабні мережеві атаки на інформаційну інфраструктуру підприємств та країн не є рідкістю. Досить часто проводяться DDoS-атаки значної потужності проти комерційних та урядових організацій. Такі атаки можуть не лише паралізувати ресурси організації, але й створити перешкоди в глобальній мережі або, принаймні, на значній її частині. У 2021 році зафіксовано атаку з потужністю 1,5 Тбіт/с, а потужність атак має тенденцію до зростання. Ще однією метою зловмисників є хмарна інфраструктура. Хмарні технології використовуються в освіті, науці, банківській сфері. Сервіси, такі як Amazon, Google, Dropbox, налічують не лише сотні мільйонів приватних користувачів, але і пропонують корпоративні облікові записи організаціям. Несанкціонований доступ зловмисника до хмарних сховищ дозволяє йому отримати не лише дані про користувачів (включаючи таку інформацію, як реквізити платіжних карт, паролі від облікових записів, копії посвідчень особи), але і дані, що складають комерційну і навіть, можливо, державну таємницю.

Незважаючи на прийняті заходи для захисту корпоративних інформаційних систем від таких комплексних деструктивних впливів, їхня поширеність не зменшується. Постійне розширення функціональності інформаційних систем та

зростання залежності від інформаційної інфраструктури створює ситуацію, коли атаки на цю інфраструктуру можуть мати наслідки, подібні наслідкам терористичної активності.

Об'єкт дослідження: системи захисту корпоративних інформаційних систем

Предмет дослідження: моделі, методи та алгоритми захисту корпоративних інформаційних систем від комплексних деструктивних впливів.

Мета дослідження: підвищення захисту корпоративних інформаційних систем від комплексних деструктивних впливів.

Завдання дослідження: на основі моделі захисту корпоративної мережі від комплексних деструктивних впливів розробити метод оцінювання ефективності захисту корпоративних інформаційних систем від комплексних деструктивних впливів; розробити метод адаптивного захисту корпоративної інформаційної системи від комплексних деструктивних впливів; створення рекомендацій щодо підвищення ефективності захисту корпоративних інформаційних систем від комплексних деструктивних впливів.

1 ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД КОМПЛЕКСНИХ ДЕСТРУКТИВНИХ ВЛИВІВ

1.1 Мета, завдання та можливості захисту корпоративних інформаційних систем

Відомо, що корпоративні інформаційні системи (КІС) призначені для комплексної автоматизації всіх видів діяльності корпорацій (великих і середніх підприємств, організацій). Успішність управління цими підприємствами, досягнуті ними економічні, соціальні та інші результати, в значній мірі залежать від ефективності сучасних КІС. Тим часом, на саму ефективність КІС суттєвий вплив мають заходи, що вживаються для захисту їх від комплексних деструктивних інформаційних впливів (КДВ). Захист від таких загроз дозволяє знижувати можливі ризики порушення безпеки, однак це також може призводити до значних витрат на забезпечення безпеки. Бажано, щоб був збережений баланс між рівнем наданої захисту КІС у конкретних умовах і витратами на її забезпечення. З урахуванням цього мети і завдання захисту КІС від КДВ можуть значно відрізнятися в залежності від утворених умов. У деяких випадках основними цілями захисту КІС може бути максимальне зниження можливих ризиків, як для самих цих систем, так і для забезпечуючих прикладних процесів. В інших випадках можуть ставитися завдання зниження витрат на сам захист при забезпеченні заданого рівня функціонування КІС та підприємства. Досягнення цих цілей залежить від багатьох факторів, включаючи класи захищених КІС. Серед КІС виділяють автоматизовані системи управління підприємством (АСУП), корпоративні інтелектуальні простори (КІС), кіберфізичні простори (КФП). Такі системи використовують сучасні методи та засоби ІКТ - реляційні та NoSQL- бази даних, комп'ютерну графіку, сервіс-орієнтовану архітектуру (СОА), CASE-технології. Концепції та засоби реалізації КІС динамічно розвиваються і набувають рис, характерних для

систем Industry 4.0 [1-3]. Також ERP реалізуються на засадах відкритих систем [4-5].результатів атаки. Якщо результати оцінки свідчать про неуспішність функціонування, то ботнет стає неефективним, і всі ресурси, витрачені на попередні етапи, залишаються марними.

Наприклад, корпоративний інтелектуальний простір у якості класу КІС є сервіс-орієнтованою інфраструктурою для забезпечення можливості спільного доступу до інформації за допомогою різних пристроїв [6]. Однією з областей використання інтелектуальних просторів є розвиток інформаційної інфраструктури підприємств, що дозволяє користувачам (співробітникам та гостям підприємства) взаємодіяти з цією інфраструктурою та отримувати доступ до ряду корпоративних сервісів (наприклад, до сервісів корпоративного телебачення, довідкової системи, відеоконференцзв'язку). Ефективність роботи цих сервісів в різних умовах може оцінюватися за допомогою відомих показників якості обслуговування (Quality of Service, QoS) та якості сприйняття (Quality of Experience, QoE).

У літературі [7-8] запропоновані об'єктивні та суб'єктивні визначення QoE. Об'єктивне QoE визначає якість сприйняття, надану користувачеві інформаційної системи з точки зору вимірюваних показників продуктивності послуг, мережі та додатків. Суб'єктивне QoE визначає якість, сприйняту користувачем з позиції отримуваних ним емоцій, білінгу послуг та відповідності досвіду його взаємодії з системою.

У роботах [9-10] наводиться така оцінка для сервісу корпоративного телебачення, а в [11] також враховуються умови функціонування такого сервісу в середовищі "Інтернету речей". Такі характеристики відображають частку виконаних користувачем завдань і ступінь їх виконання, часові затримки, актуальність виконання завдань та інші подібні величини.

Забезпечення інформаційної безпеки комп'ютерних інформаційних систем (КІС) передбачає збереження цілісності, доступності та конфіденційності інформації, що знаходиться в КІС. Це дозволяє досягати прийнятних значень показників якості обслуговування і сприйняття. Для забезпечення

конфіденційності інформації використовують відомі моделі розділення доступу, методи ідентифікації, аутентифікації та авторизації, а також криптографічні методи захисту інформації [12-15]. Контроль цілісності ґрунтується на хешуванні, електронно-цифровому підписі та резервному копіюванні [16-18]. Для забезпечення доступності інформації використовують системи безперебійного живлення, резервне копіювання та розподіл потужностей для забезпечення необхідної пропускної здатності [19-20]. Ці методи є екстенсивними, і їх реалізація вимагає збільшення витрат, а в деяких випадках такі методи неможливо впровадити через обмежену можливість людини сприймати інформацію. Наприклад, коли йдеться про інтерактивне корпоративне телебачення в багатокористувацькому середовищі, неможливо задовольнити одночасні запити користувачів на отримання різної інформації без часткової втрати доступності. Процес взаємодії користувачів та КІС має ряд особливостей, які слід враховувати при їх захисті від кіберзагроз.

Основні характеристики включають наступне:

– Універсальність. Система інтегрована у своє оточення, і процес взаємодії не обмежується окремою точкою доступу. Це дозволяє забезпечити зручний та природний спосіб комунікації. З точки зору безпеки це означає, що інформація надходить в систему через численні розподілені канали доступу, що збільшує ризики використання загроз, але водночас створює додаткові можливості для аналізу отриманої інформації з різних джерел з точки зору достовірності та протирічливості.

– Сервіс-орієнтована архітектура. КІС є набором слабко зв'язаних, відносно незалежних мікросервісів, що вирішують окремі задачі.

– Цілісність. Сервіси працюють в єдиному інформаційному просторі, спрямовані на вирішення загальних завдань КІС (забезпечення зв'язку, поширення інформації, збір даних).

– Гетерогенність. Система включає компоненти, які відрізняються типом апаратного та програмного забезпечення, пропускною здатністю та використовуваними протоколами, що негативно впливає на вразливість системи. У

[21-22] відзначається складність побудови уніфікованих моделей для вивчення таких систем.

– Відкритість. Система динамічно включає нові компоненти, такі як мобільні пристрої користувачів, які можуть працювати з помилками або бути джерелом загрози, що потрібно враховувати при розробці методів забезпечення інформаційної безпеки.

– Багатомодальність. Різні модальності (програмні, мовленнєві, жести) характеризуються різними ймовірностями помилкового сприйняття та можливостями успішного підроблення інформації, але в багатомодальних системах можна знижувати ці ймовірності за допомогою інтегрованих методів обробки інформації.

– Велика кількість користувачів. Різні користувачі можуть конкурувати за ресурси сервісів і створювати протиріччя в запитаннях, тому необхідно вирішувати завдання пріоритизації запитань, яка враховує їхню достовірність і відсутність протиріччя.

– Розподіленість. Архітектура системи передбачає просторовий розподіл компонентів, причому система може досягати масштабу міст [23], а також складатися з компонентів, що знаходяться в різних країнах і на різних континентах.

– Врахування просторового і часового зв'язку. Для коректної оцінки властивостей отриманої інформації необхідно оцінювати не тільки її зміст, але і просторовий і часовий контекст, який впливає на її достовірність. Інформація, як правило, є достовірною не сама по собі, а в певному контексті, який включає простір, час або інші фактори, які можуть не вказуватися або в метаданих інформаційного об'єкта, або в його метаданих. Без врахування цього існує високий ризик отримати хибну оцінку інформації, що, в свою чергу, може вплинути на оцінку її джерела.

Як приклади загроз доступності інформації в КІС можуть виступати:

– Цілеспрямовані деструктивні впливи на КІС за допомогою недостовірної чи некоректної інформації. У цьому випадку джерелом загрози є

користувач КІС, який може бути як легітимним, так і нелегітимним. Типовим прикладом реалізації такої загрози є атака "відмова в обслуговуванні" (DoS), зокрема, атака розподіленої відмови в обслуговуванні (DDoS), що генерується мережами інфікованих комп'ютерів (ботнетами) [24-25].

– Ненамірені впливи на КІС в умовах отримання великої кількості запитів від користувачів, які не можуть бути виконані сервісами КІС у строк, при якому актуальність заявок зберігається. У цьому випадку джерелом загрози є легітимний користувач КІС. Приклад реалізації загрози – вичерпання пропускної здатності каналу передачі даних при виникненні ефекту "flash crowd" [26-27].

– Помилкове сприйняття сервісами КІС надходячих запитів. Ця загроза ймовірна при використанні багатомодальних засобів людино-машинного взаємодії - при взаємодії з сервісами за допомогою мови, жестів, розпізнавання образів на відео. Також загроза може реалізуватися через помилки в клієнтському чи серверному програмному забезпеченні. Джерелом загрози є програмне забезпечення КІП. Обробка сервісами помилково сприйнятих даних негативно впливає на доступність сервісів для легітимних користувачів. Зазвичай реалізація загрози виявляється у аномаліях мережевого трафіку [28].

Аномалії мережевого трафіку можуть мати різні причини і бути пов'язані з діяльністю хакерів, некомпетентними користувачами, несправністю обладнання та дефектами програмного забезпечення. Аномалії можуть бути видимими і проявлятися безпосередньо в некоректній роботі інформаційно-обчислювальної системи, або можуть не мати видимих ознак, але призвести до збоїв через тривалий час. Вони можуть бути пов'язані як із атаками, так і з некоректною або недостовірною інформацією [29-30]. Крім того, слід враховувати змінливість умов функціонування ІОС, пов'язану зі зміною складу користувачів, даних, сервісів, програмних та апаратних компонентів системи, а також зміною множини загроз і їх джерел. Для врахування цих умов необхідно забезпечити адаптивність засобів захисту. Наприклад, автори [31-33] описують біоінспірований гібридний підхід до побудови засобів захисту інформації, адаптивність яких відображена у розділенні

функцій захисту на імунні, що перевіряють форму представлення інформації, і рецепторні, які реалізують взаємодію з середовищем та накопичення досвіду. Таким чином, для забезпечення оптимальної якості обслуговування користувачів в ІОС необхідно вдосконалення систем і розробка адаптивних методів захисту від КДВ, які враховують особливості умов функціонування.

1.2. Особливості інформаційних загроз корпоративним інформаційним системам

Для конкретизації загроз, які є актуальними для корпоративних інформаційних систем (КІС), необхідно розглянути можливі джерела цих загроз. Джерела загроз систематизовані на рис. 1.1.

Рисунок 1.1 - Класифікація джерел загроз

Загрози, у свою чергу, розподіляються за наступними критеріями:

- за джерелом;
- за аспектом ІБ (цілісність, доступність, конфіденційність);
- за цільовим компонентом системи (АО, СПО, ППО). Таким чином, загрози можна узагальнити у таблицю 1.1.

Таблиця 1.1 - Загрози КІС

Джерело	Аспект	Мета	Загрози	Події ризику
1	2	3	4	5
Оператор	Цілісність	Системне ПЗ	Неправильні дії в адміністративному інтерфейсі	Втрата даних
Гість	Доступність	СПЗ	Не виконані запити	Недоступність керування для інших користувачів
Несанкціонований користувач	Цілісність	Прикладне ПЗ	Ін'єкція (SQL)	Втрата чи модифікація даних
	Доступність	ППЗ	Ін'єкція (XSS)	Недоступність адміністративного інтерфейсу
		Апаратне забезпечення, СПЗ, ППЗ	DoS, DDoS	Недоступність інтерфейсів завантаження даних
	Конфіденційність	ППЗ	Використання вразливостей в автентифікації (недостатня автентифікація, індексація каталогів і т. д.)	Крадіжка ідентифікаційних даних
Системне ПЗ	Доступність	ППЗ	Відмова	Неможливість роботи сервісу
Сервісне ПЗ	Доступність	ППЗ	Дефект	Некоректна робота сервісу

Кінець таблиці 1.1

1	2	3	4	5
Нелегітимне ПЗ	Доступність	АЗ, СПЗ, ППЗ	Виснаження програмних або апаратних ресурсів	Недоступність інтерфейсів або сервісу в цілому
	Цілісність	АЗ, СПЗ, ППЗ	Несанкціонований доступ	Втрата даних
	Конфіденційність	ППЗ	Несанкціонований доступ	Крадіжка ідентифікаційних даних
	Доступність, Цілісність, Конфіденційність	ППЗ	Організація каналів обміну інформацією	Втрата, крадіжка даних
Апаратне забезпечення	Доступність, Цілісність	ППЗ	Збій живлення	Неможливість роботи сервісу, втрата даних
Мережеве апаратне забезпечення	Доступність	ППЗ	Відмова	Недоступність інтерфейсів
	Конфіденційність	ППЗ	Перехоплення трафіку	Крадіжка ідентифікаційних даних
Апаратне забезпечення зберігання даних	Доступність	ППЗ	Відмова	Неможливість роботи сервісу
	Доступність	ППЗ	Відмова	Втрата даних
Апаратне забезпечення обробки даних	Доступність	ППЗ	Відмова	Неможливість роботи сервісу

Важливо відзначити, що у значній кількості випадків загрози вразливі одразу кілька компонентів системи та аспектів інформаційної безпеки. Такі загрози називають комплексними. При забезпеченні безпеки слід надавати пріоритет саме цим загрозам, оскільки вони стають все поширенішими у зв'язку із зростанням складності захищених систем та є більш загальним класом порівняно з конкретними загрозами.

1.3. Відомі системи захисту корпоративних інформаційних систем від комплексних деструктивних інформаційних впливів.

В загальному існує велика кількість систем, які дозволяють проводити оцінку властивостей надходження інформації. Для аналізу таких систем використовуємо наступні критерії:

а) Архітектурні:
   1) Розширюваність;
   2) Наявність відкритого коду;
   3) Залежність від інших систем.

б) Функціональні:
   1) Тип оброблюваної інформації;
   2) Тип виявлюваних загроз;
   3) Робота з розподіленими системами;
   4) Використані методи;
   5) Можливості врахування контексту.

До систем, які виконують виявлення аномалій у вхідному потоці інформації, належать Snort.AD і Cerberus. Розглянемо ці системи детальніше. На рис. 1.2 показана структура системи Snort.AD:

Система включає в себе препроцесор (AD Preprocessor - збір даних про трафік та видача попереджень), генератор профілів (AD Profile Generator - прогнозування трафіку) та модуль оцінки профілю (AD Evaluator - порівняння передбачених даних з реальними). Препроцесор читає зразок (передбачені об'єми трафіку) з файлу "профіль" і генерує тривогу, якщо поточне значення виходить за межі допустимого (тобто не знаходиться в межах від мінімуму до максимуму). Здійснюється збір таких даних: кількість пакетів TCP, UDP, ICMP (як загальна кількість, так і кількість вхідних та вихідних), кількість таких же пакетів з власної підмережі, кількість пакетів TCP з прапорцями SYN/ACK, кількість вхідних та вихідних пакетів WWW (під цим розуміються TCP-пакети на стандартний порт 80), кількість

вхідних/вихідних пакетів DNS (UDP на 53), кількість запитів та відповідей ARP, кількість пакетів не-TCP/IP, швидкості трафіку по всіх цих складових трафіку.

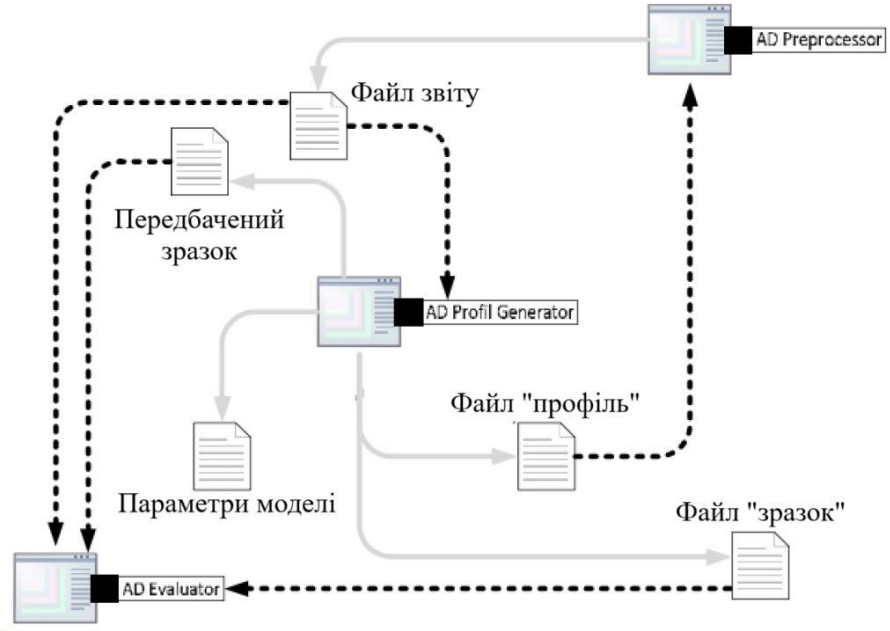


Рисунок 1.2 - Схема Snort.AD системи (Сіра стрілка позначає, що модуль записує дані в файл, пунктирна - що модуль читає з файлу)

Основними обмеженнями Snort.AD є те, що він не враховує значущі компоненти контексту інформації (простір, ідентифікатор користувача), а також аналізує виключно сигнальну інформацію у форматі часових рядів та лише інформацію про мережевий трафік. Якщо другу проблему можна вирішити за допомогою розробки додаткових модулів збору та аналізу інформації, то перша породжує архітектурні проблеми в області інтеграції даних з різних вузлів КІП.

Система Cerberus [34], навпаки, оптимізована для розподілених систем і дозволяє максимально враховувати контекст отриманої інформації. Наприклад, оцінка достовірності аутентифікації користувача може бути різною залежно від контексту. Однак у Cerberus розглядається лише інформація про аутентифікацію. Крім того, Cerberus може дозволяти чи забороняти доступ до ресурсів залежно від статусу аутентифікації, але не враховує можливість конфліктів доступу.

Фреймворк ConSec також розглядає контекст в КІП, але захищає лише

комунікаційний процес між компонентами системи.

У роботі [35] розглядаються питання захисту інтелектуальних просторів на основі платформи Smart-M3, але розглядається лише аспект аутентифікації та надання доступу до даних.

Узагальнимо розглянуті системи в таблицю 1.2. У цілому аналіз існуючих систем та фреймворків показує, що їхньою метою є захист конфіденційності та забезпечення високої точності при аутентифікації користувачів. При цьому питання забезпечення доступності при великій кількості користувачів, які легітимні, але користуються різною ступенем довіри, розглядаються лише в Snort у контексті протидії DDoS-атакам. Однак Snort має дуже обмежені можливості врахування контексту та роботи в багатокористувацьких системах.

Таблиця 1.2 - Системи забезпечення ІБ КІС

Критерії	Системи			
	Snort.AD	Cerberus	ConSec	Semantic security framework
1	2	3	4	5
Функціональні:				
тип інформації	Тільки часові ряди	Аутентифікаційні дані та контекст	Аутентифікаційні дані та контекст	Аутентифікаційні дані та контекст
Методи обробки	Математична статистика	Логічне виведення	?	Онтології, логічне виведення
тип загроз	DoS, DDoS	НСД	НСД	НСД
розподіленість	ні	так	так	Так
контекст	не повністю	так	так	так
Архітектурні:				
відкритий код	Так	?	-	-

Кінець таблиці 1.2

1	2	3	4	5
Архітектурні:				
Масштабованість	Так	-	-	-
Залежності	ні	Gaia		Smart-M3

Отже, поки не існує систем та фреймворків, що повністю відповідали б вимогам. Тим не менше, багато методів, які використовуються у цих системах і опубліковані в науковій літературі, можна застосовувати для вирішення поставлених завдань.

1.4 Відомі методи захисту корпоративних інформаційних систем від комплексних деструктивних інформаційних впливів

У зв'язку з наявністю у КІС гетерогенних програмних та апаратних компонентів, а також бататомодальних інтерфейсів, інформація, що надходить від користувачів, є різноманітною. Методи аналізу властивостей цієї інформації відрізняються, і їх застосування залежить переважно від типу інформації. Тип інформації в значній мірі визначається не самою інформацією, а способом її сприйняття. Таким чином, одна й та ж інформація може відноситися до різних типів. У КІП використовуються наступні типи інформації:

– Сигнальна – інформація подається як окрема команда від одного компонента до іншого;

– Структурна – інформація представлена як набір організованих елементів (наприклад, у вигляді JSON- або XML-структур);

– Текстова – інформація у вигляді послідовності текстових символів;

– Медіа – інформація представлена аудіо, відео або зображенням;

– Комбінована – інформація містить кілька логічно пов'язаних компонентів, можливо, різних типів.

Відомі методи [36-37] можна розглядати як класифікацію, зображену на рис. 1.3.

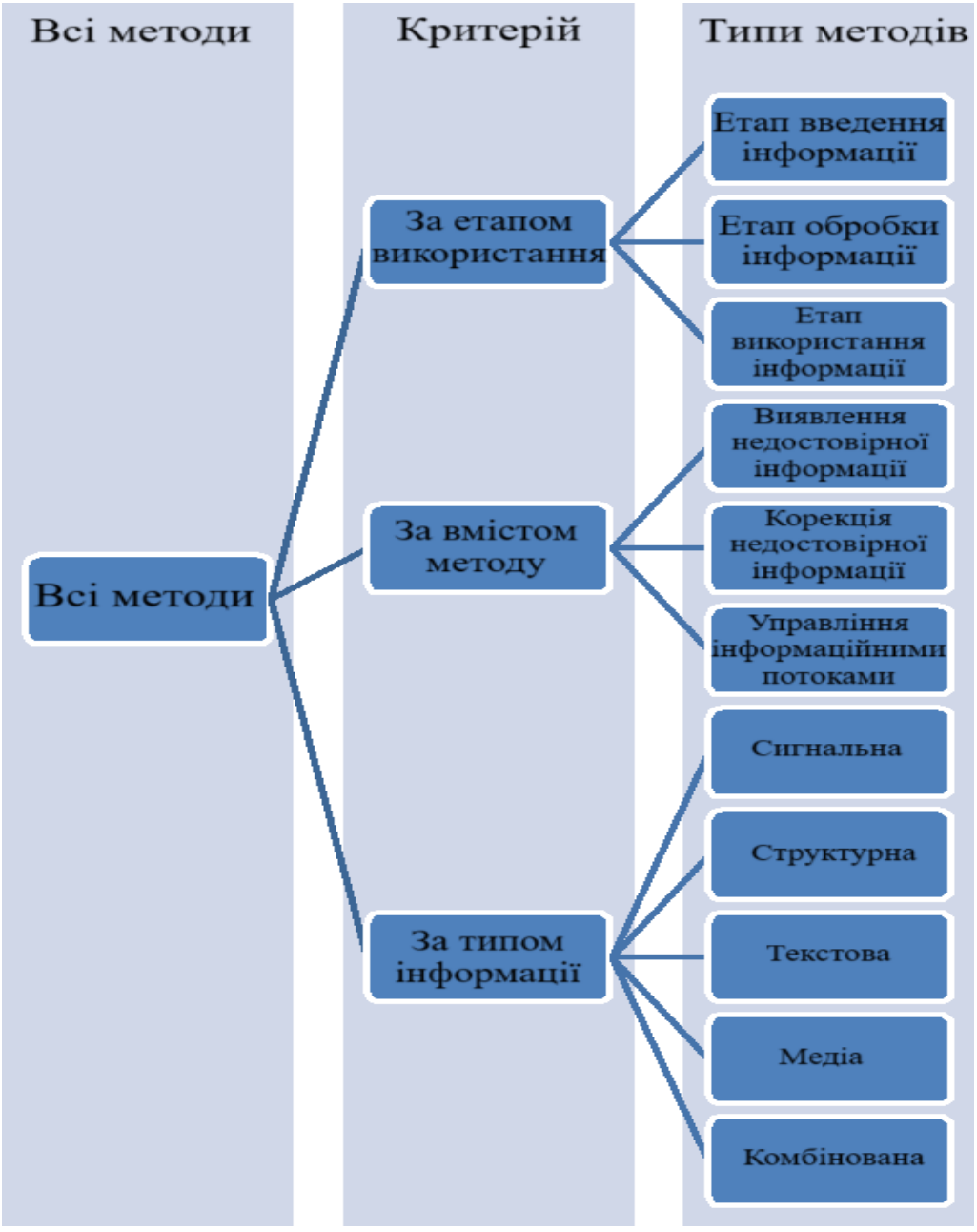


Рисунок 1.3 - Класифікація методів аналізу інформації

Розглянемо більш детально методи обробки інформації з метою забезпечення інформаційної безпеки КІП в залежності від типу надходячої інформації. Деякі методи обробки сигнальної інформації наведено в таблиці 1.3.

Таблиця 1.3 - Методи аналізу сигнальної інформації

Метод	Обчислювальна складність	Інші особливості	Використовувані метрики
1	2	3	4
На основі розподілів			
пороговий аналіз	низька	необхідність обґрунтування вибору значень порога	Кількість пакетів або байт
обчислення коефіцієнтів відстані та подібності між розподілами	висока; застосовуються паралельні обчислення	розглядається відмінність атак від масового легального трафіку	Кількість пакетів із загальною властивістю (наприклад, адреса джерела, розмір)
модель гауссівських сумішей	висока	виконується розрахунок розподілу трафіку та розкладання його на гауссівські компоненти; нерозкладний трафік вважається недостовірним	Відношення вхідного трафіку до вихідного
модель на базі Simple Network Management Protocol	низька	Метод дозволяє враховувати сесії та потоки. Зазначається, що облік потоків ведеться роутерами, що полегшує збір даних.	Відношення SYN/FIN; i/o відносини для UDP та ICMP
Моделі на основі частотності протоколів та прапорів	низька		Частотності прапорів та протоколів, їх співвідношення

Продовження таблиці 1.3

1	2	3	4
На основі ентропії			
обчислення різниці ентропій	висока; обробка даних має бути розподіленою та багатопоточною	необхідно обґрунтування вибору порогів	Можливості пакетів із заданою адресою джерела, призначення або розміром
обчислення різниці ентропій	середня, ускладнюється	виконується аналіз окремих сесій;	Швидкість виконання
	необхідністю сортувати пакети за сесіями	використовується шаблон; необхідно обґрунтувати вибір порогів	запити, час перегляду сторінки (для кожної сесії)
ентропія розраховується для пакетів, які мають відношення до TCP-рукостискання (SYN, ACK, RST)	проста		Кількість TCP пакетів із прапорами SYN, ACK, RST, FIN для кожної сесії
На основі машинного навчання			
метод опорних (поворотних) точок	висока	виконується багаторівневе вилучення параметрів трафіку	Частота пакетів, швидкість даних, частоти прапорів SYN, FIN, RST
розрахунок частот різних прапорів, допустимі межі частот визначаються методом машинного навчання	проста за умови, що виконано навчання	використовуються FIN, ACK та SYN прапори у вхідних та вихідних пакетах; розглядається можливість вивчення решти прапорів	Відношення частот прапорів FIN та SYN; частот SYN та ACK

Кінець таблиці 1.3

1	2	3	4
На основі вейвлет-аналізу			
Виявлення вторгнень на основі вейвлет-аналізу мережевого трафіку	середня		Швидкість передачі даних (у байтах та пакетах), рівень завантаження процесора
На основі нечіткої логіки			
Модель виявлення DDoS-атак	середня		Частоти протоколів та TCP-прапорів

Ці методи спрямовані на обробку мережевого трафіку, але при цьому багато з них використовують закономірності, що є характерними для потоків подій. Таким чином, методи, які не жорстко прив'язані до структури мережевих протоколів, можна адаптувати для фільтрації сигнальної інформації. Таким чином, методи можуть бути використані для аналізу сигнальної інформації.

Також розроблено достатньо багато методів аналізу достовірності мультимедійної інформації. Така інформація надходить в КІП через багатомодальні інтерфейси і камери і може використовуватися зловмисником для введення системи в оману. Крім того, така інформація піддавана перешкодам, оскільки вимагає більше значущих мережевих та обчислювальних ресурсів для передачі та обробки порівняно із сигнальною інформацією. Розглянемо відомі методи більш детально.

У роботах [38-41] розглядається метод виявлення прийомів копіювання та вставки в зображеннях. Цей метод ґрунтується на артефактах, що виникають у вейвлет-аналізі зображення при порушенні його цілісності. Метод дозволяє виявляти факт втручання, а також встановлювати модифіковані області. Відомі методи пасивного виявлення модифікованих відеозаписів, що ґрунтуються на

виявленні таких ознак, як багаторазова компресія відеопотоку, виявлення модифікованих областей та виявлення міжкадрового підроблення (inter-frame forgery). Наприклад, до останнього класу відноситься метод, в якому в якості ознак втручання виступають значення помилок квантування.

Оскільки формально відеозапис складається зі зображень (кадрів) та аудіопотоку, у деяких випадках аналіз відео може бути розглянутий як дві окремі задачі. Проте такий підхід не враховує динаміку відеозапису – взаємозв'язку рухомих об'єктів між собою та із звуковим потоком, що може надавати додаткову інформацію. З урахуванням цього, в [42-43] для підвищення точності розпізнавання об'єктів використовується аналіз послідовних серій кадрів. У роботі [44] запропонований метод машинного навчання, який дозволяє розпізнавати вирази обличчя. У цьому методі обробляються одночасно аудіо- та відеопотоки. Крім того, глибоке навчання дозволяє виявляти емоції людини за її обличчям, які характерні для неправдивих висловлювань, страху, радості, гніву.

У більшості робіт, присвячених аналізу достовірності текстової інформації, використовуються:

– фактологічний метод, що ґрунтується на семантичному аналізі контенту, витяганні з нього елементарних фактів та порівнянні їх із зразковими образцями (перевірка на протиріччя);

– стилістичний аналіз та методи, спрямовані не на виявлення фактів, а на аналіз форми їх вираження, що дозволяє робити висновки про об'єктивність, достовірність та компетентність представлення інформації;

– підхід, заснований на аналізі метаданих, що дозволяє залучати додаткову інформацію про контент (його походження, зв'язок з іншими зразками, форму представлення).

До фактологічного підходу можна віднести дослідження [45]. У ньому запропоновано оцінку достовірності веб-ресурсів на основі перевірки коректності фактів, що містяться в ресурсі. Факти автоматично витягаються з ресурсу за допомогою методів, які використовуються для створення баз знань. Визначення

неправдивості фактів на веб-ресурсах передбачається за допомогою спільного логічного виводу та багаторівневої ймовірнісної моделі. Джерела, які містять менше неправдивих фактів, вважаються надійними.

У роботі [46] розглядається питання використання контекстно-залежних рекомендаційних систем для аналізу документів на основі подібності. Особливістю запропонованого підходу є використання гібридного методу фільтрації та метрик подібності, що визначають взаємини в парах документів. Це дозволило врахувати як змістовний аспект документів, так і особливості сторони, яка робить запит. Застосований апарат онтологічного моделювання, що дозволяє виявляти протиріччя в документах і на їх основі виявляти недостовірну інформацію.

У роботі [47] вивчаються евристичні принципи, які людина використовує для визначення достовірності інформації, отриманої з мережі. Автори розглядають фактори репутації ресурсу, його підтримки іншими користувачами, узгодженості з іншими ресурсами, а також суб'єктивні аспекти, пов'язані з апріорною інформацією. Ці фактори впливають на сприйняття ресурсу людиною, але дозволяють лише опосередковано судити про достовірність ресурсу.

У роботі [48] розглядаються питання довіри до текстової інформації. Особливістю цього дослідження є виокремлення факторів, які впливають на сприйняття інформації людиною як достовірної.

У статті [49] розглядаються тематика ресурсу, дизайн і технології, мова і стиль, а також інші чинники, які можуть бути враховані в автоматизованій системі оцінки достовірності ресурсу.

У деяких роботах розкриті методи вирішення завдань пошуку текстів за запитом, пошуку відповідей на запитання, класифікації, кластеризації текстів, виявлення запозичень та схожих за смислом текстів. Ці методи враховують, крім лексем, семантичні значення текстів. Вони також можуть бути застосовані для виявлення недостовірної інформації в комп'ютерних мережах.

У роботі [50] обговорюються підходи до обробки природної мови, засновані на машинному навчанні. Більшість методів передбачають розподіл документів по

класах на основі ознак цих документів. Одним з широко використовуваних методів класифікації є класифікація повідомлень за тоном на позитивні, негативні і нейтральні, а також визначення емоцій (сум, ненависть, сором), тематики і напрямку повідомлень.

Використання вищезгаданих методів у аналізі метаданих та супутнього контенту ресурсу дозволяє уточнити оцінки. В якості вхідних даних використовуються мета-теги документа, такі як заголовок, ключові слова та опис (перевіряється відповідність змісту та наявність маркерів), доменне ім'я і хостинг (враховується рівень домена і репутація хостингу), характер і обсяг рекламних блоків, дата публікації. Подібні підходи є ефективними для аналізу структурної або частково структурної інформації, представленої у таких форматах, як XML, JSON, HTML і т.д.

1.5 Постановка задачі

Аналіз мети, завдань та можливостей забезпечення інформаційної безпеки корпоративних інформаційних систем в умовах комплексних деструктивних інформаційних впливів показав, що існуючі системи захисту КІС в багатьох випадках не відповідають потребам практики. Зокрема, вони не враховують швидкозмінювані умови забезпечення такого захисту. З'являються нові, більш вдосконалені комплексні деструктивні впливи на КІС, які враховують специфіку застосовуваних методів та засобів захисту.

Відомі системи забезпечення інформаційної безпеки КІС та методи, що лежать в їх основі, не володіють високою адаптивністю до швидкозмінних умов. Усе це негативно впливає на ефективність захищених КІС.

Для розробки методів та моделей, спрямованих на підвищення ефективності інформаційного захисту комп'ютерних інформаційних систем (КІС), передбачено:

– Розроблення методу оцінювання ефективності захисту корпоративних інформаційних систем від комплексних деструктивних впливів.

– Розроблення методу адаптивного захисту корпоративної інформаційної системи від комплексних деструктивних впливів.

– Обґрунтування рекомендацій щодо підвищення ефективності захисту корпоративних інформаційних систем від комплексних деструктивних впливів.

2 МОДЕЛЬ ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

2.1. Показники ефективності захисту корпоративних інформаційних систем від комплексних деструктивних впливів

Для знаходження обґрунтованих методів і засобів захисту корпоративних інформаційних систем (КІС) від комплексних деструктивних впливів (КДВ) потрібно наявність відповідних методів оцінювання ефективності такого захисту.

Виходячи з загальних положень щодо оцінки захищеності подібних систем, ця ефективність може розглядатися на різних рівнях ієрархії. На найвищому рівні ефективність захисту КІС від КДВ здійснюється за приростами основних показників корпорації. Такими показниками можуть бути зростання прибутку, обсягу виробленої продукції корпорацією, скорочення сумарних витрат людських, матеріальних та інших ресурсів завдяки використанню захищених КІС порівняно з незахищеними системами.

На нижчому рівні ефективність захисту КІС здійснюється за приростами показників успішності функціонування адміністративних та виробничих структур. Щодо адміністративних структур ефект від використання відповідних КІС може виявлятися в оперативності та точності прийнятих управлінських рішень, зниженні витрат часових ресурсів на адміністративну діяльність. Для структур безпосередньо виробничих окремих видів продукції, включаючи нові знання і технології, ефективність використання захищених КІС може оцінюватися за такими показниками. Це прирости основних показників цих підрозділів (ймовірностей і часу виконання планів, отриманих конкретних результатів).

Якщо врахувати, що КІС надає різні рівні ієрархії для стимулювання діяльності корпорації, то в деяких випадках ефективність захисту від комплексних деструктивних впливів можна оцінювати за зростанням показників цих сервісів

через реалізацію заходів забезпечення безпеки. Наприклад, ефективність кожного окремого сервісу КІС можна оцінити ймовірністю відповідності його встановленим вимогам. До таких вимог можуть відноситися різні умови забезпечення функціональності, якості наданої інформації, затримок у задоволенні запитань та інші.

Для оцінки виконання сценаріїв багатомодальної взаємодії користувачів із пристроями, які забезпечують оточуючий кіберфізичний простір, також можна виділити показники якості обслуговування, унікальні для кожного сервісу. Кожен запит користувача потребує обслуговування (виконання), що передбачає використання певних апаратних та програмних ресурсів (екран, звук, сесія користувача) протягом певного часу. Деякі деталізовані показники ефективності надання сервісів КІС наведено в таблиці 2.1, де використовуються наступні позначення:

- t_{UI} - максимальний час реакції інтерфейсу користувача, який користувач вважає комфортним. У [45, 68] описано види лімітів для часу реакції інтерфейсу користувача. Зокрема, при часі реакції до 0,1 с користувач сприймає взаємодію без затримок. При часі реакції до 1 с користувач вважає процес взаємодії як добре контрольований. При досягненні 10 с затримки користувач високою ймовірністю відволікається на інші завдання;

- p_D - максимально допустима ймовірність відмови у виконанні користувальницького завдання, яку можна вибирати, керуючись стандартом.

Таблиця 2.1 - Показники ефективності реалізації сервісів, не пов'язані з видами

Показник	Одиниця вимірювання	Позначення	Можливі значення	Допустимі значення
1	2	3	4	5
Час завантаження додатку	с	t_l^{App}	$[0; \infty)$	$[0; t_{UI}]$

Продовження таблиці 2.1

1	2	3	4	5
Час ініціалізації додатку	с	t_i^{App}	$[0; \infty)$	$[0; t_{UI}]$
Час актуалізації даних в додатку	с	t_a^{App}	$[0; \infty)$	$[0; t_{UI}]$
Відносна частка виконаних заявок (відносна пропускна здатність)	-	$f_{np}^{Success}$	$[0; 1]$	$[1 - p_D; 1]$
Відносна частка виконаних заявок , що завершена за пріоритетом	-	$f_p^{Success}$	$[0; 1]$	$[1 - p_D; 1]$
Відносна частка відмов у виконанні користувацьких завдань при відсутності конкурентних завдань	-	f_{normal}^{Denial}	$[0; 1]$	$[1; p_D]$
Відносна частка відмов у виконанні користувацьких завдань при наявності конкурентних завдань	-	f_{stress}^{Denial}	$[0; 1]$	$[1; p_D]$
Час затримки у виконанні користувацьких завдань при відсутності конкурентних завдань	с	$f_{norm}^{Request}$	$[0; \infty)$	$[0; t_{UI}]$
Час затримки у виконанні користувацьких завдань при наявності конкурентних завдань	с	$f_{stress}^{Request}$	$[0; \infty)$	$[0; t_{UI}]$

Дослідження вказують, що найбільший вплив на сприйняття користувачем

веб-сервісів, на відміну від мультимедійних аудіо- та відеосервісів, справляє час очікування кінцевого користувача. Таким чином, час обробки запиту є ключовим фактором у системах інформаційно-комунікаційних сервісів (СІКС). Окрім перелічених параметрів, на які впливає якість сприйняття сервісів, суттєвий вплив має модальність інтерфейсу, через який користувач взаємодіє із системою. Зокрема, ефективність сервісу може залежати від точності використовуваних алгоритмів розпізнавання мови та алгоритмів розпізнавання обличчя, зручності графічного інтерфейсу.

Щодо конкретних показників ефективності наданих СІКС сервісів, за якими також може оцінюватися захищеність цієї системи, пояснимо їх на прикладі сервісу інтерактивного корпоративного телебачення. Сервіс інтерактивного корпоративного телебачення взаємодіє з користувачами за допомогою стаціонарних камер і екранів, розташованих в різних місцях організації. Крім того, користувачі можуть управляти сервісом за допомогою мобільних пристроїв. Функції сервісу включають трансляцію інформації для співробітників та відвідувачів на стаціонарні екрани (інформація про підприємство та його діяльність, оголошення, вітання) за їх запитом та/або відповідно до розкладу. Показники цього сервісу пов'язані з затримками, відмовами та втратами, які виникають під час трансляції медіаконтенту.

Для оцінювання показників сервісу інтерактивного корпоративного телебачення можуть використовуватися параметри, наведені у таблиці 2.2. У таблиці використовуються наступні позначення: $t_{distraction}$ - час, після якого користувач із великою ймовірністю відволічеться на інші; I - кількість інформації у медіафайлі, біт; I_{max} - норма максимально допустимої кількості інформації у медіафайлі, біт; R_{min}, R_{max} - оцінки мінімальної та максимальної швидкості сприйняття інформації користувачем, біт/с.

Крім цих показників для оцінювання ефективності захисту СІКС від КДУ можуть бути використані і інші. У всіх випадках для розрахунку подібних показників необхідно мати моделі аналізованих процесів, що відбуваються в СІКС.

Таблиця 2.2 - Показники якості обслуговування для сервісу інтерактивного корпоративного телебачення

Показник	Одиниця вимірювання	Позначення	Можливі значення	Допустимі значення
Затримка між очікуваним та фактичним часом трансляції медіа	с	r_{delay}^{CT}	$[0; \infty)$	$[0; t_{distraction}]$
Відносний час постою	-	f_{down}^{CT}	$[0; 1]$	$[0; t_{distraction}]$
Співвідношення часу трансляції та об’єму інформації, що транслюється	біт/с	$r_{perception}^{CT}$	$[0; \infty)$	$[R_{min}; R_{max}]$
Час заміни медіафайлів	с	t_{load}^{CT}	$[0; \infty)$	$[0; t_{UI}]$
Відносна частка невдалих завантажень контенту	-	f_d^{CT}	$[0; 1]$	$[0; p_D]$
Відносна частка часових втрат	-	f_t^{CT}	$[0; 1]$	$\left[0; 1 - \frac{I}{I_{max}}\right]$
Відносна частка втрат за областю відтворення	-	f_i^{CT}	$[0; 1]$	$\left[0; 1 - \frac{I}{I_{max}}\right]$
Коефіцієнт спотворення	-	k_d^{CT}	$[0; 1]$	$\left[0; 1 - \frac{I}{I_{max}}\right]$

Метод комплексного оцінювання стійкості КІС від КДУ на основі численних

ключових показників повинен передбачати аналіз їх систем або різних комбінацій. У найпростіших випадках метод полягає у розрахунку приросту зважених сум значень окремих показників КІС без застосування заходів захисту, а також за використання заходів захисту. Крім того, ефективність КІС та її системи захисту може бути віднесена до типових умов і станів функціонування. Для цих станів можуть бути заздалегідь визначені досяжні ефекти КІС. Враховуючи вищезазначені положення, для оцінювання стійкості КІС від КДУ, розглянемо модель цієї системи у просторі базових станів.

2.2 Модель функціонування захищеної корпоративної інформаційної системи

Для визначення вихідних даних для запропонованого методу можна використовувати математичну модель, що описує функціонування об'єкта захисту. Для більшості практичних випадків процес функціонування корпоративної інформаційної системи в умовах, коли можлива наявність певної визначеної загрози та реалізація певного способу її виявлення та протидії, може бути формалізований у вигляді графу на рис. 2.1.

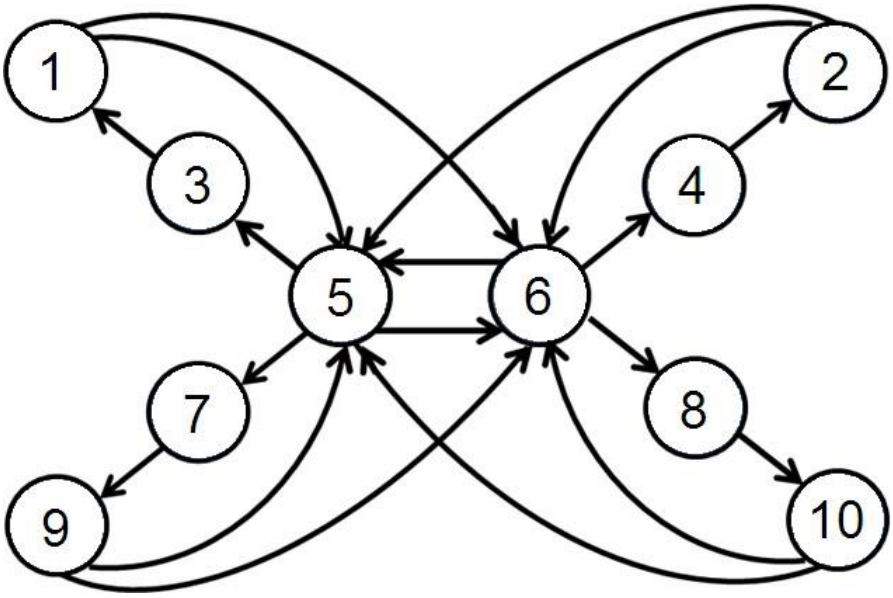


Рисунок 2.1 - Модель функціонування захищеної КІС

Вершини графа позначають стани процесу, стрілки - переходи від одних станів до інших. Можна виділити 10 станів (S_1-S_{10}) розглядуваного процесу, які перераховані в таблиці 2.3. Різниця між цими станами полягає в умовах, за яких система функціонує в певний момент часу. Наведений набір станів є повною групою подій. Переходи між станами, показані на рис. 2.1, визначаються характером аналізованого процесу. Переходи $S_5 \rightarrow S_6$, $S_6 \rightarrow S_5$ можуть відбуватися при посиленні чи ослабленні активності зловмисників, реконфігурації системи, зміні її контрагентів, а також при модифікації інших умов функціонування системи. Зміна цих умов суттєво впливає на процеси актуалізації та деактуалізації загроз.

Таблиця 2.3 - Стани процесу функціонування системи

Номер стану	Умови функціонування
1	Реалізація захисних заходів для усунення виявленої загрози
2	Коректна оцінка ситуації за відсутності загрози
3	Отримання істинної інформації про загрозу
4	Отримання істинної інформації про відсутність загрози
5	Відсутність інформації про загрози за наявності загрози
6	Відсутність інформації про загрози за відсутності загрози
7	Пропуск загрози за її наявності
8	Хибне розпізнавання загрози за її відсутності (хибна тривога)
9	Сприйняття неправдивої інформації як істинної
10	Реалізація помилкових заходів захисту за відсутності загрози

Переходи $S_5 \rightarrow S_3$, $S_5 \rightarrow S_7$ можливі, коли система використовує засоби захисту для виявлення загроз. Перехід $S_5 \rightarrow S_3$ вказує на успішне виявлення загрози, тоді як перехід $S_5 \rightarrow S_7$ характеризує пропуск загрози, незважаючи на використання засобів захисту. Перехід $S3 \rightarrow S_1$ виконується, якщо виявлену загрозу ліквідовано, $S_7 \rightarrow S_9$ – якщо хибна інформація про загрозу приймається за істинну. Переходи $S_6 \rightarrow S_4$, $S_6 \rightarrow S_8$, $S_4 \rightarrow S_2$, $S_8 \rightarrow S_{10}$ відповідають випадкам, коли розглядувана загроза відсутня.

Незважаючи на відсутність загрози, засоби захисту можуть генерувати сигнали помилкової тривоги. Ці сигнали можуть призводити до реалізації неадекватних захисних заходів, що відображено в переході $S_8 \rightarrow S_{10}$. Перехід $S_4 \rightarrow S_2$ відбувається, коли системи захисту визначили відсутність загрози правильно, і жодних додаткових захисних заходів не приймається. Під час розробки вищезазначеної моделі використовувалася наступна логіка. На самому високому рівні систему можна описати лише двома станами (рис.2.2, А), які означають, що задана загроза відсутня (2, 4, 6, 8, 10) або присутня (1, 3, 5, 7, 9). Кожен з цих станів може бути розділений на два інших стани на основі використання засобів виявлення загрози. У результаті отримується 4 стани (рис.2.2, В). Два з них відповідають наявності загрози при використанні (1, 3, 7, 9) та без використання засобів виявлення загрози. Інші стани характеризують функціонування системи при відсутності загрози і при використанні (2, 4, 8, 10) та без використання (6) засобів виявлення загрози. Кожен стан, який характеризує роботу системи з використанням засобів виявлення загрози, розділяється на два стани за критерієм результативності виявлення (рис.2.2, С). Таким чином, стани 3 і 7 означають виявлення і пропуск загрози відповідно. Стани 4 і 8 аналогічно означають правильну оцінку ситуації при відсутності загрози і помилкову тривогу. Стани 3, 7, 4 і 8 змінюються станами 1, 9, 2 і 10, які передбачають прийняття захисних заходів відповідно до результатів виявлення загрози. Таким чином, в результаті отримується модель на рис. 2.2. Правильність цієї моделі базується на її відповідності загальним закономірностям функціонування захищених систем.

У таблиці 2.4 наведено класифікацію станів за критеріями, описаними вище. З урахуванням центральної граничної теореми в теорії ймовірностей для потоків подій граф на рис. 2.1 може бути описаний за допомогою математичного апарату марківських процесів [51]. Цей апарат дозволяє подати модель аналізованого процесу у вигляді системи лінійних диференціальних рівнянь.

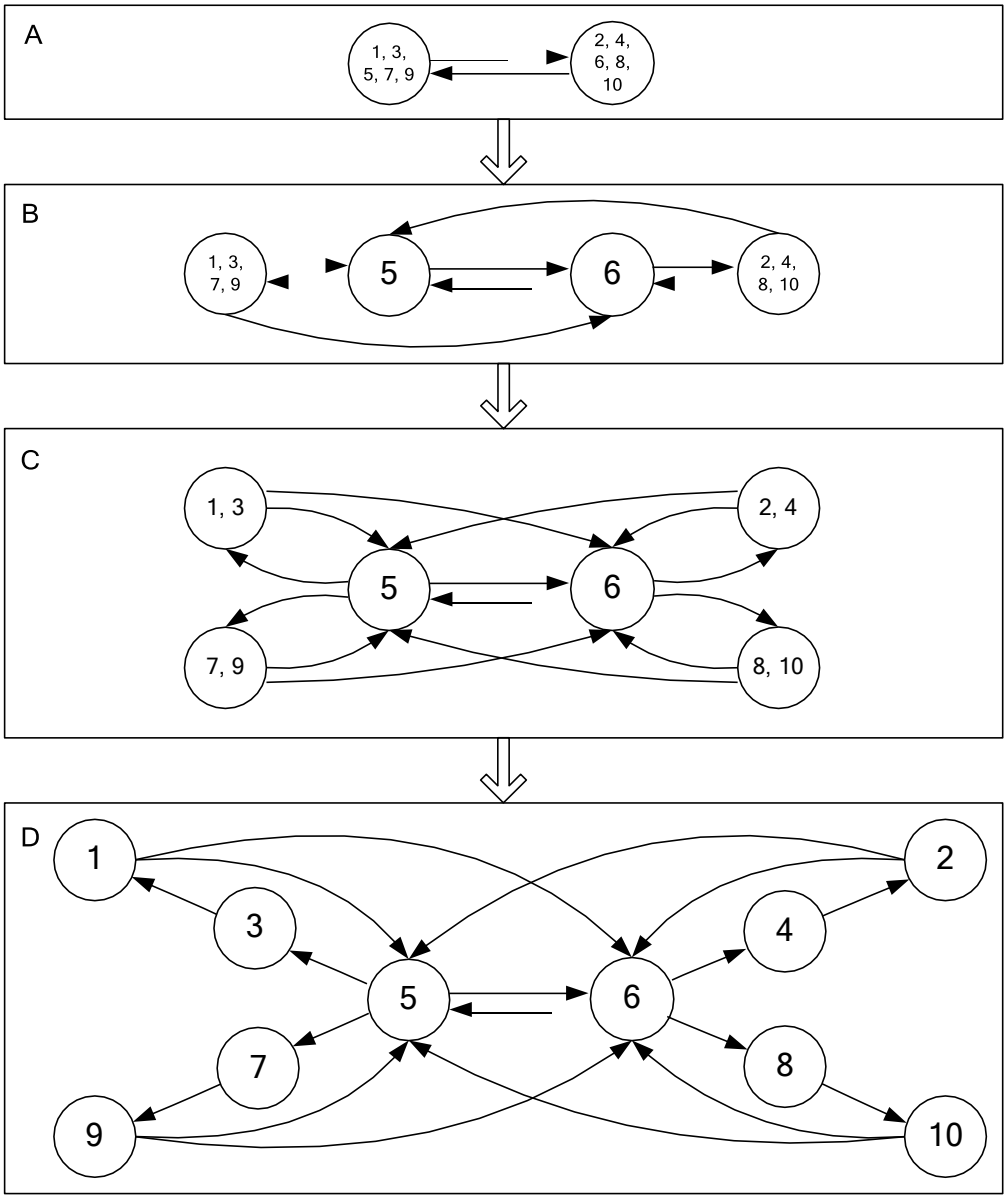


Рисунок 2.2 - Процес побудови моделі функціонування системи

Таблиця 2.4 - Класифікація станів

Номер стану	Наявність загрози	Наявність інформації	Наявність засобів захисту	Адекватність засобів захисту
1	2	3	4	5
6	–	–	–	N/A
4	–	+	–	N/A
8	–	+	–	N/A
2	–	+	+	+
10	–	+	+	–

Кінець таблиці 2.4

1	2	3	4	5
5	+	–	–	N/A
3	+	+	–	N/A
7	+	+	–	N/A
1	+	+	+	+
9	+	+	+	–

Розглянутому вище графу відповідає система з 10 лінійних диференціальних рівнянь, кожне з яких описує залежність ймовірностей перебування системи в відповідних станах $S_1 \ldots S_{10}$ від часу:

$$\frac{dP_1(t)}{dt} = \lambda_{31}P_3(t) - (\lambda_{15} + \lambda_{16})P_1(t)$$
$$\frac{dP_2(t)}{dt} = \lambda_{42}P_{43}(t) - (\lambda_{25} + \lambda_{26})P_2(t)$$
$$\frac{dP_3(t)}{dt} = \lambda_{53}P_5(t) - \lambda_{31}P_3(t)$$
$$\frac{dP_4(t)}{dt} = \lambda_{64}P_6(t) - \lambda_{42}P_4(t)$$
$$\frac{dP_5(t)}{dt} = \lambda_{15}P_1(t) + \lambda_{25}P_2(t) + \lambda_{65}P_6(t) + \lambda_{95}P_9(t) + \lambda_{10,5}P_{10}(t) - (\lambda_{53} + \lambda_{56} + \lambda_{57})P_5(t)$$
$$\frac{dP_6(t)}{dt} = \lambda_{16}P_1(t) + \lambda_{26}P_2(t) + \lambda_{56}P_5(t) + \lambda_{96}P_9(t) + \lambda_{10,6}P_{10}(t) - (\lambda_{64} + \lambda_{65} + \lambda_{68})P_6(t)$$
$$\frac{dP_7(t)}{dt} = \lambda_{57}P_5(t) - \lambda_{79}P_7(t)$$
$$\frac{dP_8(t)}{dt} = \lambda_{68}P_6(t) - \lambda_{8,10}P_8(t)$$
$$\frac{dP_9(t)}{dt} = \lambda_{79}P_7(t) - (\lambda_{95} + \lambda_{96})P_9(t)$$
$$\frac{dP_{10}(t)}{dt} = \lambda_{8,10}P_8(t) - (\lambda_{10,5} + \lambda_{10,6})P_{10}(t)$$

У розглянутої системі рівнянь $P_1(t),\ldots, P_{10}(t)$ представляють собою імовірності перебування системи у станах 1…10 у момент часу t; λ_{ij} - інтенсивності переходів між станами і та j. Значення λ_{ij} залежать від вибору реалізованої програми захисту PRGk.

Слід відзначити, що розв'язок конкретної системи рівнянь надає ймовірності, які описують поведінку системи при захисті від конкретної загрози за допомогою

конкретної програми захисту PRGk. Проте у цьому прикладі для спрощення форми подання взаємозв'язок ймовірностей і коефіцієнтів рівнянь від PRGk виключено.

Також слід зауважити, що інтенсивності λ_{ij} переходів між станами можуть бути визначені як

$$\lambda_{ij} = \frac{q_{ij}}{\overline{t_{ij}}}, \tag{2.1}$$

де $\overline{t_{ij}}$ середній час переходу між станами і та j при ідеальних умовах; q_{ij} - ймовірність такого переходу.

Якщо відомі інтенсивності переходів та початкові умови, система диференціальних рівнянь може бути легко вирішена числовими або аналітичними методами. Визначення початкових умов для визначення фактичного стану системи здійснюється модулем аналізу ефектів системи захисту, який розглядається у розділі 4. Крім того, для кожного типу загроз та програм захисту модель повинна мати власні початкові значення та параметри. У разі можливості визначення фактичного стану системи та відомих значень λ_{ij} поява загроз може бути передбаченою.

Варто відзначити, що кожний стан у розглянутій моделі може бути "розгорнутий" у допоміжну модель у випадку необхідності більш детального вивчення цього стану. При цьому можна використовувати як марківські моделі, так і альтернативні моделі, які описують поведінку систем з точки зору інформаційної безпеки.

2.3 Оцінювання ефективності захисту корпоративних інформаційних систем за допомогою марківських моделей

Розглянемо особливості використання запропонованих марківських моделей аналізу процесів, які досліджуються, для оцінки ефективності захисту КІС. Ці

особливості включають такі етапи:

Етап 1. Розрахунок ймовірностей $P_z^*(t), P_{zk}(PRG_k, t)$ знаходження КІС у визначених станах без використання заходів захисту та з ними на визначений момент часу.

Етап 2. Оцінка t_z^* та $t_{zk}(PRG_k)$ сумарного часу перебування КІС у станах $S_z \epsilon \{S_1, \dots, S_{10}\}$ у випадку відсутності та при реалізації захисних заходів програми PRG_k:

$$t_z^* = \int_0^T P_z(t)dt, \tag{2.2}$$

$$t_{zk}(PRG_k) = \int_0^T P_{zk}(PRG_k, t)dt, \tag{2.3}$$

де $P_{zk}(PRG_k, t)$ означає ймовірність перебування системи в стані z при реалізації захисної програми PRG_k; T – аналізований період часу.

Етап 3. Кожному стану z ставиться у відповідність величина ефекту V_z, пов'язана з показниками якості обслуговування, яку система забезпечує користувачеві в одиницю часу.

Етап 4. Обчислюються загальні ефекти L^*, $L(PRG_k)$ заходів захисту КІС та без них:

$$L^* = \sum_{z=1}^{z} V_z * t_z^*, \tag{2.4}$$

$$L(PRG_k) = \sum_{z=1}^{z} V_z * t_{zk}^*(PRG_k), \tag{2.5}$$

де Z – загальна кількість станів КІС.Важливо врахувати, що значення ефектів V_z можуть бути як додатніми, так і від'ємними (вираженням збитків). Оскільки показники якості обслуговування залежать від часу, розрахунок загального ефекту може здійснюватися за формулами:

$$L^* = \sum_{z=1}^{Z} L_z^*, \tag{2.6}$$

$$L(PRG_k) = \sum_{z=1}^{Z} L_z(PRG_k), \tag{2.7}$$

$$L_z^* = \int_0^T V_z(t) P_z^*(t) dt, \tag{2.8}$$

$$L_z(PRG_k) = \int_0^T V_z(t) P_{zk}(PRG_k, t) dt, \tag{2.9}$$

Етап 5. Оцінка приросту $\Delta L = L_z(PRG_k) - L_z^*$ ефективності КІС завдяки реалізованим заходам захисту.

Для прикладу розглянемо показники QoS для послуги інтерактивного корпоративного телебачення, пов'язані з спотворенням, затримкою та відмовою виконання завдань. Для оцінки ефекту $V_z(t)$ ці показники слід звести до єдиного показника.

Розглянемо спочатку коефіцієнт спотворення k_d, який визначається як середнє значення спотворення елементів медіафайла:

$$k_d = \frac{1}{N}\sum_{i=1}^{N} \Delta E(P_i, P_i^*) \tag{2.10}$$

де N – кількість елементів медіафайла (пікселів), ΔE – функція кольорової різниці між пікселями P_i (фактичним) і P_i^* (ідеальним). В більш простому випадку, використовуючи бінарну функцію кольорової різниці, коефіцієнт можна виразити як відношення площі деформованої області до загальної площі зображення. У ідеальному випадку залежність k_d від часу для сигналу тривалістю l виражається функцією Хевісайда:

$$k_d * (t) = \theta(t) - \theta(t - l) \tag{2.11}$$

де θ – функція Хевісайда.

Для врахування затримки t_{delay} введемо допоміжну функцію затримки (рис. 8), що характеризує вчасність виконання користувацького завдання:

$$d(t) = \begin{cases} 1, t \leq 1 \\ e^{-\alpha(t-1)}, t > 1' \end{cases} \tag{2.12}$$

де α – коефіцієнт, що визначає швидкість втрати актуальності завдання при його затримці.

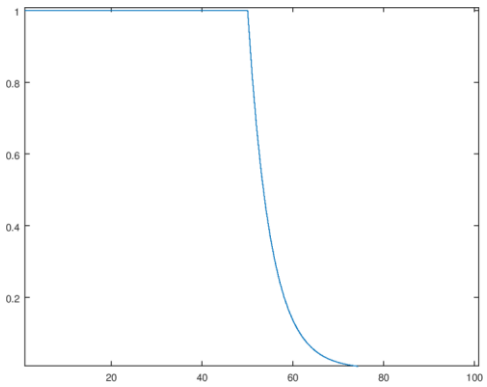


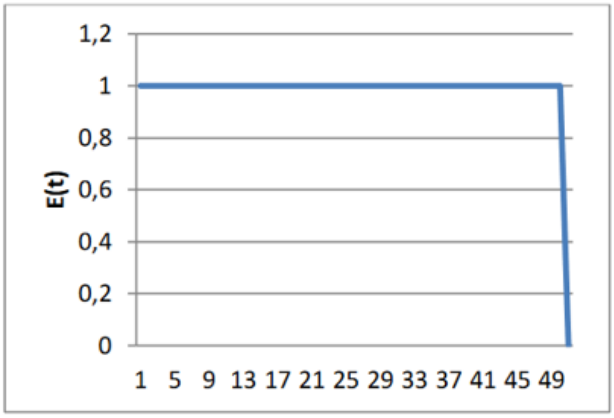
Рисунок 2.3 - Функція $d(t)$

У цьому випадку величина

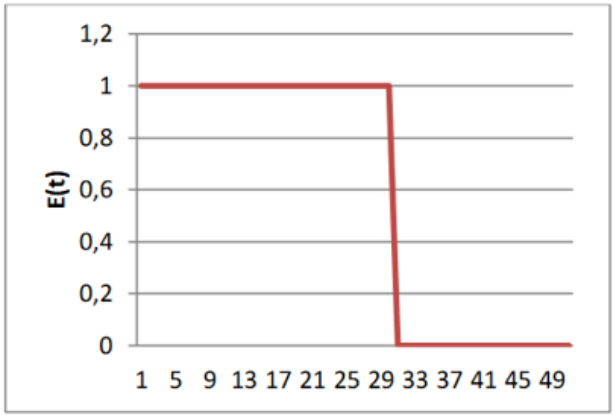
$$E(t) = k_d(t)d(t) \tag{2.13}$$

характеризує як можливі спотворення, так і затримки. Для урахування відмови системи виконати завдання у цьому випадку можна прийняти $t_{delay} = \infty$.

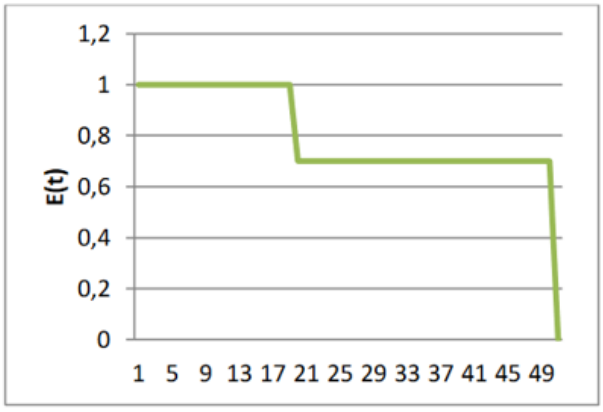
На графіках на рис. 2.4 відображено поведінку величини при відсутності втрат даних та при наявності втрат даних різного типу. Зокрема, представлені приклади залежностей при $l = 50$ для ідеального випадку (а), випадку передчасного завершення завдання в момент $t = 30$ с (б), випадку виникнення спотворень в момент $t = 20$ с (в) і випадку затримки виконання на 28 с (г).



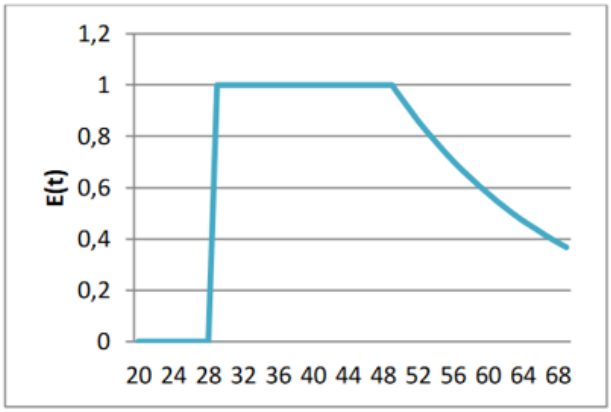
а) Відсутність спотворень



б) Відміна завдання при t = 30 с



в) Втрата даних при t = 20 с



г) Затримка на 28 с

Рисунок 2.4 - Залежності функції ефекту від можливих спотворень

2.4 Висновки до розділу

Розроблено новий метод оцінювання ефективності захисту корпоративних інформаційних систем від комплексних деструктивних впливів. Цей метод ґрунтується на використанні запропонованої нової марківської моделі функціонування захищеної КІС у умовах комплексних деструктивних інформаційних загроз. Формалізація процесу здійснюється в раніше не дослідженому просторі станів КІС. Пропонується проводити оцінку ефективності захисту за допомогою цієї моделі за інтегральним показником ефективності функціонування КІС з урахуванням часу перебування її в кожному стані та досягнутого часткового ефекту в ньому.

3 МЕТОД АДАПТИВНОГО ЗАХИСТУКОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВІД КОМПЛЕКСНИХ ДЕСТРУКТИВНИХ ВПЛИВІВ

3.1. Архітектура системи адаптивного захисту корпоративної інформаційної системи від комплексних деструктивних впливів

Розглянемо модель системи адаптивного захисту КІС від комплексних деструктивних впливів. Структура цієї системи наведена на рис. 3.1. Особливість системи полягає в новому наборі функціональних блоків та зв'язків між ними. Вона дозволяє підвищити здатність прикладної системи виявляти та усувати деструктивні інформаційні впливи в автоматичному режимі. Мета цієї системи – адаптивний захист від гетерогенних деструктивних інформаційних впливів на комп'ютерні мережі. Для досягнення цієї мети використовуються різноманітні методи. Адаптація системи до актуальних умов функціонування виконується за допомогою її реконфігурації. Реконфігурація передбачає підлаштування блоків системи до поточної системи, а також вибір відповідних методів захисту.

Згідно з рис. 3.1, процес захисту починається із збору даних від джерел. Система може отримувати дані у вигляді дампів інтернет-трафіку, контенту у статистичній, структурній, текстовій або мультимедійній формі. Джерелами даних можуть бути вузли локальної чи глобальної мережі, апаратне та програмне забезпечення. Залежно від кількості та чіткості джерел даних можуть застосовуватися три підходи:

– Постійний моніторинг конкретних джерел інформації з аналізом отримуваної від них інформації. Цей підхід застосовний для невеликої кількості чітко визначених джерел, оскільки обчислювальний ресурс аналізатора обмежений. Прикладом такого спостереження може бути постійне перехоплення трафіку з мережевого вузла інтерфейсом, що працює в режимі повного

перехоплення.

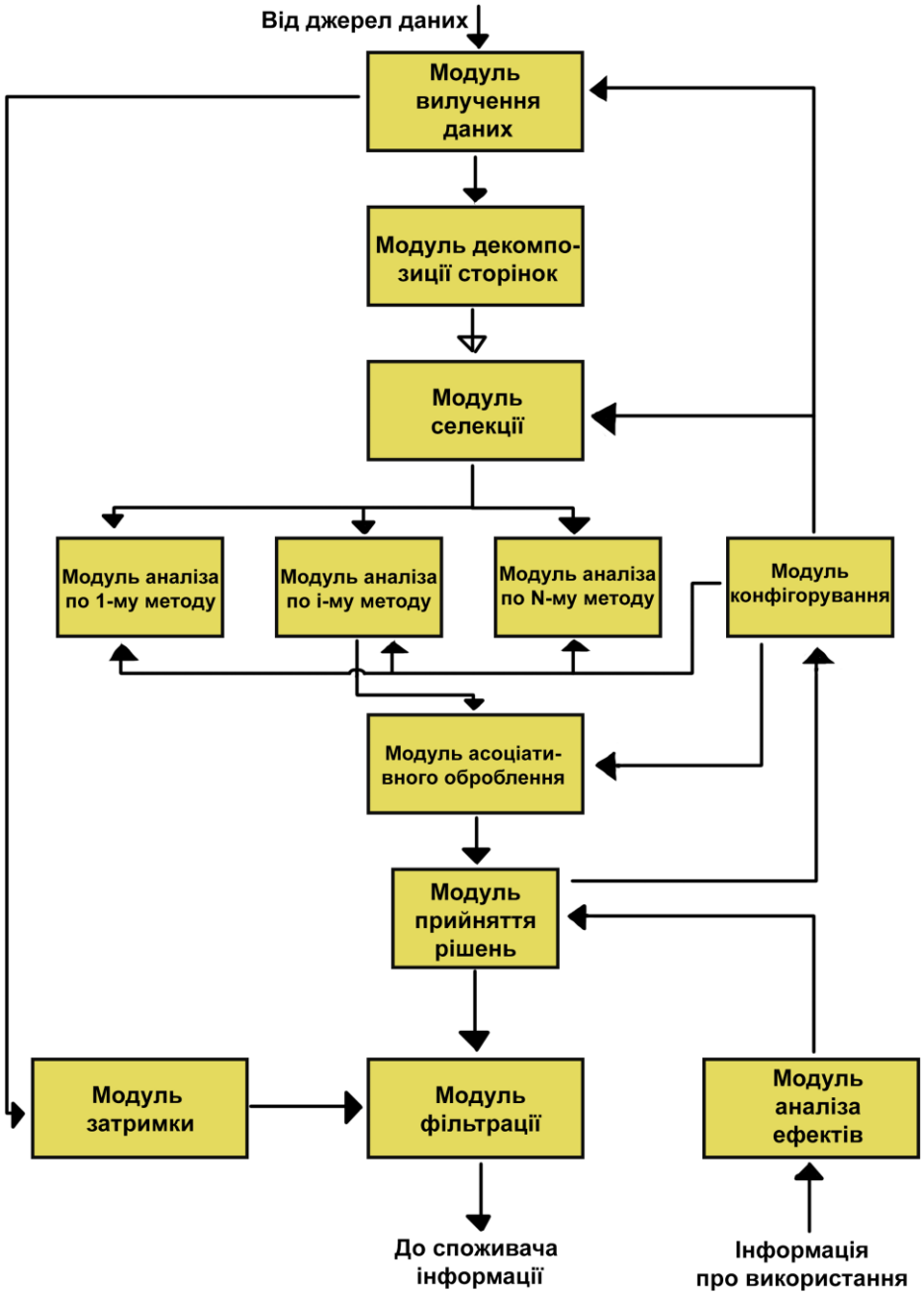


Рисунок 3.1 - Структура системи адаптивного захисту

– Періодичний моніторинг джерел інформації з частковим аналізом отримуваної від них інформації. Цей підхід використовується при обмежених можливостях у сфері спостереження та аналізу в ситуаціях, коли необхідно контролювати значну кількість джерел. Прикладом такого моніторингу є

використання контрольних сум (хешів) та регулярних виразів для визначення змін та виявлення необхідних елементів даних в великому обсязі інформації.

– Пошук джерел інформації, яка представляє інтерес. Цей підхід використовується, якщо множина джерел не визначена. Підхід застосовний як для пошуку нової інформації, так і для валідації існуючої. Прикладом є розсилка широкомовних повідомлень у комп'ютерній мережі для пошуку вузлів, що підтримують той чи інший протокол обміну інформацією.

Вхідні дані включають як інформацію для аналізу, так і зворотню, отриману від користувача. Розглянемо приклад, коли система аналізує дані, представлені у веб-форматі. Після отримання даних із зовнішнього джерела система завантажує пов'язані компоненти (фрейми з іншими документами, медіафайли, стилі, сценарії і т. д.). Потім система будує їх структурну модель. Так, при обробці HTML-сторінок парсер перетворює простий текст в ієрархічну структуру тегів DOM (Document Object Model). Після визначення структури даних обираються компоненти для аналізу: система ідентифікує складові документа (текст, зображення, відео) як окремі інформаційні об'єкти. Ідентифікація для HTML-документів виконується на основі видів тегів та їх вмісту, наприклад: теги <title>, <h1>…<h6> означають текстові блоки, що містять заголовки документа та його секцій; <p>, , <article> - блоки тексту; <img>, <canvas>, <figure> - зображення; <video>, <object>, <embed> - відеофайли або вкладені об'єкти; <audio> - звукові файли, <a> - гіперпосилання.

Ідентифіковані інформаційні об'єкти можна аналізувати різними методами в залежності від типу та характеристик об'єктів. Окрім вмісту об'єктів, слід враховувати також такі фактори:

– цілісну структуру документа (відносини послідовності та композиції між окремими об'єктами), яка визначається ієрархією HTML-тегів;

– зв'язки з іншими документами, які можуть бути реалізовані у вигляді гіперпосилань та фреймів;

– просторове співвідношення компонентів документів, яке може бути

статичним, визначеним набором стилів або, рідше, атрибутами HTML-тегів; або динамічним, сформованим сценаріями документа після того, як документ завантажено.

Інформацію про класи інформаційних об'єктів, методи їх аналізу та їх параметри надає модуль конфігурації.

На основі проведеного аналізу інформаційних об'єктів, кожному з них призначаються властивості, які відображають його характеристики. До важливих властивостей інформаційних об'єктів належать їх структурні, частотні та змістові особливості окремих конструкцій та об'єктів в цілому. В результаті маємо справу із багаторівневою структурою властивостей інформаційних об'єктів та правил їх оцінки, що дозволяють перейти від оцінки характеристик інформаційного об'єкта, обчислених безпосередньо, до оцінки суттєвих властивостей об'єкта як носія інформації, а від них – до визначення класу інформаційного об'єкта в цілому. Схему оцінки інформаційних об'єктів представлено на рис. 3.2, де вершинами позначені реалізовані функції, а дугам ставляться у відповідність вагові коефіцієнти.

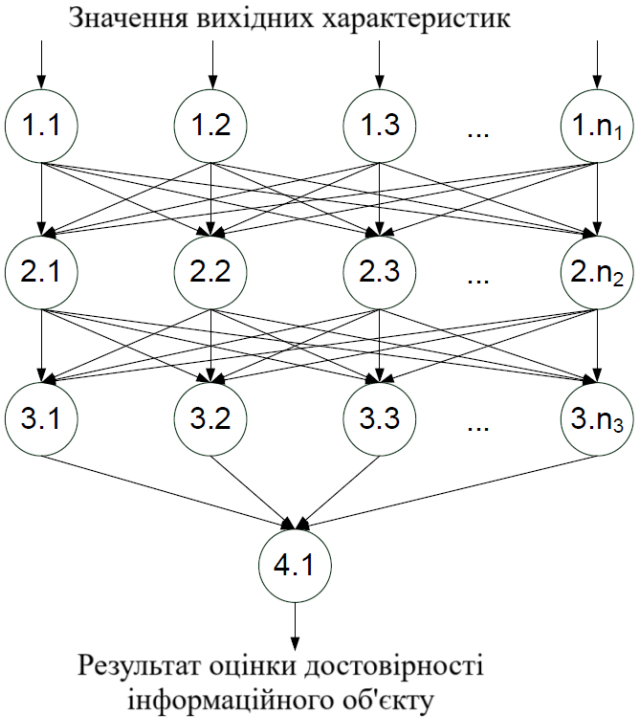


Рисунок 3.2 - Схема оцінки достовірності інформаційних об'єктів

У певному розумінні таку схему оцінки можна розглядати як класифікатор інформаційних об'єктів за рівнями легітимності.. Кожному інформаційному об'єкту можна привести багаторівневу систему його характеристик. Класифікація таких об'єктів як шкідливої інформації загалом передбачає аналіз його характеристик на різних рівнях ієрархії з урахуванням їх взаємозв'язків. Для випадків, коли відома багатовимірна щільність $f(y_1, \dots, y_n)$ розподілу характеристик $y_1, \dots, y_n$ інформаційного об'єкта, ймовірність $P_{\text{ді}}$ його класифікації як легітимної інформації можна розрахувати за формулою:

$$P_{\text{ді}} = P_a \int_{Y_1} \dots \int_{Y_n} f(y_1, \dots, y_n) dy_1, \dots, dy_n \tag{3.1}$$

де P_a – апріорна ймовірність наявності легітимної інформації; $y_1, \dots, y_n$ – області значень для справжніх характеристик інформаційного об'єкта.

Якщо вважати характеристики незалежними одна від одної,

$$P_{\text{ді}} = P_a \int_{Y_1} f_1(y_1) dy_1, \dots, \int_{Y_n} f_n(y_n) dy_n \tag{3.2}$$

де $f_1(y_1), \dots f_n(y_n)$ – одновимірні щільності розподілу характеристик $y_1, \dots, y_n$. Згідно з цими виразами інформаційний об'єкт може бути класифікований як шкідлива інформація при низькій апріорній ймовірності P_a або при низькій ймовірності достовірності хоча б однієї з його характеристик.

На практиці потрібно враховувати нерівнозначність внеску кожної характеристики в P_a. Для визначення достовірності набору одновимірних, але нерівнозначних характеристик інформаційного об'єкта, які відображають певну його властивість, можна використовувати вираз:

$$P^*_{\text{ді}} = \sum_{i\in\Omega} a_i P_{\text{ді}_i}, \tag{3.3}$$

де $P^*_{\text{ді}}$ – ймовірність достовірності і-ї характеристики об'єкта; a_i – відносна вага цієї характеристики, $P^*_{\text{ді}} \leq 1$.

З урахуванням цього інтегральний показник W оцінки інформаційного об'єкта можна розрахувати за правилом: $W = W_{zi}$ при $z = Z$ та $i = 1$

$$W_{zi} = \sum_{j=1}^{n_{z-1}} a_{zij} W_{z-1,j}; i = \overline{1, n_z}; z = \overline{1, Z} \tag{3.4}$$

де z – номер рівня обробки характеристик; Z – кількість рівнів; n_z – кількість різних характеристик, що впливають на достовірність властивостей інформаційного об'єкта на рівні $z + 1$; a_{zij} – відносний внесок показника $W_{z-1,i}$ в W_{zi}. На рівні z = 1 в якості показників W_{zi} можуть використовуватись ймовірності достовірності вихідних характеристик інформаційного об'єкта. Фізичний зміст такого інтегрального показника полягає в зваженій сумі часткових нормованих показників.

Для класифікації об'єктів на основі цих властивостей можна використовувати асоціативну обробку. Вона дозволяє встановлювати зв'язки (включаючи неявні) між властивостями інформаційних об'єктів та їх класами (наприклад, достовірна інформація, помилкова, неправдива, деструктивна і т.д.).

Результати асоціативної обробки використовуються для формулювання висновків щодо типу аналізованої інформації та заходів захисту, які слід застосовувати в актуальних умовах. Після цього інформація, за необхідності, коригується і передається її споживачеві. Процедура фільтрації може включати такі дії, як видалення шкідливої інформації, корекція помилок, введення додаткової маркування в інформаційний об'єкт.

З урахуванням можливості оцінити отриманий загальний ефект в різних

умовах функціонування системи, можна побудувати метод реконфігурації системи захисту. Зокрема, реконфігурація може включати в себе корекцію процедур обробки даних в інформаційних об'єктах, якщо вони задовольняють ряду умов (наприклад, належність до певного класу, походження від певного джерела даних). Корекція може включати додавання та видалення методів обробки інформаційних об'єктів, зміну параметрів цих методів для підвищення точності обробки інформації, що, в свою чергу, призводить до підвищення ефекту.

3.2. Алгоритм адаптивного захисту корпоративної інформаційної системи від комплексних деструктивних впливів

Використовуючи розглянуту вище модель, опишемо алгоритм, що лежить в основі запропонованого методу адаптивного захисту КІС. Цей алгоритм враховує змінюючіся умови при функціонуванні захищеної системи. Блок-схема цього алгоритму наведена на рис. 3.3. Метою роботи цього алгоритму є пошук і реалізація доцільної конфігурації системи захисту, забезпечуючи максимальні можливості захисту в складних умовах.

Під час налаштування системи захисту визначається склад використовуваних методів і систем захисту, а також їх параметри. Налаштування повинно здійснюватися з урахуванням як активних, так і можливих загроз, а також стану захищеної системи. Загалом, для знаходження відповідного методу захисту від розглянутих загроз потрібно вирішувати оптимізаційну задачу. Для цього необхідно мати модель процесів в захищеній системі.

Процеси отримання блоків інформації та їх аналізу з точки зору вимог до безпеки мають свої особливості, залежно від конфігурації системи. Інформація може надходити з різних джерел, вона може бути різних типів і якості, мати протиріччя. Бажано, щоб апріорні дані, включаючи результати прогнозу, а також комплексні методи оперативного виявлення деструктивних впливів, використовувалися настільки широко, наскільки це можливо. Для підвищення

повноти та достовірності отриманої інформації джерела даних можуть бути розподілені між обчислювальними ресурсами. Якщо у розглянутому зразку даних виявлена загроза, алгоритм передбачає захисні заходи як на рівні системи, так і на рівні конкретного зразка даних (корекція, видалення). Тільки після цього зразок даних передається компонентам захищеної системи.

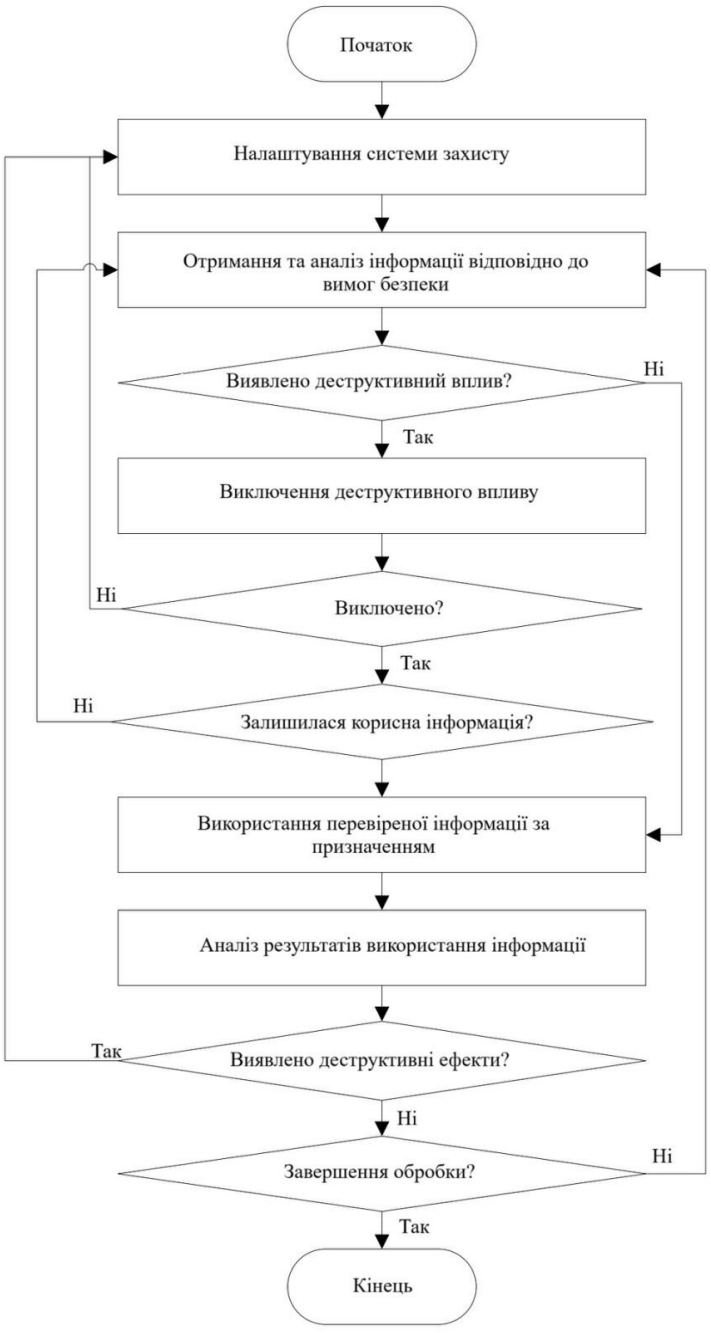


Рисунок 3.3 - Алгоритм адаптивного захисту від комплексних інформаційних загроз

Ризик пропуску загрози залишається через недосконаліть методів захисту. Це може викликати негативні наслідки в роботі захищеної системи. Для виявлення цих наслідків слід аналізувати результати функціонування захищеної системи. Якщо виявлені негативні наслідки, систему захисту слід реконфігурувати для усунення таких наслідки у майбутньому.

При реконфігурації важливо враховувати не лише поточний стан системи, а й результати прогнозів, побудованих за допомогою відповідних моделей. Такі моделі повинні передбачати як самі загрози, так і їх наслідки.

3.3 Метод оптимізації конфігурації системи захисту:

У межах алгоритму, викладеного у пункті 3.2, передбачається оптимізація конфігурації системи захисту інформаційно-комунікаційної системи (ІКС) від комплексних деструктивних впливів. Для оптимізації такої конфігурації пропонується вирішувати математичну задачу, яка полягає у знаходженні оптимальної програми PRG_{opt} для конфігурації системи захисту від обраних загроз, при реалізації якої досягається максимальний загальний ефект $L_{opt}(PRG_{opt})$ протягом інтервалу часу $[0; T]$:

$$L_{opt}(PRG_{opt}) = \max_{k} \sum_{z=1}^{Z} \int_{0}^{T} V_z(t) P_{zk}(PRG_k, t) dt \tag{3.5}$$

при наступних обмеженнях:

$$t_k(PRG_k) \leq t_D \tag{3.6}$$

$$PRG_k \in R \tag{3.7}$$

$$z = \overline{1, Z}, k = \overline{1, K} \quad (3.8)$$

У формулах (3.1)-(3.4) використовуються наступні позначення:

- R – кінцева множина результативних програм конфігурації системи захисту (під результативною програмою розуміється програма, яка досягає поставленої мети протягом скінченної кількості кроків);

- K – кількість програм у множині R;

- Z – кількість станів у моделі захищеної системи;

- $V_z(t)$ – ефект, досягнутий системою у момент часу t при умові, що система знаходиться у стані z;

- $P_{zk}(PRG_k, t)$ - ймовірність перебування захищеної системи у стані z у момент часу t за умови, що програма PRG_k реалізована;

- T – інтервал часу, протягом якого оцінюються загальні ефекти;

- $t_k(PRG_k)$ - час виконання програми PRG_k;

- t_D - максимально допустимий час виконання програми.

Ця модель передбачає, що пошук оптимальної програми PRG_{opt} для конфігурації системи захисту може виконуватися лише на множині програм, які відповідають умовам (3.2) і (3.3). Врахування цих обмежень значно спрощує задачу. У деяких випадках така оптимізація також може виконуватися з метою мінімізації можливого збитку протягом заданого інтервалу часу.

Згідно (3.1)-(3.4), алгоритм вирішення сформульованої задачі пошуку оптимальної програми PRG_{opt} складається з таких кроків:

1. Визначення початкових даних - значень T, Z, K, t_D, множин $\{V_z(t)\}, \{P_{zk}(t=0)\}, \{PRG_k\}, \{t_k(PRG_k)\}, \{\lambda_{ijk}\}$ – інтенсивностей переходу в Марківській моделі захищеного процесу після реалізації конфігураційної програми PRG_k. Встановлення початкових значень змінних: $k = 0, L_{opt} = 0$.

2. $k = k + 1; z = 0;\ L_k = 0$.

3. Якщо $k < K$, перейти до кроку 16.

4. Вибрати k-у альтернативну програму з множини $\{PRG_k\}$.

5. Перевірити умову (3.3): перейти до кроку 2, якщо $PRG_k \in R$. Якщо умова не виконується, перейти до кроку 2.

6. Перевірити умову (3.2): $t_k(PRG_k) \leq t_D$. Якщо умова не виконується, перейти до кроку 2.

7. Вибрати відповідні програмі PRG_k інтенсивності переходів $\{\lambda_{ij}\}_k$ з множини $\{\lambda_{ijk}\}$.

8. $z = z + 1$.

9. Якщо $z < Z$, перейти до кроку 14.

10. Обрахувати значення $P_{zk}(PRG_k, t)$ за допомогою Марківської моделі захищеного процесу, використовуючи початкові умови $\{P_{zk}(t = 0)\}$ і інтенсивності переходів $\{\lambda_{ij}\}_k$ для програми PRG_k.

11. Обрахувати $L_{kz} = \int_0^T V_z(t) P_{zk}\,(PRG_k, t)dt$.

12. $L_k = L_k + L_{kz}$.

13. Перейти до кроку 8.

14. Якщо $L_{opt} < L_k$, то $L_{opt} = L_k, PRG_{opt} = PRG_k$.

15. Перейти до кроку 2.

16. Виконати програму PRG_{opt}.

У розглянутому випадку значення $t_k(PRG_k)$ повинні бути відомі (визначені до вирішення оптимізаційної задачі) для заданих програм конфігурації з множини $\{PRG_k\}$. У більш загальному випадку альтернативні програми можуть бути не визначені заздалегідь і можуть синтезуватися автоматично. У цьому випадку значення $t_k(PRG_k)$ повинні бути розраховані в залежності від структури програми та часу виконання її функцій.

Один із можливих способів визначення конфігурації розглянуто у пункті 3.3 для програм $t_k(PRG_k)$ обраних програм. Для великої кількості альтернативних програм повний пошук може бути замінений відомими методами оптимізації, такими як метод гілок та меж або іншими.

Розглянутий метод оптимізації конфігурації системи захисту ІКС відрізняється від інших відомих рішень новим набором правил, що дозволяють реалізовувати адаптивний захист від комплексних інформаційних загроз. Реконфігурація системи захисту повинна виконуватися з метою досягнення максимального зростання загального ефекту або мінімізації збитку протягом визначеного часового інтервалу з обмеженнями на час пошуку та реалізації керуючої програми. У контексті структури системи захисту у пункті 3.1, рішення оптимізаційної задачі (3.1)-(3.4) може бути реалізоване в модулі конфігурації на рис. 3.3.

3.4 Висновки до розділу

Запропоновано новий метод адаптивного захисту корпоративної інформаційної системи від комплексних деструктивних впливів. Цей метод орієнтований на нову архітектуру системи захисту КІС від комплексних деструктивних впливів, яка відрізняється новим набором функціональних блоків і зв'язків між ними. Метод відрізняється тим, що базується на розробленому алгоритмі адаптивного захисту, а також методу оптимізації конфігурації системи такого захисту. Алгоритм відрізняється тим, що передбачає як виключення деструктивного впливу, так і реконфігурацію системи захисту у випадку, якщо використання цієї системи не надає достатнього ефекту. У такому випадку використовується метод оптимізації конфігурації системи захисту, який відрізняється тим, що використовує запропоновану в розділі 2 модель функціонування системи при виборі оптимальної конфігураційної програми. Запропонований метод дозволяє розширити можливості систем захисту щодо виявлення та усунення комплексних деструктивних впливів.

4 РОЗРОБКА ДОСЛІДНОГО ПРОТОТИПУ МУЛЬТИАГЕНТНОЇ СИСТЕМИ ВИЯВЛЕННЯ БОТНЕТІВ

4.1. Умови захисту корпоративних інформаційних систем від комплексних деструктивних впливів

Розглянемо можливі умови забезпечення інформаційної безпеки корпоративної багатомодальної інформаційно-навігаційної хмарної системи. Система базується на сервіс-орієнтованій архітектурі (СОА) і складається з слабкозв'язаних сервісів, що взаємодіють за допомогою уніфікованих протоколів із використанням веб-сокетів. У порівнянні із підходом REST застосування веб-сокетів дозволяє тривалий час утримувати з'єднання в активному стані та не виконувати його відкриття і закриття при кожній передачі даних. Це особливо важливо при використанні безпечного з'єднання (у протоколах TLS, HTTPS та ін.), коли створення логічного каналу вимагає генерації ключів. Ця операція триває довше, ніж передача середньостатистичного JSON-повідомлення, і використання традиційного підходу REST може призвести до значних накладних витрат і зменшення часу реакції сервісів. Крім того, веб-сокети дозволяють контролювати статус з'єднань та оперативно визначати та відновлювати сервіси, які з якихось причин відключилися від системи. Усі сервіси поділяються на дві категорії: системні, які забезпечують виконання завдань, необхідних для функціонування системи в цілому, і застосовні, що реалізують цілі системи. Перелік сервісів системи та їх опис подані в таблиці 4.1. Структура сервісу відображена на рис. 4.1. Кожен сервіс визначається контрактом (деталізацією формату взаємодії з іншими сервісами), інтерфейсом та реалізацією. Сервіси надають користувачам розділений доступ до інформації через свої інтерфейси.

Таблиця 4.1 - Сервіси Системи

Сервіс	Опис
1	2
Системні сервіси	
Сервіс доступу до даних	надає доступ до інформації, яка може бути використана різними сервісами (наприклад, відомості про облікові записи, користувачів тощо), та контролює правомірність доступу
Репозиторій сервісів	надає інформацію про зареєстровані в системі сервіси, їх статус і методи доступу до сервісів
Інтерфейс адміністратора	дозволяє керувати системою в режимі онлайн
Управління акаунтами	дозволяє запитувати та змінювати список облікових записів, їх ролей та привілеїв
Класна дошка	дозволяє сервісам публікувати інформацію про свої події для обробки іншими сервісами
Прикладні сервіси	
Сервіс корпоративного телебачення	транслює медіаконтент (відеоролики, оголошення, інформаційні повідомлення) на клієнтські пристрої (стаціонарні екрани)
Сервіс корпоративного порталу	дозволяє використовувати інформацію від сервісів системи на сайті організації
Сервіс комунікації	дозволяє користувачам керувати інформаційним простором за допомогою багатомодальних технологій (мова, жести)
Сервіс навігації	надає клієнтським пристроям інформацію про їхнє фізичне розташування в корпоративному просторі, про розташування підрозділів організації та маршрути їх досягнення

Кінець таблиці 4.1

1	2
Сервіс відеоконференцзв'язку	організує відеоконференцзв'язок між клієнтськими пристроями у корпоративному просторі
Сервіс ідентифікації	дозволяє ідентифікувати відвідувачів у різний спосіб (за допомогою електронних ключів, біометричних ознак)

Розглянемо взаємодію користувачів із сервісами інтерактивного корпоративного телебачення, локалізації та навігації Системи. Ці сервіси реалізуються у вигляді комплексу веб-камер, стаціонарних екранів і неттопів з метою спростити отримання користувачами інформації про організацію, новини, а також дані про розташування користувачів. Веб-камери використовуються під час реєстрації, ідентифікації та розпізнавання облич користувачів, що дозволяє автоматизувати їх аутентифікацію. Використання багатомодальних інтерфейсів спрощує процес отримання інформації користувачами.

Рисунок 4.1 - Структура сервісу

Однією з особливостей розроблюваного модуля корпоративного телебачення є його інтерактивність. Взаємодія може бути забезпечена за допомогою багатомодальних інтерфейсів. Користувачі створюють запити до сервісів, використовуючи різні інтерфейси (голосові, жестові) або за допомогою веб-додатків. Це дозволяє реалізувати управління модулем за допомогою голосу та жестів. Також модулем КТ можна управляти за допомогою портативних пристроїв користувачів. Адміністратори також можуть контролювати сервіси за допомогою спеціального веб-інтерфейсу. Загальний алгоритм взаємодії між користувачем і модулем виглядає наступним чином:

– Модуль КТ генерує одноразові токени для доступу до управління і виводить їх на стаціонарні екрани у вигляді QR-кодів.

– Користувач сканує QR-код за допомогою мобільного додатка і отримує токен.

– Мобільний додаток підключається до API КТ за допомогою отриманого токена і надає користувачеві графічний інтерфейс.

– Користувач використовує графічний інтерфейс для отримання даних про вміст і управління корпоративним телебаченням.

Схема управління подана на рис. 4.2.

В якості API КТ використовується інтерфейс на основі GraphQL. GraphQL – це мова запитів, яка дозволяє запитувати та оновлювати дані, що знаходяться в зовнішніх джерелах. GraphQL спрощує представлення структури даних між взаємодіючими сторонами та створює проміжний рівень, який забезпечує правильну передачу, маршрутизацію та трансформацію даних, обробку тригерів, незалежність від конкретних джерел та одержувачів інформації.

Модуль КТ надає два типи запитів GraphQL: query для отримання поточного стану сервісу та mutation для зміни стану (надсилання управляючих команд).

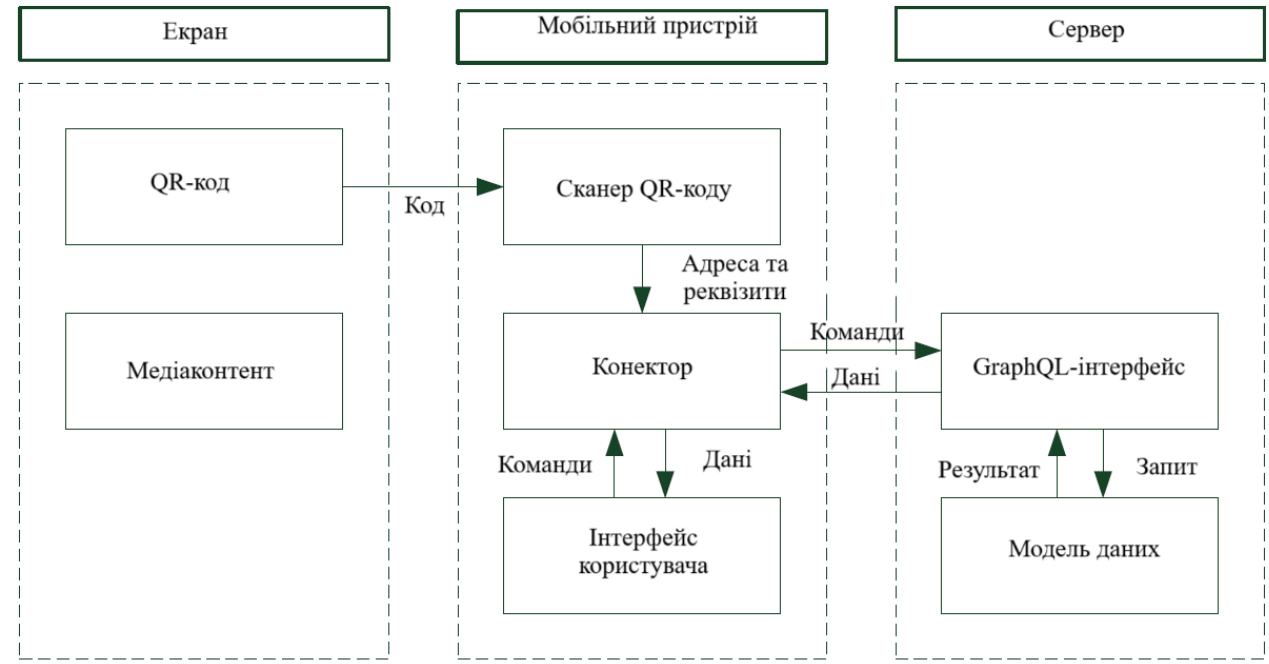


Рисунок 4.2 - Схема керування модулем КТ за допомогою мобільного додатка

Запит query має наступний вигляд:

```
query {
  monitor(id: <ID>, key: <key>) {
    currentMedia,
    status,
    medias {
      id,
      name
    }
  }
}
```

У запиті <ID> вказує унікальний ідентифікатор екрану КТ,

<key> - авторизаційний токен, обов'язковий при відправці першого запиту в сесії. Поля currentMedia, status, id, name є необов'язковими і визначають склад запитуваних даних. Склад полів наведений в таблиці 4.2.

Таблиця 4.2 Поля запиту

Поле		Опис
currentMedia		ID активного медіафайлу
status		Прапори стану екрана: 1 – помилка, 2 – режим налагодження включень, 4 – кешування увімкнено, 8 – пауза, 16 – блокування
medias.	id	ID наступного медіафайлу
medias.	name	Назва наступного медіафайлу

Запит на мутацію має наступний вигляд:

```
mutation {
  sendMessage(id: <ID>, commands: <commands>) {
    status
  }
}
```

Поле <ID> вказує ідентифікатор екрану, поле <commands> містить одну чи кілька керуючих команд, розділених символом «;». Запит повертає стан дисплею після виконання команди. Список команд наведено в таблиці 4.3.

Таблиця 4.3 - Керуючі команди КТ

Команда	Опис
1	2
next	Перемикання на наступний файл
prev	Перемикання на попередній файл
load <ID>	Завантаження файлу із заданим ID
pause [on | off]	Зупинка/відновлення
lock [on | off]	Блокування/розблокування екрану
reload	Перезавантаження програми

Кінець таблиці 4.3

1	2
debug [on | off]	Увімкнути/вимкнути режим налагодження

Кожен запит користувача повинен бути оброблений, що передбачає створення окремого завдання, яке вимагає виділення ресурсів (аудіо- та відеоканали, пам'ять, процесор, користувацькі сесії) протягом певного часу. Недостатність ресурсів хоча б одного типу під час виконання цих завдань може призвести до зниження доступності сервісу. Наприклад, у випадку єдиного користувача, який працює з корпоративним телебаченням, кожен наступний запит передбачає призупинення попереднього, якщо ці запити конфліктують за ресурс. У такому випадку загроза доступності не виникає. Проте при наявності кількох користувачів виділити необхідний ресурс для всіх завдань може бути неможливим. У цьому випадку використовуються стратегії управління користувацькими запитами, які повинні максимізувати метрики доступності сервісу. Вибір стратегій управління запитами і їх параметрів залежить від структури та характеру виникнення запитів. Таким чином, оптимальна стратегія може змінюватися залежно від умов функціонування сервісу. У цьому випадку для забезпечення доступності необхідно використовувати адаптивні методи вибору управляючих конфігурацій.

4.2 Структура програмного забезпечення системи адаптивного захисту КІС

Представимо схему потоків даних, що виникають при виконанні алгоритму вибору оптимальної програми захисту. На рис. 4.3 модуль конфігурації зберігає та надає низку початкових даних. Диспетчер програм зберігає та надає доступ до набору $\{PRG_k\}$ реалізованих програм захисту. Фільтр програм перевіряє ці програми на відповідність обмеженням. Компонент моделювання та

прогнозування оцінює ймовірності знаходження КІС у визначених станах у залежності від часу та дозволяє передбачити подальшу поведінку системи. Компонент оцінки ефекту використовується для розрахунку ефекту, досягнутого при функціонуванні КІС в актуальних умовах. Значення цього ефекту використовується як цільова функція для вибору оптимальної програми захисту.

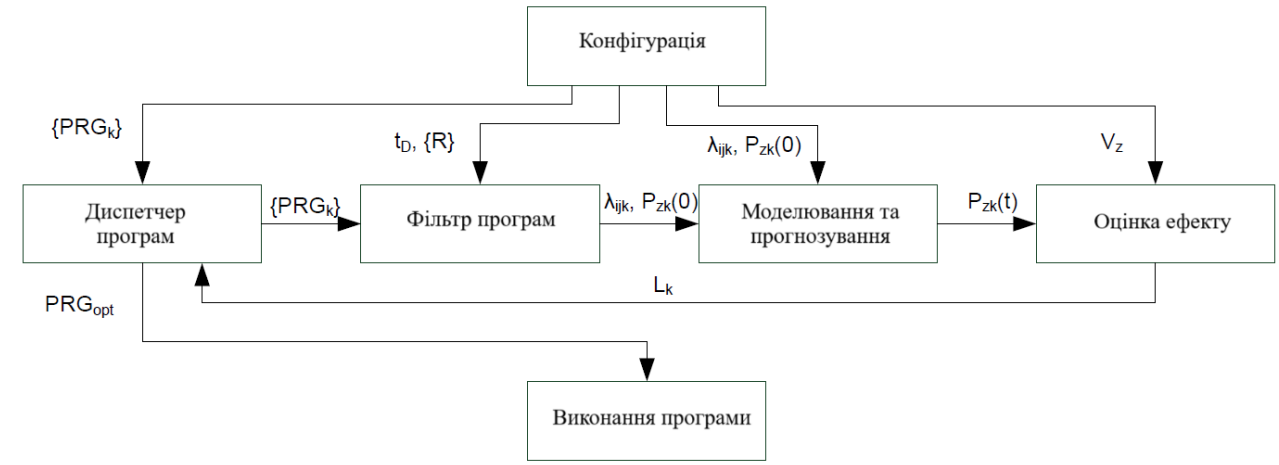


Рисунок 4.3 - Схема потоку даних для модуля адаптації

На рис. 4.4 представлений цикл виконання обраної програми захисту. Цей цикл включає в себе створення набору завдань з моніторингу даних (диспетчер завдань), визначення набору джерел даних для моніторингу (диспетчер джерел), отримання даних (конектор), структурування даних (парсер), аналіз даних за допомогою методів, визначених обраною програмою захисту (аналізатор), фільтрації даних (процесор) та передачі даних до застосункової системи (ЗС) для подальшого використання. Цей цикл включає зворотний зв'язок, дані в якому можуть передаватися оператором вручну або автоматично через диспетчера зворотного зв'язку.

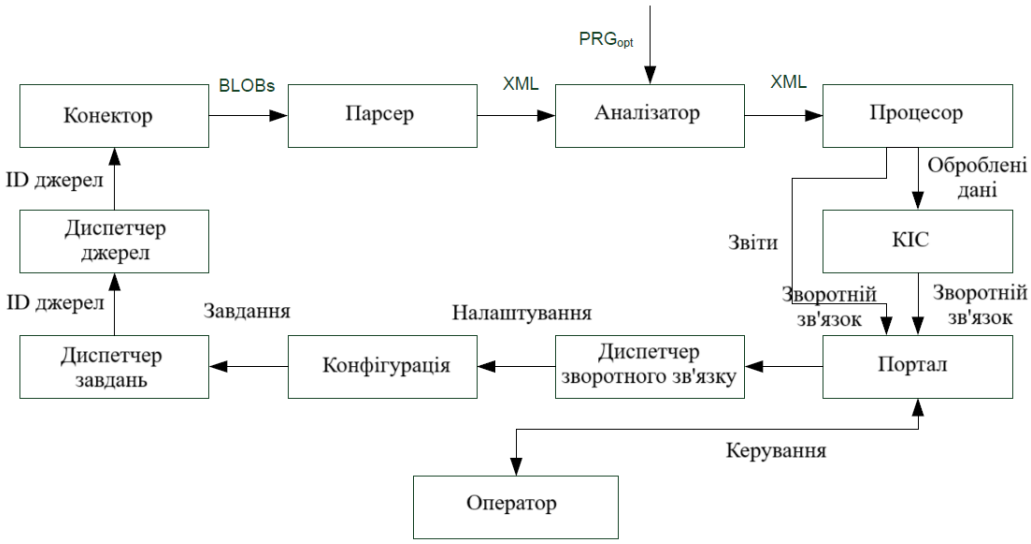


Рисунок 4.4 - Схема потоків даних для модуля виконання

Система захисту складається із наступних компонентів: модуль конфігурації, який зберігає активний стан системи захисту; модуль адаптації, що виправляє стан системи для досягнення оптимальних значень ефекту; модуль реалізації, який виконує програми конфігурування системи захисту, та адміністративний інтерфейс. Розглянемо діаграми класів, що характеризують структуру окремих компонентів додатка, побудовані за допомогою UML. На рис. 4.5 зображено UML-діаграму, що характеризує структуру класів для компонента "Диспетчер завдань" і визначає його зв'язки з іншими компонентами.

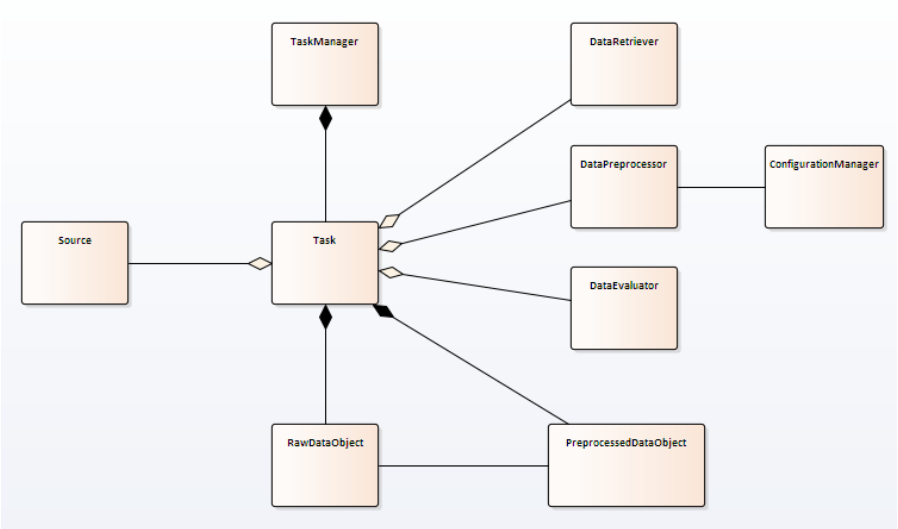


Рисунок 4.5 - Діаграма класів для диспетчера завдань

На рис. 4.6 представлена аналогічна структура для диспетчера джерел даних.

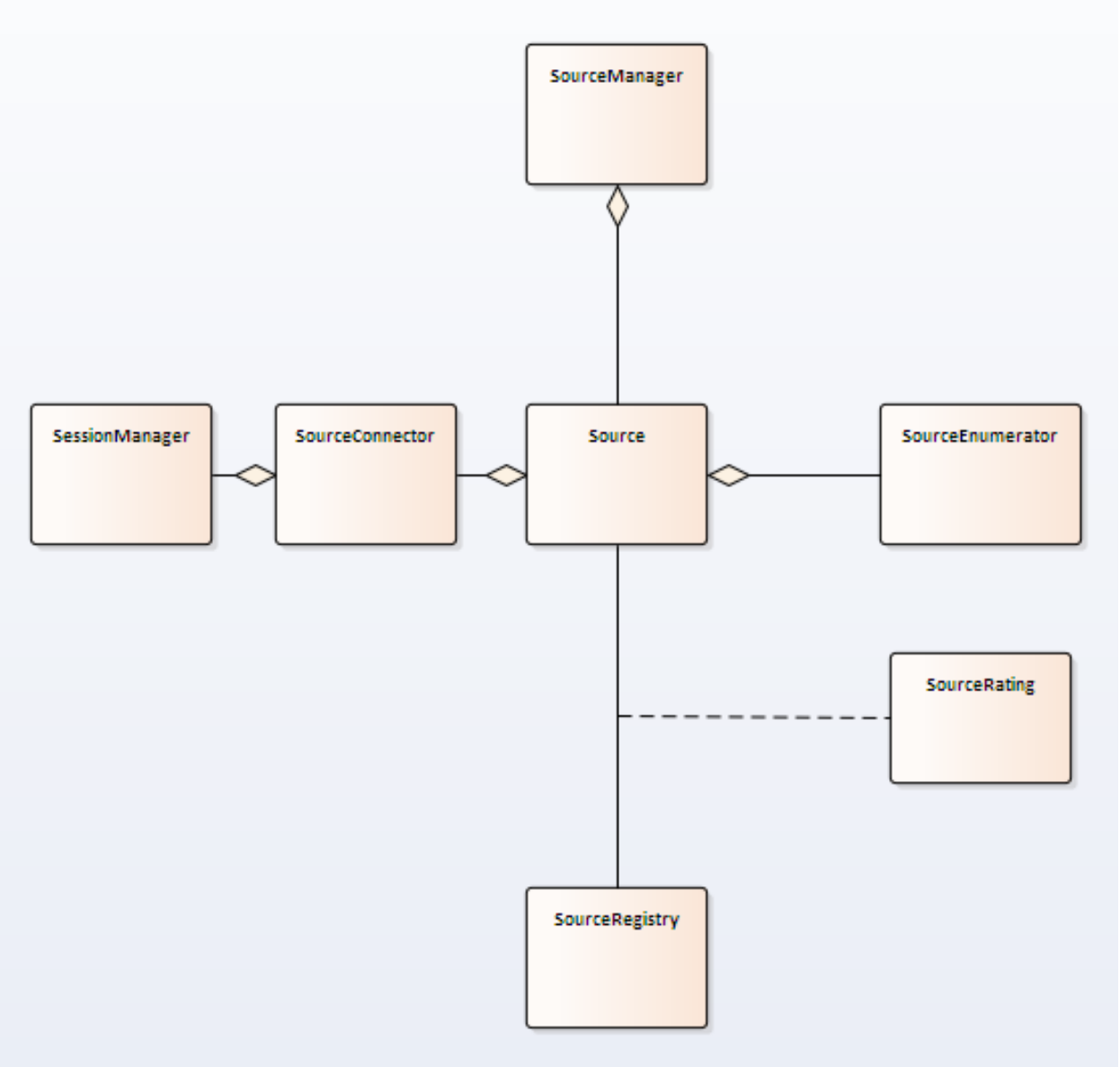


Рисунок 4.6 - Діаграма класів для диспетчера джерел даних

4.3. Типові ситуації та заходи захисту

У таблиці 4.4 представимо типові ситуації, в яких розроблені методи, моделі та технічні рішення можуть бути застосовані.

Для прикладу розглянемо завдання пов'язане з протидією ненаправленим впливам на сервіси КІС, що може призвести до порушення їх доступності. Розглянемо це на прикладі сервісу інтерактивного корпоративного телебачення,

який здійснює доставку контенту за запитами користувачів на мобільні додатки та екрани. Використовуємо модель, описану в пункті 4.1

Таблиця 4.4 - Типові задачі та ситуації

№	Завдання	Приклад ситуації	Джерело загрози	Використовувані методи та моделі
1	2	3	4	5
1	Протидія цілеспрямованим деструктивним впливам на КІС	Атака «відмова в обслуговуванні» (DoS)	Користувач, який може бути як легітимним, так і нелегітимним	Пропозиції щодо нових способів захисту (п.3.2)
2	Протидія нецілеспрямованим деструктивним впливам на КІС	Вичерпання пропускної спроможності каналу передачі даних	Легітимний користувач	Метод оцінювання ефективності захисту
3	Протидія помилковому сприйняттю сервісами заявок, що надходять	Обробка помилково сприйнятих даних при використанні багатомодальних засобів людино-машинної взаємодії	Програмне забезпечення	Метод оцінювання ефективності захисту. Метод адаптивного захисту.

Як альтернативи для захисту розглядається множина стратегій управління

заявками, які можна уявити як набір дій <AH, AE, AL>, які виконуються відповідно при вищому, рівному або нижчому пріоритеті конфліктної заявки. При цьому оптимальність тієї чи іншої стратегії залежить від характеру потоку запитів та даних.

Для прикладу приведемо оцінку ефективності сервісу при різних стратегіях управління заявками. Рисунок 4.7 ілюструє, що при низькій інтенсивності виникнення запитів користувачів доцільно використовувати чергу, а при більш високих значеннях – стратегії з відмовами. Іншими словами, оптимальна конфігурація сервісу може змінюватися з часом при зміні умов функціонування сервісу, у даному випадку – інтенсивності запитів.

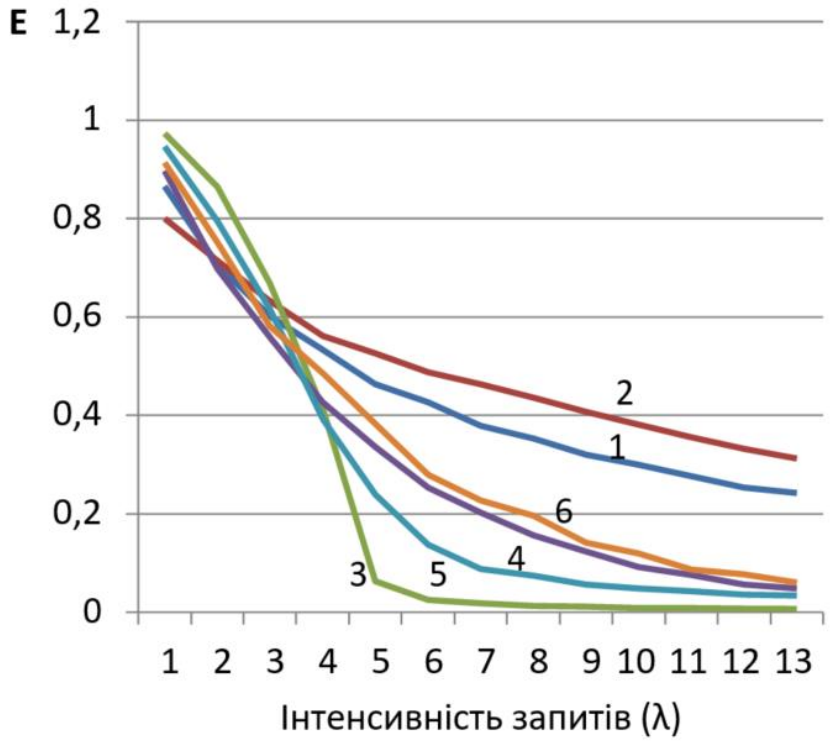


Рисунок 4.7 - Залежність ефекту при використанні різних стратегій управління запитами

На рис. 4.7 використовуються такі позначення стратегій: 1 – відхилення нового запиту; 2 – відхилення конкуруючих запитів; 3 – черга FIFO; 4 – черга LIFO; 5 – черга FIFO (максимальна затримка 1); 6 – черга LIFO (максимальна затримка

1).

Для адаптивного управління конфігурацією сервісу використовуємо метод, описаний у розділі 2. Графіки отриманого ефекту для трьох стратегій без застосування запропонованого методу та з його застосуванням наведено на рис. 4.8.

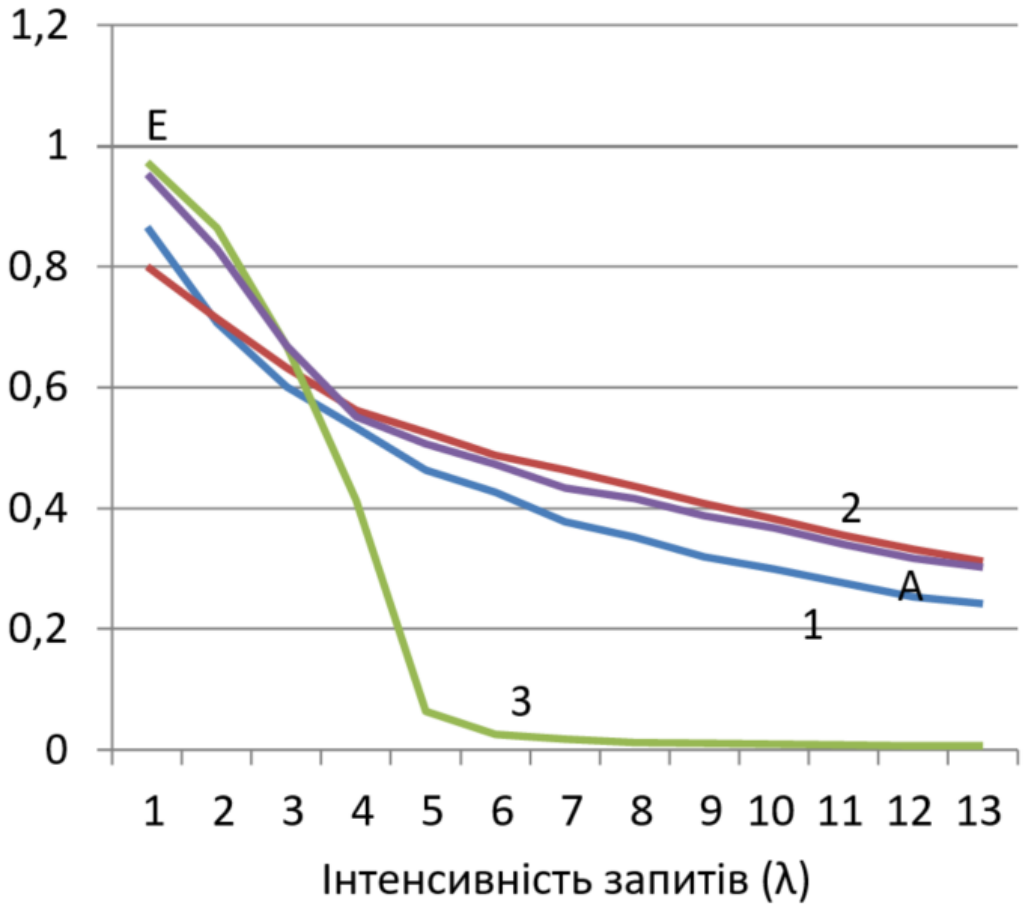


Рисунок 4.8 - Ефект у залежності від інтенсивності запитів при використанні статичних стратегій (1, 2, 3) та запропонованого методу (А).

На рисунку 4.9 показане відхилення ΔE, яке обчислюється для і-го рішення так:

$$\Delta E_i = \max_i E_i - E_i \qquad (4.1)$$

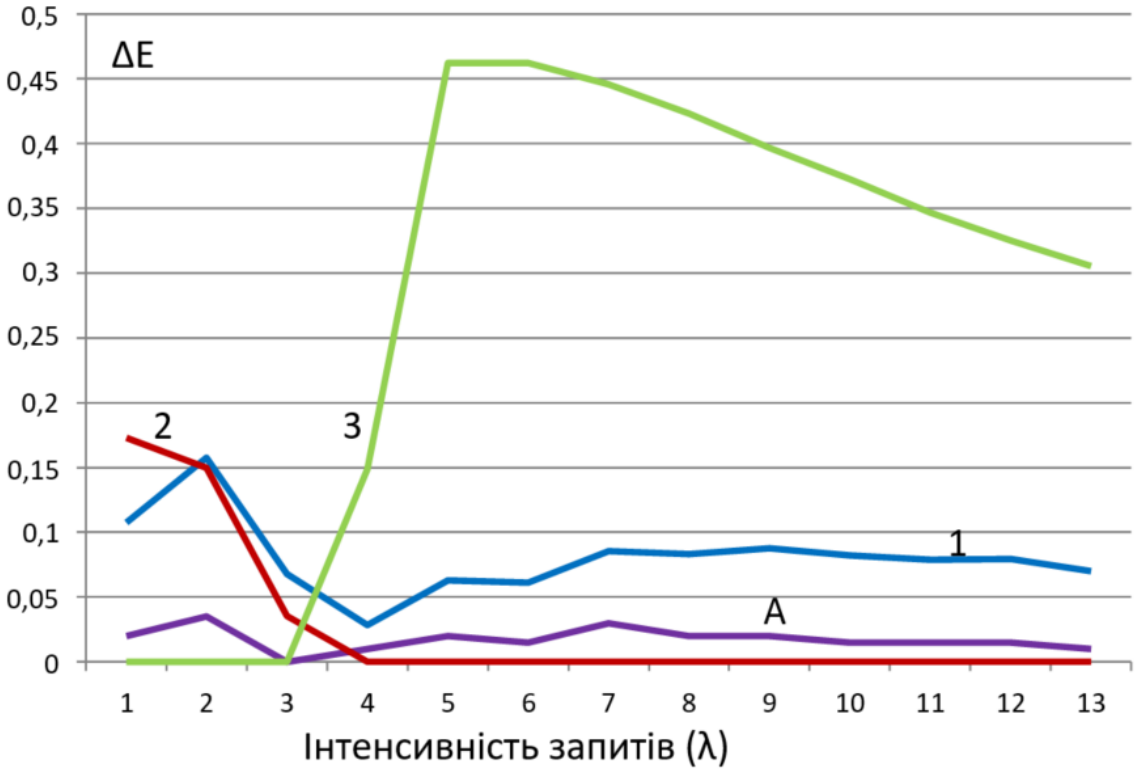


Рисунок 4.9 - Відхилення ефектів від максимальних значень

У таблиці 4.5 представлені значення середньоквадратичних відхилень отриманого ефекту від максимально досяжного ефекту при застосуванні розглянутих стратегій.

Таблиця 4.5 Середньоквадратичні відхилення ефекту від максимального значення

Використовувана стратегія	Середньоквадратичне відхилення
1	0,31
2	0,23
3	1,20
А (Адаптивне управління)	0,07

Проведення експериментів свідчить, що хоча для кожного значення

інтенсивності виникнення запитів використання запропонованого методу демонструє менший ефект порівняно з методом, оптимальним у даному контексті, але у середньому використання запропонованого методу дозволяє досягти найменшого відхилення від максимально можливого ефекту в різних умовах функціонування системи.

4.4 Висновки до розділу

Запропонована архітектура програмної системи адаптивного захисту корпоративної інформаційної системи від комплексних інформаційних загроз відрізняється новим набором функціональних блоків та їх взаємозв'язків і може бути використана в перспективних системах захисту інформації, що реалізують запропоновані методи та моделі. Також надано метод виявлення атак на комп'ютерні системи, особливість якого полягає в можливості протидії комплексним атакам. Запропоновано типові сценарії використання заходів захисту в різних ситуаціях інформаційної безпеки - при наявності цільових і нецільових деструктивних впливів, технічних помилок. Проведено моделювання, яке показує ефективність запропонованих рішень. Запропоновані рішення дозволяють якісно оцінювати процеси, що відбуваються в захищених системах. Вони дозволяють обґрунтовувати обґрунтовані заходи в галузі управління даними при захисті прикладних систем від комплексних інформаційних загроз. Ці рішення можуть бути використані як для планування та здійснення протидії шкідливим впливам, так і для оперативного управління інформаційною безпекою систем. Зокрема, розглянуті моделі і методи можуть бути використані для високорівневої формалізації процесів функціонування корпоративних інформаційних систем на підприємствах, в соціальних установах, транспортних об'єктах, торговельних центрах та ін. Подібні моделі та методи також можуть успішно використовуватися в завданнях планування та вибору захисних програм для протидії загрозам в цих організаціях. Ця можливість обґрунтована відповідністю результатів моделювання загальним закономірностям.

ВИСНОВКИ

В даній роботі була вирішена задача підвищення рівня захисту корпоративних інформаційних систем від комплексних деструктивних впливів за рахунок проведення аналізу інформаційних потоків в інформаційних системах.

Розроблений метод оцінювання ефективності захисту корпоративних інформаційних систем від комплексних деструктивних впливів ґрунтується на використанні запропонованої марківської моделі функціонування захищеної КІС у умовах комплексних деструктивних інформаційних загроз дозволяє підвищити рівень захищеності корпоративних систем.

Запропонований метод адаптивного захисту корпоративної інформаційної системи від комплексних деструктивних впливів орієнтований на нову архітектуру системи захисту КІС від комплексних деструктивних впливів, яка відрізняється новим набором функціональних блоків і зв'язків між ними. Ефективність забезпечується за рахунок використання розробленого алгоритму адаптивного захисту, а також методу оптимізації конфігурації системи такого захисту. Особливість алгоритму полягає в виключенні деструктивного впливу, так і реконфігурації системи захисту у випадку, якщо використання цієї системи не надає достатнього ефекту.

Запропонована архітектура програмної системи адаптивного захисту корпоративної інформаційної системи від комплексних інформаційних загроз відрізняється новим набором функціональних блоків та їх взаємозв'язків і може бути використана в перспективних системах захисту інформації, що реалізують запропоновані методи та моделі.

Розроблені аглоритми, методи та система дозволяють підвищити рівень захисту корпоративних інформаційних систем від комплексних деструктивних впливів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Daniel Alejandro Rossit, Fernando Tohmé, Mariano Frutos. Industry 4.0: Smart Scheduling. *International Journal of Production Research*. 2019. Vol. 57, No 12. PP. 3802-3813. DOI: 10.1080/00207543.2018.1504248

2. G. Aceto, V. Persico, A. Pescapé. A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges. *IEEE Communications Surveys & Tutorials*. 2019. Vol. 21, No. 4. PP. 3467-3501. DOI: 10.1109/COMST.2019.2938259.

3. Невлюдов І.Ш., Євсєєв В.В., Андрусевич А.О., Максимова С.С. Моделі та методи кіберфізичних виробничих систем в концепції Industry 4.0 Монографія. – Oktan Print – Prague. 2023. – 321 с.

4. Грибовська, Ю., Кононенко, Ж. Застосування інформаційних систем в управлінні підприємством. *Економіка та суспільство*. 2023. Vol. 47. DOI: https://doi.org/10.32782/2524-0072/2023-47-84

5. Кириченко О. Сучасні аспекти та технології управління розвитком підприємств. *Вчені записки Університету «КРОК»*. 2022. Вип. 2. С. 107–115. DOI: https://doi.org/10.31732/2663-2209-2022-66-107-115

6. Asif Qumer Gill, Eng Chew. Configuration information system architecture: Insights from applied action design research. *Information & Management*. 2019. Volume 56, Issue 4. Pages 507-525. https://doi.org/10.1016/j.im.2018.09.011.

7. Fizza K., Banerjee A., Mitra K. et al. QoE in IoT: a vision, survey and future directions. *Discov Internet Things.* 2021. Vol. 1, No 4. DOI: https://doi.org/10.1007/s43926-021-00006-7

8. G. Kougioumtzidis, V. Poulkov, Z. D. Zaharis and P. I. Lazaridis. A Survey on Multimedia Services QoE Assessment and Machine Learning-Based Prediction. *IEEE Access*. 2022. Vol. 10. PP. 19507-19538. DOI: 10.1109/ACCESS.2022.3149592.

9. T. Hoßfeld, P. E. Heegaard, M. Varela, L. Skorin-Kapov and M. Fiedler. From QoS Distributions to QoE Distributions: a System's Perspective. *6th IEEE*

Conference on Network Softwarization (NetSoft). 2020. PP. 51-56. DOI: 10.1109/NetSoft48620.2020.9165426.

10. A. A. Barakabitze et al.. QoE Management of Multimedia Streaming Services in Future Networks: A Tutorial and Survey. *IEEE Communications Surveys & Tutorials*. 2020. Vol. 22, No. 1. PP. 526-565. DOI: 10.1109/COMST.2019.2958784.

11. A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal and S. W. Kim. Multimedia Internet of Things: A Comprehensive Survey. *IEEE Access*. 2020. Vol. 8. PP. 8202-8250. DOI: 10.1109/ACCESS.2020.2964280.

12. U. Thirupalu, E. Kesavulu Reddy. Performance Analysis of Cryptographic Algorithms in the Information Security. *International Journal of Engineering Research & Technology (IJERT)*. 2019. Vol. 8, No 02. PP. 64-69

13. Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi. Research on Various Cryptography Techniques. *International Journal of Recent Technology and Engineering (IJRTE)*. 2019. Vol. 8, No 2S3. PP. 395-405.

14. M. Zhang, Y. Chen and J. Huang. SE-PPFM: A Searchable Encryption Scheme Supporting Privacy-Preserving Fuzzy Multikeyword in Cloud Systems. *IEEE Systems Journal*. 2021. Vol. 15, No. 2. PP. 2980-2988. DOI: 10.1109/JSYST.2020.2997932.

15. P. Ranaweera, A. D. Jurcut and M. Liyanage. Survey on Multi-Access Edge Computing Security and Privacy. *IEEE Communications Surveys & Tutorials*. 2021. Vol. 23, No. 2. PP. 1078-1124. DOI: 10.1109/COMST.2021.3062546.

16. Dichenko S.A., Finko O.A. Controlling and Restoring the Integrity of Multi-Dimensional Data Arrays through Cryptocode Constructs. *Program Comput Soft*. 2021. Vol. 47. PP. 415–425. DOI: https://doi.org/10.1134/S0361768821060049

17. Kumar R., Venkatesh K. Centralized and Decentralized Data Backup Approaches. *Proceedings of International Conference on Deep Learning, Computing and Intelligence. Advances in Intelligent Systems and Computing*. 2022. Vol. 1396. DOI: https://doi.org/10.1007/978-981-16-5652-1_60

18. Muniyal B. Analysis of Execution Time for Encryption During Data

Integrity Check in Cloud Environment. *Security in Computing and Communications*. *SSCC 2018. Communications in Computer and Information Science*. 2019. Vol. 969. DOI: https://doi.org/10.1007/978-981-13-5826-5_48

19. Xiaohua Ge, Qing-Long Han, Xian-Ming Zhang, Derui Ding, Fuwen Yang. Resilient and secure remote monitoring for a class of cyber-physical systems against attacks. *Information Sciences*. 2020. Vol. 512. PP. 1592-1605. DOI: https://doi.org/10.1016/j.ins.2019.10.057.

20. Muhammad Sohail Ibrahim, Wei Dong, Qiang Yang. Machine learning driven smart electric power systems: Current trends and new perspectives. *Applied Energy*. 2020. Vol. 272. DOI: https://doi.org/10.1016/j.apenergy.2020.115237.

21. Zhuotao Liu, Yangxi Xiang, Jian Shi, Peng Gao, Haoyu Wang, Xusheng Xiao, Bihan Wen, and Yih-Chun Hu. HyperService: Interoperability and Programmability Across Heterogeneous Blockchains. *In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery*. 2019. PP. 549–566. DOI: https://doi.org/10.1145/3319535.3355503

22. X. Wang, D. Bo, C. Shi, S. Fan, Y. Ye and P. S. Yu. A Survey on Heterogeneous Graph Embedding: Methods, Techniques, Applications and Sources. *IEEE Transactions on Big Data*. 2023. Vol. 9, No. 2. PP. 415-436. DOI: 10.1109/TBDATA.2022.3177455.

23. Березький О.М. Дослідження і проектування компютерних систем та мереж: навч.посіб. Тернопіль: ЗУНУ, 2022. – 252 с

24. J. F. Balarezo, S. Wang, K. Gomez Chavez, A. Al-Hourani and S. Kandeepan. Dynamics of Botnet Propagation in Software Defined Networks Using Epidemic Models. *IEEE Access*. 2021. Vol. 9. PP. 119406-119417. DOI: 10.1109/ACCESS.2021.3108181.

25. J. F. Balarezo, S. Wang, K. Gomez Chavez, A. Al-Hourani and S. Kandeepan. Dynamics of Botnet Propagation in Software Defined Networks Using Epidemic Models. *IEEE Access*. 2021. Vol. 9. PP. 119406-119417. DOI: 10.1109/ACCESS.2021.3108181.

26. Mahsa Nooribakhsh, Mahdi Mollamotalebi. A review on statistical approaches for anomaly detection in DDoS attacks. *Information Security Journal: A Global Perspective*. 2020. Vol. 29, No 3. PP. 118-133. DOI: 10.1080/19393555.2020.1717019

27. N. Ravi, S. M. Shalinie, C. Lal, M. Conti. AEGIS: Detection and Mitigation of TCP SYN Flood on SDN Controller. *IEEE Transactions on Network and Service Management*. 2021. Vol. 18, No. 1. PP. 745-759. DOI: 10.1109/TNSM.2020.3037124.

28. Ageyev D., Radivilova T., Mulesa O., Bondarenko O., Mohammed O. Traffic Monitoring and Abnormality Detection Methods for Decentralized Distributed Networks. *Information Security Technologies in the Decentralized Distributed Networks. Lecture Notes on Data Engineering and Communications Technologies*. 2022. Vol. 115. DOI: https://doi.org/10.1007/978-3-030-95161-0_13

29. Fernandes G., Rodrigues J.J.P.C., Carvalho L.F. et al. A comprehensive survey on network anomaly detection. *Telecommun Syst*. 2019. Vol. 70. PP. 447–489. DOI: https://doi.org/10.1007/s11235-018-0475-8

30. M. P. Novaes, L. F. Carvalho, J. Lloret and M. L. Proença. Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment. *IEEE Access*. 2020. Vol. 8. PP. 83765-83781. DOI: 10.1109/ACCESS.2020.2992044.

31. Mohammad A. H., Alwada'n T., Almomani O., Smadi S., & Elomari N. Bio-inspired Hybrid Feature Selection Model for Intrusion Detection. *Computers, Materials and Continua*. 2022. Vol. 73, No 1. PP. 133-150. DOI: https://doi.org/10.32604/cmc.2022.027475

32. M. M. Ahsan, K. D. Gupta, A. K. Nag, S. Poudyal, A. Z. Kouzani and M. A. P. Mahmud. Applications and Evaluations of Bio-Inspired Approaches in Cloud Security: A Review. *IEEE Access*. 2020. Vol. 8. PP. 180799-180814. DOI: 10.1109/ACCESS.2020.3027841.

33. Omar Almomani. A Hybrid Model Using Bio-Inspired Metaheuristic Algorithms for Network Intrusion Detection System. *Computers, Materials & Continua*. 2021. PP. 409-429. DOI: 10.32604/cmc.2021.016113

34. H. Zhou and G. Gu. Cerberus: Enabling Efficient and Effective In-Network Monitoring on Programmable Switches. *IEEE Symposium on Security and Privacy (SP)*. 2023. PP. 16. DOI: 10.1109/SP54263.2024.00016

35. S. Marchenkov, D. Korzun. Smart Spaces Middleware: A Requirement-Oriented Overview. *Conference of Open Innovations Association (FRUCT)*. 2020. PP. 134-143. DOI: 10.23919/FRUCT49677.2020.9211076.

36. Babak V.P., Babak S.V., Myslovych M.V., Zaporozhets A.O., Zvaritch V.M. Methods and Models for Information Data Analysis. *In: Diagnostic Systems For Energy Equipments. Studies in Systems, Decision and Control*. 2020. Vol. 281. DOI: https://doi.org/10.1007/978-3-030-44443-3_2

37. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020.– 236 с.

38. Lilei Zheng, Ying Zhang, Vrizlynn L.L. Thing. A survey on image tampering and its detection in real-world photos. *Journal of Visual Communication and Image Representation*. 2019. Vol. 58. PP. 380-399. DOI: https://doi.org/10.1016/j.jvcir.2018.12.022.

39. Rahul Thakur, Rajesh Rohilla. Recent advances in digital image manipulation detection techniques: A brief review. *Forensic Science International*. 2020. Vol. 312. DOI: https://doi.org/10.1016/j.forsciint.2020.110311.

40. Meena K.B., Tyagi V. A copy-move image forgery detection technique based on Gaussian-Hermite moments. *Multimed Tools Appl*. 2019. Vol. 78. PP. 33505–33526. DOI: https://doi.org/10.1007/s11042-019-08082-2

41. Meena K.B., Tyagi V. Image Forgery Detection: Survey and Future. *Data, Engineering and Applications. Springer*. 2019. DOI: https://doi.org/10.1007/978-981-13-6351-1_14

42. Hossain S, Lee D-j. Deep Learning-Based Real-Time Multiple-Object Detection and Tracking from Aerial Imagery via a Flying Robot with GPU-Based Embedded Devices. *Sensors*. 2019. Vol. 19, No 15. DOI: https://doi.org/10.3390/s19153371

43. L. Jiao et al.. New Generation Deep Learning for Video Object Detection: A Survey. *IEEE Transactions on Neural Networks and Learning Systems*. 2022. Vol. 33, No. 8. PP. 3195-3215. DOI: 10.1109/TNNLS.2021.3053249.

44. Melnyk K., Bahniuk N., Lavrenchuk S., Khrystynets N., Boba R., Omelchuk D. Application of machine learning methods for face recognition. Computer-integrated technologies: education, science, production. 2023. Vol. 51. PP. 73-78. DOI: https://doi.org/10.36910/6775-2524-0560-2023-51-09

45. Nathan Walter, Jonathan Cohen, R. Lance Holbert & Yasmin Morag. *Fact-Checking: A Meta-Analysis of What Works and for Whom, Political Communication*. 2020. Vol. 37, No 3. PP. 350-375. DOI: 10.1080/10584609.2019.1668894

46. Петрасова С. В. Сучасні інформаційні технології в лінгвістиці : навч. посібник. Харків : Панов А. М., 2020. – 124 с.

47. С.А. Положаєнко, Ф.Г. Гаращенко, Л.Л. Прокоф’єва. Математитчне моделювання надійності тензометричних систем на основі евристичних моделей вимірювальних процедур. *Informatics and Mathematical Methods in Simulation*. 2022. Vol. 12, No. 4. PP. 358-366. DOI: 10.15276/imms.v12.no4.358

48. М.М. Браіловський, І.С. Іванченко, І.Р. Опірський, В.О. Хорошко. Інформаційно-психологічне протиборство в Україні. НАУ: Науковий журнал «Безпека інформації». 2019. Том 25, №3. С.144-149.

49. Choi Wonchan, Stvilia Besiki. Web credibility assessment: Conceptualization, operationalization, variability, and models. *Journal of the Association for Information Science and Technology*. 2015. Vol. 66. DOI: 10.1002/asi.23543.

50. Ivano Lauriola, Alberto Lavelli, Fabio Aiolli. An introduction to Deep Learning in Natural Language Processing: Models, techniques, and tools. *Neurocomputing*. 2022. Vol. 470. PP. 443-456. DOI: https://doi.org/10.1016/j.neucom.2021.05.103.

51. О. В. Барабаш, О. В. Свинчук, А. П. Мусієнко. Математичне моделювання та оптимізація процесів і систем. Частина 1. Навчальний посібник. КПІ ім. Ігоря Сікорського, 2023. – С. 160.

ДОДАТОК А ПЕРЕЛІК НАУКОВИХ ПРАЦЬ

Міжнародний науково-технічний журнал
«Вимірювальна та обчислювальна техніка в технологічних процесах»
ISSN 2219-9365

https://doi.org/10.31891/2219-9365-2023-74-1
УДК 004.056

МОСТОВИЙ Сергій
Хмельницький національний університет
https://orcid.org/0000-0002-9505-3206
e-mail: serhii.mostovyi@khmnu.edu.ua
ПЕТЛЯК Наталія
npetlyak@khmnu.edu.ua
Хмельницький національний університет
ГОЛОТА Ірина
holota@khmnu.edu.ua

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ІНСТРУМЕНТІВ ВИЯВЛЕННЯ І ЗАПОБІГАННЯ ВТОРГНЕНЬ НА ВУЗЛИ В КОРПОРАТИВНИХ МЕРЕЖАХ

В роботі наведено результати досліджень ефективності систем виявлення вторгнень в корпоративну мережу при різній інтенсивності трафіка та для різних типів атак.
Ключові слова: корпоративна мережа, виявлення вторгнень, ефективність виявлення та запобігання вторгненням.

MOSTOVYI Serhii, PETLYAK Nataliia, HOLOTA Iryna
Khmelnytskyi National University

RESEARCH OF TOOLS EFFICIENCY FOR DETECTION AND PREVENTION OF INTRUSIONS ON CORPORATE NETWORKS NODES

The increase in the number of various methods of intrusions and their implementation in the form of attacks requires the need to improve existing technologies and means of data protection in corporate computer networks. Among the conditions that have a serious impact on the suitability of various methods, it is possible to single out a rapid increase in the volume of traffic and bandwidth of the communication channel. This means that there is a need to find an algorithm that reduces the amount of calculations. The mechanism for detecting intrusions into the system is based on the assumption of stationarity of network traffic, that is, any deviation from the stationary characteristics of network traffic is understood as an attack. It follows that the problem of traffic analysis and detection of intrusions into the corporate network requires further research.

Despite the large number of methods, they all work in real time and are based on signature analysis, which makes them unsuitable for detecting new, previously unknown types of attacks. Most of the free software systems for detecting and preventing attacks available today use signature analysis.

The paper presents the results of research into the effectiveness of systems for detecting intrusions into the corporate network at different traffic intensities and for different types of attacks.

The effectiveness of the most common systems for detecting intrusions into the corporate network was investigated experimentally. The results showed that these systems give a stable result with a small amount of traffic and only for known types of attacks, since they are based on signature analysis. When the amount and intensity of traffic increases, these systems show rather poor results: they have a lot of packet loss and heavily load server resources. In order to increase the reliability of information security of corporate networks, there is a need to improve approaches to attack detection and traffic analysis.
Keywords: corporate network, intrusion detection, intrusion detection and prevention effectiveness.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Стрімкий та активний розвиток мережних технологій призводить до появи нових типів атак на корпоративні комп'ютерні мережі [1]. Зростання кількості різноманітних методів вторгнень та їх реалізацій у вигляді атак вимагає необхідності удосконалення наявних технологій та засобів захисту даних у корпоративних комп'ютерних мережах. Серед умов, що мають серйозний вплив на придатність різних методів, можна виділити швидке збільшення обсягу трафіку та смуги пропускання каналу зв'язку. Це означає, що виникає необхідність у пошуку алгоритму, який скорочує обсяг обчислень. В основі механізму виявлення вторгнень в систему лежить припущення про стаціонарність мережного трафіку, тобто під атакою розуміють будь-які відхилення від стаціонарних характеристик мережного трафіку. Звідси випливає, що проблема аналізу трафіку та виявлення вторгнень в корпоративну мережу потребує подальших досліджень.

Аналіз досліджень та публікацій

В роботі [2] проаналізовано сучасні підходи до виявлення та прогнозування атак на корпоративні мережі. Проте, незважаючи на велику кількість методів, вони всі працюють в реальному режимі часу та грунтуються на синатурному аналізі, що робить їх непридатними до виявлення нових, раніше невідомих типів атак. Більшість безкоштовних програмних систем для виявлення та запобігання атакам, що доступні на сьогодні, використовують саме сигнатурний аналіз.

Міжнародний науково-технічний журнал
«Вимірювальна та обчислювальна техніка в технологічних процесах»
ISSN 2219-9365

Формулювання цілей статті

Метою роботи є: дослідження ефективності таких систем для подальшого вдосконалення інформаційної безпеки в корпоративних мережах.

Виклад основного матеріалу

Критичне порівняння проводиться між системами виявлення та запобігання вторгненням Suricata та Snort [3,6].

Показниками, що використовуються для вимірювання ефективності систем є: швидкість виявлення атак, помилкові спрацьовування [4].

Для кількісної оцінки метрик, що використовуються для оцінки точності системи виявлення та запобігання вторгненню, можна використати наступні: охоплення (кількість атак, які можна виявити), ймовірність помилкових спрацьовувань, ймовірність виявлення резистивних атак, здатність обслуговувати канал з високою пропускною здатністю і ємністю [4]. Що стосується продуктивності, вона має ряд компонентів, і тому не є метрикою. У табл. 1 наведено деякі показники, що відображають ємність.

Необхідно реєструвати такі показники: байти в секунду, пакети в секунду та кількість мережевих атак. Крім того, для кожної системи виявлення та запобігання вторгненню в мережу зменшено кількість втрачених пакетів, також були записані фактичні тригери, помилкові спрацьовування, негативні тригери та загальна кількість тривог. Нарешті, хост відстежує використання центрального процесора та пам'яті, постійне зберігання, пропускну здатність інтерфейсу та статистику файлів підкачки.

Тестовий стенд налаштований у віртуальному середовищі, що сприяє мобільності та безпеці експерименту. Це було необхідно для частого повторення та реконфігурації експериментальних випробувань.

VMware Workstation 15 була використана як платформа для віртуалізації, багато в чому завдяки хорошій продуктивності вводу-виводу та жорсткого диска порівняно з іншими засобами віртуалізації. В якості операційної системи було обрано 32-розрядну Ubuntu 18.04 LTS. Ubuntu регулярно оновлюється і має хорошу базу спільнот. Це також найпопулярніша операційна система Linux.

Таблиця 1

Оцінка потенціалу

Показник, що перевіряється	Використання ресурсів
Пакетів в секунду	Цикли CPU, пропускна здатність інтерфейсів, пропускна здатність шини
Байт в секунду (середній розмір пакета)	Цикли CPU, пропускна здатність інтерфейсів, пропускна здатність шини
Протоколи	Цикли CPU і пропускна здатність шини
Кількість унікальних хостів	Розмір пам'яті, цикли CPU, пропускна здатність шини
Кількість нових з'єднань в секунду	Цикли CPU і пропускна здатність шини
Кількість одночасних з'єднань	Розмір пам'яті, цикли CPU, пропускна здатність шини
Попередження в секунду	Розмір пам'яті, цикли CPU, пропускна здатність шини

За замовчуванням апаратна конфігурація для системи виявлення та запобігання вторгнень в мережу становила 2,8 ГГц чотирьохядерним процесором Intel Xeon (E5462) з 4-ядерною 3 ГБ DDR2 800 МГц повністю буферованою пам'яттю. Кожна система також мала максимальний об’єм жорсткого диска 20 ГБ. Мережевий трафік передавався окремо для кожної системи. Система, що використовується для відтворення мережевого трафіку, використовує одне ядро та 1 Гб оперативної пам'яті. VMware хост операційної системи, що використовує 2 Гб оперативної пам'яті і 1 ядро, що перешкоджає хосту з якого виробляє на випробувальному стенді.

Snort і Suricata були налаштовані на роботу з однаковими правилами. Suricata використовує різні класифікації конфігурації Snort, яка використовує 134 декодери та 174 правила препроцесора. Ідентичні методи реєстрації, які називаються Barnyard, MySQL та AcidBase, використовувались як для систем виявлення вторгнень в мережі, так і для систем запобігання. Версії Snort та Suricata були v2.9.8.3 та v4.1.2 відповідно.

Обидві системи використовували набір правил VRT Snort v2.9.8.3 у поєднанні з набором правил для нових загроз.

Для тестування було використано реальний мережевий трафік у фоновому режимі [5]. Однак повторення експериментів із трафіком у реальному часі було б непередбачуваним через його динаміку. Було обрано використання трафіку, захопленого з файлу pcap. Це сприяло їх обробці системою виявлення та попередження вторгнення мережі в автономному режимі, дозволяючи відтворювати в мережі з різною швидкістю, використовуючи TCPReplay. Крім того, усунуто всі ризики для критично важливих мереж. Використовуваний трафік було зафіксовано для запуску атак Metasploit на комп'ютері під керуванням Microsoft Windows 2000. Windows 2000 було обрано як найбільш підходящий Metasploit для цієї операційної системи порівняно з іншими.

Атаки, перелічені в таблиці 2, реєструються за допомогою Wireshark [7]. Частина програми

Міжнародний науково-технічний журнал
«Вимірювальна та обчислювальна техніка в технологічних процесах»
ISSN 2219-9365

Wireshark, Edicap, була використана для зміни часової позначки використовуваного трафіку та співвіднесення її з трафіком у фоновому режимі. У цій дії вони були об'єднані в хронологічному порядку, щоб атакуючий трафік перемістився на другий план.

Відстежувались такі ресурси: використання центрального процесора, використання пам'яті, опір пропускної здатності пам'яті та пропускна здатність мережі. Це було зроблено за допомогою інструмента командного рядка Linux dstat. Кожного разу, коли запускалося тестування, реєструвались початок і кінець трафіку запуску NIDPS. Трафік проходив через хости 192.168.16.2 та 192.168.16.128, але був позначений як небажаний трафік.

Таблиця 2

Вивчення атак

Код	Ім'я	Опис
ms03_026_dcom	Microsoft RPCDCOM Interface Overflow	Модуль використовуваного стеку переповнення буфера в службі RPCSS
ms05_039_pnp	Microsoft Server Service NetpwPathCanonicalize Overflow	Стек переповнення буфера в службі Windows Plug and Play
ms05_047_pnp	Microsoft Plug and Play Service Registry Overflow	Стек переповнення буфера в службі Windows PnP. Причина перезавантажень.
ms06_040_netapi	Microsoft Server Service NetpwPathCanonicalize Overflow	Стек переповнення буфера в NetApi32 CanonicalizePathName () використовуючи функцію NetpwPathCanonicalize RPC виклик служби Server
ms05_017_msmq	Microsoft Message Queueing Service Path Overflow	Використовуваний стек переповнення буфера в RPC інтерфейсі в службі Microsoft Message Queueing
ms01_033_idq	Microsoft IIS5.0 IDQ Path Overflow	Використовуваний стек переповнення буфера в IDQ ISAPI обслуговування для Microsoft Index Server

Для визначення точності використаний контроль попереджень. Ці попередження, отримані без системи стресів, використовувались як еталон. Відхилення від базової лінії в умовах стресу показувало зміни в точності виявлення. У табл. 3 наведено кількість типів попередження, що генеруються під час нападу на кожну NIDPS.

Таблиця 3

Попередження згенеровані Snort і Suricata

Попередження	Snort	Suricata
ms05_040_pnp	4	4
ms05_047_pnp	1	1
ms05_039_pnp	1	6
ms03_026_dcom	1	2
ms01_033_1dq	2	4
ms05_017_msmq	2	3

На рис. 1 показані попередження Suricata на кожен експлоїт у всіх конфігураціях, але деякі попередження втрачені, що призводить до зменшення діапазону виявлення.

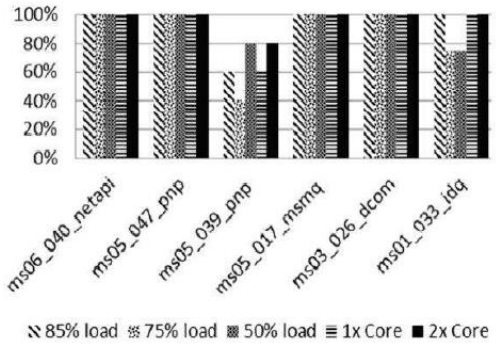


Рис 1 – Попередження у Suricata

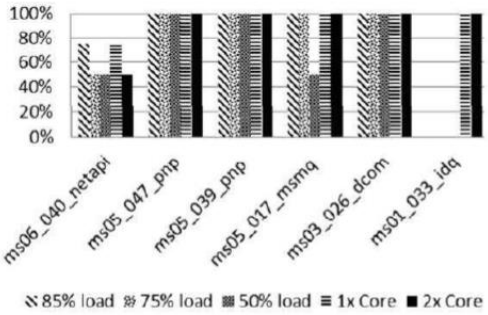


Рис 2 – Попередження у Snort

На рис. 2 показано провальні попередження Snort на ms01_033_idq. Ці помилкові негативні результати обумовлені надмірним навантаженням.

У Suricata спостерігається більша точність, ніж у Snort Частково це пов'язано з тим, що Snort менше

Міжнародний науково-технічний журнал
«Вимірювальна та обчислювальна техніка в технологічних процесах»
ISSN 2219-9365

контролює функціонування оповіщень під час атаки, ніж Suricata (два проти чотирьох). Snort не зміг попередити ms01_033_idq двома правилами з набору правил VRT, ідентифікаторами 1245 та 1244. Suricata був успішним, і ці сповіщення спрацьовували. Suricata має високі вимоги до обробки, саме тому він досягає більших експлуатаційних можливостей, ніж Snort. Snort має набагато нижчі системні вимоги, тому він не може працювати з втратою пакетів при максимальному навантаженні системи. При роботі в багатоядерній конфігурації Suricata показує менше втрат пакетів, ніж Snort. Suricata використовує наявні ядра більш рівномірно. Тести в автономному режимі показують, що Suricata набагато повільніша за Snort. Хоча Suricata використовує багатоядерну систему більш чітко, ніж Snort. З огляду на це, можна сказати, що Suricata має кращу масштабованість. Однак, якщо Snort отримує хороші результати пропускної здатності, рекомендується запускати кілька екземплярів Snort на декількох ядрах. Це може запропонувати таку ж масштабованість, як Suricata, але з додатковими витратами на обробку однопотокових додатків на декількох ядрах.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Експериментальним шляхом було досліджено ефективність роботи найбільш поширених систем виявлення вторгнень в корпоративну мережу. Результати показали, що дані системи дають стабільний результат при невеликому обсязі трафіка та лише для відомих типів атак, оскільки базуються на сигнатурному аналізі. При зростанні кількості та інтенсивності трафіка дані системи показують досить низькі результати: мають багато втрат пакетів та сильно навантажують ресурси сервера. З метою підвищення надійності інформаційної безпеки корпоративних мереж є необхідність в удосконаленні підходів до виявлення атак та аналізу трафіка.

Література

1. Методи проникнення в корпоративні мережі [Інтернет-ресурс]. – Режим доступу: https://www.kitgsm.com.ua/stati/bezpeka/metodi-proniknennya-v-korporativni-merezhi.html, вільний.

2. Husák M., Komárková J., Bou-Harb E., Čeleda P.Survey of Attack Projection, Prediction, and Forecasting in Cyber 5. Security. IEEE Communications Surveys Tutorials. September 2018. Vol. 21, No. 1. P. 640-660

3. Обзор систем обнаружения вторжений [Інтернет-ресурс]. Режим доступу: http://www.connect.ru вільний.

4. Критерии сравнения систем обнаружения атак [Інтернет-ресурс]. – Режим доступу: http://inf-bez.ru/?p=480, вільний.

5. Paxon V., Floyd S. Wide-area traffic: The failure of Poisson modeling. / V. Paxon, S. Floyd // IEEE/ACM Transactions on Networking. – 1995. – Vol. 3. – p. 226 – 244.

6. Snort [Інтернет-ресурс] / Web-сайт: snort; Режим доступу http://www.snort.org, вільний.

7. Wireshark [Інтернет-ресурс] / Web-сайт: wireshark; Режим доступу http://www.wireshark.org, вільний.

References

1. Metody pronyknennia v korporatyvni merezhi [Internet-resurs]. – Rezhym dostupu: https://www.kitgsm.com.ua/stati/bezpeka/metodi-proniknennya-v-korporativni-merezhi.html, vilnyi.

2. Husák M., Komárková J., Bou-Harb E., Čeleda P.Survey of Attack Projection, Prediction, and Forecasting in Cyber 5. Security. IEEE Communications Surveys Tutorials. September 2018. Vol. 21, No. 1. P. 640-660

3. Obzor sistem obnaruzheniya vtorzhenij [Internet-resurs]. Rezhym dostupu: http://www.connect.ru vilnyi.

4. Kriterii sravneniya sistem obnaruzheniya atak [Internet-resurs]. – Rezhym dostupu: http://inf-bez.ru/?p=480, vilnyi.

5. Paxon V., Floyd S. Wide-area traffic: The failure of Poisson modeling. / V. Paxon, S. Floyd // IEEE/ACM Transactions on Networking. – 1995. – Vol. 3. – p. 226 – 244.

6. Snort [Internet-resurs]./ Web-сайт: snort; Rezhym dostupu http://www.snort.org, vilnyi.

7. Wireshark [Internet-resurs]./ Web-сайт: wireshark; Rezhym dostupu http://www.wireshark.org, vilnyi.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Голоти Ірини Олександрівни
ПІБ здобувача вищої освіти

Студентки ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

19.12.23
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 6%**

	Документ		Сумарний збіг по Базі Даних	
ID: 123708 Назва: Метод захисту корпоративних інформаційних систем від комплексних деструктивних впливів Додано в БД: 2023-12-18 Автора: Голота І.О. Керівники: Орленко В.С. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	76523	623	528 (1%)	6 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016017616

Дата перевірки:
18.12.2023 14:13:38 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
18.12.2023 14:18:12 EET

ID користувача:
100008300

Назва документа: **Голота_Плагіат**

Кількість сторінок: 71 **Кількість слів:** 11278 **Кількість символів:** 89807 **Розмір файлу:** 2.29 MB **ID файлу:** 1015704887

2.23%
Схожість

Найбільша схожість: **0.7% з джерелом з Бібліотеки** (ID файлу: **1015654798**)

1.61% Джерела з Інтернету	68	Сторінка 73
0.95% Джерела з Бібліотеки	41	Сторінка 73

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	31

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Метод захисту корпоративних інформаційних систем від комплексних деструктивних впливів

Автор: Голота Ірина Олександрівна
Спеціальність: 125 – Кібербезпека
Освітня програма: освітньо-професійна
Науковий керівник: Орленко Вікторія Сергіївна, к.т.н, доцент
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 2,23%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 1%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ В.С. Орленко

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

освітньо-кваліфікаційного рівня «магістр»

Магістр Голота Ірина Олександрівна

Тема: Метод захисту корпоративних інформаційних систем від комплексних деструктивних впливів

Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека денної форми навчання

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень - ; кількість сторінок записки 79 ;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена розробці методу адаптивної реконфігурації захисту корпоративної інформаційної системи, що використовує аналіз інформаційних потоків в системі та оцінює результативність спрацювання системи захисту. Робота описує структуру системи, складові компоненти та принципи взаємодії. Проведено експериментальне дослідження, яке підтвердило ефективність розробленого методу.

2. Висновок про відповідність КР завданню Магістерська робота у повній мірі відповідає поставленому завданню як у теоретичній і практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми дослідження; її зв'язок із науковими програмами, планами, темами та сформульовано мету та основні завдання дослідження. У першому розділі було досліджено завдання та можливості сучасних систем захисту корпоративних інформаційних систем, описано відомі системи та методи захисту. У другому розділі визначено показники ефективності захисту корпоративних інформаційних систем, описано модель функціонування захищеної корпоративної інформаційної системи та підхід до оцінювання ефективності захисту таких систем. У третьому розділі запропоновано архітектуру системи адаптивного захисту інформаційних систем, представлено алгоритм адаптивного захисту та метод оптимізації конфігурації системи захисту. У четвертому розділі представлено структуру програмного забезпечення системи адаптивного захисту корпоративних інформаційних систем від комплексних деструктивних впливів.

4. Позитивні сторони проекту полягають в підвищенні захисту корпоративних інформаційних систем від комплексних деструктивних впливів за рахунок адаптивної оптимізації конфігурації системи захисту

5. Негативні сторони проекту: У роботі недостатньо висвітлено шляхи розгортання системи та оновлення її компонентів в процесі експлуатації.

6. Оцінка графічного оформлення та пояснювальної записки роботи.

7. Відгук про роботу в цілому В загальному дипломна робота заслуговує позитивної оцінки, однак є має незначні зауваження

8. Інші зауваження

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої дипломної роботи, можна зробити висновок, що дипломна робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) д.т.н., проф. Мартинюк Валерій Володимирович.
Завідувач кафедри АКІТР, доктор технічних наук, професор.

« 18 » грудня 2023 . (підпис)