Хмельницький національний університет
Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Оптимізація системи захисту комп'ютерних систем з використанням методів багатокритеріальної оптимізації
Назва теми

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

КРМКІ. 170176.19.01.02.ПЗ

Виконав: студент 2 курсу, група КІ1м-19-1 _____ Шевчук І.М.
Підпис

Керівник доц., к. т. н, доцент кафедри КбКСМ _____ Тітова В.Ю.
Підпис

Нормоконтролер доц., к. т. н, доцент кафедри КбКСМ _____ Муляр І.В.
Підпис

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

10 12 2020 р.

Хмельницький, 2020

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ПРОГРАМУВАННЯ ТА КОМП'ЮТЕРНИХ І ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Кафедра КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ПРОГРАМУВАННЯ ТА ЗАХИСТ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"1" 09 2020 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Шевчука Іллі Михайловича

Прізвище, ім'я, по батькові студента

Тема проєкту (роботи) Оптимізація системи захисту комп'ютерних систем з використанням методів багатокритеріальної оптимізації

1. Керівник проекту (роботи) к.т.н., доц. Тітова В.Ю.

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

Затверджена наказом № 118 ректора університету додаток №23 від 01.09.2020

2. Строк подання студентом проєкту (роботи) на кафедру 1.12.2020

3. Вихідні дані до проекту (роботи) Удосконалена модель захисту комп'ютерних систем

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Моделі захисту інформації в комп'ютерних системах. Класифікація загроз. Метод оптимізації рішень. Оцінювання ефективності запропонованих рішень.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Аналіз захисту інформації в комп'ютерних мережах. Моделі захисту інформації в комп'ютерних системах. Метод багатокритеріальної оптимизації захисту інформації в комп'ютерних системах

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання
Нормоконтроль	Муляр І.В. доцент каф. КбКСМ		

7. Дата видачі завдання «_____» _____ 2020 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів проекту (роботи)
1	Вибір напряму дослідження та узгодження тематики ДРМ з керівником	2.02.2020
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	2.03.2020
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	1.04.2020
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	1.05.2020
5	Робота над науковою статтею	1.06.2020
6	Робота над розділом 3 – розробка алгоритмів та технологій, їх аналіз	1.09.2020
7	Робота над розділом 4 – проектування ПЗ для вирішення поставленої задачі	1.10.2020
8	Узгодження отриманих; оформлення пояснювальної записки згідно вимог	1.11.2020
9	Оформлення графічної частини	11.11.2020
10	Попередній захист КРМ	15.11.2020
11	Захист КРМ на засіданні ЕК	10.12.2020

Студент _____ Шевцов І.В.
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Гіоєв В.М.
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Оптимізація системи захисту комп'ютерних систем з використанням методів багатокритеріальної оптимізації

Автор роботи: Шевчук Ілля Михайлович

Керівник роботи: к.т.н., доц. Тітова В.Ю.

Пояснювальна записка: 98 с., 14 рис., 8 табл., 2 дод., 41 джерел.

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, БАГАТОКРИТЕРІАЛЬНА ОПТИМІЗАЦІЯ, МЕТОД АНАЛІЗУ ІЄРАРХІЙ, МЕТОД ПАРЕТО.

Метою магістерської роботи є максимізація захищеності комп'ютерних систем шляхом вдосконалення захисту інформації в комп'ютерних системах, зокрема від вірусів-шифрувальників, за рахунок введення в структуру існуючих систем захисту підсистеми моніторингу на основі методів багатокритеріальної оптимізації.

Дана робота присвячена оптимізації систем захисту комп'ютерних систем з використанням методів багатокритеріальної оптимізації.

Дата 10.11.2020 Підпис студента

ANNOTATION

Theme of qualification work: Optimization of computer systems protection system using multicriteria optimization methods

Author of the work: Shevchuk Ilya Mikhailovich

Supervisor: Ph.D., Assoc. Titova V.Y.

Explanatory note: 98 pages, 14 figures, 8 tables, 2 appendices, 41 sources.

INFORMATION PROTECTION SYSTEMS, MULTICRITERIAL OPTIMIZATION, METHOD OF ANALYSIS OF HIERARCHIES, METHOD OF PARETO.

The purpose of the master's thesis is to maximize the security of computer systems by improving the protection of information in computer systems, in particular from encryption viruses, by introducing into the structure of existing security systems monitoring subsystem based on multicriteria optimization methods.

This paper is devoted to the optimization of computer systems protection systems using multicriteria optimization methods.

Date 30.11.2020 Student's signature

ЗМІСТ

ВСТУП

Актуальність роботи. Захист інформації в сучасних комп'ютерних інформаційних системах (ІС) є пріоритетним завданням. Викрадення конфіденційної інформації, знищення даних, спотворення інформації, виведення з ладу комп'ютерних систем (КС) – далеко не повний перелік усіх ризиків, що виникають у процесі експлуатації та використання сучасних ІС.

Комплексний характер системи безпеки для протидії різноманітним загрозам ІС має забезпечувати контроль за діяльністю службовців, які використовують різноманітні внутрішні ресурси системи, а також мають доступ до Інтернет-додатків [1].

Репутація і безпека сучасних компаній багато в чому залежить від діяльності її співробітників, а системи контролю і введення обмежень для персоналу є важливою складовою комплексу заходів, які спрямовані на підтримку інформаційної безпеки (ІБ).

В цьому напрямку актуальними є не тільки обмеження та фільтрація ресурсів і мережевих сервісів Інтернет з метою захисту корпоративної мережі (КМ), але й система, що контролює всі дії користувачів з метою подальшого аналізу й організаційних висновків [1].

Контроль за використанням комп'ютерів і пристроїв у мережі має за мету попередити несанкціонований доступ як до КМ в цілому, так і до окремих об'єктів спільного доступу, таких як мережеві файлові системи (ФС), директорії з конфіденційною інформацією, бази даних (БД), та запобігти втраті чи розголошенню цінної та важливої інформації.

Актуальним завданням є також моніторинг дій системних адміністраторів, які зазвичай можуть мати необмежені повноваження в системах та іноді стають джерелом витоку даних з компаній. При цьому важливо мати відповіді на ряд запитань: хто і коли працював у КС; хто мав доступ до БД та ФС спільного доступу; чим займаються співробітники в певний час; у разі надзвичайної події – чому деякі сервіси перестали бути доступними; які зміни в конфігурації було зроблено, з якої причини і ким?

Актуальність проведеного дослідження обумовлюється необхідністю вирішення завдань виявлення вторгнень превентивними методами. Значимість застосування штучного інтелекту в контексті виявлення атак полягає в його ефективності прийняття рішень в умовах невизначеності.

Сучасний світ не можна уявити без читання і обробки інформації. Обсяг інформації, яку отримує людина, росте у величезній кількості. І ця інформація може бути оброблена різними інформаційними системами. На даний час найпростіший для інженера-програміста спосіб, це нейронна мережа. Нейронна мережами обробляється будь-яка інформація, від графічної до величезних масивів даних [2].

Отже, із вищесказаного випливає, що тема магістерського дослідження є актуальною.

Метою магістерської роботи є максимізація захищеності комп'ютерних систем способом вдосконалення захисту інформації в комп'ютерних системах, зокрема від вірусів-шифрувальників, за рахунок введення в структуру існуючих систем захисту підсистеми моніторингу на основі методів багатокритеріальної оптимізації.

Для досягнення цієї мети під час навчання необхідно вирішити наступні завдання:

1. Проаналізувати системи захисту інформації, зв'язки та відношення між типовими процесами захисту інформації у КС.

2. Проаналізувати нормативно-правові документи, що регламентують інформаційну безпеку в КС

3. Розглянути загрози комп'ютерній інформації, у тому числі віруси-шифрувальники.

4. Провести класифікацію загроз інформації у КС.

5. Розробити концептуальну модель існуючих на сьогоднішній день систем захисту інформації.

6. Розробити метод оптимізації системи захисту за рахунок багатокритеріальної оптимізації.

7. Впровадити та протестувати розроблений метод.

8. Визначити сферу застосування розробленого методу.

Об'єктом дослідження є системи захисту інформації, зв'язки та відношення між типовими процесами захисту інформації у комп'ютерних системах, загрози комп'ютерній інформації, у тому числі віруси-шифрувальники.

Предметом дослідження є методи та моделі захисту інформації в комп'ютерних системах, які базуються на сучасних методах багатокритеріальної оптимізації, таких як аналіз ієрархій, ELECTRE, Парето, тощо.

Методи дослідження, що використовуються в даній роботі, базуються на багатокритеріальній оптимізації.

Наукова новизна:

1. Розроблено класифікацію типових процесів захисту інформації та класифікацію загроз у комп'ютерних системах, які відрізняються від вже існуючих більш повною структурою та систематизованим набором вимог, що відповідає основним положенням нормативно-правових документів, що регламентують інформаційну безпеку.

2. Вдосконалено концептуальну модель існуючих на сьогоднішній день систем захисту інформації, за рахунок введення в неї блоку моніторингу, який базується на багатокритеріальній оптимізації.

3. Запропоновано метод оптимізації системи захисту за рахунок багатокритеріальної оптимізації, що дозволяє прискорити обробку динамічних даних (загроз, їх характеристик, тощо) та підвищити ефективність захисту даних у комп'ютерних системах в цілому..

Практична цінність: розроблений метод удосконалює системи захисту інформації в КС та підвищує цілісність, конфіденційність та доступність інформації в цілому.

Магістерська робота складається з 4-ьох розділів. У першому розділі розглянуто поняття систем захисту інформації, проаналізовано сучасні нормативно-правові акти, які регулюють діяльність таких систем. Досліджено особливості використання найбільш відомих методів багатокритеріальної оптимізації у питаннях захисту інформації. Проаналізовано різні типи комп'ютерних загроз, зокрема віруси-шифрувальники. Сформульовані основні

задачі магістерської роботи.

Основна увага приділяється аналізу недоліків сучасних систем захисту інформації від вірусів-шифрувальників та виявленню супутніх проблем, вирішення яких можливо за рахунок використання багатокритеріальної оптимізації.

У другому розділі сформульовано основні вимоги до концептуальної моделі захисту комп'ютерних систем, проведено класифікацію типових процесів захисту інформації в комп'ютерних системах, яка описує характер їх реалізації через математичну модель.

У третьому розділі на основі запропонованих у другому розділі залежностей між класами загроз та їх характеристиками, а також враховуючи особливості математичної моделі вірусів-шифрувальників обрано метод багатокритеріальної оптимізації, який найкраще підходить для вирішення поставленої задачі.

Четвертий розділ містить результати тестування запропонованого методу та оцінку його ефективності.

За темою магістерської роботи опубліковано 1 стаття у фаховому журналі і 1 стаття у нефаховому журналі.

1 ОСНОВНІ ПРИНЦИПИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

1.1 Поняття систем захисту інформації

Основні методи обробки, передачі і накопичення інформації сприяли появі загроз, які пов'язані з можливістю втрат, пошкодження і розшифрування даних, адресованих чи які належать кінцевим користувачам. Тому забезпечення інформаційної безпеки в комп'ютерних системах і мережах являється одним з найважливіших напрямів розвитку ІТ.

Захист інформації в ІТС (information protection, information security, computer system security) – робота головною метою якої є забезпечити безпеку інформації яка обробляється в ІТС та самої ІТС в загальному, відповідно має на меті запобігти або створити перешкоди для реалізації певних загроз, а також знизити показник можливих збитків внаслідок реалізації загроз [3].

Об'єкт захисту – це інформація або той хто являється носієм інформації або процес який являється інформаційним , відповідно до яких необхідно забезпечити захист який залежить від поставленої мети захисту інформації[4].

Мета захисту інформації - це бажаний результат захисту інформації. Його метою може бути запобігання шкоди власнику, користувачеві інформації, якщо буде мати місце витік інформації і/ або несанкціонований і ненавмисний чинник на інформацію.

Ефективність захисту інформації – це ступінь з яким корелюють результати захисту інформації відповідно до поставленої цілі.[4]

Захист інформації від витоку - діяльність щодо контролює запобігання неконтрольованого розповсюдження інформації, несанкціонованого доступу (НСД) до інформації, яка перебуває під захистом і отримання інформації, яка захищається, зловмисниками.

Захист інформації від розголошення – робота головною метою якої є запобігання несанкціонованого доведення захищеної інформації до неконтрольованої кількості адресатів інформації.

Захист інформації від неправомірного доступу – процеси щодо запобігання отримання інформації, що відповідно перебуває під захистом зацікавленого суб'єкта з порушенням встановлених нормативно-правових документів або прав та правил доступності до інформації, яка захищається. Зацікавленим суб'єктом, що здійснює НСД до інформації яку потрібно захистити, може виступати держава, фізична особа, юридична особа, група юридичних або фізичних осіб, в т.ч. громадська організація.

Система захисту інформації - сукупність органів і/ або виконавців, техніка яку вони використовують для захисту інформації, а також об'єкти захисту, Системи захисту повинні бути організовані і функціонувати за правилами, які в свою чергу встановленні відповідними правовими, організаційно-розпорядчими та нормативними документами щодо захисту інформації.

Інформаційна безпека являє собою захищеність інформації від незаконного ознайомлення, зміна або спотворення, блокування доступу, та захищеність інформаційних ресурсів від чинників, які насамперед спрямовані на зниження їх працездатності. Природа цих чинників може бути найрізноманітнішою.

До природи цих чинників можна віднести спроби проникнення зловмисників, помилки до яких призвів персонал, вихід з робочого стану і програмних і апаратних засобів, та стихійні лиха (землетрус, ураган, пожежа) і т. д.

Сучасна автоматизована система обробки інформації сьогодні являє складну систему, вона має в собі з велику кількість компонентів які мають різний ступінь автономності, що пов'язані між собою і передають данні. Кожен з цих елементів може піддатися зовнішньому чиннику і вийти з ладу. Компоненти системи можна поділтити на наступні групи:

- апаратні засоби - комп'ютери і комп’ютерні складові;
- програмне забезпечення - куплені програми, вихідні, об'єктні, модулі-завантажувачі; ОС та системні утиліти, приграми для діагностики і т. д .;
- дані - збережені тимчісово та постійно, на носіях, друковані, архіви, системні журнали і т. д .;

- користувачі та персонал.

Абстрактним поняттям таким як інформація, об’єкти та суб’єкти системи відповідно відповідають фізичні уявлення в комп’ютерному середовищі. Що і є відповідно однією з особливостей інформаційної безпеки:

- для представлення інформації - апаратні носії інформації у вигляді зовнішніх пристроїв комп'ютерних систем (друкуючих пристроїв, різних накопичувачів, терміналів, ліній і каналів зв'язку), оперативної пам'яті, файлів, записів і т. д .;
- об'єктів системи - пасивні компоненти системи, що зберігають, які беруть або передають інформацію. Доступ до об'єкту означає доступ до даних, інформації що міститься в ньому;
- суб'єктам системи - активні компоненти системи, які в свою чергу мають можливість стати причиною руху інформації від об'єкта до суб'єкта, а також можуть привести до зміни стану системи. В якості суб'єктів можуть виступати користувачі, деякі програми і процеси.

Інформаційна безпека комп'ютерних систем забезпечується забезпеченням конфіденційності, цілісності та достовірності даних, що проходять обробку,та забезпечення доступності і цілісності інформаційних ресурсів системи. Згадані відповідно вище базові властивості інформації потребують більш повного роз’яснення.

Конфіденційність даних - це статус, який відповідно наданий даними та визначає відповідний ступінь їх захисту. До конфіденційних даних можна віднести, наприклад, такі: особисті дані користувачів; їхні облікові записи (імена і паролі); а також дані про кредитні картки; ще дані про розробки і різні внутрішні документи; бухгалтерські відомості. Конфіденційна інформація повинна бути відома тільки допущеним та, що пройшли перевірку суб'єктам системи (користувачам, процесам, програмам). Для інших суб'єктів системи така інформація повинна бути невідомою.

Під цілісністю інформації мається на увазі можливість інформації зберігати свою структуру або данні під час передачі та зберігання. Цілісність

інформації виконується лише в тому випадку, якщо дані в системі є однаковими в семантичному відношенні до відповідно даних у поточних документах. Якщо не відбулося їх ненавмисного або навмисного спотворення або знищення. Забезпечення цілісності даних є однією з складних завдань, пов’язаних з захистом інформації.

Достовірність інформації - властивість інформації, яка виражається в суворій приналежності суб'єкту, який є її джерелом, або тому об’єкту, суб’єкту, від якого ця інформація прийнята. Юридична значимість інформації означає, що документ, який є носієм інформації, та має певну юридичну силу. Доступність даних. Робота користувача з даними може бути можлива тільки в такому випадку, якщо він має до них хоч якийсь доступ.

Доступ до інформації – це процес надання можливості ознайомлення для суб'єкта з інформацією, також можливість отримання прав доступу за допомогою відповідних технічних та апаратних засобів. Суб'єкт доступу до інформації – це учасник правовідносин в інформаційних процесах.

Оперативність доступу до інформації - це властивість даних, інформації або деякого інформаційного ресурсу бути доступними для кінцевого користувача відповідно до його оперативними потребами.

Власник інформації - суб'єкт, який володіє даними або інформацією та в повному обсязі виконує повноваження володіння, користування, керування інформацією відповідно до законодавчих та нормативних актів [4].

Користувач (споживач) інформації - суб'єкт, що користується інформацією, відповідно до деяких встановлених прав і правил доступу до інформації, яка захищається, або з їх порушенням, які отримав від її власника або посередника.

Право доступу до інформації - перелік правил доступу до інформації, які встановлюються нормативними документами або власником інформації.

Правило доступу до інформації - перелік правил, що складають порядок та умови, які надають суб'єкту доступ до інформації та її носіїв[4,5].

Розрізняють санкціонований та несанкціонований доступ до інформації.

Про перший тип доступу до інформації можна сказати, що він є регламентованим і виконує встановлені правила розмежування доступу. Правила

розмежування доступу використовуються і використовуються для регламентації права доступу до компонентів системи.

Несанкціонований доступ до інформації – порушення правил розмежування доступу. Суб’єкт (особа), об’єкт чи процес, які здійснюють несанкціонованого доступу до інформації, є порушниками правил доступу. НСД є найбільш поширеним видом комп'ютерних порушень.

Відповідальним за захист комп'ютерної системи від несанкціонованого доступу до інформації є адміністратор захисту.

Доступність інформації полягає та має на увазі також доступність компонента або ресурсу комп'ютерної системи. Властивість компонента або ресурсу – це можливість бути доступним для законних суб'єктів системи. Приблизний перелік ресурсів, які можуть бути доступні, включає в себе: сервери, робочі станції принтери, дані деяких користувачів, будь-які критичні дані, що необхідні для роботи.

Цілісність ресурсу або цілісність компонента системи - це властивість ресурсу або компонента бути незмінним в семантичному понятті під час функціонування системи в умовах спонтанних чи навмисних спотворень або при руйнівних чинниках[5].

З допуском до інформації та ресурсів системи також пов'язана група таких досить важливих понять, як ідентифікація та аутентифікація та авторизація. З кожним суб'єктом системи або мережі пов'язують деяку інформацію, саме: число, рядок символів, що ідентифікує суб'єкт. Ця інформація є ідентифікатором суб'єкта системи або мережі. Суб'єкт, який має для себе зареєстрований ідентифікатор, є законним, тобто легальним, суб'єктом. Ідентифікація суб'єкта - це процедура розпізнавання суб'єкта за його ідентифікатором. Ідентифікація виконується при спробі суб'єкта увійти в систему (мережу). Наступним кроком взаємодії системи з суб'єктом є аутентифікація суб'єкта. Аутентифікація суб'єкта - це перевірка достовірності суб'єкта з даним ідентифікатором. Процедура аутентифікації встановлює, чи є суб'єкт саме тим, за кого він себе видає. Після ідентифікації та аутентифікації суб'єкта виконують процедуру його авторизації. Авторизація суб'єкта - це процедура, що надає надання законному суб'єкту, що

успішно пройшов ідентифікацію та аутентифікацію, відповідних повноважень і доступних ресурсів системи або мережі

Під поняттям загрози безпеки АС розуміються можливі дії, здатні прямо або побічно нанести шкоду її безпеці. Під збитком безпеки розуміється порушення стану захищеності інформації, що міститься і обробляти в системі (мережі). З визначенням загрози безпеки тісно пов'язане поняття уразливості комп'ютерної системи. Уразливість комп'ютерної системи - це притаманне системі невдала властивість, яка може стати причиною реалізації загрози. Атака на комп'ютерну систему - це пошук і використання зловмисником тієї або іншої уразливості системи. Інакше говорячи, атака - це створення загрози для безпеки.

Протидія загрозам безпеки є метою засобів захисту комп'ютерних систем і мереж.

Захищена система - це система із засобами захисту, які якісно і ефективно протистоять загрозам безпеки.

Спосіб захисту інформації – це певний порядок і правила його застосування відповідно до деяких основних принципів і засобів захисту інформації, яка захищається.

Засіб захисту - технічний, програмний спосіб, призначений або використовуються для захисту інформації, яка захищається.

Комплекс засобів захисту (КСЗ) – це така сукупність програмних і технічних засобів, що створюються і підтримуються для забезпечення інформаційної безпеки системи. КСЗ створюється, підтримується, вдосконалюється відповідно до прийнятої в даній організації політики безпеки.

Техніка захисту інформації – це такі засоби захисту інформації, методи контролю ефективності захисту інформації, засоби і системи керування, призначені для забезпечення захисту інформації.

Політика безпеки - це множина практичних рекомендацій, норм та правил, що управляють роботою засобів захисту комп'ютерної системи від заданої множини загроз. Більш докладні відомості про види політики безпеки і процесі її розробки будуть приводитися в наступних статтях.

1.2 Міжнародні стандарти захисту інформації в комп’ютерних системах

Головна задача стандартів інформаційної безпеки – має на меті в створення певної основи для взаємодії між експертами, виробниками, та споживачами щодо якості продуктів інформаційних технологій. Відповідно ці групи мають кожна свої інтереси і кожна свої погляди на проблему інформаційної безпеки.

Відповідно до міжнародних стандартів інформаційної безпеки в любій організації має бути наступне:

- Вибір елементів для забезпечення інформаційної безпеки комп’ютерних систем;
- Створення якісної системи управління інформаційною безпекою;
- Розрахунок множини деталізованих якісних і кількісних показників щоб оцінити відповідності інформаційної безпеки поставленим задачам;
- Використання інструментарію забезпечення інформаційної безпеки і оцінки її теперішнього стану;
- Використання методик управління безпекою, дозволяючи об’єктивно оцінювати захищеність інформаційних активів і керувати інформаційною безпекою компанії[6,7].

Найбільш відомі міжнародні стандарти в області захисту інформації. На сьогоднішній день Міжнародний стандарт який має назву ISO / IEC 17799: 2000 (BS 7799-1: 2000) «Управління інформаційною безпекою - Інформаційні технології. - Information technology- Information security management» вважається одним з вагомих стандартів в області захисту інформації. Він був створений на основі Британської стандарту, а саме першої частини частини «BS 7799-1» стандарт був створений в 1995 році "Практичні рекомендації з управління інформаційною безпекою та є частиною нової системи стандартів інформаційної безпеки комп'ютерних інформаційних систем[6].

Остання версія стандарту ISO / IEC 17799: 2000 (BS 7799-1: 2000) розглядає найбільш важливі питання забезпечення інформаційної безпеки організацій та фірм, компаній:

- Необхідність забезпечення інформаційного захисту та безпеки;
- Основні поняття і визначення для розуміння інформаційної безпеки;
- Політика інформаційної безпеки компанії;
- фізична безпека;
- Організація інформаційної безпеки в компанії;
- Ранжування та управління внутрішньовиробничими інформаційними ресурсами;
- Кадровий менеджмент і інформаційна безпека;
- Адміністрування безпеки виробничих інформаційних систем;
- керування доступом;
- Основні вимоги з безпеки до виробничих інформаційних систем в процесі їх розробки, використання і супроводу ІС;
- Управління бізнес-процесами компанії з точки зору інформаційної безпеки;
- Аудит інформаційної безпеки всередині компанії;

Інша частина стандарту BS 7799-2: 2000 [6,7]. "Специфікації систем управління інформаційною безпекою» надає можливі функціональні специфікації корпоративних систем управління інформаційною безпекою відповідно до їх відповідності на вимоги першої частини зазначеного стандарту. У відповідності до положень цього стандарту також визначається процедура перевірки корпоративних систем.

Також додаткові рекомендації для керування інформаційною безпекою містять керівництва Британського інституту стандартів, виданих в період 1995-2003 у вигляді такої серії:

- Введення в проблему управління інформаційної безпеки;
- Можливості сертифікації на вимоги стандарту BS 7799;
- Управління BS 7799 з оцінки та управління ризиками;

- Чи готові ви до перевірки на вимоги стандарту BS 7799;
- Керівництво для проведення аудиту на вимоги стандарту;
- Практичні рекомендації з управління безпекою інформаційних технологій;

На противагу від ISO 17799 німецьке "Керівництво щодо захисту інформаційних технологій для базового рівня захищеності" яке було прийняте у 1998 присвячено більш ретельному розгляду приватних питань управління інформаційної безпеки компанії [7].

У німецькому стандарті BSI представлений загальний метод управління інформаційною безпекою.

Описи елементів сучасних інформаційних технологій:

- Описи основних елементів організації режиму інформаційної безпеки (організаційний і технічний рівні захищеності даних, побудова плану дій у надзвичайних ситуаціях, підтримка безперебійної роботи) .
- Характеристики об'єктів інформатизації.
- Характеристики основних активів компанії які прив’язані до інформації (у тому числі апаратне і програмне забезпечення, наприклад персональні комп’ютери та мережеве обладнання керування яким здійснюють ОС сімейства DOS, сімейства Windows і сімейства UNIX).
- Характеристики комп'ютерних мереж, що базуються на основі варіативних мережевих технологій, до прикладу мережі Novell NetWare, Windows і UNIX).
- Характеристика активного та пасивного мережевого або телекомунікаційного обладнання провідних вендорів, наприклад Cisco.
- Детальний реєстр загроз безпеки, а також відповідно заходів контролю (більше 600 найменувань у кожному реєстрі).

На відмінну німецькому стандарту BSI, що дає можливість використовувати певні "приватні" сценарії для захисту інформаційних активів корпорації, стандарти ISO 15408, ISO 17799 дозволяють проаналізувати тільки найбільш загальні принципи управління інформаційною безпекою, які

відповідають процесам захисту інформації в цілому. Однак перераховані підходи мають деякі обмеження.

1.3 Аналіз захисту інформації в комп’ютерних системах

Основні особливості будь якої мережевої системи (структури) є те, що її компоненти розміщені в різних точках і зв'язок між ними виконується фізично за допомогою мережевих з’єднань і програмно – за допомогою сценарію повідомлень. При цьому всі повідомлення керування і данні, пересилаються між об’єктами розподіленої системи, передаються між собою по мережевим з’єднанням у вигляді пакетів обміну[8].

Мережеві механізми характерні тим, що, в порівнянні зі звичайними ненавмисними діями і атаками, які виконуються в межах однієї комп’ютерної системи, до них використовують ще специфічний вид атак, який обумовлений розподілом ресурсів інформації в просторі. Це так звані мережеві (або дистанційні) атаки (Remote Network Attacks). Характиризуться тим, що зловмисник може знаходитися на довільній відстані від цілі атаки, а також тим що ціллю нападу може бути не конкретний комп’ютер, а інформація яка передається по мережевим з’єднанням.

З розвитком локальної і глобальної мережі часто саме віддалені атаки успішно використовуються для нападу на комп’ютерну систему. Відповідно через збільшення таких атак збільшився і пріоритет для захисту від них[4,8].

Сучасні системи захисту функціонують в розподіленій мережі, тому потрібно враховувати наявність як локальних, так і мережевих небезпек в якості загальних можна виділити наступні небезпеки[9]:

- Створення зловмисником фізичного доступу до комп’ютерної системи;
- Обхід захисних засобів;
- Перехід системи в небезпечний стан в результаті збою;

- Спроба зловмисника видати себе за іншого користувача(перехоплення індентифікації/аунтефікації);
- Помилки при адмініструванні;
- Використання зловмисником чужого мережевого з’єднання;
- Аналіз потоків даних з цілю отримання конфіденційної інформації;
- Перенаправлення потоків даних;
- Блокування потоків даних;
- Пошкодження або втрата інформації яка чинникає на безпеку функціювання комп’ютерної системи
- Збереження остаточної інформації в багатократних багатократних об’єктах які часто використовуються.

В умову великої небезпеки таких так – особливо для державних структур і органів влади – до системи захисту інформації пред’являють великі вимоги.

Методи захисту інформації поділяються на наступні:

1.Організаційно правові;

2.Інженерно-технічні, які в свою чергу поділяються на фізичні, апаратні, програмні, криптографічні.

Технологічна модель підсистеми інформаційної безпеки

Базисом комп’ютерної інформаційної системи (КІС) являється загальносистемне програмне забезпечення, яке включає операційну систему і програмні оболонки, програми загального і прикладного призначення: автоматизовані робочі місця (АРМ) і Web-сервіси загального і спеціального призначення, СУБД і управління інтегрованими обчислювальними і мультимедійними додатками, а також доступом до локальної і зовнішньої мережі[8].

Фізичний нижній рівень КІС базується на серверах, станціях, персональних комп’ютерах різного призначення і комунікаційних приладів а також на програмному забезпечені, що реалізує роботу цих пристроїв. В зв’язку з цим підсистема інформаційної безпеки починається з захисту саме цього програмно-апаратного обладнання. З цією ціллю можна використовувати популярні захисні

засоби операційних систем, антивірусні пакети, засоби і прилади аутентифікації користувача, засоби криптографічного захисту паролей і даних прикладного рівня.

Другий фізичний рівень КІС – працюючі станції, персональні комп'ютери. І мова йде про засобів інформаційного захисту другого рівня – рівня захисту локальних мереж, який включає в себе:

- Засоби захисту мережевих ОС;
- Засоби аунтифікації користувачів(UAF);
- засоби фізичного та програмного розмежування доступу до розподілених та розділених інформаційним ресурсам;
- засоби захисту домену локальної мережі (LAND);
- засоби проміжного доступу (Proxy Server) і міжмережеві екрани (Firewall);
- засоби організації віртуальних локальних підмереж (Virtual Local Area Network - VLAN);
- засоби виявлення атаки і вразливостей в системі захисту локальних мереж.

Наступний рівень реалізації КІС – об'єднання деяких локальних мереж, в загальну корпоративну через відкриту мережу на базі сучасних технологій підтримки і супровіду таких мереж з використанням відкритої мережі в якості комутаційного середовища. В такому випадку на третьому рівні використовуються технології захисту віртуальних мереж (VPN).

Четвертий рівень захисту КІС – організація захищеного між корпоративного обміну. Методологічною і технологічною основою такого захисту являються методи і технології керування публічними ключами і сертифікатами криптографічного захисту (PKI). Суть цих технологій полягає в реалізації двох глобальних функцій: генерації і коректному розповсюджені ключів та сертифікатів і відслідковування їхнього життєвого циклу. Базою для реалізації захисту будуть електронно цифровий підпис і VPN технології[8,9].

Криптографія – це сукупність методів перетворення даних, а саме технічних, математичних, алгоритмічних і програмних, яка робить їх безкорисними для любого користувача, в якого немає ключа для розшифрування. Криптографічні перетворення забезпечують рішення наступних базових задач захисту – конфіденційність і цілісність.

Технології криптографії дозволяють реалізувати наступні процеси інформаційного захисту:

- Ідентифікацію об’єкту чи суб’єкту мережі чи інформаційної системи;
- Аунтифікацію об’єкту чи суб’єкту мережі;
- Контроль/розмежування доступу до ресурсів локальної мереж чи поза мережевим сервісам.
- Забезпечення і контроль цілісності даних.

Брандмауер (Firewall) - програмно-апаратна система між мережевий захисту, яка певною мірою розділяє одну частину мережі від другої частини та реалізує набір правил які використовуються для проходження даних з однієї частини в другу. Так званим «кордоном» є розділ між корпоративною локальною мережею і зовнішніми Internet-мережами або різними частинами локальної розподіленої мережі. Той екран виконує роль фільтрування поточного трафіку, пропускаючи лише пакети інформації які відповідають правилам та відсіваючи інші[6,8].

Налаштування брандмауер, тобто рішення для допуску інформації, або не допуску інформації залежать від топології розподіленої мережі і політики інформаційної безпеки яку було прийнято. Відповідно до прийнятої політики інформаційного захисту реалізації міжмережевих екранів надає правила доступності до ресурсів внутрішньої мережі. Ці правила побудовані на двох загальних принципах - забороняти все, що не є дозволеним в загальній формі, і дозволяти все, що не є забороненим в загальній формі. Перший принцип надає менші можливості користувачам і охоплює чітко окреслену область мережевої взаємодії. Політика, яка притаманна другому принципу, є більш м'якою, але в багатьох випадках через її таки м’якість вона є менш бажаною, так як вона

дозволяє користувачам більше можливостей для «обходу» МЕ і використовувати сервіси що були заборонені через нестандартні порти (UDP), які в свою чергу не заборонені політикою безпеки. Функціональні засоби МЕ окреслюють такі розділи реалізації інформаційної безпеки:

- налаштування правил для здійснення процедури фільтрації;
- фільтрацію на мережевому рівні системи;
- фільтрацію на прикладному рівні системи;
- створення мережевої аутентифікації;
- адміністрування доступу для внутрішньої мережі;
- ведення журналів трафіку і обліку користувачів.

Програмно-апаратні компоненти МЕ можна поділити на три категорії а саме: фільтруючі маршрутизатори, шлюзи сеансового рівня і шлюзи рівня додатків. Саме ці компоненти МЕ - кожен окремо і в різних комбінаціях – дають змогу зрозуміти базові можливості МЕ і саме вони відрізняють їх один від одного.

Також можна відзначити, що міжмережеві екрани, нажаль, не можуть вирішити усі питання інформаційної безпеки розподілених систем і локальних мереж – тому існує ряд обмежень на їх застосування та перелік загроз, від яких МЕ фізично не має можливості захисту. Тому можна зробити висновок, що технології МЕ потрібно застосовувати лише комплексно - з іншими технологіями і засобами захисту

Під час виходу локальної мережі у відкрите Internet-простір з’являються загрози двох основних типів: несанкціонований доступ (НСД) до інформації, даних в період їх передачі по відкритій мережі та недозволеного доступу до внутрішніх ресурсів систем. Захист інформації при передачі даних по доступних та відкритих каналах реалізується наступними заходами:

- двохстороння аутентифікація сторін;
- пряме і зворотнє криптографічне перетворення даних;
- перевірка достовірності і повноти отриманих даних;

Організація захисту з використанням технології віртуальних частих мереж (VPN) має за мету створення захищеного «віртуального тунелю» між доступними вузлами відкритої мережі, доступ до цього тунелю є неможливий для потенційного зловмисника. До переваг цієї технології над іншими можна віднести наступне: досить проста апаратна реалізація, немає необхідності створювати або орендувати дорогі виділені фізичні мережі, дає змогу використовувати відкритий дешевий Internet, швидкість передачі даних по тунелю буде такою ж , як по виділеному каналу. На сьогодні існує чотири основних види архітектури для організації захисту інформації за допомогою використання технології VPN [9].

Локальна мережа VPN (Local Area Network-VPN). Дає можливість захисту потоків даних і інформації від несанкціонованого доступу в самій мережі компанії, інформаційна безпека надається і на рівні розмежування доступу, надання системних і персональних паролів, безпечне функціонування ОС, ведення реєстру колізій, шифрування таємної або приватної інформації.

Внутрішня корпоративна мережа VPN (Intranet-VPN). Забезпечує захищені з'єднання між внутрішніми підрозділами розподіленої компанії.

Мережі VPN з віддаленім доступом (Internet-VPN). Забезпечують захищений віддаленій доступ віддаленіх підрозділів розподіленої компании и мобільніх співробітніків и відділів через Відкритий простір Internet.

Міжкорпоративна мережа VPN (Extranet-VPN). Надає ефективно захищений обмін інформацією з відповідними елементами, які є невід'ємною частиною роботи корпорації. Передбачає використання надійних та сертифікованих VPN-продуктів, що виконують роботу у відкритих гетерогенних середовищах і дають максимальну захищеність конфіденційного трафіку, що включає аудіо- і відеопотоки інформації – конфіденційні телефоні переговори і телеконференції з клієнтами.

Комп'ютерний вірус - це спеціально написана програма, яка володіє можливістю дописувати себе до інших програмам, тобто проводити процедуру їх зараження з метою виконання шкідливих, небажаних процесів на комп'ютері і в мережі. Коли вірус програма починає роботу, то вона, як правило, отримує

управління над системою. Дії вірусу можуть бути самостійними, виконання певних шкідливих дій (зміна файлів або таблиць файлів розміщення на диску, погіршує роботу оперативної пам'яті, заміна адресатів звернень щодо зовнішніх пристроїв і т.д.), або «заражає» інші програми [11,12]. Отже відповідно ці програми можуть бути розповсюджені на інші комп'ютери за допомогою носіїв інформації або мережі. Форми організації вірусних атак вельми варіативні, але в цілому практично їх можна розтащувати по наступним категоріям:

- проникнення в комп’ютер за допомогою віддаленого доступу – отримання неавторизованого доступу програмами через глобальну або внутрішню мережу;
- внутрішнє (за допомогою локальної мережі) проникнення в комп'ютер – отримання програмами неавторизованого доступу до комп’ютера на якому вони знаходяться;
- віддалене блокування комп'ютера - програми, які через глобальну мережу (або мережа) заблоковують повністю роботу віддаленого комп'ютера або деяких програм які знаходяться на ньому;
- локальне блокування комп'ютера - програми, що блокують роботу комп'ютера, на якому вони знаходяться;
- мережеві сканери - програми, які здійснюють накопичення інформації про мережу, щоб дізнатися, які з комп'ютерів і програм, що використовуються на них можуть бути використанні для атак;
- сканери вразливих місць програмного забеспечення - програми, що перевіряють великі групи комп'ютерів в Internet в пошуках комп'ютерів, уразливих до відповідного виду атаки;
- «злом» паролів - програми, які виявляють легко здогадливі паролі що містяться в зашифрованих файлах паролів відповідно;
- мережеві аналізатори (sniffers) - програми, які аналізують мережевий трафік; часто в них є можливості автоматичного забору імен користувачів, паролів і номерів кредитних карт з трафіку;
- перетворення передачі даних або підміна інформації;

- підміна відповідального об'єкта розподіленої ВС (виконується робота від його імені) або об'єкт що є помилковий відповідно до розподіленої ВС (РВС).
- «соціальна інженерія» - це доступ до інформації який являється не санкціонованим іншими способами, ніж способом злому програмного забезпечення.

Мета - обманути співробітників, користувачів, адміністраторів для отримання логінів, паролів до системи або іншої інформації, яка допоможе обійти або знищити безпеку системи. До шкідливих програмних засобів відносяться класичні файлові віруси, мережеві черв'яки, хакерські утиліти, троянські програми, інші програми, що мають за ціль завдати якомога більшу шкоду комп'ютеру,[13,14] на якому вони запускаються для виконання, або іншим комп'ютерам що знаходяться в мережі.

1. 4 Постановка задачі

Враховуючи недоліки систем захисту, а також активний розвиток комп’ютерних загроз. Функціонування більшості систем захисту, зводиться до розпізнавання множин, активних в комп’ютері процесів, їх класифікації з метою визначення шкідливих та небезпечних процесів та прийняття рішень щодо їх блокування або ігнорування. Причому процес прийняття рішень ґрунтується на врахуванні великої множини вимог які суперечать між собою і оцінюванні варіантів рішень за багатьма критеріями. Суперечливість характеристик процесів, неоднозначність оцінювання процесу, неповнота отриманої інформації великою мірою роблять складним процес прийняття остаточного рішення і суттєво чинникають на його якість.

Для підвищення ефективності остаточного рішення конче необхідно ввести в структуру систем захисту інформації модуль, який надасть можливість вибору кращої або найкращої альтернативи за допомогою методу оцінювання ефективності рішень, тобто буде реалізовувати багатокритеріальну оптимізацію

рішень. Розроблення методу зазначеної багатокритеріальної оптимізації рішень і є метою даної роботи.

2 МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

2.1 Аналіз моделей безпеки систем

Розглянемо модель HRU (Harrison M., Ruzzo W., Ullman J.), її розробку слід вважати вагомим етапом в розвитку теорії захисту інформації. Важливість її створення проявляється в тому, що вона стала майже основою для одного з методів дослідження дискреційних моделей безпеки [14]. Модель HRU виконує роботу аналізу системи захисту, які відповідно реалізують дискреційну політику безпеки та відповідно основного її елемента – матриці доступів. Система захисту в цій моделі представляється кінцевим автоматом, принцип якого є у функціонуванні відповідно до деяких правил переходу. Модель HRU була вперше розроблена у 1971 році. Основні позначення. O - безліч об'єктів системи. S - безліч суб'єктів системи

R - безліч прав доступу суб'єктів до об'єктів.

У ній 3 види прав: R = {read, write, own} own - володіння. M - матриця доступу.

Рядки відповідають суб'єктам, а стовпці відповідають об'єктам. $M[S, O] \subseteq R$ права доступу суб'єкта S до об'єкта O зі всієї множини прав R. Автомат побудований відповідно до положень моделі називається системою.Примитивний оператор α. Загалом 6 примитивних операторі.

1. Внести r∈R в матрицю $M[S,O]$ – означає додавання суб'єкту прав багато правного доступу до об'єкту .

2. Видалити правило мається на увазі видалення в суб'єкта деякого права доступу.

3.Створення суб'єкту, в матрицю додається рядок відповідний суб'єкту.

4. Видалення суб'єкту.

5. Створення об'єкту, в матрицю додається стовпчик відповідний об'єкту.6.Видалення об'єкту.

Стан системи $Q = (S,O,M)$

При виконанні примітивного оператора α система з Q переходить в Q' $Q \vdash_{\alpha} Q'$. $Q'=(S',O',M')$.

З примітивного оператора складають команди. Кожна команда складається з двух частин.

1. Умова при якій виконується команда
2. Послідовність примітивних операторів.

command $C(x_1,\ldots,x_n)$

if $r_1 \in M[x_{S1},X_{O1}]$ and…and $r \in M[x_{Sn},X_{On}]$

$\alpha_1 \ldots \alpha_2$

end

$Q \vdash_{C(x1,\ldots xn)} Q'$

Приклад створення файла f S –суб'єкт,(користувач).

command C(f,S)

"создать" об'єкт f

"внести" право володіння M[f,S]

"внести" право читання M[f,S]

"внести" право запису M[f,S]

End

Передача прав.

Суб'єкт S передає право на читання іншому користувачу.

command (C,S',f)

if own M[S,f] then

“внести” право читання (read) M[S’,f]

End

Тепер звернемось до визначення основного поняття будь-якої системи захисту – тотожне поняттю безпеки системи. Відповідно до вимог більшості критеріїв оцінки безпеки, системи захисту повинні бути побудованими на основі певних математичних моделей, відповідно до яких повинно бути теоретично обґрунтована відповідність системи захисту інформації вимогам для заданої на підприємстві політики безпеки[14]. Для вирішення даної задачі необхідною є наявність алгоритму, який буде здійснювати перевірку такої відповідності. Однак, як показують результати аналізу моделі HRU, задача побудови алгоритму перевірки безпеки систем, що має можливість реалізації дискреційної політики розмежування прав доступу, не має розв’язків в загальному випадку. Щоб сформулювати цей висновок, введемо ряд означень. На початку визначимо шанс витоку певного права, що і є представленням порушення безпеки.

1.Рахується, що можливий виток прав в результаті виконання команд які мають примітивний оператор, який заносить в матрицю доступу деяке право доступу, яке раніше було відсутнє.

2.Початковий стан Q_0 буде називатися безпечним по відношенню до деякого права r, якщо перехід системи неможливий в такий стан q, в якому може статися втрата прав.

3. Монооперацiйною називають систему в якій кожна команда виконує лише примітивний оператор.

В моделі використовують дві основні теореми для доказу її надійності системи.

1.Існує алгоритм, який перевіряє, чи являється початковий стан моно-операційної системи безпеки для даного права.

2. Задача перевірки безпеки довільних систем алгоритмічно нерозв’язувана.

З цих теорем виникають лише два способи для вибору моделей систем захисту. В першу чергу, загальна модель нажаль і не дає можливості формально

довести їх безпеку, але в свою чергу дає багато різноманітних політик дискреційного розмежування доступу, отже з точки зору їх складності та практичної доцільності зникає необхідність розв'язку до кінця задач перевірки безпеки.

А, по-друге, є можливість використання більш обмежених (в розумінні визначення і наявності певних операцій в моделі) систем, для яких можна довести спроможність забезпечення безпеки, тобто розглядати конкретні або специфічні моделі системи. Але слід зауважити що, в таких обмежених системах інколи не вдається реалізувати вимоги деяких політик безпеки.

До недоліків можна сказати що маленькі за розміром системи працюють нормально, а великі стають громіздкими; наявність поділюваних областей доступу; шкідливі програми, $S1$ може записати шкідливу програму в $F2$, яку надалі отримає $S2$.

Модель розповсюдження прав доступу Take-Grand Використовується для аналізу систем дискреційного доступу. Для аналізу способу розповсюдження прав доступу. Основним елементом даної моделі це граф доступу[15]. Мета моделі – дати результат який буде відповідати на наступні питання: про можливість отримання прав доступу суб'єктом системи на відповідний об'єкт що перебуває стані, що описується графом доступів. В наступному модель Take-Grant отримала покращення, як розширена модель Take-Grant, в якій розглядаються способи виникнення інформаційних потоків в системах з дискреційним розмежуванням доступу.

O – множина об'єктів.

SO – активний об'єкт (користувачі, процеси).

$R = \{r1, \dots, rm\}\{t, g\}$ – множина прав доступу.

t– право брати права доступу

g – право давати права доступу

$\otimes$ - різниця двох множин O/S

• - графічне зображення суб'єкта системи

$G = \{S, O, E\}$ кінцевий позначений орієнтований граф без петлей.

E – множина дуг графа.

Операція, або правило перетворення позначають $Q \vdash_{OP} Q'$

В класичній моделі T-G правила перетворення может бути одним з чотирьох.

1.Правило «брати»

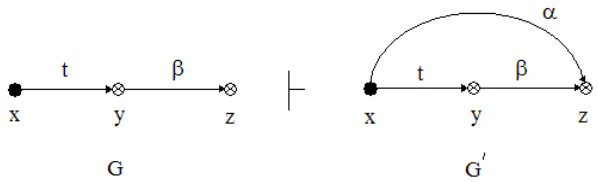


Рисунок 2.1 – Правило перетворення «брати»

$take(,x,y,z)$, x - суб'єкт, $y,z0$, α- доступ.

2.Правило «давати»

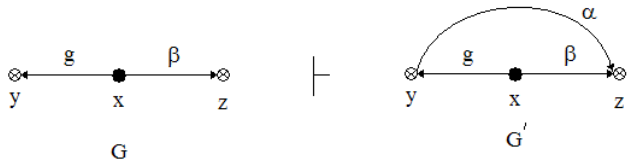


Рисунок 2.2 – Правило перетворення «давати»

$grand(,x,y,z)xSy,zOR,$ визначає порядок отримання доступу. Суб'єкт x дає об'єкту y права α на об'єкт z.

3.Правило «створювати»

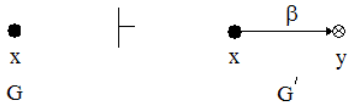


Рисунок 2.3- Правило «створення»

$create(,x,g)xSyOR$ Для суб'єкту x існує об'єкт y надаючи доступ .

4.Правило «видалення»

Рисунок 2.4 – Правило «видалення»

$remove(,x,g)xSyOR,$

У суб’єкта x видаляють права доступу y.

Правила брати, давати, створювати, видаляти в класичній моделі T-G називаються деюре. В моделі T-G основна увага приділяється умовам при яких в системах можливе розповсюдження прав доступу певним способом (в даній моделі їх два).

Перший спосіб санкціоноване отримання прав доступу. Характеризується тим, що при передачі прав доступу не накладаються обмеження на взаємодію суб’єктів системи, які беруть участь в цьому процесі.

Другий викрадання прав доступу. Передбачається що передача прав доступу об’єкту, виконується без його згоди.

Також існує ще розширена модель T-G. В якій приймаються правила «Де-факто»,створюються уявні дуги(6 правил):два без найменування і чотири: post, Spy, Find, pass, до яких не можна використати правило Де-юра.

Розширена модель T-G використовується для аналізу системи захисту що реалізує дискретну політику безпеки і її основного елементу матриці доступу. Уній три види прав R={read, write, own} own – володіння. M – матриця доступу. Рядки які відповідають суб’єктам, стовпці які відповідають об’єктам, $M[S,O] \subseteq R$ виступає у ролі права доступу суб’єкта S до об’єкту O зі всієї множини прав R. Автомат побудований відповідно з положення моделі називають системою.Примітивний оператор α. Всього 6 примітивних операторів. 1.Внести rR в матрицю $M[S,O]$ – означає добавити суб’єкту право багато правного доступу до об’єкту.2. Видалити право.3.Створити суб’єкт(в матрицю добавляємо рядок).4.Створюєм об’єкт (в матрицю додаєм стовпчик).5.Видалити сую’єкт.6.Видалити об’єкт. Стан системи $Q = (S, O, M)$. При виконанні примітивного оператора α система з Q переходить в $Q'Q \vdash Q'. Q' = (S', O', M')$. З примітивного оператора складаються команди які в свою чергу складаються з двух частин (1.Умова при якій виконуються команди.2.Послідовність примітивних операторів).

Що до безпеки системи то рахується що витік прав можливий в результаті виконання команди яка має примітивний оператор який вносить в матрицю

доступу деяке право доступу яке раніше було відсутнім. Початковий стан Q_0 називають безпечним по відношенню до деяких прав r, якщо перехід системи неможливий в такий стан q витік прав в якому може виникнути. Система називається моно операційною якщо кожна команда виконує один примітивний оператор.

Теореми доказу надійності такі як і в моделі HRU. В розширеній моделі розглядають способи і вартість появи інформаційних потоків в системах з дискредиційним розмежуванням доступу. Як було вище зазначено в розширеній моделі розглядють 6 правил перетворення доступу. Правила де-факто використовуються для пошуку появ можливих інформаційних потоків в системі. В результаті використовують граф доступу правил де-факто, в нього добавляють уявні дуги[14]. А в графічному представленні вони позначаються направленим пунктиром(напрямок показує направлення інформаційних потоків)

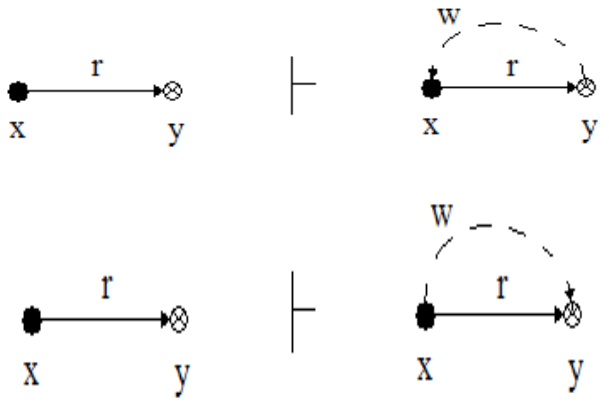


Рисунок 2.5 - Правила де-факто

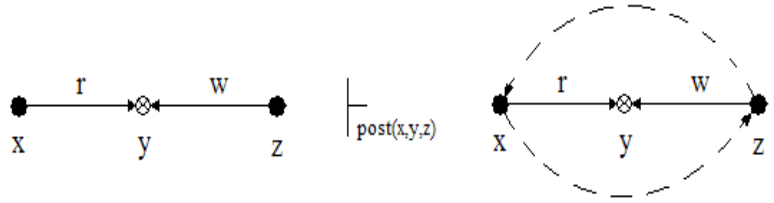


Рисунок 2.6- post

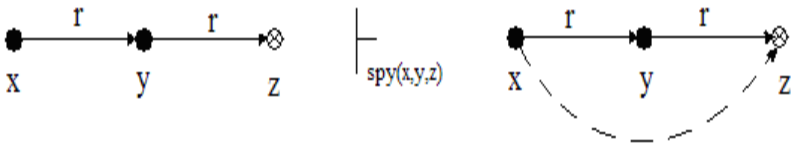


Рисунок 2.7- spy.

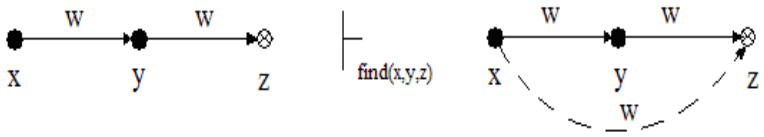


Рисунок 2.8- find

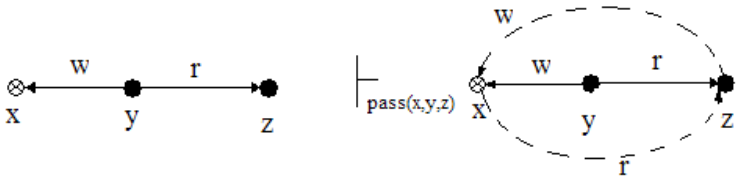


Рисунок 2.9- pass

До уявних дуг правило де-юре не використовують по причині того що можна буде найти замикання графа доступу, яке буде мати дуги які відповідають всім інформаційним канал системи. Для вирішення цієї проблеми існує два підходи:1) Вартість присвоюється кожній дузі на способу графа доступу;2)Присвоєння вартості кожного правила (де-факто, де-юре)

2.2 Концептуальна модель захисту в комп’ютерних системах

Для забезпечення захисту від загроз необхідно розробити концептуальну модель захисту інформації, яка б відповідала нашим вимогам. Сама концептуальна модель дає уяву про структуру безпеки, яка передбачає захист інформації від широко спектру загроз у нашому випадку це віруси-шифрувальники.

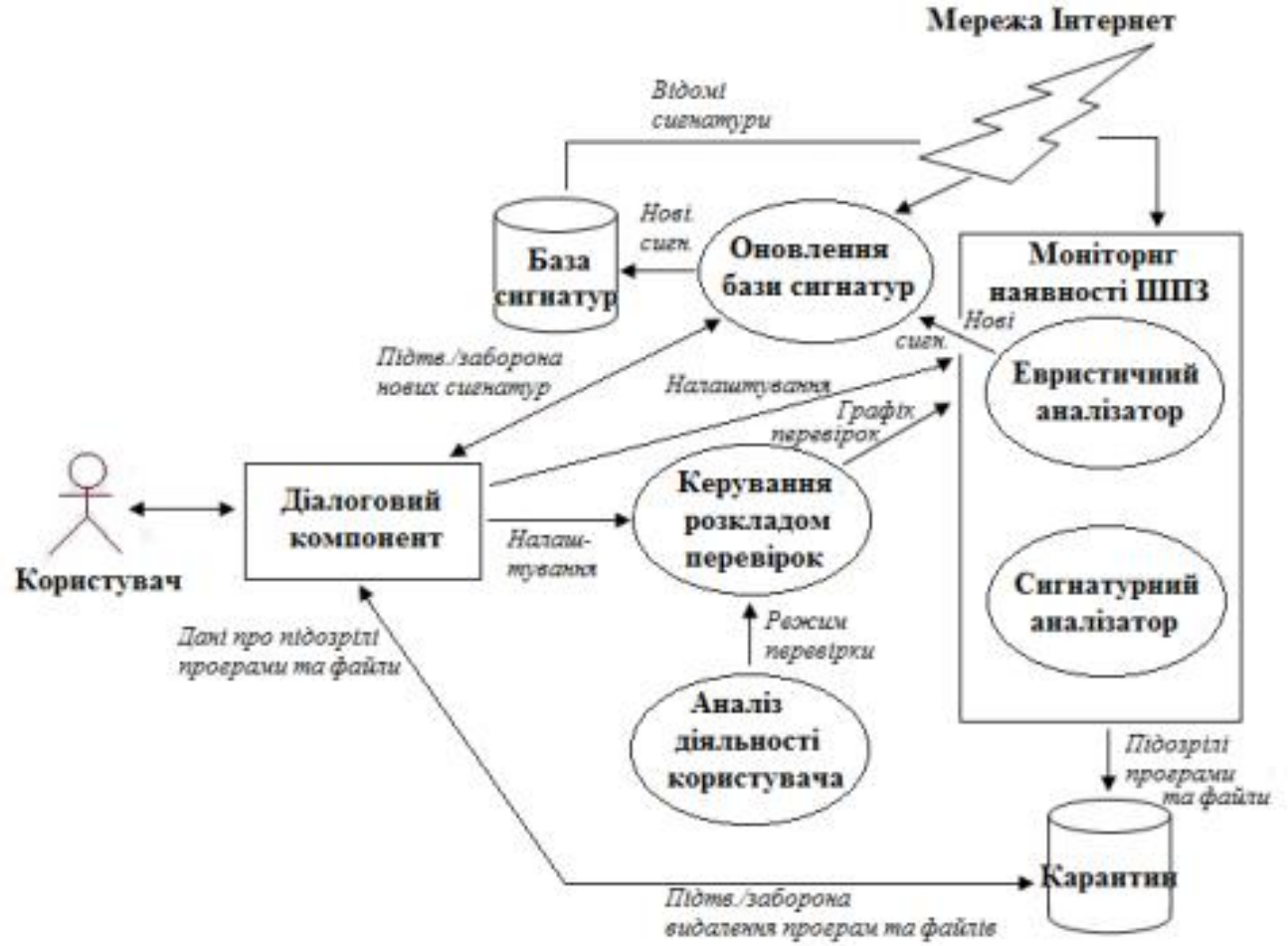


Рисунок 2.10 – Концептуальна модель захисту інформації

Мережа інтернет в даній моделі слугує, як джерелом загрози так і джерелом оновлення бази сигнатур вірусів-шифрувальників. При надходженні даних вони потрапляють в моніторинг, який перевіряє на наявність в ній загроз[15,16,17].

Сам моніторинг наявності складається з двох складових, а саме евристичний аналізатор та сигнатурний аналізатор. Евристичний аналізатор шукає файли сигнатури які схожі з вірусами-шифрувальниками, що дозволяє значно скоротити обсяг застосовуваних для пошуку вірусів баз даних. Іншими словами – призначення евристичний аналізатор є пошук невідомих раніше вірусів. При аналізі та перевірці будь-якої програми аналізатор виконує її моделювання, виконання й записує всі її «підозрілі» дії, до прикладу можна взяти наступне, відкриття або запис у файл, або перехоплення векторів переривань та т.п. На основі цього протоколу евристичного аналізатора

приймається рішення про можливе зараження програми вірусом. За допомогою сигнатурного аналізатора можливо точно ідентифікувати вірус його тип, але його недоліком є те що він не може протидіяти новим загрозам тому він працює в парі з евристичним аналізатором. Якщо було виявлено підозрілі програми чи файли вони поміщаються в карантин і користувач вже сам вибирає через діалоговий компонент у якому йому відображаються дані про підозрілі програми та файли, що йому робити з підозрілою інформацією.

Через діалоговий компонент користувач також має можливість керувати оновленням бази сигнатур для поліпшення роботи евристичного аналізатора, право вибору є через те що одним з головних недоліків евристичного аналізатора є те що можливе спрацювання навіть на звичайні файли чи програми через його надмірну підозрілість[16].

Користувач має можливість керувати перевірками своєї системи на віруси-шифрувальники. Для цього використовується аналіз діяльності користувача та моніторинг наявності ШПЗ.

2.3 Аналіз комп’ютерних загроз

Розгляд можливих загроз інформаційної безпеки проводиться з ціллю виявлення повного набору вимог до різних систем захисту. В теперішній час є доволі великий перелік загроз безпеки комп’ютерної системи, які в собі мають сотню пунктів. Перелік загроз, оцінки можливостей їх реалізації, а також модель порушення служить основою для аналізу ризику реалізації загроз і формуванню вимог щодо системи захисту[18].

Під загрозою безпеки мається на увазі різноманітні дії, які можуть привести до порушення стану захисту інформації. Іншими словами це потенційно можливі ситуації, процеси чи дії, які можуть нанести збиток інформаційним і комп’ютерним системам.

Загрози інформаційної безпеки діляться на два типи: природні і штучні. До природних можна віднести любі природні явища які не залежать від людини. А до штучних загрози які напряму залежать від людини і можуть бути навмисними і ненавмисними . Ненавмисні виникають через необережність, неуважність або незнання. Прикладом таких загроз може бути встановлення програм, які не входять в перелік необхідних для роботи і в подальшому порушують роботу системи, що і призводить до втрати інформації. Навмисні загрози створюється спеціально до них можна віднести атаки зловмисників як поза так і всередині структури. Результатом реалізації такого виду загроз є втрати як матеріальні так і інтелектуальні[18,17,8].

Одна з класифікацій загроз інформаційної безпеки є поділ на такі основні підгрупи як:

- Небажаний контент - це не тільки шкідливий код, потенційно небезпечні програми і спам (тобто те, що безпосередньо створено для знищення або крадіжки інформації), але і сайти, заборонені законодавством, а також небажані ресурси з інформацією, що не відповідає віку споживача;
- Несанкціонований доступ - перегляд інформації співробітником, який не має дозволу користуватися нею, способом перевищення посадових повноважень. Несанкціонований доступ призводить до витоку інформації. Залежно від того, які дані і де вони зберігаються, витоку можуть організовуватися різними способами, а саме через атаки на сайти, злом програм, перехоплення даних по мережі, використання несанкціонованих програм[21].;
- Витік інформації - можна розділяти на умисні й випадкові. Випадковий витік відбуваються через помилки обладнання, програмного забезпечення та персоналу. Умисні, в свою чергу, організовуються навмисно з метою отримати доступ до даних, завдати шкоди.;
- Втрата даних - можна вважати однією з основних загроз інформаційній безпеці. Порушення цілісності інформації може бути викликано несправністю обладнання або навмисними діями людей, будь то співробітники або зловмисники.;

- Шахрайство - не менш небезпечною загрозою є шахрайство з використанням інформаційних технологій («фрод»). До шахрайства можна віднести не тільки маніпуляції з кредитними картами («кардинг») і злом онлайн-банку [22], але і внутрішній фрод. Цілями цих економічних злочинів є обхід законодавства, політики безпеки або нормативних актів, привласнення майна ;
- Кібервійни;
- Кібертероризм;

Відповідно до теми та новизни в процесі виконання роботи поділимо класи можливих загроз наступним чином:

- загрози що спрямованні на дані у пам’яті;
- загрози які пов’язані з коректністю вхідних даних;
- загрози пов’язанні із нестійкістю комп’ютерної системи;
- клас загроз пов’язаних з рівнем привілеїв та доступу;
- загрози пов’язані з відмовою обслуговування;
- атака на систему;
- загрози які пов’язані з апаратними складовими;

Для аналізу цих загроз та методу захисту було вибрано віруси-шифрувальники (Virus-Encoder, Trojan-Encoder). Вони являють собою шкідливі програми, які шифрують файли на жорсткому диску комп’ютера і вимагають гроші (останнім часом криптовалюту)за їх розшифровку. Зашифрованими можуть бути фали типу *.mp3, *.doc, *.docx, *.pdf, *.jpg, *.rar і так далі. Зараз вони мають більш серйозний і стійкий код чим на початку їхнього виникнення.

Оскільки шифрувальники відносяться до шкідливих програм, для них використовується ті ж класифікаційні основи, що і для інших видів небезпечного коду. Наприклад, можна поділити їх по способу розповсюдження: через фішингові або спам розсилки, завантаження заражених файлів, використання файлообмінних сервісів і т.д.

Після того, як вона завантажиться на комп’ютер програма активується перетворивши файл користувача і блокує роботу всієї операційної системи. Після цього вірус-шифрувальник зазвичай залишає інструкцію: у вигляді фону

робочого стола, як текстовий документ на робочому столі, в кожній папці з зашифрованими фалами або навіть при старті операційної системи одразу ж отримуємо відповідне повідомлення з сумою викупу яку потрібно заплатити за збереження файлів. При цьому комп'ютер залишається працездатним, але всі файли є недоступними. До цих програм можна віднести: Trojan-Ransom.Win32.Gpcode або Trojan-Ransom.Win32.Cryzip, або Trojan-Ransom.Win32.Rector, або Trojan-Ransom.Win32.Xorist і так далі.

Зазвичай цілю є невеликі організації, але були і випадки атак на великі компанії. Одним з останніх найбільш розповсюдженим вірусом якій сколихнув велику кількість країн був так званий Petya, який використовуючи уразливість протоколу SMB в ОС Windows масово блокував комп'ютери в приватних компаніях та держструктурах. Тим не менш, об'єктом також можуть бути і персональні комп'ютери звичайних користувачів.

Віруси-шифрувальники розповсюджуються так само як і любі інші програми-вимагачі. Методи і способи їх доставки жертві поступово ускладнюються: зловмисники маскують їх під офіційне ПО. Але найпопулярнішим способом залишається розповсюдження спаму.

Програми-вимагачі представляють проблему для підприємств, освітніх установ і системи охорони здоров'я. Дослідники кібербезпеки продемонстрували, що це сімейство шкідливого ПО здатне без проблем вивести з ладу базову інфраструктуру, необхідну для функціонування міст.

Недоліком сучасних систем захисту відносно вірусів шифрувальників є їхня простота потрапляння в систему[21,22], адже код цих шкідливих програм завжди вдосконалюється через це бібліотека антивірусних програм не завжди може розпізнати вірус-шифрувальник. Вони шукаються так звані «дірки» в мережевих протоколах, також важливим фактором, є сам користувач який через небезпечний сайт або посилання добровільно завантажує вірус на комп'ютер який через корпоративну мережу може розповсюдиться на всіх інших.

2.4 Класифікація процесів захисту і загроз та математична модель захисту

Класифікуєм типові процеси захисту інформації в комп’ютерних системах, описавши характер їх реалізації через математичну модель.

$$C = F, I, Z, G, N > \quad (2.1)$$

де С – клас процесу,

F – класифікаційні ознаки функційної належності (обробка інформації, систематизація інформації, прийняття управлінських рішень, тощо);

I – класифікаційні ознаки за характером інформації, що надходить (вихідна, для подальшої обробки, фінальна, тощо);

Z – класифікаційні характеристики за засобами захисту (автентифікація, парольний захист, криптографічний захист, тощо);

G – класифікаційні характеристики за часом (динамічна зміна даних, статичне накопичування даних, тощо);

N – класифікаційні характеристики за пріоритетом (високий, низький середній, тощо);

Проведемо формалізовану класифікацію загроз інформації в комп'ютерних системах, формалізована модель представлена у вигляді двох складових[23].

Перша складова, це правило:

$Y_i = <Y_1, Y_2, \ldots Y_n>$, де Y_i – клас поточної загрози, Y_1-Y_n – класи можливих загроз. Наприклад, Y_1 – клас загроз, що спрямовані на дані у пам'яті; Y_2 – клас загроз, пов'язаних з коректністю вхідних даних; Y_3 – клас загроз, пов'язаних з нестійкістю комп'ютерної системи; Y_4 – клас загроз, пов'язаних з рівнем привілеїв та доступу; Y_5 – клас загроз, пов'язаних з відмовою обслуговування; Y_6 – клас загроз, пов'язаних з атаками на систему; Y_7 – клас загроз, пов'язаних з апаратними складовими.

Друга складова – це матриця відповідності загроз та їх характеристик, взаємозв’язки між характеристиками та класами загроз наведені в табл. 2.1. a1 – наприклад, це «висячий покажчик», a17 – проблеми з конфігуруванням апаратних засобів, a19 – фізичний доступ до носіїв інформації, тощо.

Таблиця 2.1 – Взаємодія між характеристиками та матрицями загроз.

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}
Y_1	+	+														+	+	+	
Y_2			+	+	+	+	+			+								+	
Y_3			+	+			+	+									+		
Y_4						+		+	+	+							+		
Y_5	+	+	+					+	+		+	+	+			+			+
Y_6				+	+	+	+			+	+	+	+	+	+		+	+	+
Y_7																+	+	+	+

Причому треба враховувати, що в один момент часу можуть мати місце як один, так і кілька класів загроз, а характеристики можуть змінюватися в процесі прийняття рішення. І з їх зміною один клас загрози може перейти в інший або корелювати з ним.

Визначення того чи іншого класу загрози здійснюється на основі множини характеристик. Причому в один момент часу можуть мати місце, як один, так і кілька класів загроз, а характеристики можуть змінюватися в процесі прийняття рішення[15,16].

Приклад залежностей між класами загроз та їх характеристиками для класу Y1 має вигляд:

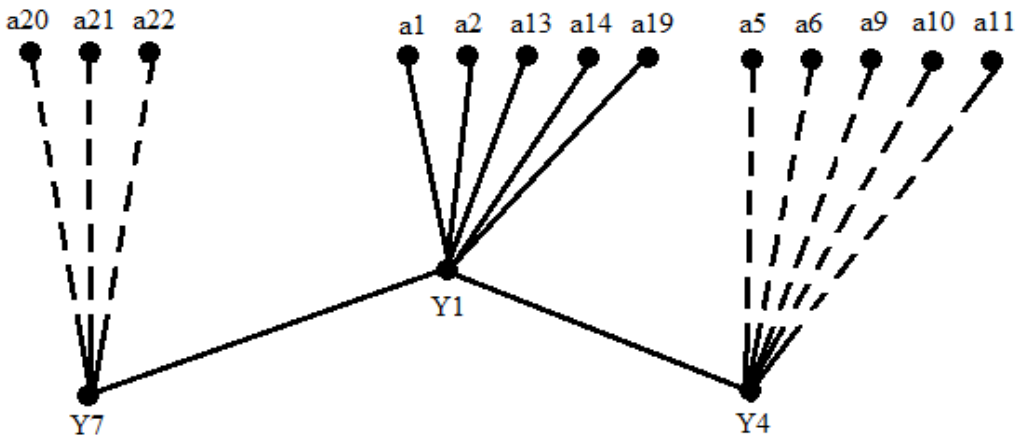


Рисунок 2.11 – Залежність між класами загроз та їх характеристиками

При цьому штрих-пунктирні лінії вказують, що при додатковій появі однієї чи кількох характеристик, клас Y1 може переходити в інший або корелювати з ним.Аналогічним чином будуються залежності і для інших класів.

На основі проведеної класифікації загроз та їх залежностей було побудовано математичну модель захисту інформації в комп'ютерних системах.

$$R_i = \begin{cases} a_1 \vee a_2 \vee a_{13} \vee a_{14} \vee a_{19} \\ a_3 \vee a_4 \vee a_5 \vee a_6 \vee a_7 \vee a_{15} \vee a_{16} \vee a_{22} \\ a_8 \vee a_9 \vee a_{17} \vee a_{18} \vee a_{22} \\ a_5 \vee a_6 \vee a_9 \vee a_{10} \vee a_{11} \vee a_{19} \\ a_4 \vee a_{12} \vee a_{13} \vee a_{20} \\ a_3 \vee a_5 \vee a_7 \vee a_9 \vee a_{11} \vee a_{12} \vee a_{13} \vee a_{14} \vee a_{15} \vee a_{16} \vee a_{17} \vee a_{18} \vee a_{21} \vee a_{22} \\ a_2 \vee a_{19} \vee a_{20} \vee a_{21} \vee a_{22} \end{cases} \quad (2.2)$$

де Ri – реакція системи захисту в поточний момент часу, яка є прямо пропорційною класу загрози чи групі класів, тобто є прямо пропорційною об'єднаній множині характеристик тієї чи іншої загрози.

На основі проведеного у першому розділі огляду вірусів-шифрувальників та класифікації загроз було зроблено висновок про те, що віруси-шифрувальники формують окремий клас загроз, який поєднує в собі характеристики загроз, пов'язаних з доступом, атаками на систему, коректністю вхідних даних та частково апаратними складовими.

Отже, узагальнена математична модель віруса-шифрувальника представлена наступним чином:

$$Y_v = Y_2 \cup Y_4 \cup Y_5 \cup Y_6 \cup Y_7$$

що вимагає від системи захисту відповідної реакції.

2.5 Висновки

У другому розділі сформульовано основні вимоги до концептуальної моделі захисту комп'ютерних систем. Проведено класифікацію типових процесів захисту інформації в комп'ютерних системах, яка описує характер їх реалізації через математичну модель.

Проведено формалізовану класифікацію загроз інформації в комп'ютерних системах, формалізована модель представлена у вигляді двох складових: правила, прописаного за допомогою теорії множин, та графів залежностей між класами загроз та їх характеристиками.

На основі проведеної класифікації загроз та їх залежностей було побудовано математичну модель захисту інформації в комп'ютерних системах.

3 МЕТОД БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМИЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Методи вирішення багатокритеріальних задач

Багатокритеріальна оптимізація являє собою невід'ємну частину діяльності по оптимізації і має велике практичне значення, оскільки майже всі реальні проблеми оптимізації ідеально підходять для моделювання з використанням декількох конфліктних цілей. Класичні засоби вирішення таких проблем зосереджені на перетворенні декількох цілей в одну ціль, тоді як еволюційні засоби мають за мету вирішення задачі багатокритеріальної оптимізації як такої [25,26].

Багатокритеріальними називають задачі оптимізації, в яким є декілька цільових функцій. Потрібно отримати рішення, яку в деякому сенсі буде найкращим по всіх складових цільової функції. Цільові функції в задачах багатокритеріальної оптимізації називають приватними критеріями або локальними оцінками альтернатив. Такі задачі називають також задачами векторної оптимізації. Це пов'язано з тим що глобальні критерії ми можемо приставити у вигляді вектору елементами якого являються значення приватних критеріїв тобто в такому вигляді $F(X) = (f1(X), f2(X), \dots, fn(X))$.

В загальному випадку можна представити задачу багатокритеріальної оптимізації в такому вигляді

$$\begin{cases} f_1(X) \to min, X \in D; \\ f_2(X) \to min, X \in D \\ \quad \dots \\ f_n(X) \to min, X \in D \end{cases} \qquad (3.1)$$

Де D – допустима множина

Цільова функція f_1 направляється до мінімума функція f_2 поводить себе аналогічно і всі наступні функції включаючи функцію f_n теж досягають мінімума при умові що керованні змінні відповідають допустимій множині. Якщо якийсь критерій нам потрімо максимізувати то для цього потрібно перемножити

відповідну цільову функцію на -1 і таким чином задача максимізації зведеться до задачі по пошуку мінімуму[27].

Для кожної допустимої множини можна побудувати його відображення у вигляді множини можливих значень приватних критеріїв Y.

3.1.1 Аналіз методу ієрархій та методу багатокритеріальної оптимізації по Парето

Один з методів запропонував американський математик Томас Сааті. Метод являє собою математичний інструмент системного підходу для вирішення проблем прийняття рішень. MAI використовується в найрізноманітніших сферах людської діяльності щодо прийняття. Але слід відзначити, що MAI не «нав'язує» якесь рішення, а дає змогу ОПР знайти таке рішення, яке б найкраще співпадало з його розумінням проблеми та способами вирішення проблеми. Тобто MAI надає можливість з різних сторін оцінити та проаналізувати проблему[30].

Цей метод є високо універсальним: використовується в різноманітних задачах, до прикладу розподіл ресурсів, прийняття вагомих рішень відповідно до критичної ситуації, прогнозування (аналіз можливих результатів).

Приклад задачі для пошуку рішень має такий вигляд: мається кілька варіантів рішень: $Y_1, Y_2, \dots Y_n$ – наша множина альтернатив, вони характеризуються набором критеріїв: $a1, a2, \dots an$. З цієї множини потрібно вибрати найкращу.

З огляду на постановку задачі для MAI випливає що вона є дуже близькою до задачі прийняття рішень, що виникає в реальних ситуаціях: є декілька варіантів для вирішення проблеми, які в свою чергу характеризуються різними критеріями . MAI використовується в найрізноманітніших сферах людської діяльності щодо прийняття. Тобто для представлення оцінок в кількісному виразі було запропоновано використовувати шкалу попарних порівнянь ці критерії характеризують наскільки варіант підходить для розв'язку даної проблеми.

Таблиця 3.1 – Шкала попарних порівнянь Т.Сааті

Відносна важливість, визначена в балах	Визначення важливості	Пояснення
1	Однакова важливість	Альтернативі рівнозначні за даним критерієм
3	Одна альтернатива незначно важливіша за іншу	Одна з альтернатив незначно домінує над іншою за критерієм
5	Одна альтернатива суттєво переважає над іншою	Можна говорити про безумовну перевагу однієї альтернативи над іншої за критерієм
7	Одна альтернатива значно переважає над іншою	Альтернатива настільки переважає над іншою, що це є практично значимим
9	Альтернатива абсолютно переважає над іншою	Очевидність даної переваги підтверджується більшістю
2,4,6,8	Проміжні оцінки між судженнями	Компромісні рішення щодо порівняння альтернатив
Обернені значення оцінок	Якщо при порівнянні a альтернатив визначено, що A_1 домінує над A_2 з величиною 7, то A_2 буде домінувати над A_1 з величиною 1/7	

Згідно MAI процес вибору рішень виконується на основі попарних порівнянь.[31] Наприклад, за допомогою попарних порівнянь можна визначити найвищого студента серед групи студентів A, B, C : все що потрібно це попарно прівняти цих студентів між собою. Так само можна порівняти відносту важливість кількісно невизначених факторів. Кількісно можуть виражатися критерії якими характеризуються альтернативи, наприклад як з зростом студентів. Але відповідно є і критерії які неможливо кількісно виміряти, в такому випадку потрібно порівнювати альтернативи за цим критерієм.

Для представлення оцінок в кількісному виразі було запропоновано використовувати шкалу попарних порівнянь, яка показана у таблиці 3.1 Ця

шкала детально описується в [32]. Згідно цієї шкали можливо здійснювати порівняння критеріїв, не зважаючи на відсутність фізичних чи об'єктивних одиниць виміру. Тому що такий спосіб є безрозмірним, то виключається необхідність проведення значень до однакових одиниць вибору

Алгоритм застосування описаний в [30]. Математичні процедури за допомогою яких можна отримати наближені значення для MAI.

На першому етапі виконується структурування проблеми у виді ієрархії. Домінантна ієрархія будується з вершини – вузла, він в свою чергу відповідає головній меті, через критерії ві яких залежать наступні рівні - проміжні рівні і так до найвищого рівня – переліку варіантів вибору. Приклад ієрархії,що будується в ході застосування MAI, приведений на рисунку 3.1

Рисунок 3.1 – Ієрархічне представлення задачі.

Вершиною є ціль вибору, згідно з раніше описаною підходу до побудови ієрархії. Проміжним рівнем є критерії і найнижчим рівнем представлені альтернативи .

Як видно з математичної точки зору, структури які присутні в MAI, є направленні графи. Зв'язки формують так звані способи, що ведуть від одних вузлів до інших. Ці способи є частинами основних способів, що ведуть від мети задачі через фактори, критерії до варіантів рішень – альтернатив.

Наступним кроком в MAI є встановлення відповідних пріоритетів критеріїв в ході цього ранжування вони розташовуються в порядку зменшення важливості. Ранжування критеріїв проводиться за допомогою методів попарних порівнянь.

Далі процес ранжування пов’язується з заповненням таблиці попарних порівнянь загальний вид якої показаний у таблиці 3.2. Таблиця може мати певні відмінності, відрізнятися головним в ній є попарне порівняння критеріїв.

Таблиця 3.2 – Ранжування критеріїв

	Y_1	Y_2	…	Y_n	Середні геометричні	НВП
Y_1						
Y_2						
…						
Y_n						
Всього						
λ_{max}						
ІУ						
ВУ						

В процесі заповнення проводяться попарні порівняння критеріїв Y_i та Y_j в відповідні клітинки таблиці і та j, ставлять відповідну оцінку відносно шкали попарних порівнянь(Таблиця 3.1). В клітинку j, і ставлять обернене значення до того, що поставлене в і, j.

Так, наприклад, якщо критерій Y_1 переважає над критерієм Y_2 з оцінкою 5, то в клітинку (1, 2) ставиться оцінка 5, а в клітинку (2, 1) – оцінка 1/5.

Спочатку заповнюються найбільш важливі критерії виставляючи цілі оцінки, а потім – оберненні. Чим більше цілочисельних оцінок тим важливіша критерія. Головна діагональ таблиці (матриці попарних порівнянь) буде дорівнювати одиниці.

Відповідно до формули розраховуються середні геометричні для рядка. Вони використовуються для приблизного розрахунку компонентів власного вектора, які в свою чергу будуть нормалізовані та будуть використовуватися в якості нормалізованого вектору пріоритетів

$$a_t = \sqrt[n]{v_{i1} * v_{i2} * \dots * v} \qquad (3.2)$$

Де а – середнє геометричне;

і – номер рядка таблиці;

n – кількість критеріїв (альтернатив); v_{i1}, v_{i2}, …, v_{in} – оцінки переваги критерію (альтернативи) Ki (Ai) над

відповідними критеріями (альтернативами) - значення в клітинках (i, 1), (i, 2),

…, (i, n) відповідно

Нормалізований вектор пріоритетів (НВП), його значення обчислюються за формулою

$$k_j = \frac{a_j}{\sum a_i} \qquad (3.3)$$

де k_j – компонент нормалізованого вектора пріоритетів;

j – номер рядка, для якого розраховується компонент;

a_j – середнє геометричне відповідного рядка;

$\sum a_i$ – сума середніх геометричних таблиці.

НВП містить величину кожного пріоритету або альтернатив якщо матриця, тобто за допомогою НВП виражається важливість або ступінь чиннику кожного критерію на рішення.

Наступні значення потрібні для оцінки адекватності суджень – узгодження пріоритетів локальних. Відповідно розраховується максимальне власне значення матриці - λ_{max}, формула має наступний вигляд

$$\lambda_{max} = \sum_{i=1}^{n} \qquad (3.4)$$

λ_{max} де – максимальне власне значення матриці;

n – кількість рядків;

і – номер рядку;

j – номер стовпцю;

v_j – значення оцінки переваги критерію (альтернативи) Y_i (A_i) над іншими критеріями (альтернативами) – елементи стовпця j;

k_i – компонент НВП, що відповідає рядку і. Після цього розраховується ІУ – індекс узгодженості. Він є оцінкою суперечливості результатів порівнянь. Вони виникають в наслідок помилок

експертів які є суб'єктивними і залежать від кількості попарних порівнянь.ІУ це позитивне число і розраховується за формулою

$$\text{ІУ} - \frac{\lambda_{max} - n}{n-1} \qquad (3.5)$$

Останнє в заповнені таблиці 3.2 є обчислення ВУ- відношення узгодженості

$$\text{ВУ} = \frac{\text{ІУ}}{\text{ПВУ}} \qquad (3.6)$$

де ІУ – індекс узгодженості;

ПВУ – показник випадкової узгодженості.

ПВУ визначається теоретично для випадку, коли оцінки в матриці (таблиці) представлені випадковим чином та узгодженість матриці залежить лише від розміру матриці, так як показано в таблиці 3.3.). В клітинку j, і ставлять обернене значення до того, що поставлене в і, j.

Таблиця 3.3 – Значення показника випадкової узгодженості залежно від розміру матриці

Розмір матриці	1	2	3	4	5	6	7	8	9	10
ПВУ	0	0	0,5	0,90	1,12	1,24	1,32	1,41	1,45	1,49

Його значення не повинно бути більшим чи меншим ніж 10-15%. При перевищенні матриця буде вважатися суперечливою і її потрібно переоцінити.

Наступним етапом використання МАІ буде попарне порівняння альтернатив (варіантів) за відповідними критеріями. Відповідно до цього заповнюється таблиця цих порівнянь, яка відображена в таблиці 3.4.

Таблиця 3.4- Попарне порівняння альтернатив за критеріями

	a_1	a_2	…	a_n	Середні геометричні	НВП
a_1						
a_2						

…						
a_n						
Всього						
$\lambda_{max,j}$						
$ІУ_j$						
$ВУ_j$						

Вигляд даної таблиці не є універсальним та може відрізнятися, але в ній важлива наявність попарного порівняння альтернатив та розрахунку НВП. Сама таблиця заповняється відповідно до таблиці 2.2, різницею є лише те що порівняння в цій таблиці виконується відповідно критерію $К_j$. У всіх інших розрахунках то вони проводяться аналогічно матриці попарного порівняння. Після порівняння всіх альтернатив за всіма критеріями, виконуються розрахунки підсумків значення пріоритетів (ПЗП), ці значення називають глобальним значенням пріоритетів. Визначається рішення яке підходить найкраще та перевіряться його достовірність. ПЗП визначає перевагу кожної альтернативи над іншою враховуючи переваги критеріїв один над одним.

Коли усі ПЗП розраховані, отримується найкраща альтернатива – це альтернатива яка має найкраще значення підсумкового значення пріоритетів. Узгодженість ієрархії можна визначити, розрахувавши узагальнений індекс узгодженості (ЗІУ) та узагальнене відношення узгодженості (ЗВУ).ЗІУ розраховується за наступною формулою

$$ЗІУ = \sum_{j=1}^{n} ІУ_j * k_{НВП,j} \quad (3.7)$$

де $ІУ_j$ – індекс узгодженості за критерієм Кj;

$k_{НВП,j}$ – компонент НВП для критерію Кj;

n – кількість критеріїв;

j – номер стовпця.

Значення ЗІУ ділиться на вираз аналогічного ж типу, але з випадковим індексом узгодженості, який відповідає розмірам кожної зваженої пріоритетами матриці. Таким чином, буде отримано значення ЗВУ. [30,31,32]

Процес прийняття рішень найчастіше пов’язують з поняттям зрівнянності чи незрівнянності за Парето. Під питанням рішення також розуміють питання оптимізації яка пов’язана з оптимізації певних процесів чи функціонуванні певних систем.

Для кращого розуміння методу оптимізації по Парето розглянемо процес проектування інформаційної системи з використанням багатокритеріальної оптимізації.

В цьому прикладі основний акцент буде відселений на загальних і резервних каналів для обробки інформації в системі. При цьому проблема багатокритеріальної оптимізації формулюється в проблемі оптимізації топології мережі по критеріям:

- максимізація кількості зв’язків між загальним та резервним каналом у випаку виходу з ладу загального каналу.

- вартість – повинна бути як найменшою(мінімізація);

- при нормальній роботі основного каналу зв’язки з додатковим повинні бути мінімальні.

Наводяться наступні цільові функції :

1.Цільова функція 1 – повинна мінімізувати вартість каналів між отримувачем і джерелом. Відображення цієї функції наступне:

$$min \sum_{i=1}^{N} c\big(\text{загальнийканал}(s_i, d_i)\big) + \sum_{i=1}^{N} c\big(\text{резервнийканал}(s_i, d_i)\big) \quad (3.8)$$

Де с – вартість кожного каналу;

(s,d) – пара джерело – отримувач.

2.Цільова функція 2 – при поломці інформаційної системи, має існувати резервний канал про який ми знаєм та основний канал і резервний це дві різні частини які не є одним цілим. Отже метою функції є мінімізація зв’язків між основним та резервним каналом, що показується в наступній формулі

$$max \sum_{i=1}^{N} \text{спільні границі}\big(\text{основнийканал}(s_i, d_i), \text{додатковіканали}(s_i, d_i)\big)$$

3.Цільова функція 3 – функція має за мету максимізувати спільні зв’язки між способами копіювання резервного і має наступний вигляд

$$max \sum_{i=1,j=1 i\neq j}^{N} \text{спільні границі}$$

Оскільки всі три функції пов’язані між собою то можна сказати дана задача це задача багатокритеріальної оптимізації. Одним з найпростіших методів вирішення даної задачі є метод Парето-переваги, що використовує стандартний Парето підхід до знаходження оптимальних рішень.

Множина Парето-оптимальних рішень містить ті варіанти що будуть задовольняти в формулі

$$\Phi = \{argextr[\lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_i f_i]\} \quad (3.9)$$

Де вагові коефіцієнти $\lambda_1, \lambda_2, \ldots, \lambda_i$ обираються з умови $\lambda_i > 0$, і сума ваговиг коефіцієнтів буде дорівнювати 1. При різних допустимих комбінаціях вагових коефіцієнтів.

В цій моделі вирішення представляє собою множину основного каналу разом з додатковим каналом. Для того щоб отримати рішення будується множини всіх цих допустимих способів між вузлами інформаційної системи. Для відповідної пари вузлів формується відповідний набір основних та додаткових каналів. Роблять н основі випадкової вибірки. Множина оптимальних рішень змінюється відповідно і генерується в процесі ітераційного оптимізаційного процесу.

Рішення шукаються наступним чином:

1.обиремо поточний вузол як вузол-джерело;

2.якщо способ безпосередній з поточного вузла в вузол-отримувача, то виконується перехід в цей вузол. В зворотньому випадку – потрібно вибрати наступний вузол, та вибрати його поточним наступній ітерації алгоритму;

3.якщо поточний вузолє вузлом отримувача відповідно потрібно припинити процес пошуку. Та перейти до другого кроку.

Цей алгоритм накладає наступні обмеження:

1.один вузол використовується лише один раз при пошуку шляху;

2.якщо з вузла не можливо потрапити в інший вузол, то процес пошуку рішень припиняється.

Звісно існують шляхи покращення отриманих рішень. Якщо до певного рішення бо комбінацій рішень застосувати методику удосконалення.

Як бачимо з аналізу методу Парето подібні методи не можуть бути використані в системах захисту інформації, оскільки головною метою захисту пошук єдиного ефективного рішення, яке б дозволило максимізувати захищеність та мінімізувати загрози інформації, тому данні методи слід використовувати в комбінації з іншими методами.

3.2 Метод оптимізації системи захисту за рахунок багатокритеріальної оптимізації

Ефективна робота системи захисту інформації залежить від правильного комбінування двох методів оптимізації спираючись на їх недоліки. В методі Парето вагомим недоліком є те що самостійно використовуватися в системах захисту інформації він не може так, як його головною метою є пошук єдиного ефективного рішення що в свою чергу дозволить максимізувати захищеність та мінімізувати загрози інформації. До недоліків також відносять суб’єктивізм у досліджені вагових коефіцієнтів критеріїв та компенсацію значень часткових критеріїв [33,34]. Останній недолік може призвести до хибного результату, так як рішення яке було обране за найкращим загальним результатом, може мати не найкращі результати за критеріями з найбільшими значеннями вагових коефіцієнтів, які компенсуються кращими результатами за критеріями з меншими значеннями вагових коефіцієнтів. Відповідно результатом буде те, що обране рішення буде не найкращим, а це, як можна зрозуміти, може призвести до ігнорування небезпечного або шкідливого процесу, реалізації сценарію його загрозу та, як наслідок, порушення конфіденційності, цілісності або доступності інформації.

Вищезазначені недоліки фактично нівелюються аналітичною ієрархічною процедурою Сааті, з іншого боку ця процедура має ряд недоліків, а саме з

методом Сааті виникають проблеми які заключні в наступних питаннях таких як складність оцінок. Не дивлячись на те, що присутня відповідна шкала, яка в свою чергу дозволяє оцінити, як кількісні так і некількісні фактори. Відношення узгодженості будується на відхиленні статичної величини. Що може призвести до результатів, що важко інтерпретуються. В результаті цього матриця попарних порівнянь буде мати значення відношення узгодженості у допустимих межах незважаючи на те що результат порівняння буде відрізнятися від більшості результатів порівняння,які дають експерти в таких ситуаціях. Сама процедура парних порівнянь є трудомістким процесом[35].

Тому, для оцінювання ефективності рішень в системах захисту інформації використаємо переваги двох вищезазначених методів.

Сучасні комп'ютерні системи (КС) є складними програмними-апаратними комплексами, що весь час перетворюються, розвиваються та модернізуються. Використання комп'ютерних систем у вагомих високотехнологічних сферах життя, діяльності суспільства: системи управління складними технологічними процесами, зв'язок, медицина, банківська справа тощо, вимагає забезпечення надійного захисту їх компонентів. Одним із засобів підвищення захисту є розроблення і впровадження ефективних методів захисту комп'ютерних систем.

Неповнота та неточність систем захисту інформації, низький рівень загрозостійкості комп'ютерних систем та їх складових, відсутність або відносно висока вартість захисних програм та апаратних засобів захисту, відсутність технічної документації ускладнюють реалізацію процесу захисту КС та їх складових. Вартість виявлення загроз та їх ліквідування у комп'ютерних систем збільшує відповідний показник на порядки при переході з нижчих на вищі рівні.

Перспективним напрямком розвитку засобів захисту є використання у їх складі компонентів багатокритеріальної оптимізації. Відомі засоби захисту комп'ютерних систем, що використовують інтелектуальні компоненти, орієнтовані на вирішення окремих вузькоспеціалізованих захисних задач та не дають бажаного рівня універсальності, через що проблема підвищення ефективності захисту за рахунок розроблення і вдосконалення інтелектуальних засобів [36] є актуальною та потребує в свою чергу подальших досліджень. У

тому числі ця проблема вирішується способом розроблення інноваційних теоретичних основ захисту інформації з врахуванням чиннику інтелектуалізації на реалізацію процесу захисту.

У зв'язку з розширенням галузей застосування комп'ютерної техніки, а саме, її використання при створенні систем керування, нових засобів зв'язку, “обчислювальних механізмів” для критичних додатків і для мобільного користувача, засобів “електронної комерції”, “мультимедійних” систем і т. і., до КС висуваються жорсткі вимоги захисту та надійності захисних систем.

Найбільших збитків завдає саме відмова КС через потрапляння в неї тих чи інших загроз що провокують її зупинку. У нинішніх умовах жорсткої конкуренції відмови в обслуговуванні клієнтів компаніями, що надають оперативні послуги (банківське Internet – обслугову-вання, WEB-сервери, телефонія та електронна комерція), можуть призвести до втрати клієнтів[37].

На сьогодні все частіше виникає об'єктивна необхідність відмовитися від багатьох відомих методів та засобів захисту інформації на етапі експлуатації КС. Ця необхідність диктується безпосередньо умовами застосування КС. Так, усе більше з'являється систем, до яких неможливий або заборонений доступ для традиційного експлуатаційного обслуговування, що передбачає захист комп’ютерної системи, діагностику систем захисту та її компонентів, відновлення робочих процесів, або вимоги ринку збуту не допускають більших витрат коштів і часу на звичайне обслуговування з використанням спеціального персоналу. У зв'язку із цим постає необхідність розроблення нової методології захисту КС на етапі експлуатації.

Тому, підвищення ефективності процесу захисту комп'ютерних систем на етапі експлуатації в умовах неповноти інформації шляхом розвитку теоретичних основ, засобів та методів інтелектуального захисту є актуальною науково-прикладною проблемою.

Вирішення науково-прикладних задач інтелектуалізації процесу захисту, що забезпечує збільшення його ефективності шляхом підвищення достовірності у випадку неповноти діагностичної інформації є актуальною проблемою сьогодення.

У якості об’єкта захисту інформації розглядається комп’ютерна система. Суть захисту полягає у виявленні так званих «дірок» в системі захисту за результатами її аналізу. В залежності від обраного нами набору параметрів захисту, методів опрацювання результатів сканування, витрати часу на побудову системи захисту та її результат буде різний. Відповідно потрібно розробити таку систему захисту інформації, при якій будуть мінімізуватися витрати та зростатиме ефективність.

Розгляд особливостей моделювання комп’ютерних систем як об’єктів захисту дає різну можливість її представлення: булеві вирази, таблиці істинності, автоматні представлення (таблиці, графи переходів).

До складових сучасних КС можна віднести: комп’ютери, мережеве обладнання, лінії зв’язку, програмне забезпечення і навіть самих користувачів, що в свою чергу є одною із найбільших загроз для безпеки КС. Тому моделі комп’ютерних систем найчастіше представляють у вигляді багаторівневих моделей де кожному елементу відповідає певний рівень. І сама узагальнена модель представляється множиною моделей[38] $M = \{m_i\}, (i = \overline{1,n})$, де модель m_i відображає компонент КС на деякому рівні абстракції на *i*-му рівні деталізації.

Треба враховувати, що функціонування більшості систем захисту інформації, по факту, зводиться до розпізнавання множини активних в комп’ютері процесів, їх класифікації з метою визначення шкідливих та небезпечних процесів та прийняття рішень щодо їх блокування або ігнорування. Причому процес прийняття рішень ґрунтується на врахуванні великої множини вимог які суперечать між собою і оцінюванні множини рішень за багатьма критеріями. Суперечливість характеристик процесів, неоднозначність оцінювання процесу, неповнота отриманої інформації у досить значній мірі роблять складним прийняття остаточного рішення та суттєво чинникають на його якість.

Особливості сучасних КС як об’єктів захисту створили нові проблеми реалізації процесу захисту у порівнянні з моментом появи перших моделей захисту інформації, що покладені в їх основу. Згадані вище труднощі не можна подолати без істотної модифікації відомих методів захисту або розроблення

нової методології захисту КС, що ґрунтується на принципах: переваги програмного контролю і захисту КС над апаратним, призначеним тільки для захисту їх складових; відмови від методів структурного та покомпонентного захисту інформації для сучасних складових КС в класичному їх розумінні за причиною неможливості використання багатоконтактних пристроїв при намаганні реалізувати по компонентний захист; багаторівневого моделювання КС як об'єктів захисту; інтелектуалізації процесу захисту комп'ютерної системи.

Вище перераховані принципи пов'язанні з новими особливостями комп'ютерних систем як об'єктів захисту. Кожен з яких відображає одну бо декілька особливостей.

Взявши до уваги аналіз методу Сааті [32] зрозуміло що метод аналізу ієрархій полягає в розбитті проблеми на більш прості складові і в подальшій обробці послідовних суджень. Причому треба враховувати, що в один момент часу можуть мати місце як один, так і кілька класів загроз, а характеристики можуть змінюватися в процесі прийняття рішення. І з їх зміною один клас загрози може перейти в інший або корелювати з ним [33]. Тому формальний опис моделі для задачі оцінювання ефективності рішень виглядає так:

$$E_{r_j} = M(A_p, k_p)$$

де E – це ефективність рішення rj, M – це метод, за допомогою якого ведеться пошук ефективного рішення; A_p – характеристики процесу p; k_p – множина критеріїв для оцінювання характеристик процесу p, згідно з якими оцінюється ефективність можливих рішень.

На основі множин які ми отримали можна сформуємо три матриці. В першу (A) будемо заносити дані відношень критеріїв, в другу матрицю (B) і третю матрицю (C) значення, які відображають характеристики для кожного процесу за кожним з критеріїв.

Обчислення значень критеріїв виконується за допомогою методу попарних порівнянь з застосуванням шкали переваг Сааті. Спочатку попарно порівнюється лише один окремий критерій з усіма іншими критеріями. В результаті

знаходиться перевага критерію k_i. Потім отримані в результаті цього дані заносяться у перший рядок матриці A (2). Всі наступні переваги обчислюються за допомогою математичних розрахунків. Таким чином, ми уникаємо обмежень, що накладає шкали переваг методу Сааті.

$$A = \begin{bmatrix} 1 & \mathrm{kx}_1/\mathrm{kx}_2 & \dots & \mathrm{kx}_1/\mathrm{kx}_n \\ \mathrm{kx}_2/\mathrm{kx}_1 & 1 & \dots & \mathrm{kx}_2/\mathrm{kx}_n \\ \dots & \dots & \dots & \dots \\ \mathrm{kx}_n/\mathrm{kx}_1 & \mathrm{kx}_n/\mathrm{kx}_2 & \dots & 1 \end{bmatrix}, \qquad (3.11)$$

де $\mathrm{kx}_1 \dots \mathrm{kx}_n$– відповідні критерії, n – максимально можлива кількість критеріїв, за якими здійснюється оцінювання.

Далі значення критеріїв ми нормуємо таким чином, щоб їх сума дорівнювала одиниці, тобто визначаємо для кожного критерію його ваговий коефіцієнт. При порівняні критерій потрібно в матриці буде відображено перевагу одного критерію над іншим. Для цього вони обчислюються за такими формулами:

$$\mathrm{kx}_j^{\sim} = \sum_{i=1}^{n} \mathrm{kx}_{ij}, j = \overline{1,m} \qquad (3.12)$$

$$v_i = \mathrm{kx}_i^{\sim} \Big/ \sum_{j=1}^{n} \mathrm{kx}_j^{\sim}, i = \overline{1,m}$$

де $v_1 \dots v_n$– вагові коефіцієнти відповідних критеріїв.

Аналогічним чином виконуються порівняння наступних критеріїв. Після цього розраховуються компоненти нормалізованого порівняння і відповідно до отриманих значень отримуємо інформацію про важливість критерію з точки зору ОПР.

Матриця (А) повинна бути перевірена на узгодженість (неузгодженість). Перевірка виконується за допомогою максимального власного значення матриці – λ_{max} .

Далі необхідно виконати попарне порівняння альтернатив за критеріями. В матрицю B (3) заносяться характеристики процесів за кожним обраним критерієм. При чому порівняння виконуються так само як і для критеріїв тобто

одна альтернатива переважає над іншою. Аналогічно виконується ранжування та пошук середнього значення.

$$B = \begin{bmatrix} ax_{11} & ax_{12} & \dots & ax_{1n} \\ ax_{21} & ax_{22} & \dots & ax_{2_n} \\ \dots & \dots & \dots & \dots \\ ax_{f_1} & ax_{f2} & \dots & ax_{f_n} \end{bmatrix}, \quad (3.13)$$

де $ax_{11}…ax_{fn}$– значення відповідних характеристик процесів за відповідними критеріями, f – максимально можлива кількість рішень, для яких здійснюється оцінювання.

Далі дані нормуються таким способом, щоб сума їхніх значень у кожному стовпчику дорівнювала одиниці, і матриця B перетворюється в матрицю $B^{\sim}$.

$$B^{\sim} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2_n} \\ \dots & \dots & \dots & \dots \\ a_{f_1} & a_{f2} & \dots & a_{f_n} \end{bmatrix}, \quad (3.14)$$

де $a_{11}…a_{fn}$– нормовані характеристики процесів.

В матрицю C (5) також заносяться характеристики процесів за кожним обраним критерієм.

$$C = \begin{bmatrix} ax_{11} & ax_{12} & \dots & ax_{1n} \\ ax_{21} & ax_{22} & \dots & ax_{2_n} \\ \dots & \dots & \dots & \dots \\ ax_{f_1} & ax_{f2} & \dots & ax_{f_n} \end{bmatrix}, \quad (3.15)$$

Вираховуються компоненти нормалізованого вектору пріоритетів для кожного попарного порівняння відповідно до критерію. Аналізуючи результат проявляється закономірність важливості того чи іншого процесу до відповідної характеристики. Перетворення над нею виконуються наступним способом. Якщо найкращим результатом для j-го критерію є найбільше значення наслідку рішення, то $n_{ij}^{o} = n_{ij}/n_{max j}$, де n_{ij}^{o} – нормоване значення відповідного наслідку, $n_{max j}$ – найбільше значення наслідку в j-му стовпці. Якщо ж для j-го критерію найкращим результатом є найменше значення наслідку рішення, то $n_{ij}^{o} = n_{ij}/n_{min j}$,

де $n_{\min j}$ – найменше значення наслідку в j-му стовпці. В результаті, матриця $C^{\sim}$ в нас буде мати вигляд:

$$C^{\sim} = \begin{bmatrix} a^{o}_{11} & a^{o}_{12} & \dots & a^{o}_{1n} \\ a^{o}_{21} & a^{o}_{22} & \dots & a^{o}_{2n} \\ \dots & \dots & \dots & \dots \\ a^{o}_{f_1} & a^{o}_{f2} & \dots & a^{o}_{fn} \end{bmatrix}, \qquad (3.16)$$

де $a^{o}_{11} \dots a^{o}_{fn}$ – нормовані значення відповідних наслідків.

Після завершення формування усіх матриць для кожного конкретного рішення обчислюється його ефективність за формулою:

$$E_{r_j} = \sum_{i=1}^{n} k_i \, n_{i_j} n^{o}_{ij} \qquad (3.17)$$

Ціллю даного методу в захисті являє собою прийняття рішення і реалізації, які б дозволили в найкоротший період виявити проблему при мінімальних витратах на механізм захисту. В загальному випадку математична задача захисту інформації формується у вигляді наступної багатокритеріальної задачі вибору [2]:найти такий варіант системи $\overrightarrow{X} \in П \subset D$,для якого $Q \dots, q_m$

Де П – множина Парето – оптимальних рішень; D – множина допустимих значень, в межах якого виконується функціональні і критеріальні обмеження; q_i – критерії оптимальності.

В деякому випадку при m=1 задача являє собою відому в літературі задачу вибору системи захисту інформації за критеріями [2,5] .

Таким чином, задача багатокритеріальної оптимізації перетворюється в звичайну задачу вибору при m>1, забезпечуючи більш прийнятне представлення реальної задачі на вибору системи захисту інформації.

Методика розв’язку багатокритеріальних задач включає в себе наступні етапи [39,40]: побудова множини Парето – оптимальних рішень; вибір одного оптимального рішення з множини Прето – оптимального рішення. Побудова множини Парето є по собі доволі складним і в той же час дуже важливою задачею.

До прикладу розглянем алгоритм побудови множини Парето при m=2. Множина Парето представляє собою певну грань множин альтернатив. Найти множину Парето в даному випадку можливо методом поступового приближення, використовуючи лінійну (кусочно-лінійну, багатогранну) апроксимацію, коли наближення здійснюється відрізками прямих і в результаті отримують ламану лінію, точки зламів якої належать апроксимируємої кривої.

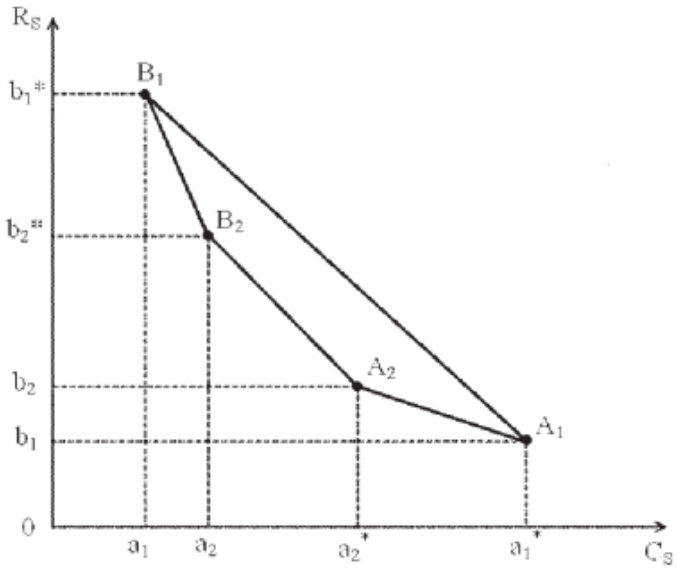


Рисунок 3.2 – Побудова множини Парето

Алгоритм вирішення виглядає наступним чином:

1.Вважається $C(\vec{X}) = a_1; R_S(\vec{X}) = b_1$, де a_1, b_1 які належать множині оцінок та $\vec{X} \in D$-множина альтернатив.

2.Вирішують оптимізаційні завдання$C(\vec{X}) \to min; \vec{X} \in D; R_S(\vec{X}) = b_1$ та $R_S(\vec{X}) \to min; \vec{X} \in D; \mathrm{C}(\vec{X}) = a_1$. Вирішення цих задач дозволяє отримати відповідні точки $A_1(a_1^*, b_1)$ та $B_1(a_1, b_1^*)$, які лежать на множині Парето.

3.Чрез точки A_1 і B_1 проводять пряму, яка і буде першим приближеним значенням множини Парето.

4. Наступне приблизне значення отримується після вирішення наступних двох оптимізаційних задач при виборі наступних точок із множини оцінок a_2, b_2:

$$C(\vec{X}) \to min; \vec{X} \in D; R_S(\vec{X}) = b_2;$$

$$R_S(\vec{X}) \to min; \vec{X} \in D; \mathrm{C}(\vec{X}) = a_2$$

Що в свою чергу дає наступні точки $A_2(a_2^*, b_2)$ та $B_2(a_2, b_2^*)$.

5.Ломана $A_1\ A_2\ B_2\ B_1$ є другим приблизним множини Парето.

6. При необхідності отримання більш точного результату,між точками B_1B_2, задача вирішується алогічно, тобто береться на відрізку (a_1,a_2) нове значення для $C(\vec{X})$, а на відрізку (b_2^*, b_1^*) нове значення $R_S(\vec{X})$ і вирішуються ці дві оптимізаційні задачі так само як в 2 і 4 пункт алгоритму[43,44].

3.3 Висновки

На основі запропонованих у другому розділі залежностей між класами загроз та їх характеристиками, а також враховуючи особливості математичної моделі вірусів-шифрувальників обрано метод багатокритеріальної оптимізації, який найкраще підходить для вирішення поставленої задачі.

Зазначений метод, оснований на використанні матриці відношення критеріїв та врахуванні результатів рішень. Запропонований метод оцінювання ефективності рішень дає змогу підвищити відсоток визначених правильних рішень та має наступні переваги:

- в результаті завжди знаходиться єдине та ефективне рішення;
- можливість компенсації значень часткових критеріїв повністю усунена.

4 ТЕСТУВАННЯ МЕТОДУ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМИЗАЦІЇ

4.1 Оцінювання ефективності методу оптимізації захисту інформації в комп'ютерних системах.

Для оцінювання ефективності методу було обрано такі показники: P_q – показник правильності, P_t – показник вчасності, P_d – показник повноти бази даних.

$$P_q = K_{\text{rp}}/K_z, \tag{4.1}$$

де K_{rp} – кількість правильно розпізнаних загроз, K_z – загальна кількість розпізнаних системою загроз.

$$P_t = T_{\max}/T_{\text{pr}}, \tag{4.2}$$

де T_{pr} – час, затрачений системою на виявлення поточної загрози, $T_{\max}$– максимальний час, який система опрацьовує новий процес.

$$P_d = M_b/M_z, \tag{4.3}$$

де M_b – наявна кількість моделей загроз у базі системи, M_z – загально відома кількість моделей загроз.

Показники вчасності та повноти бази є незалежними між собою. А показник правильно розпізнаних загроз залежить від показника якості навчання.

У якості тестування [46] одну й ту саму множину процесів у комп'ютерній системі було проаналізовано за допомогою оптимізованої системи захисту інформації (ОСЗ) та неоптимізованої системи захисту (НСЗ). Правильність розпізнавання чи не розпізнавання загроз оцінювала група системних адміністраторів, які є експертами у захисті комп'ютерних систем.

Результати тестування показано у таблиці 4.1.

Таблиця 4.1. Результати тестування множини процесів на виявлення загроз

	НСЗ	ОСЗ
Відсоток прав. рішень	78%	96%
Повнота бази даних по відношенню до відомих на сьогодні баз	95%	95%
Середній затрачений час, сек.	2,4	2,5

Враховуючи, що показники правильності та досвіду залежні між собою та при цьому незалежні від показника вчасності для визначення ефективності роботи кожного ОЧ використаємо адитивний та мультиплікативний критерії:

$$E = P_t * (P_q + P_d), \quad (4.4)$$

де Е – ефективність роботи.

Підставивши наведені вище значення у (4.4) отримуємо: $E_{НСЗ}$=1,8, $E_{ОСЗ}$=1,91;

Отже, застосування методу оптимізації рішень у системі захисту дозволило підвищити ефективність розпізнавання загроз на 6% за рахунок збільшення відсотку правильно розпізнаних загроз.

4.2. Оцінювання зниження ризику реалізації загроз інформації в комп’ютерних системах.

Процес управління ризиками, загрозами інформаційної безпеки складається з визначення підходів до оцінювання ризиків, опрацювання, а також перегляду і покращення процесу.

Рисунок 4.1 відображає вигляд в три етапи запропонованого підходу до управління ризиками інформаційної безпеки: ціллю даного запропонованого підходу можна віднести задачу зменшення ризику порушення безпеки, розуміння причин, які роблять інформаційні системи вразливими.

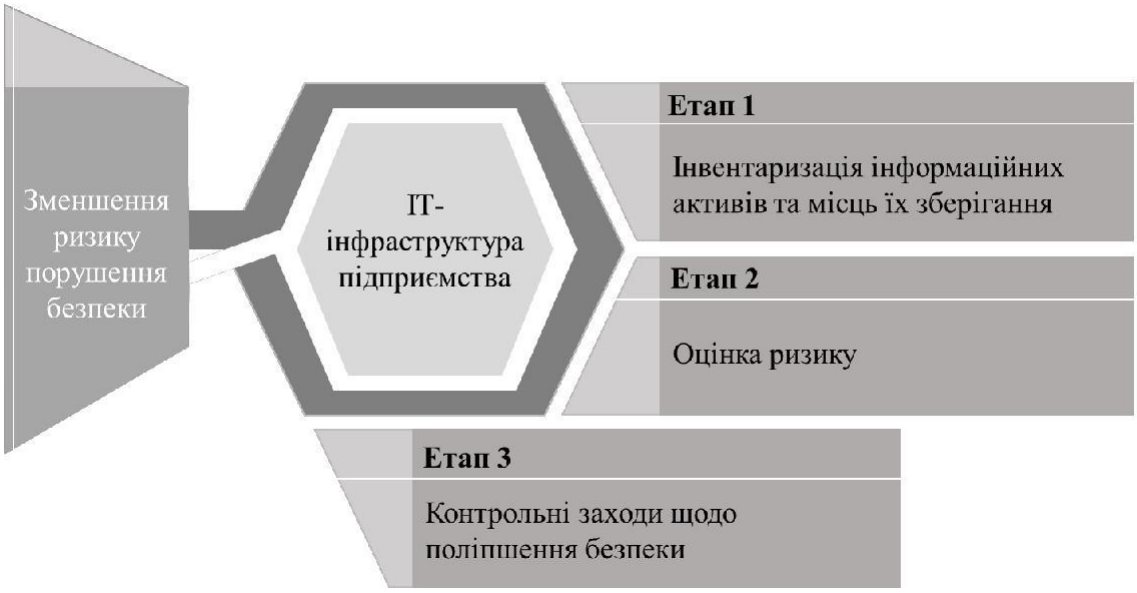


Рисунок 4.1 – Графічне зображення процесу управління ризиками інформаційної безпеки

В першому етапі виконується процес збирання інформації про те, що за інформація зберігається та обробляться та передається за допомогою певного місця збереження (місцем збереження можуть виступати персональні комп'ютери співробітників підприємства, мережеві папки, сервери, роздруковані паперові документи, системи електронного документообігу, а також і інші інформаційні системи, зовнішні місця збереження та т.п.).

Другий етап базується навколо розуміння того, які місця збереження і інформаційні активи мають найвищі ризики.

Третій етап фокусується на створенні дієвого плану контрольних заходів по обробці ризиків.

4.2.1 Оцінка наслідків порушення рівня захисту активів

Для кожного інформаційного активу визначаються наслідки від реалізації ризиків порушення його показників конфіденційності, цілісності, доступності (Таблиця 4. 1).

Таблиця 4.1 – Наслідки при порушенні рівня захисту активів

Рівень наслідків порушення КЦД	**Наслідки комерційним Інтересам організації**	**Наслідки операційної діяльності**	**Наслідки відносинам з клієнтами і партнерами**
1	2	3	4
3	Комерційні інтереси або Фінансове становище Організації можуть бути істотно підірвані, втрата частки ринку	Критична втрата управлінського контролю, повна зупинка операційної діяльності, скасування діючих проектів	Серйозне погіршення Іміджу організації, втрата довіри з боку значної частини клієнтів і партнерів, широка негативна популярність
2	Інформація становить інтерес для конкурентів і приносить їм комерційну вигоду на суму від 50 000 до 100 000 грн.	Середня втрата управлінського контролю, часткове зупинення операційної діяльності і труднощі в реалізації діючих проектів	Негативна інформація про підприємство поширюється в ЗМІ, втрата довіри з боку деякої частини клієнтів і партнерів

Кінець таблиці 4.1

1	2	3	4
1	Інформація становить інтерес для конкурентів і приносить їм комерційну вигоду на суму від 10 до 50 000 грн	Низька втрата управлінського контролю, незначні переривання операційної діяльності і	Втрата довіри деяких клієнтів або потенційних клієнтів, зниження довіри з боку деяких партнерів
0	Порушення конфіденційності, цілісності та доступності інформації не має відчутних наслідків. Дана інформація документується в реєстрі інформаційних активів, але не бере участь в оцінці ризиків ІБ		

Відповідно до даного підходу для активу знаходиться рівень наслідків по кожному типу для усіх можливих властивостей інформації. Ступінь наслідків порушення конфіденційності, цілісності та доступності обчислюється за формулою:

$$L = \max\{L_c, L_v, L_o\}$$

Де L_c- наслідки комерційним інтересам, L_v- наслідки відносин з партнерами та клієнтами, L_o- наслідки операційної діяльності.

4.2.2. Визначення рівня ризику ІБ

Для того щоб вирішити проблему пошуку ступеня ризику необхідно визначити величину збитку від впливу загрози на місце збереження та обробки інформаційних активів.

$$L = L_R * C$$

L - фінансовий збиток від одночасного впливу загрози, спрямованої на вразливість місця збереження інформаційного активу;

L_R - рівень вразливості місця збереження інформації до чиннику ризику, $L_R = \frac{L}{3}$

C – фінансова вартість інформації, що зберігається в даному конкретному місці збереження;

Вартість інформації може формуватися на основі таких факторів, як:

- Вартість заміни або відновлення активу;
- Вартість утримання активу (наприклад, носіїв та засобів обробки);
- Витрати в разі недоступності активу;
- Зниження річного доходу;
- Санкції за невідповідність законодавству.

$$R = L_f * F$$

Величина ризику від здійснення загрози протягом певного проміжку часу (наприклад, року) обчислюється як добуток збитків від її одноразового здійснення на коефіцієнт, що характеризує середньорічну частоту проявів загрози:

де R – ризик від здійснення загрози, спрямованої на вразливість того місця, де зберігають актив;

L_f – фінансовий збиток від здійснення загрози, спрямованої на вразливість того місця, де зберігають актив;

F – середньорічна частота реалізації загрози, розраховується як відношення кількості загроз даного типу до загальної кількості усіх можливих загроз, $F = [0,1]$

Розрахований ризик є підставою для оцінювання множини доступних контрольних заходів. Якщо контрольні заходи за своєю вартістю не перевищують вартість ризику, це означає, що вони є прийнятними. Якщо перевищують, то це говорить про їх недоцільність, оскільки їх впровадження дозволяє уникнути одних збитків лише за рахунок несення інших.

В останньому випадку підприємство може відмовитися від контрольних заходів та виконати одну чи кілька дій:

- прийняти ризик – це рішення залежить від розрахованої суми втрат від реалізації ризику і від очікуваної частоти загроз, а також політики, розробленої в організації, в ставленні до діяльності, яка призводить до даного ризику;
- передати ризик третій стороні, наприклад, перекласти питання захисту на якусь іншу фірму чи адміністративну установу, сюди ж відноситься і страхування ризику;
- уникнути ризику способом відмови від певної діяльності або бізнес-процесів.

Ефективність від впровадження запропонованих контрольних заходів можна оцінити за формулою:

$$E = \frac{R_{\text{old}} - R_{\text{new}}}{R_{\text{old}}}$$

де E – ефективність реалізації контрольних заходів зі зменшення ризиків інформаційної безпеки;

R_{old} – ризик до впровадження контрольних заходів;

R_{new} - ризик після впровадження контрольних заходів.

4.3 Висновки

У розділі проведено оцінювання ефективності розробленого у роботі методі та визначено рівень зниження ризику підчас впровадження запропоновано методу у системи захисту інформації в КС.

Зазначений метод був реалізований та апробований у підсистемі оцінювання ефективності рішень системи виявлення вторгнень на базі мереж глибинного навчання та як засіб багатокритеріальної оптимізації рішень для системи захисту комп’ютерних систем.

ВИСНОВКИ

У першому розділі розглянуто поняття систем захисту інформації, проаналізовано сучасні нормативно-правові акти, які регулюють діяльність таких систем. Досліджено особливості використання найбільш відомих методів багатокритеріальної оптимізації у питаннях захисту інформації. Проаналізовано різні типи комп'ютерних загроз, зокрема віруси-шифрувальники. Сформульовані основні задачі магістерської роботи.

Основна увага приділяється аналізу недоліків сучасних систем захисту інформації від вірусів-шифрувальників та виявленню супутніх проблем, вирішення яких можливо за рахунок використання багатокритеріальної оптимізації.

У другому розділі сформульовано основні вимоги до концептуальної моделі захисту комп'ютерних систем. Проведено класифікацію типових процесів захисту інформації в комп'ютерних системах, яка описує характер їх реалізації через математичну модель.

Проведено формалізовану класифікацію загроз інформації в комп'ютерних системах, формалізована модель представлена у вигляді двох складових: правила, прописаного за допомогою теорії множин, та графів залежностей між класами загроз та їх характеристиками.

На основі проведеної класифікації загроз та їх залежностей було побудовано математичну модель захисту інформації в комп'ютерних системах.

На основі запропонованих у другому розділі залежностей між класами загроз та їх характеристиками, а також враховуючи особливості математичної моделі вірусів-шифрувальників обрано метод багатокритеріальної оптимізації, який найкраще підходить для вирішення поставленої задачі.

Зазначений метод, базується на використанні матриці залежності критеріїв та врахуванні наслідків прийнятих рішень. Запропонований у роботі метод оцінювання ефективності рішень полягає у тому, що дозволяє підвищити відсоток правильно визначених рішень та має наступні переваги:

- його результатом завжди є єдине та ефективне рішення;
- в ньому усунена можливість компенсації значень часткових критеріїв.

У третьому розділі проведено оцінювання ефективності розробленого у роботі методі та визначено рівень зниження ризику підчас впровадження запропоновано методу у системи захисту інформації в КС.

Зазначений метод був реалізований та апробований у підсистемі оцінювання ефективності рішень системи виявлення вторгнень на базі мереж глибинного навчання та як засіб багатокритеріальної оптимізації рішень для системи захисту комп’ютерних систем.

ПЕРЕЛІК ДЖЕРЕЛ ТА ПОСИЛАНЬ

1. Програмний комплекс моніторингу активності користувачів корпоративної комп'ютерної мережі/ Є. В. Красовська // Електротехнічні та комп'ютерні системи, № 08(84), 2012. – С. 85 – 92.

2. Штойер Р. Многокритериальная оптимизация. Теория вычислений и приложения/ Р. Штойер. – М.: Наука, 1992. – 204 с.

3. Інформаційна безпека. Практикум/ В.М. Ахрамович, В.М. Чегренець.- К.: ДУТ, 2017. - 396с.

4. Технології захисту інформації: конспект лекцій/ А.Ф.Карачка. – Тернопіль: ТНЕУ, 2017. – 86 .

5. Інформаційна безпека держави: навч. посіб./ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.

6. Кащенко А.Г. Математические модели выбора комплекса средств защиты информации у автоматизированных системах /А.Г. Кащенко // Кибернетика и высокие технологии XXI века: матер. науч. конф. 13 – 15 мая 2008 г. – Воронеж. 2008. – С. 876 – 888.

7. ISO/IEC 27002. Information technology – Security techniques – Code of practice for information security management. // 2013.

8. ISO/IEC 27001. Information technology -- Security techniques -- Information security management systems – Requirements // 2015.

9. Кини Р.Л. Принятие решений при множестве критериев: предпочтения и замещения/ Р.Л. Кини, Х. Райфа. – Москва: Радио и связь, 1981. – 560 с.

10. Аналіз основних складових небезпеки при побудові системи інформаційної безпеки підприємства/ Л.А. Асєєва// Сучасний захист інформації. - 2019. - №2 (38). – с. 42-46.

11. Інформаційна безпека держави: методичні вказівки до виконання лабораторних робіт/ уклад. О.А. Смірнов, С.А. Смірнов, О.К. Конопліцька-Слободенюк, В.Д. Хох/ – Кропивницький – 2017. – 90 с.

12. Комплексна інформаційна безпека соціотехнічних систем: моделі чиннику та захисту: монографія/ А. В. Дудатьєв. – Вінниця : ВНТУ, 2017. – 128 с.

13. Сучасні інформаційні системи і технології: управління знаннями: навчальний посібник/ В. М. Антоненко, С. Д. Мамченко, Ю. В. Рогушина. – Ірпінь: Національний університет ДПС України, 2016. – 212 с.

14. Антонюк А.О. Теоретичні основи захисту інформаці: Конспект лекцій. — Київ: НТУУ "КПІ", 2003. — 233 с.

15. Огляд моделей захисту інформації в інформаційних системах/ В.Ю. Тітова, С.О Савчук //«Інтелектуальний потенціал – 2019» - Хмельницький: ПВНЗ УЕП, 2019. – Ч.1: Комп’ютерні системи та кібербезпека. – с. 82-84.

16. Концептуальна модель системи захисту інформації в сучасних комп’ютерних системах/ В.Ю. Тітова, С.О Савчук, В.Ю. Черниш// Вісник Хмельницького національного університету. Технічні науки. – 2019. – №3. – с. 164-167.

17. Моделирование системы защиты информации. Практикум: Учеб. пособие./ Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2015. - 120 с.

18. Моделювання систем: конспект лекцій / В. М. Задачин, І. Г. Конюшенко. – Харків : Вид. ХНЕУ, 2012. – 268 с.

19. Аналіз основних складових небезпеки при побудові системи інформаційної безпеки підприємства/ Л.А. Асєєва// Сучасний захист інформації. - 2019. - №2 (38). – с. 42-46.

20. Моделювання систем захисту інформації/ А.О. Антонюк. - Ірпінь: Національний університет ДПС України, 2015. - 273 с.

21. Імітаційне моделювання систем масового обслуговування: Навч. посібник/ В.Б. Толубко, А. Д. Кожухівський, В.В. Вишнівський, Г.І. Гайдур, О.А. Кожухівська. – Київ, 2018. - 175 с.

22. Моделювання систем: навчальний посібник/ І. П. Гамаюн, О. Ю. Чередніченко. – Харків: Факт, 2015. – 228 с.

23. Математичне моделювання: навчальний посібник/ О.В. Махней. – Івано-Франківськ: Супрун В. П., 2015. – 372 с.

24. Математичне моделювання: навчальний посібник/ В.Г. Маценко. – Чернівці: Чернівецький національний університет, 2014. – 519 с.

25. Simulation Modeling and Arena / Manuel D. Rossetti. – 2nd ed. – Hoboken: John Wiley & Sons, Inc., 2016. – 744 p.

26. Optimization Concepts and Applications in Engineering. 3rd Edition/ A.D. Belegundu, T.R. Chandrupatla. – Cambridge University Press, 2019. – 465 p.

27. Optimization Models/ G. C. Calafiore, L. El Ghaoui. – Cambridge University Press, 2014. – 627 p.

28. A Gentle Introduction to Optimization/ B. Guenin, J. Könemann, L. Tunçel. – Cambridge University Press, 2014. – 267 p.

29. Optimization in Practice with MATLAB: For Engineering Students and Professionals/ A. Messac. – Cambridge University Press, 2015. – 494 p.

30. Саати Т. Принятие решений. Метод анализа иерархий / пер. з англ. Р. Г. Вачнадзе. Москва, 1993. 278 с

31. Saaty R. W. The analytic hierarchy process – what it is and how it is used // Mathematical Modeling. 1987. Vol 9, №3-5 с 161-176

32. Саати Т., Кернс К. Аналитическое планирование. Организация систем / пер. з англ. Р. Г. Вачнадзе. Москва, 1991. 224 с.

33. Оцінювання ефективності рішень в системах захисту інформації/ В.Ю. Тітова, В.С. Орленко, І.М. Шевчук, В.С. Даценко.

34. Simulation Modeling and Arena / Manuel D. Rossetti. – 2nd ed. – Hoboken: John Wiley & Sons, Inc., 2016. – 744 p.

35. Optimization Concepts and Applications in Engineering. 3rd Edition/ A.D. Belegundu, T.R. Chandrupatla. – Cambridge University Press, 2019. – 465 p.

36. Optimization Models/ G. C. Calafiore, L. El Ghaoui. – Cambridge University Press, 2014. – 627 p.

36. A Gentle Introduction to Optimization/ B. Guenin, J. Könemann, L. Tunçel. – Cambridge University Press, 2014. – 267 p.

37. Optimization in Practice with MATLAB: For Engineering Students and Professionals/ A. Messac. – Cambridge University Press, 2015. – 494 p.

38. Теорія систем масового обслуговування: навч. посібник/ А. Л. Литвинов. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. – 141 с.

39. Модель порушника в інформаційно-комунікаційних системах / О. Кіреєнко. – Правове, нормативне й метрологічне забезпечення системи захисту інформації в Україні. – 2017. – Вип. 2. – С. 69-77.

40. Математична модель порушника інформаційної безпеки/ Ю.М. Щебланін, Д.І. Рабчун. – Кібербезпека: освіта, наука, техніка. – 2018. – №1(1). – С. 63-72.

41. Інформаційно-орієнтована модель як реалізація методики виявлення чиннику на достовірність інформації в інформаційному просторі/ А.О. Аносов, З.М. Пузняк // Сучасний захист інформації. - 2017. - №4 (32). – с. 55-59.

42. A game theoretic approach to cyber security risk management./ S. Musman, A. Turner// Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. – 2018. - vol. 15(2). – p.127–146.

43. Методы для принятия решений / И.Г. Черноруцкий. – СПб.: БХВ – Петербург, 2005. – 416 с.

44. Моделювання та оптимізація систем: підручник / В.М. Дубовой, Р.Н. Квєтний, О.І. Михальов., А.В.Усов – Вінниця : ПП «ТД«Едельвейс», 2017. – 804 с.

45. Загальні принципи проведення тестування інформаційної безпеки підприємства/ О.А. Курченко, М.В. Бржевський, А.Б. Гребенніков, В.І. Корсун// Сучасний захист інформації. - 2018. - №4 (36). – с. 27-34.

46. НД ТЗІ 3.7-003-05 «Порядок проведення робіт для створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

ДОДАТОК А
(ОБОВЯЗКОВИЙ)
КОПІЇ НАУКОВИХ ПРАЦЬ

УДК 004.832.2

В.Ю. ТІТОВА, В.С. ОРЛЕНКО, І.М. ШЕВЧУК, В.С. ДАЦЕНКО
Хмельницький національний університет

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ РІШЕНЬ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

В даній статті розглянуто відомі методи оцінювання ефективності рішень. Проаналізовано можливість їх використання для оцінювання ефективності рішень, що приймаються системами захисту інформації стосовно класифікації та визначення загроз. На основі визначених переваг та недоліків існуючих методів запропоновано власний метод оцінювання ефективності рішень, який дозволяє підвищити відсоток прийнятих правильних рішень та оптимізувати ефективність системи захисту інформації в цілому.

Ключові слова: *системи захисту інформації, багатокритеріальна оптимізація, метод аналізу ієрархій, метод Парето.*

VERA YURIIVNA TITOVA, VIKTORIIA SERHIIVNA ORLENKO, ILLIA MYKOLAIOVYCH SHEVCHUK,
VLADYSLAV SERHIIOVYCH DATSENKO
Khmelnytskyi National University

EVALUATION OF DECISIONS EFFICIENCY IN INFORMATION SECURITY SYSTEMS

The functioning of most information security systems is reduced to the recognition of many active processes, their classification in order to identify malicious and dangerous processes and make decisions to respond to them. The decision-making process is based on taking into account a large number of conflicting requirements and evaluating decision options according to many criteria. The inconsistency of the characteristics of the processes, the ambiguity of the evaluation of the process, the incompleteness of the information obtained greatly complicate the final decision and significantly affect its quality.

To increase the efficiency of the final decision, it is necessary to develop a method of multi-objective optimization of decisions, which is why this work was devoted. To evaluate the efficiency of decisions in information security systems, the method was proposed that includes the advantages of the analytic hierarchy process and the Pareto efficiency. It is based on three matrices. Two of these matrices contain normalized values of threat characteristics, one - a set of decisions that need to be optimized, ranked on the analytic hierarchy process scale of preferences. Criteria for optimization are also calculated using pairwise comparisons of analytic hierarchy process preference scale values.

The proposed method provides increasing the percentage of identified correct decisions and has the following advantages: the result is always a single and effective decision; the possibility of compensation of values of partial criteria is eliminated. The method was implemented and tested in the subsystem for evaluating the decision efficiency of intrusion detection system based on in-depth learning networks and was used as the tools of multi-objective optimization of decisions for computer systems protection system.

Keywords: *information security system, multi-objective optimization, analytic hierarchy process, Pareto efficiency.*

Вступ. Забезпечення захисту інформації в комп'ютерних системах є однією з ключових проблем сьогодення. При цьому треба враховувати, що функціонування більшості систем захисту інформації, по факту, зводиться до розпізнавання множини активних в комп'ютері процесів, їх класифікації з метою визначення шкідливих та небезпечних процесів та прийняття рішень щодо їх блокування або ігнорування. Причому процес прийняття рішень ґрунтується на врахуванні великої кількості суперечливих вимог і оцінюванні варіантів рішень за багатьма критеріями. Суперечливість характеристик процесів, неоднозначність оцінювання процесу, неповнота отриманої інформації значною мірою ускладнюють прийняття остаточного рішення і суттєво впливають на його якість. Для підвищення ефективності остаточного рішення необхідно ввести в структуру систем захисту інформації модуль, який забезпечить можливість вибору кращої альтернативи за допомогою методу оцінювання ефективності рішень, тобто буде реалізовувати багатокритеріальну оптимізацію рішень. Розроблення методу зазначеної багатокритеріальної оптимізації рішень і є метою даної роботи.

Характеристика предметної області. На сьогоднішній день методи вирішення задач багатокритеріальної оптимізації розділяють на два класи [1], [2]: методи, що дозволяють виділити деяку множину прийнятних варіантів, та методи пошуку єдиного ефективного рішення.

До методів першого класу, наприклад, належить метод Парето. Але подібні методи не можуть бути використані в системах захисту інформації, оскільки головною метою захисту пошук єдиного ефективного рішення, яке б дозволило максимізувати захищеність та мінімізувати загрози інформації.

До методів другого класу, наприклад, відносяться методи з використанням узагальнюючого критерію (адитивний, мультиплікативний, максимінний) [1] та аналітична ієрархічна процедура (Analytic Hierarchy Process) Сааті або метод попарних порівнянь [2].

Перевагою перших методів є те, що завжди вдається визначити єдиний оптимальний варіант рішення. До недоліків відносять суб'єктивізм у визначенні вагових коефіцієнтів критеріїв та компенсацію значень часткових критеріїв [1], [3]. Останній недолік може призвести до того, що рішення, обране за найкращим сумарним результатом, має не найкращі результати за критеріями з найбільшими ваговими коефіцієнтами, які компенсуються найкращими результатами за критеріями з меншими ваговими коефіцієнтами. Як результат, обране рішення буде не самим ефективним, а це, в свою чергу, може призвести до ігнорування небезпечного або шкідливого процесу, реалізації сценарію його загрозу та, як наслідок, порушення конфіденційності, цілісності або доступності інформації.

Вищезазначені недоліки фактично ліквідовані аналітичною ієрархічною процедурою Сааті, але ця процедура має ряд недоліків, а саме: недосконалість шкали переваг та отримання результатів типу «критерій К1 важливіший за критерій К2» [2], не завжди враховуючи наскільки саме важливіший. Сааті пропонує таку шкалу переваг:

1 – рівноцінність;

3 – помірна перевага;

5 – велика перевага;

7 – дуже велика перевага;

9 – найвища перевага.

Розглянемо ситуацію, коли критерій К1 має дуже велику перевагу над критерієм К2, критерій К2 має дуже велику перевагу над критерієм К3. Що можна сказати про перевагу критерію К1 над критерієм К3?

Логічно зробити висновки, що критерій К1 має перевагу над К3 в 49 разів (7 помножити на 7), але цей висновок не входить у рамки даної шкали. Єдиним рішенням залишається зробити висновок, що критерій К1 має найвищу перевагу над критерієм К3, і в подальшому використовувати градацію шкали «9». Проте, при оцінювання ефективності рішень в системах захисту інформації через велику кількість прямих і зворотних зв'язків між характеристиками загроз, розглянути у [4] перевага кожного критерію над іншими має дуже велике значення, тому цей метод не може бути використаний.

Тому, для оцінювання ефективності рішень в системах захисту інформації використаємо переваги двох вищезазначених методів.

Метод оцінювання ефективності рішень в системах захисту інформації. Як вже зазначалося вище, в ході свого функціонування система захисту інформації здійснює вибір рішення зі скінченої множини можливих рішень $R = \{r_j\}, j = \overline{1,q}$. Ці рішення є реакціями на діяльність одного з активних процесів p з множини усіх процесів $P = \{p_t\}, t = \overline{1,w}$. Щоб прийняти рішення r_j для процесу p, система має проаналізувати характеристики кожного процесу $A = \{a_{\text{jm}}\}, j = \overline{1,q}, m = \overline{1,n}$ для кожного критерію, обраного з відповідної множини $\{k_m\}, m = \overline{1,n}$, де n – максимальна можлива кількість критеріїв, та визначити для кожного рішення r_j його ефективність.

Причому треба враховувати, що в один момент часу можуть мати місце як один, так і кілька класів загроз, а характеристики можуть змінюватися в процесі прийняття рішення. І з їх зміною один клас загрози може перейти в інший або корелювати з ним [4]. Отже, формальний опис моделі задачі оцінювання ефективності рішень має такий вигляд:

$$E_{r_j} = M(A_p, k_p), \tag{1}$$

де E_{r_j} – ефективність рішення r_j, M – це метод, за яким ведеться пошук ефективного рішення; A_p – характеристики процесу p; k_p – множина критеріїв для оцінювання характеристик процесу p, згідно з якими оцінюється ефективність можливих рішень.

На основі наведених множин сформуємо три матриці. В першу (A) заносяться дані відношень критеріїв, в другу (B) і третю (C) значення, які відображають характеристики для кожного процесу за кожним з критеріїв.

Значення критеріїв обчислюються за допомогою методу попарних порівнянь з використанням шкали переваг Сааті. Попарно порівнюється лише один окремий критерій з усіма іншими. У результаті визначається перевага критерію k_i. Після цього дані заносяться у перший рядок матриці A (2). Всі подальші переваги обчислюються за математичними розрахунками. Таким чином, можна уникнути обмежень, що накладаються градацією шкали переваг.

$$A = \begin{bmatrix} 1 & \mathrm{kx}_1/\mathrm{kx}_2 & \dots & \mathrm{kx}_1/\mathrm{kx}_n \\ \mathrm{kx}_2/\mathrm{kx}_1 & 1 & \dots & \mathrm{kx}_2/\mathrm{kx}_n \\ \dots & \dots & \dots & \dots \\ \mathrm{kx}_n/\mathrm{kx}_1 & \mathrm{kx}_n/\mathrm{kx}_2 & \dots & 1 \end{bmatrix}, \quad (2)$$

де $\mathrm{kx}_1 \dots \mathrm{kx}_n$– відповідні критерії, n – максимальна кількість критеріїв, за якими виконується оцінювання.

Далі значення критеріїв нормуються таким чином, щоб їх сума дорівнювала одиниці, тобто визначається ваговий коефіцієнт кожного критерію. Для цього вони обчислюються за такими формулами:

$$\mathrm{kx}_j^{\sim} = \sum_{i=1}^{n} \mathrm{kx}_{\mathrm{ij}}, j = \overline{1,m}$$

$$v_i = \mathrm{kx}_i^{\sim} \Big/ \sum_{j=1}^{n} \mathrm{kx}_j^{\sim}, i = \overline{1,m}$$

де $v_1 \dots v_n$– вагові коефіцієнти відповідних критеріїв.

В матрицю B (3) заносяться характеристики процесів за кожним обраним критерієм.

$$B = \begin{bmatrix} \mathrm{ax}_{11} & \mathrm{ax}_{12} & \dots & \mathrm{ax}_{1n} \\ \mathrm{ax}_{21} & \mathrm{ax}_{22} & \dots & \mathrm{ax}_{2_n} \\ \dots & \dots & \dots & \dots \\ \mathrm{ax}_{f_1} & \mathrm{ax}_{f2} & \dots & \mathrm{ax}_{f_n} \end{bmatrix}, \quad (3)$$

де $\mathrm{ax}_{11} \dots \mathrm{ax}_{\mathrm{fn}}$– значення відповідних характеристик процесів за відповідними критеріями, f – максимальна кількість рішень, для яких виконується оцінювання.

Далі дані нормуються таким чином, щоб сума значень у кожному стовпчику дорівнювала одиниці, і матриця B перетворюється в матрицю $B^{\sim}$.

$$B^{\sim} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2_n} \\ \dots & \dots & \dots & \dots \\ a_{f_1} & a_{f2} & \dots & a_{f_n} \end{bmatrix}, \quad (4)$$

де $a_{11} \dots a_{\mathrm{fn}}$– нормовані характеристики процесів.

В матрицю C (5) також заносяться характеристики процесів за кожним обраним критерієм.

$$C = \begin{bmatrix} \mathrm{ax}_{11} & \mathrm{ax}_{12} & \dots & \mathrm{ax}_{1n} \\ \mathrm{ax}_{21} & \mathrm{ax}_{22} & \dots & \mathrm{ax}_{2_n} \\ \dots & \dots & \dots & \dots \\ \mathrm{ax}_{f_1} & \mathrm{ax}_{f2} & \dots & \mathrm{ax}_{f_n} \end{bmatrix}, \quad (5)$$

Перетворення над нею виконуються наступним чином. Якщо найкращим результатом для j-го критерію є максимальне значення наслідку рішення, то $n_{\mathrm{ij}}^o = n_{\mathrm{ij}}/n_{\max j}$, де n_{ij}^o – нормоване значення відповідного наслідку, $n_{\max j}$ – максимальне значення наслідку в j-му стовпці. Якщо для j-го критерію найкращим результатом є мінімальне значення наслідку рішення, то $n_{\mathrm{ij}}^o = n_{\mathrm{ij}}/n_{\min j}$, де $n_{\min j}$ – мінімальне значення наслідку в j-му стовпці. Матриця $C^{\sim}$ буде мати вигляд:

$$C^{\sim} = \begin{bmatrix} a^{o}_{11} & a^{o}_{12} & \dots & a^{o}_{1n} \\ a^{o}_{21} & a^{o}_{22} & \dots & a^{o}_{2n} \\ \dots & \dots & \dots & \dots \\ a^{o}_{f_1} & a^{o}_{f2} & \dots & a^{o}_{fn} \end{bmatrix}, \quad (6)$$

де $a^{o}_{11} \dots a^{o}_{fn}$ – нормовані значення відповідних наслідків.

Після формування усіх матриць для кожного рішення обчислюється його ефективність за формулою:

$$E_{r_j} = \sum_{i=1}^{n} k_i \, n_{i_j} n^{o}_{ij} \quad (7)$$

Висновки.

У статті було розглянуто задачу оцінювання ефективності рішень систем захисту інформації. Аналіз зазначеної задачі показав, що вона є задачею багатокритеріальної оптимізації і потребує для свого вирішення задіювання відповідних методів. Виявлено, що існуючі методи оцінювання ефективності рішень не задовольняють вирішенню даної задачі, а тому не можуть бути використані. Було запропоновано удосконалений метод, який базується на використанні матриці відношення критеріїв та врахуванні наслідків рішень. Запропонований метод оцінювання ефективності рішень дозволяє підвищити відсоток визначених правильних рішень та має наступні переваги:

- результатом завжди є єдине та ефективне рішення;
- усунена можливість компенсації значень часткових критеріїв.

Зазначений метод був реалізований та апробований у підсистемі оцінювання ефективності рішень системи виявлення вторгнень на базі мереж глибинного навчання та як засіб багатокритеріальної оптимізації рішень для системи захисту комп'ютерних систем.

Література

1. Штойер Р. Многокритериальная оптимизация. Теория вычислений и приложения/ Р. Штойер. – М.: Наука, 1992. – 204 с.

2. Саати Т. Принятие решений. Метод анализа иерархий/ Т. Саати. – М.: Радио и Связь, 1993. – 320 с.

3. Кини Р.Л. Принятие решений при многих критериях: предпочтения и замещения/ Р.Л. Кини, Х. Райфа. – М.: Радио и связь, 1981. – 560 с.

4. Тітова В.Ю. Класифікація моделей загроз в комп'ютерних системах/ В.Ю. Тітова, Ю.П. Кльоц, С.О. Савчук. – Вісник Хмельницького національного університету. – №2, 2020 (283). – С. 201-204.

References

1. Shtoyer R. Mnogokriterialnaya optimizatsiya. Teoriya vyichisleniy i prilozheniya/ R. Shtoyer. – M.: Nauka, 1992. – 204 s.

2. Saati T. Prinyatie resheniy. Metod analiza ierarhiy/ T. Saati. – M.: Radio i Svyaz, 1993. – 320 s.

3. Kini R.L. Prinyatie resheniy pri mnogih kriteriyah: predpochteniya i zamescheniya/ R.L. Kini, H. Rayfa. – M.: Radio i svyaz, 1981. – 560 c.

4. Titova V.Iu. Klasyfikatsiia modelei zahroz v kompiuternykh systemakh/ V.Iu. Titova, Yu.P. Klots, S.O. Savchuk. – Visnyk Khmelnytskoho natsionalnoho universytetu. – №2, 2020 (283). – S. 201-204.

Інформаційна модель захисту інформації.

Даценко В.С., Шевчук І.М.
Науковий керівник – к.т.н., доц. Тітова В.Ю.
Хмельницький національний університет

Розуміючи інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян та організацій», правомірно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та цілі, а також інші умови і дії, що порушують безпеку [1]. При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до заподіяння шкоди.

Практика показала, що для аналізу такого значного набору джерел, об'єктів і дій доцільно використовувати методи моделювання. При цьому слід враховувати, що модель не копіює оригінал, а є простішою. При цьому, модель повинна бути досить загальною, щоб описувати реальні дії з урахуванням їх складності [2].

Можна запропонувати компоненти моделі захисту інформації на першому (інформаційному) рівні декомпозиції. На нашу думку, такими компонентами інформаційної моделі можуть бути:

- об'єкти загроз;
- загрози;
- джерела загроз;
- цілі загроз з боку зловмисників;
- джерела інформації;
- способи неправомірного оволодіння інформацією (способи доступу);
- напрямки захисту інформації;
- способи захисту інформації;
- засоби захисту інформації.

Об'єктами загроз інформаційної безпеки виступають відомості про склад, стан і діяльність об'єкта захисту (персоналу, матеріальних і фінансових цінностей, інформаційних ресурсів), тощо.

Загрози інформації виражаються в порушенні її доступності, цілісності і конфіденційності.

Джерелами загроз виступають конкуренти, злочинці, корупціонери, адміністративно-управлінські органи, тощо.

Джерела загроз переслідують при цьому наступні цілі: ознайомлення з відомостями, їх модифікація в корисливих цілях і знищення для нанесення прямих матеріальних збитків.

Неправомірне заволодіння відомостями можливо за рахунок їх розголошення джерелами інформації, за рахунок витоку через технічні засоби і за рахунок несанкціонованого доступу до відомостей.

Джерелами інформації є люди, документи, публікації, технічні носії інформації, технічні засоби забезпечення виробничої та трудової діяльності, продукція і відходи виробництва.

Основними напрямками захисту інформації є правовий, організаційний та інженерно-технічний захист інформації, як показники комплексного підходу до забезпечення інформаційної безпеки.

Засобами захисту інформації є фізичні засоби, апаратні засоби, програмні засоби та криптографічні методи. Останні можуть бути реалізовані як апаратно, програмно, так і змішано-програмно-апаратними засобами. В якості засобів захисту виступають всілякі заходи, шляхи, способи і дії, що забезпечують попередження протиправних дій, їх запобігання, припинення та протидія несанкціонованому доступу.

В узагальненому вигляді розглянуті компоненти у вигляді інформаційної моделі безпеки інформації наведені на наступній схемі (рис. 1).

Співставлення об'єкта (фірма, організація) і суб'єкта (конкурент, зловмисник) в інформаційному процесі з протилежними інтересами можна розглядати з позиції активності, яка призводить до оволодіння інформацією. У цьому випадку можливі такі ситуації:

- власник (джерело) не приймає ніяких заходів до збереження інформації, що дозволяє зловмисникові легко отримати цікаві для нього відомості;
- джерело інформації суворо дотримується заходів інформаційної безпеки, тоді зловмисникові доводиться докладати значних зусиль до здійснення доступу до потрібних йому відомостей, використовуючи для цього всю сукупність способів несанкціонованого проникнення;
- проміжна ситуація - це витік інформації по технічним каналам, при якій джерело ще не знає про це (інакше він прийняв би заходи захисту), а зловмисник легко, без особливих зусиль може їх використовувати в своїх інтересах.

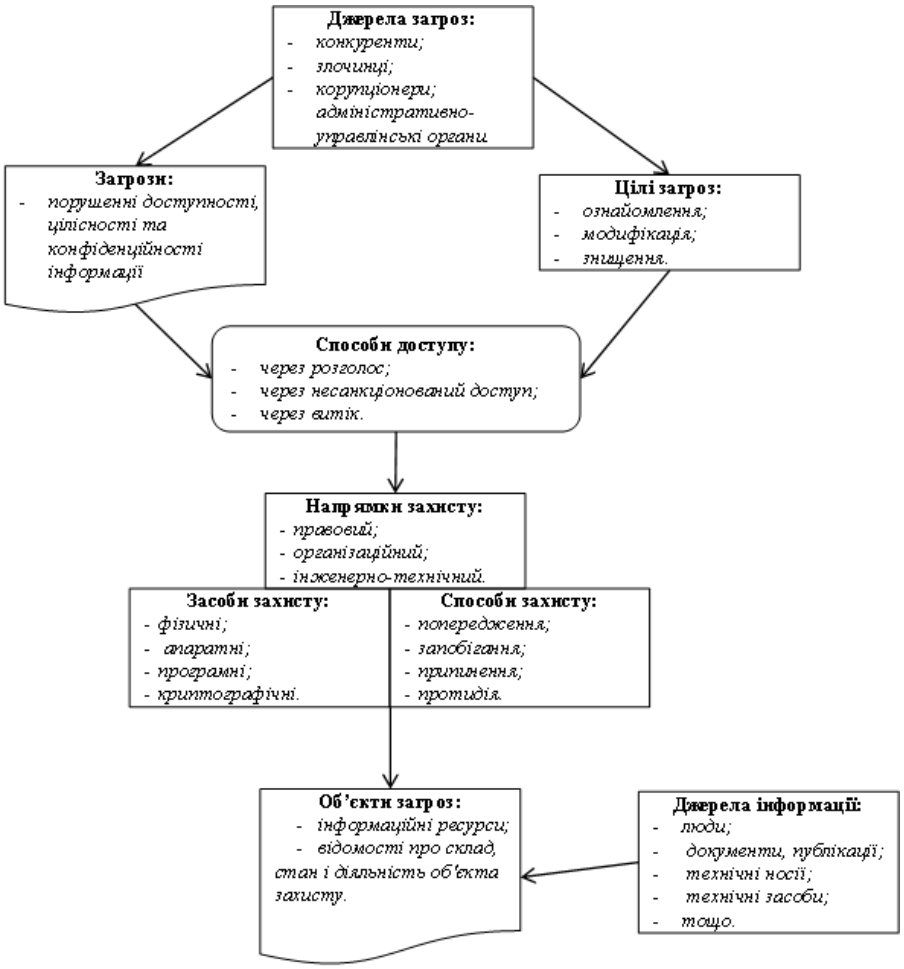


Рис. 1. – Інформаційна модель захисту інформації.

Отже, на основі вищевикладеного можна зробити наступні висновки:

1. Інформація - це ресурс. Втрата інформації приносить моральні чи матеріальні збитки.

2. Умови, що сприяють неправомірному оволодінню інформацією, зводяться до її розголошенню, витоку і несанкціонованого доступу до її джерел.

3. У сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки системою захисту інформації, яка буде протидіяти загрозам через блокування неправомірних способів доступу та охоплювати усю множину існуючих способів за засобів захисту інформації

Перелік посилань

1. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту/ О. В. Черевко. // Ефективна економіка. – 2014. – №5. – Режим доступу: http://nbuv.gov.ua/UJRN/efek_2014_5_103

2. Інформаційна безпека. Навчальний посібник. Ч.1/С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

3. Основні поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 1999. – 30 с.

ДОДАТОК В

(Обовязковий)

Презентація

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Шевчук Ілля Михайлович

Оптимізація системи захисту комп'ютерних систем з використанням методів багатокритеріальної оптимізації

Науковий керівник
к.т.н., доцент Тітова В.Ю.

кафедра кібербезпеки та комп'ютерних систем і мереж

Тема: «Оптимізація системи захисту комп’ютерних систем з використанням методів багатокритеріальної оптимізації».

Метою магістерської роботи максимізація захищеності комп'ютерних систем шляхом вдосконалення захисту інформації в комп'ютерних системах, зокрема від вірусів-шифрувальників, за рахунок введення в структуру існуючих систем захисту підсистеми моніторингу на основі методів багатокритеріальної оптимізації.

Об’єкт дослідження: є системи захисту інформації, зв'язки та відношення між типовими процесами захисту інформації у комп'ютерних системах, загрози комп'ютерній інформації, у тому числі віруси-шифрувальники.

Предмет дослідження: є методи та моделі захисту інформації в комп'ютерних системах, які базуються на сучасних методах багатокритеріальної оптимізації, таких як аналіз ієрархій, ELECTRE, Парето, тощо.

Задачі досліджень у роботі формулюються наступним чином:

1. Розглянути основні поняття систем захисту інформації, проаналізувати основні нормативно правові-акти які регулюють їх. Дослідити основні системи захисту інформації в комп’ютерних системах та проаналізувати основні загрози зокрема віруси-шифрувальники.

2.Сформулювати основні вимоги до концептуальної моделі захисту інформації. Провести класифікацію типових процесів захисту інформації в комп'ютерних системах, яка описує характер їх реалізації через математичну модель та провести формалізовану класифікацію загроз інформації в комп'ютерних системах.

3. Розробити алгоритм захисту інформації за допомогою методів багатокритеріальної оптимізації, а саме Сааті та Парето.

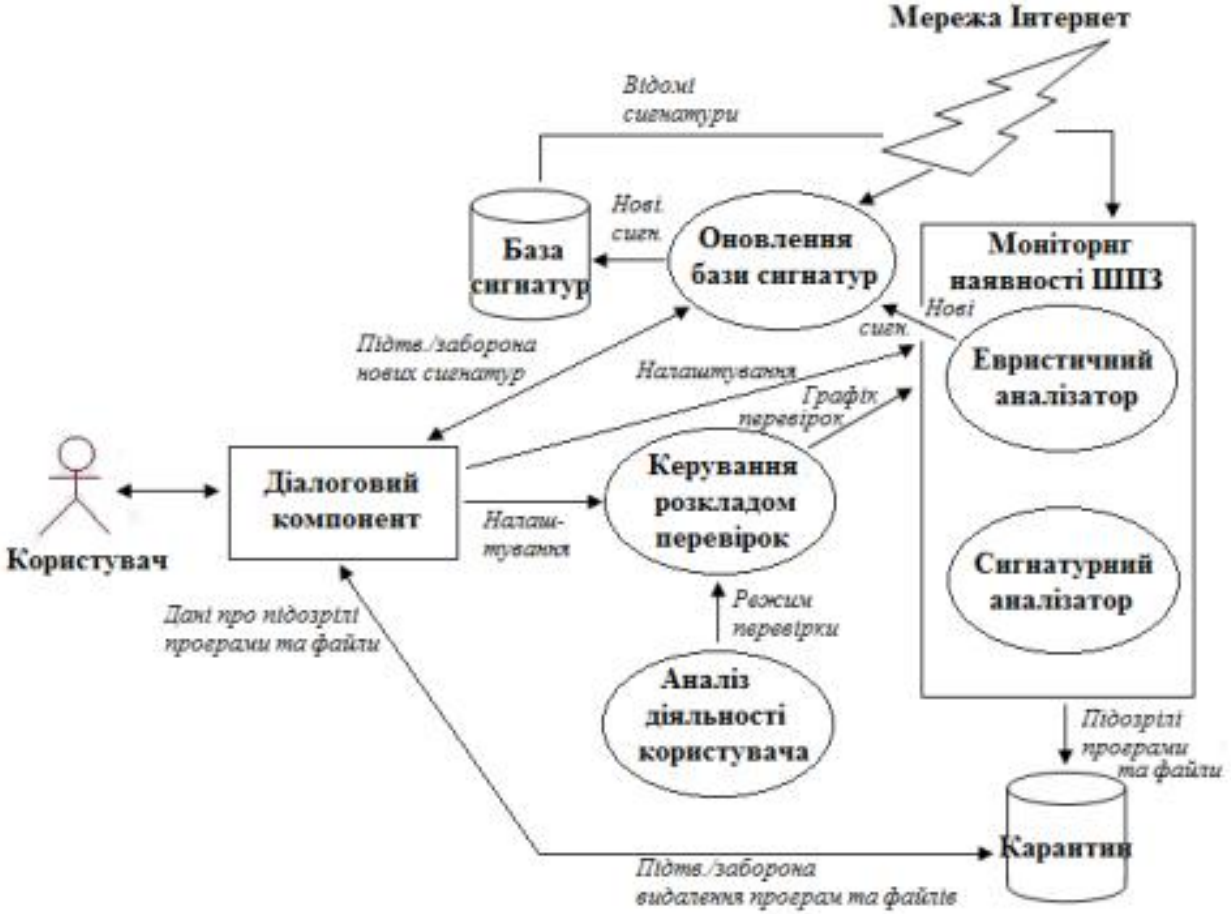
Наукова новизна роботи полягає в наступному:

1. Розроблено класифікацію типових процесів захисту інформації та класифікацію загроз у комп'ютерних системах, які відрізняються від вже існуючих більш повною структурою та систематизованим набором вимог, що відповідає основним положенням нормативно-правових документів, що регламентують інформаційну безпеку.
2. Вдосконалено концептуальну модель існуючих на сьогоднішній день систем захисту інформації, за рахунок введення в неї блоку моніторингу, який базується на багатокритеріальній оптимізації.
3. Запропоновано метод оптимізації системи захисту за рахунок багатокритеріальної оптимізації, що дозволяє прискорити обробку динамічних даних (загроз, їх характеристик, тощо) та підвищити ефективність захисту даних у комп'ютерних системах в цілому.

Практична цінність полягає в тому, що: розроблений метод удосконалює системи захисту інформації в КС та підвищує цілісність, конфіденційність та доступність інформації в цілому.

Публікації. По темі кваліфікаційної роботи опубліковано 1 стаття у фаховому журналі «Вісник ХНУ», №5, 2020. 1 стаття у нефаховому журналі (збірник НПК МНІС ІП-2020);

Концептуальна модель захисту інформації



Класифікація типових процесів захисту інформації в комп'ютерних системах через математичну модель.

C=<F,I,Z,G,N>

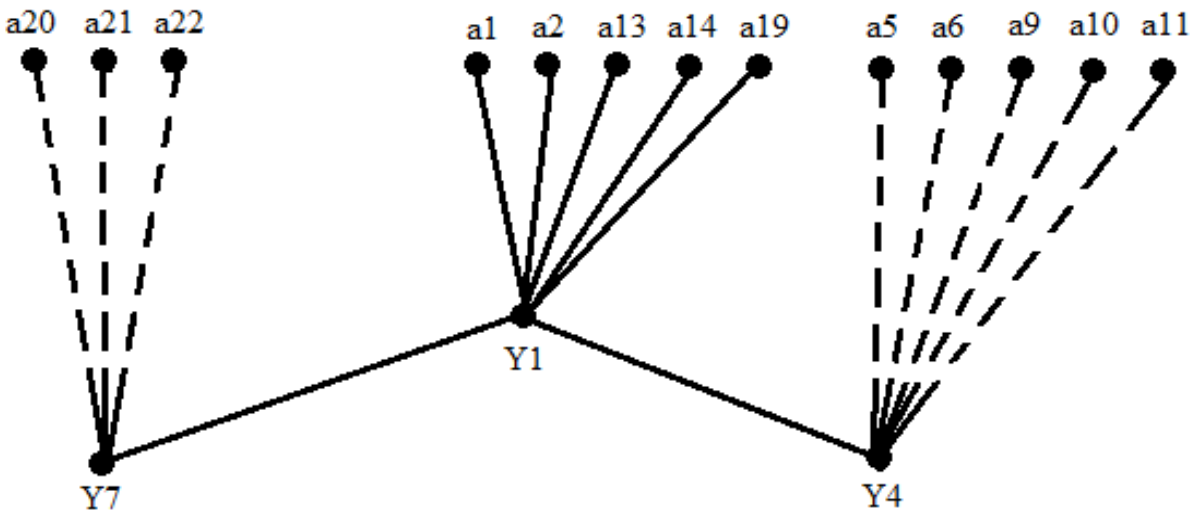
Перша складова, це правило:

Y_i= <Y_1, Y_2,… Y_n>,

Взаємозв'язок характеристик загроз з класами загроз.

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}
Y_1	+	+														+	+	+	
Y_2			+	+	+	+	+			+								+	
Y_3			+	+			+	+									+		
Y_4						+		+	+	+							+		
Y_5	+	+	+					+	+		+	+	+			+			+
Y_6				+	+	+	+			+	+	+	+	+	+		+	+	+
Y_7																+	+	+	+

Залежності між класами загроз та їх характеристиками для класу Y1 має вигляд:



Математична модель захисту інформації в комп'ютерних системах.

$$R_i = \begin{cases} a_1 \vee a_2 \vee a_{13} \vee a_{14} \vee a_{19} \\ a_3 \vee a_4 \vee a_5 \vee a_6 \vee a_7 \vee a_{15} \vee a_{16} \vee a_{22} \\ a_8 \vee a_9 \vee a_{17} \vee a_{18} \vee a_{22} \\ a_5 \vee a_6 \vee a_9 \vee a_{10} \vee a_{11} \vee a_{19} \\ a_4 \vee a_{12} \vee a_{13} \vee a_{20} \\ a_3 \vee a_5 \vee a_7 \vee a_9 \vee a_{11} \vee a_{12} \vee a_{13} \vee a_{14} \vee a_{15} \vee a_{16} \vee a_{17} \vee a_{18} \vee a_{21} \vee a_{22} \\ a_2 \vee a_{19} \vee a_{20} \vee a_{21} \vee a_{22} \end{cases}$$

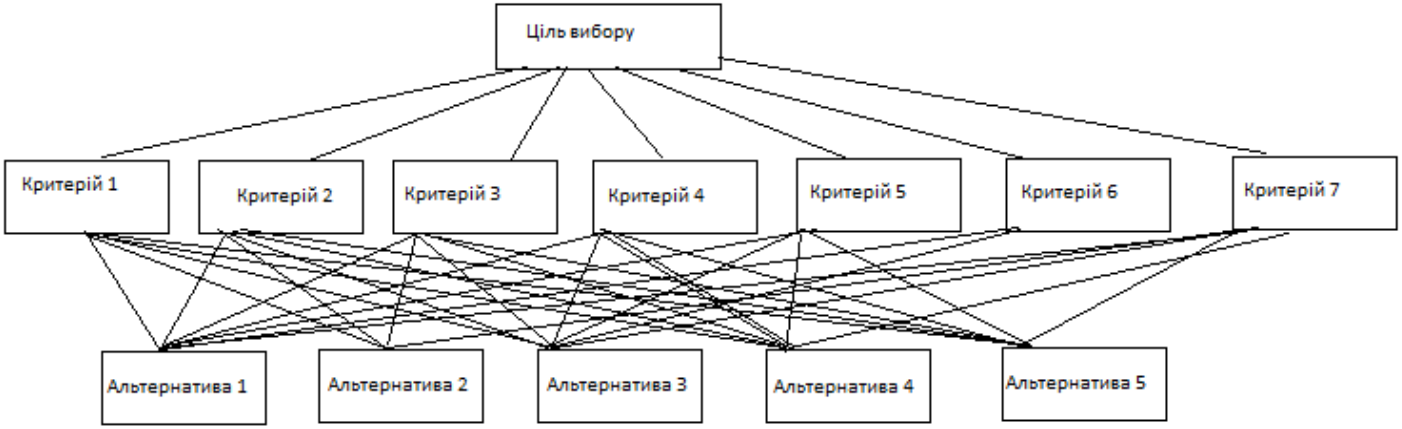
Узагальнена математична модель віруса-шифрувальника представлена наступним чином:

$$Y_v = Y_2 \cup Y_4 \cup Y_5 \cup Y_6 \cup Y_7$$

Шкала попарних порівнянь Т.Сааті

Відносна важливість, визначена в балах	Визначення важливості	Пояснення
1	Однакова важливість	Альтернативі рівнозначні за даним критерієм
3	Одна альтернатива незначно важливіша за іншу	Одна з альтернатив незначно домінує над іншою за критерієм
5	Одна альтернатива суттєво переважає над іншою	Можна говорити про безумовну перевагу однієї альтернативи над іншої за критерієм
7	Одна альтернатива значно переважає над іншою	Альтернатива настільки переважає над іншою, що це є практично значимим
9	Альтернатива абсолютно переважає над іншою	Очевидність даної переваги підтверджується більшістю
2,4,6,8	Проміжні оцінки між судженнями	Компромісні рішення щодо порівняння альтернатив
Обернені значення оцінок	Якщо при порівнянні альтернатив визначено, що A_1 домінує над A_2 з величиною 7, то A_2 буде домінувати над A_1 з величиною 1/7	

Ієрархічне представлення задачі



Здійснення вибору рішень зі скінченої множини можливих рішень

$$R = \{r_j\}, j = \overline{1,q}$$

Формальний опис моделі задачі оцінювання ефективності рішень має такий вигляд:

$$E_{r_j} = M(A_p, k_p),$$

Шкала переваг Сааті

Визначення важливості в балах	Визначення важливості
1	Рівноцінність
3	Помірна перевага
5	Велика перевага
7	Дуже велика перевага
9	Найвища перевага
2,4,6,8	Проміжні оцінки

Обчислення значення критеріїв оцінки системи

$$A = \begin{bmatrix} 1 & kx_1 / kx_2 & \dots & kx_1 / kx_n \\ kx_2 / kx_1 & 1 & \dots & kx_2 / kx_n \\ \dots & \dots & \dots & \dots \\ kx_n / kx_1 & kx_n / kx_2 & \dots & 1 \end{bmatrix}$$

Знаходження характеристик за кожним вибраним критерієм

$$B = \begin{bmatrix} ax_{11} & ax_{12} & \dots & ax_{1n} \\ ax_{21} & ax_{22} & \dots & ax_{2n} \\ \dots & \dots & \dots & \dots \\ ax_{f1} & ax_{f2} & \dots & ax_{fn} \end{bmatrix},$$

Перетворення матриці *B* в матрицю $B^{\sim}$

$$B^{\sim} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{f1} & a_{f2} & \dots & a_{fn} \end{bmatrix},$$

Побудова матриці C

$$C = \begin{bmatrix} ax_{11} & ax_{12} & \dots & ax_{1n} \\ ax_{21} & ax_{22} & \dots & ax_{2n} \\ \dots & \dots & \dots & \dots \\ ax_{f1} & ax_{f2} & \dots & ax_{fn} \end{bmatrix},$$

Матриця $C^{\sim}$ буде мати вигляд:

$$C^{\sim} = \begin{bmatrix} a^{o}_{11} & a^{o}_{12} & \dots & a^{o}_{1n} \\ a^{o}_{21} & a^{o}_{22} & \dots & a^{o}_{2n} \\ \dots & \dots & \dots & \dots \\ a^{o}_{f1} & a^{o}_{f2} & \dots & a^{o}_{fn} \end{bmatrix},$$

Обчислення ефективності рішень

$$E_{r_j} = \sum_{i=1}^{n} k_i * n_{ij} * n_{ij}^{o}$$

Оцінка ефективності методу за наступними показниками

P_q – показник правильності, P_t – показник вчасності, P_d – показник повноти бази даних.

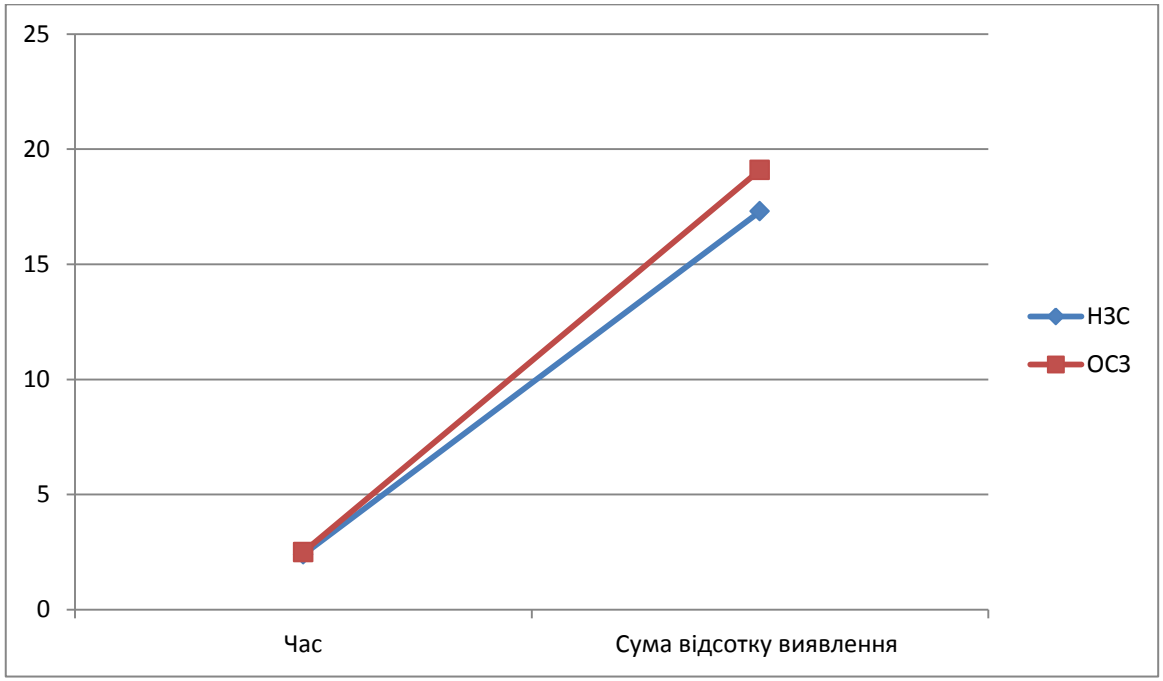
Результати тестування множини процесів на виявлення загроз

	НСЗ	ОСЗ
Відсоток прав. рішень	78%	96%
Повнота бази даних по відношенню до відомих на сьогодні баз	95%	95%
Середній затрачений час, сек.	2,4	2,5

Обчислення ефективності роботи

$$E = P_t * (P_q + P_d)$$

Результат оцінки роботи



Висновки

У магістерській роботі було вирішено завдання оптимізації системи захисту комп’ютерних систем з використанням методів багатокритеріальної оптимізації.

Основні результати магістерської роботи:

1. У першому розділі розглянуто поняття систем захисту інформації, проаналізовано сучасні нормативно-правові акти, які регулюють діяльність таких систем. Досліджено особливості використання найбільш відомих методів багатокритеріальної оптимізації у питаннях захисту інформації. Проаналізовано різні типи комп'ютерних загроз, зокрема віруси-шифрувальники. Сформульовані основні задачі магістерської роботи. Основна увага приділяється аналізу недоліків сучасних систем захисту інформації від вірусів-шифрувальників та виявленню супутніх проблем, вирішення яких можливо за рахунок використання багатокритеріальної оптимізації..

2. Сформульовано основні вимоги до концептуальної моделі захисту комп'ютерних систем. Проведено класифікацію типових процесів захисту інформації в комп'ютерних системах, яка описує характер їх реалізації через математичну модель. Проведено формалізовану класифікацію загроз інформації в комп'ютерних системах, формалізована модель представлена у вигляді двох складових: правила, прописаного за допомогою теорії множин, та графів залежностей між класами загроз та їх характеристиками. На основі проведеної класифікації загроз та їх залежностей було побудовано математичну модель захисту інформації в комп'ютерних системах.

3. Розглянуто метод багатокритеріальної оптимізації а саме метод Сааті. Зазначений метод, базується на використанні матриці залежності критеріїв та врахуванні наслідків прийнятих рішень. Запропонований метод оцінювання ефективності рішень дозволяє підвищити відсоток визначених правильних рішень та має наступні переваги:

- результатом завжди є єдине та ефективне рішення;
- усунена можливість компенсації значень часткових критеріїв

4. Проведено оцінювання ефективності розробленого у роботі методі та визначено рівень зниження ризику підчас впровадження запропоновано методу у системи захисту інформації в КС.

5. Зазначений метод був реалізований та апробований у підсистемі оцінювання ефективності рішень системи виявлення вторгнень на базі мереж глибинного навчання та як засіб багатокритеріальної оптимізації рішень для системи захисту комп’ютерних систем.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Магістр Шевчук Ілля Михайлович

Тема Метод реалізації систем ідентифікації вторгнень на базі нейромереж глибокого навчання

Спеціальність 123 – Комп'ютерна інженерія

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень 11 ; кількість сторінок записки 90

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі удосконалено модель захисту комп'ютерних систем .

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведено огляд основні принципи захисту інформації в комп'ютерних системах. У другому розділі розглянуто та проаналізовано моделі захисту інформації в комп'ютерних системах. В третьому розділі розроблено метод багатокритеріальної оптимизації захисту інформації в комп'ютерних системах. Четвертий розділ присвячено апробації методу та алгоритмів його реалізації моделюванням.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну наукову і практичну цінність. Наукова цінність полягає у розроблені класифікації типових процесів захисту інформації та класифікацію загроз у комп'ютерних системах, які відрізняються від вже існуючих більш повною структурою та систематизованим набором вимог, що відповідає основним положенням нормативно-правових документів, що регламентують інформаційну безпеку. Практична цінність результатів полягає у оптимізації системи захисту за рахунок багатокритеріальної оптимізації, що дозволяє прискорити обробку динамічних даних (загроз, їх характеристик, тощо) та підвищити ефективність захисту даних у комп'ютерних системах в цілому.

5. Негативні сторони роботи В роботі неповністю наведено програмну реалізацію розробленого методу, не до кінця розкриті результати його апробації

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження немає

9. Оцінка кваліфікаційної роботи враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «добре»/ В (4,25).

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Гурман Іван Васильович
кандидат технічних наук, доцент,
доцент кафедри інженерії програмного забезпечення

«9» 12 2020. Гурман І.В. (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.

UNICHECK

User name:
Кафедра кибербезпеки

Check ID:
1005445870

Check date:
13.12.2020 19:37:05 EET

Check type:
Doc vs Internet

Report date:
13.12.2020 19:37:45 EET

User ID:
100005590

File name: **Шевчук_магістерська_перевірка**

Page count: **76** Word count: **14969** Character count: **117908** File size: **381.75 KB** File ID: **1005736328**

3.7% Matches

Highest match: **1.17%** with Internet source (**http://elartu.tntu.edu.ua/bitstream/lib/29278/1/%21%21_Lek_print_zahust_123.pdf**)

3.7% Internet sources **318** ..... Page 78

No Library search was conducted

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters **45**

Mon Dec 07 08:58:05 EET 2020, Муляра І.В, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 2.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 7%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 82592 Название: Оптимізація системи захисту комп'ютерних систем з використанням методів багатокритеріальної оптимізації Добавлено в БД: 2020-12-07 Авторы: Шевчук І.М. Руководители: Тітова В.Ю. Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	97396	787	4949 (5%)	50 (6%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Оптимізація системи захисту комп'ютерних систем з використанням методів багатокритеріальної оптимізації

Автор: Шевчук Ілля Михайлович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: Програмування та захист комп'ютерних систем і мереж

Науковий керівник: Тітова ВираЮріївна, 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 (далі – зазначаються підстави віднесення запозичень до правомірних). 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 (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). 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.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні і являють собою загальновживані терміни та загальновідому інформацію, або мають належним чином оформленні посилання;
3) також плагіатом не можна рахувати оформлені за вимогами літературні джерела.
4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 3,7%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження.

Керівник роботи В.Ю. Тітова

Завідувач кафедри КСКСМ, гарант ОП Ю.П. Кльоц

Дата: 07.12.2020