Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій .
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського .
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський) .

Дослідження методів моделювання комплексних систем захисту інформації
(тема)

Виконала:
студентка 2 курсу, групи АМСЗІм-22-2
.
Клочкова Д.Ю. .
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека .
(код і повна назва спеціальності)
Тип програми: освітньо-професійна .
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації .
. (повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського .
Пшеничних С.В. .
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В. .
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій .
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського .
(повна назва)
Рівень вищої освіти другий (магістерський) .
Спеціальність 125 Кібербезпека .
(код і повна назва)
Тип програми освітньо-професійна .
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації .
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Клочковій Діані Юріївні .
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження методів моделювання комплексних систем захисту інформації. Затверджена наказом по університету від «03» листопада 2023р. № 1291Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 26.01.2024 р. .
3. Вихідні дані до роботи: класифікація моделей систем захисту інформації; класифікації вразливостей OWASP, CWE; нормативні документи в сфері технічного захисту інформації
4. Перелік питань, що потрібно опрацювати в роботі:
1) Аналіз моделей комплексних систем захисту інформації.
2) Аналіз загроз безпеки для сучасних інформаційних систем.
3) Аналіз методів та засобів захисту від загроз безпеки для інформаційних систем.
4) Аналіз типової інформаційної системи на прикладі корпоративної комп’ютерної мережі.
5) Розробка математичної моделі оптимального вибору засобів захисту для інформаційної системи.

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації ..

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Пшеничних Сергій Васильович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	03.11.2023	Виконано
2	Збір матеріалів для дослідження	25.11.2023	Виконано
3	Розробка 1 розділу	06.12.2023	Виконано
4	Розробка 2 розділу	19.12.2023	Виконано
5	Розробка 3 розділу	02.01.2024	Виконано
6	Розробка 4 розділу	10.01.2024	Виконано
7	Оформлення кваліфікаційної роботи	22.01.2024	Виконано

Дата видачі завдання 3 листопада 2023 року

Студентка _____ Клочкова Д.Ю.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Пшеничних С.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 104 с., 8 рис., 28 табл., 58 джерел.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА СИСТЕМА, ЗАГРОЗА, ВРАЗЛИВІСТЬ, КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ, МАТЕМАТИЧНА МОДЕЛЬ.

Об’єкт дослідження – процес моделювання комплексних систем захисту інформації.

Предмет дослідження – методи моделювання комплексних систем захисту інформації.

Мета роботи – аналіз методів моделювання комплексних систем захисту інформації, їх функцій та особливостей застосування.

Методи досліджень – спостереження, аналіз та порівняння.

У роботі досліджуються формальні підходи для оцінки комплексної системи захисту інформації, а також вибір засобів забезпечення захисту інформації для довільної інформаційної системи.

Детально описані моделі систем захисту інформації, розглянуто існуючі моделі оптимізації складу комплексу засобів захисту в комплексних системах захисту інформації.

Також, розглянуто більшість сучасних засобів забезпечення захисту інформації, включаючи конкретні продукти від різних виробників. Вибір оптимальних засобів, серед розглянутих продуктів, здійснено, в тому числи, за допомогою методів згортки.

Проведено аналіз вимог і здійснено порівняння методів моделювання комплексних систем захисту інформації, їх властивостей та застосування.

В роботі був запропонований новий показник ефективності та критерій оптимізації вибору засобів захисту по кожному каналу витоку інформації. Також був запропонований показник ефективності, критерій та алгоритм оптимізації складу комплексу засобів захисту інформації для інформаційної системи в цілому.

Результати роботи доцільно використовувати при визначенні оптимального складу комплексу засобів захисту при проектуванні комплексної системи захисту.

ABSTRACT

The report contains: 104 p., 8 fig., 28 tables., 58 sources.

COMPREHENSIVE SYSTEM OF INFORMATION SECURITY, INFORMATION SYSTEM, THEART, VULNERABILITY, SET OF SECURITY SUITE, MATHEMETICAL MODEL.

The object of research: the process of modeling comprehensive information security systems.

The subject of research: the methods of modeling comprehensive information security systems.

The purpose of the work: to analyze the methods of modeling comprehensive information security systems, their functions and application features.

Research methods - observation, analysis and comparison.

The work examines formal approaches for evaluating of comprehensive information security systems, as well as an optimal choice of information security tools for an arbitrary information system.

The stages of building an comprehensive information security system are described in details, existing models of optimization the set of a security information tools are considered.

Also, most modern security information tools (including specific products from different manufacturers) are considered. The optimal selection of information security tools is carried out using convolution methods.

An analysis of the requirements was carried out and a comparison of the modeling methods of complex information protection systems, their properties and applications was carried out.

The paper proposed a new efficiency indicator and optimization criterion for the selection of protection means for each channel of information leakage. An efficiency indicator, a criterion and an algorithm for optimizing the composition of the complex of information protection tools for the information system as a whole were also proposed.

The results of the work should be used when determining the optimal composition of the complex of protection means when designing a complex protection system.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

АС – автоматизована система
АСОД – автоматизованої системи обробки даних
ЗЗЗІ – засіб забезпечення захисту інформації
ІзОД – інформації з обмеженим доступом
ІС – інформаційна система
КЗЗ – комплекс засобів захисту
КС – комп’ютерна система
КСЗІ – комплексна система захисту інформації
НСД – несанкціонований доступ
ОІ – об’єкт інформатизації
ОС – операційна система
ПЗ – програмне забезпечення
СФП – стандартний функціональний профіль
ARP – Address Resolution Protocol
API – Application Programming Interface
CWE – Common Weakness Enumeration
DDoS – Distributed Denial-of-Service
DLP – Data Leak Prevention
DNS – Domain Name System
EDR –Endpoint Detection and Response
FTP – File Transfer Protocol
IDS/IPS – Intrusion Detection System /Intrusion Prevention System
MFA – Multi-Factor Authentication
OWASP – Open Web Application Security Project
SDN – Software-defined Networking
SIEM – Security Information and Event Management
SQL – Structured Query Language
TCP – Transmission Control Protocol
UDP – User Datagram Protocol
VPN – Virtual Private Network

ВСТУП

Розробка КСЗІ для АС є складною, комплексною задачею, що залежить від багатьох факторів, таких як ресурси системи, бажаний рівень конфіденційності та цілісності інформації, що захищається, бюджет на впровадження ЗЗЗІ тощо. У сучасному світі, загрози інформаційної безпеки постійно зростають, також зростає кількість та складність технічних та програмних ЗЗЗІ, причому кожен виробник маючи на меті охопити якомога більше ринку, пропонує захист відразу від декількох загроз. Очевидно, що ці продукти мають різну ціну, а підприємства зазвичай мають обмежений бюджет для захисту інформації. Відповідно вибір таких засобів для КСЗІ стає все більш складним.

Звідси виникають задачі вибору оптимальних засобів захисту інформації для ІС та оцінки якості розробленої КСЗІ. Ці задачі в першу чергу потребують формалізації, розробки математичних моделей та чітких критеріїв оцінки. Стандарти захисту інформації, такі як НД ТЗІ [47–49] , пропонують формальний підхід до проблеми формалізації вибору засобів захисту ІС на основі таких понять, як профіль захисту, функціональні послуги безпеки та гарантії, враховуючи вид інформаційної системи та бажаний рівень захисту інформації. Проте, рівень захищеності у них, як і у більшості документів з вимогами до захисту інформації визначається просто відсутністю чи наявністю деяких механізмів та не враховує бюджет на розробку КСЗІ та різницю у рівні захищеності, у результаті впровадження конкретних програмних чи апаратних засобів захисту.

Власне, питанням вибору оптимального КЗЗ для конкретної ІС, моделюванню КСЗІ та розробці більш детальних критеріїв захищеності КСЗІ присвячені дослідження, результати яких представлені в даній роботі.

Метою роботи є дослідження методів моделювання комплексних систем захисту інформації та розробка математичної моделі оптимального вибору засобів захисту для інформаційної системи.

У першому розділі досліджуються моделі комплексних систем захисту інформації, було проаналізовано моделі систем захисту інформації та моделі оптимізації складу комплексу засобів захисту. Проведено порівняльний аналіз моделей систем захисту інформації та приведено математичну постановку задачі «гри» сторони захисту та сторони зловмисника.

Далі, у другому розділі, проводиться дослідження загроз безпеки для інформаційних систем, розглядаються види та схеми атак, також проведений огляд ризиків безпеки. Також приведені рекомендації щодо попередження та зменшення впливу кібератак. Як результат, визначається перелік найбільш шкідливих загроз, що можливі в комп’ютерній системі.

В наступному, третьому розділі, проведено аналіз засобів захисту від загроз безпеки для інформаційних систем. На прикладі узагальненої схеми типової інформаційної системи та ресурсів інформаційної системи, приведено модель загроз та вразливостей типової інформаційної системи. Також виходячи з вищезазначеного, проведено аналіз методів та засобів захисту інформації.

У підсумок, здійснена розробка математичної моделі оптимального вибору засобів захисту для інформаційної системи. Для досягнення цього необхідно провести аналіз наявних підходів щодо вибору засобів захисту від загроз безпеки. Далі потрібно розробити математичну модель оптимального вибору засобів захисту інформації при проектуванні комплексної системи захисту на об'єкті інформатизації, та, використовуючи методи багатокритеріальної оптимізації, визначити оптимальний комплекс засобів захисту інформаційних систем.

Окремі результати досліджень доповідалися в рамках дев’ятої Міжнародної науково-технічної конференції «Інформаційно-комунікаційні технології та кібербезпека» та опубліковані за результатами його проведення [11, 49, 50].

1 АНАЛІЗ МОДЕЛЕЙ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

1. Вихідні дані для побудови моделі комплексної системи захисту інформації

Згідно НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» комплексна система захисту інформації (КСЗІ) – це сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в автоматизованій системі (АС).

Розробка комплексної системи захисту інформації починається з аналізу загроз безпеці інформації, аналізу інформаційної системи, що захищається та аналізу конфіденційності та важливості інформації в інформаційній системі (ІС). Перш за все проводиться аналіз конфіденційності та важливості інформації, яка повинна оброблятися, зберігатися і передаватися в ІС. На основі аналізу робиться висновок про доцільність створення КСЗІ. Якщо інформація не є конфіденційною і може легко відновлюватися, то створювати КСЗІ немає необхідності. Також не має сенсу створювати КСЗІ в ІС, якщо втрата цілісності та конфіденційності інформації пов'язана з незначними втратами. В таких випадках досить використовувати стандартні засоби ІС і, можливо, страхування від втрати інформації.

Під час аналізу інформації визначаються потоки конфіденційної інформації, елементи ІС, в яких вона обробляється та зберігається. На цьому етапі також розглядаються питання розподілу доступу до інформації окремих користувачів та цілих сегментів ІС. На основі аналізу інформації визначаються вимоги до її захищеності. Вимоги встановлюються шляхом надання певного грифу конфіденційності та встановлення правил розподілу доступу.

Дуже важлива початкова інформація для побудови КСЗІ отримується в результаті аналізу ІС, що захищається. Оскільки КСЗІ є підсистемою ІС, то взаємодію системи захисту з ІС можна визначити як внутрішню, а взаємодію з зовнішнім середовищем – як зовнішню.

Аналіз загроз безпеці є однією з обов'язкових умов для побудови КСЗІ. На основі проведеного аналізу створюється модель загроз безпеці інформації в ІС, яка містить систематизовані дані про випадкові та навмисні загрози безпеці

інформації в конкретній ІС. Систематизація даних моделі передбачає наявність інформації про всі можливі загрози, їх небезпеку, часові рамки дії та ймовірність реалізації.

Часто модель загроз розглядається як композиція моделі зловмисника та моделі випадкових загроз. Моделі подаються у вигляді таблиць, графіків або на вербальному рівні. При побудові моделі зловмисника використовується два підходи.

Модель спрямована тільки на висококваліфікованого зловмисника– професіонала, оснащеного всім необхідним та маючого законний доступ на всіх рубежах захисту.

Модель враховує кваліфікацію зловмисника, його оснащеність (можливості) та офіційний статус в ІС.

Перший підхід простіше реалізується і дозволяє визначити верхню межу навмисних загроз безпеці інформації. Другий підхід відрізняється гнучкістю і дозволяє враховувати особливості ІС в повному обсязі. Градація зловмисників за їх кваліфікацією може бути різною. Наприклад, може бути виділено три класи зловмисників.

– висококваліфікований зловмисник – професіонал;

– кваліфікований зловмисник – непрофесіонал;

– некваліфікований зловмисник – непрофесіонал.

Клас зловмисника, його оснащеність та статус на об'єкті ІС визначають можливості зловмисника щодо несанкціонованого доступу (НСД) до ресурсів ІС. Загрози, пов'язані з непередбаченими діями, добре вивчені, і більша частина їх може бути формалізована. Сюди слід віднести загрози безпеці, які пов'язані з кінцевою надійністю технічних систем. Загрози, породжені стихією або людиною, формалізувати складніше. Але з іншого боку, на їх вже налагоджено великий обсяг статистичних даних. На основі цих даних можна прогнозувати прояв загроз цього класу.

Модель зловмисника та модель випадкових загроз дозволяють отримати повний спектр загроз та їх характеристик. У сполученні з вихідними даними, отриманими в результаті аналізу інформації, особливостей архітектури ІС, моделі загроз безпеці інформації дозволяють отримати вихідні дані для побудови моделі КСЗІ.

2. Моделі систем захисту інформації та завдання, що вирішуються ними

Для дослідження інформаційної безпеки інформаційних систем використовують моделі систем захисту інформації. Існують різні підходи до моделювання систем захисту інформації, що відображають різні аспекти захисту. Моделі можна згрупувати за схожістю використовуваних підходів до наступних груп:

– узагальнені моделі систем захисту;
– моделі, що побудовані з використанням теорії ймовірностей;
– моделі, що побудовані з використанням теорії випадкових процесів;
– моделі, що побудовані з використанням теорії мереж Петрі;
– моделі, що побудовані з використанням теорії автоматів;
– моделі, що побудовані з використанням теорії графів;
– моделі, що побудовані з використанням теорії нечітких множин;
– моделі, що побудовані з використанням теорії катастроф;
– моделі, що збудовані з використанням теорії ігор;
– модель, що побудовані з використанням ентропійного підходу.

Відмінності даних моделей полягають у тому, які параметри вони використовують як вхідну інформацію, які параметри системи, що моделюється, розраховуються і надходять на вихід моделі. При цьому, як вхідна інформація використовується набрана статистика на існуючих ІС або дані експертів. Моделі в основному використовуються на етапі експлуатації та супроводу ІВ для проведення моніторингу та аудиту СЗІ. Цим визначається практична придатність моделі. Деякі моделі використовуються і на етапі проектування ІС.

1.2.1 Узагальнені моделі систем захисту.

У цих моделях намагаються охопити всі чинники, що можуть впливати на систему захисту.

У роботі [1] надається перелік реальних об'єктів, що захищаються, загроз з боку технічних засобів розвідки, заходів та засобів захисту, показників ефективності функціонування, комплексів технічних засобів обробки інформації та захисту, вимог до безпеки інформації, обмежень, що визначаються особливостями побудови системи захисту, різноманіттям типових структурних компонентів обробки інформації, каналів витоку конфіденційної інформації.

Для застосування даної моделі необхідне визначення таких показників, як, імовірнісний характер функціонування інформаційної системи, дестабілізуючі фактори, що впливають на систему та ефективність використовуваних засобів захисту.

Модель використовує як параметри множини загроз, засобів захисту, вразливостей тощо. Визначення взаємозв'язків між цими параметрами є складним нетривіальним завданням, що ускладнює практичне застосування моделі.

Наведена модель не здатна розрахувати такі параметри як ймовірність реалізації загрози, час виявлення атаки та час реалізації.

1.2.2 Моделі, що побудовані з використанням теорії ймовірностей.

Використання цих моделей входить в перелік найпоширеніших. Всі моделі, що використовують апарат теорії ймовірностей, засновані на добутку ймовірностей певних подій.

До переваг моделей відноситься можливість розрахувати ймовірність певної загрози. Недоліками моделей є те, що вони не дають можливості розраховувати тимчасові характеристики процесу реалізації загрози. Також нажаль отримати на практиці основні параметри моделей складно, бо присутня недостатність статистичних даних щодо реалізації загроз та скритності успішних реалізацій загроз. Також не враховується, що вибір шляху зловмисником під час реалізації загрози залежить від таких факторів, як рівень підготовки зловмисника, його обладнання тощо.

1.2.3 Моделі, що побудовані з використанням теорії випадкових процесів.

У моделях, що використовують теорію випадкових процесів виділяють моделі, що використовують:

– марківські процеси;

– напівмарківські процеси;

– розгалужені процеси.

Марківська модель загрози безпеці системи захисту інформації представлена у вигляді процесів з дискретним станом та безперервним часовим проміжком для графа загрози інформаційній безпеці. Створюється за допомогою загрози двох атак: у першій використовуються загрози першої та другої вразливості; у другій використовуються загрози першої та третьої вразливості [2].

Завдяки використанню цієї моделі, будується система диференціальних рівнянь Колмогорова для ймовірностей станів. При вирішенні якої розраховується ймовірність того, наскільки готова інформаційна система до безпечної експлуатації. Тут обґрунтовується коректність використання марківських процесів моделювання характеристик безпеки інформації, виявляються відмінності у постановці та вирішенні завдань моделювання комплексної системи захисту інформаційної системи.

Моделі, побудовані з використанням теорії випадкових процесів, з одного боку дозволяють розрахувати можливість реалізації тієї чи іншої загрози. У випадку використання напівмарківського процесу потрібно оцінити тимчасові параметри реалізації загрози. З іншого боку, підхід до визначення станів у наведених моделях призводить до складнощів практичного застосування, бо важко визначити параметри щільності потоку для марківських моделей у зв'язку з тим, що на них впливають такі параметри як, вразливість засобів захисту, джерело загрози та її особливості, що не враховуються в моделі. Також представлена напівмарківська модель не визначає час виявлення атаки.

1.2.4 Моделі, що збудовані з використанням теорії мереж Петрі.

Як приклад цього виду моделей може бути робота [3]. Там модель системи захисту визначається як попередньо виділена послідовність елементарних операцій, з яких може складатися атака. Вхідними параметрами для моделі виступають мінімальний, максимальний і ймовірний час, що витрачається зловмисником на кожну елементарну операцію та проміжок часу, відведений на атаку (час моделювання). Результатом є можливість успішної атаки за заданий час.

Перевагою моделі є те, що вона дозволяє розрахувати ймовірність реалізації загрози за заданий час. Основні параметри моделі можна відносно легко отримати за допомогою аналізу вразливостей, побудові послідовності етапів реалізації загрози та аналізу часу, що витрачається на кожен з етапів реалізації. У той же час модель не розраховує часові показники процесу реалізації небезпеки. При цьому в моделі складно відобразити вразливості засобу захисту.

1.2.5 Моделі, що побудовані з використанням теорії автоматів.

В роботі [4] пропонується модель, що описує процес комп'ютерної атаки. Модель надана як кінцевий детермінований автомат. Переходи між станами

автомата залежить від стану автомата і входу автомата у кожному стані. Вихід автомата обчислюється після переходу автомата на деякий стан і залишається незмінним до наступного переходу.

У роботі виділяються основні такі проблеми, що перешкоджають прямій реалізації моделі:

- неповнота інформації про стан систем;
- складність розрахунку перехідних функцій автомата;
- складність аналітичного подання функцій виходів автомата.

Ця модель має певні переваги. Вона точно відображає процес атаки на ІС, використовуючи послідовність станів автомата. При цьому використовуються такі формальні механізми, як нейронні мережі визначення основних параметрів моделі. До недоліків моделі можна віднести відсутність у явному вигляді оцінки часу виявлення атаки, часу, що витрачається на реалізацію загрози та ймовірності реалізації.

1.2.6 Моделі, що збудовані з використанням теорії графів.

Неформально, граф атак – це граф, що представляє всі можливі послідовності дій порушника задля досягнення загроз (цілей). Такі послідовності дій називаються трасами (шляхами) атак [5].

Неформально, граф атаки – це граф, що представляє всі можливі послідовності дій порушника для реалізації загрози. Такі послідовності дій називаються шляхами атак (рис. 1.1).

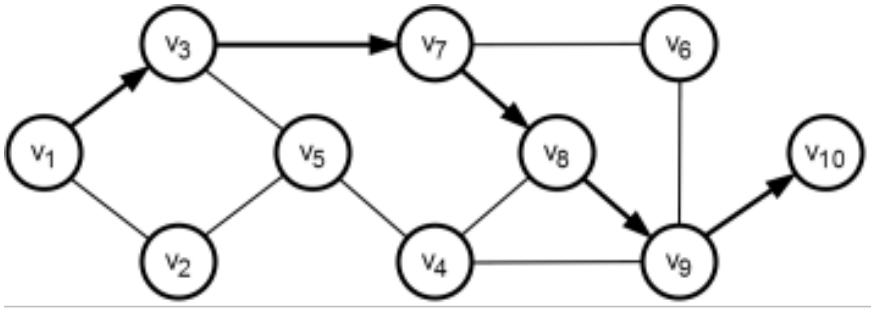

Рисунок 1.1 – Граф атаки

Вирізняють такі види графів атак [6]:

– state enumeration graph – у таких графах вершинам відповідають трійки (s, d, a), де s – джерело атаки, d – мета атаки, a – елементарна атака (або використання) вразливості); дуги позначають переходи з одного стану до іншого;

– condition–oriented dependency graph – вершинам відповідають результати атак, а дугам – елементарні атаки, що призводять до таких результатів;

– exploit dependency graph – вершини відповідають результатам атак або елементарним атакам, дуги відображають залежності між вершинами – умови, необхідні для виконання атаки та наслідок атаки. Такі моделі застосовуються в основному на етапі аудиту безпеки мереж для виявлення слабких місць системи захисту та прогнозування дій порушника.

Здебільшого графи атак розглядаються у контексті аналізу захищеності мереж. Зазвичай такий аналіз зводиться до послідовного сканування всіх хостів мережі на наявність відомих вразливостей. Результатом є перелік знайдених уразливості та рекомендації щодо їх усунення. В даний час поступово впроваджується інша парадигма аналізу захищеності, яка враховує «топологію» комп'ютерної системи (КС) – взаємозв'язок об'єктів комп'ютерної системи, їх властивостей та характеристик. Такий аналіз захищеності називається топологічним, а засоби, що його виконують, топологічними сканерами безпеки [5].

1.2.7 Моделі, що побудовані з використанням теорії нечітких множин.

В роботі [7] пропонується модель розрахунку інформаційних ризиків, що ґрунтується на використанні нечітких когнітивних карт.

Для побудови нечіткої когнітивної карти виділяється ряд концептів, визначаються взаємозв'язки та сила впливу між ними. Вага зв'язків у нечітких когнітивних картах задаються у нечіткому вигляді: з допомогою лінгвістичних терм чи інтервальних оцінок, та був за допомогою функції належності інтерпретуються для подальших розрахунків. За допомогою НКК обчислюється повний ефект впливу сукупності загроз на певний цільовий фактор. На основі отриманих даних обчислюється ризик.

Ця модель розраховує ймовірність реалізації загрози безпосередньо і при цьому визначає ризики по загрозі, але не дозволяє розрахувати час, який витрачається на реалізацію загрози і час виявлення атаки.

1.2.8 Моделі, що збудовані з використанням теорії катастроф.

В роботі [8] пропонується модель, що дозволяє оцінити час безпечного функціонування ІС та імовірність виключення несанкціонованого доступу на інтервалі, розподіленому за експонентним законом. Перевагою даної моделі є те,

що вона дозволяє отримати оцінку середнього часу безпечного функціонування системи.

З іншого боку, недоліками моделі є те, що вона передбачає можливість представлення всієї системи захисту, як програми певної довжини. До того ж передбачається, що зловмисник повинен вивчити всю систему захисту, тобто розшифрувати всю програму для НСД до інформації. Отже модель не враховує можливість доступу до інформації у випадку часткового злому системи. Також модель не може дати відповіді щодо слабких місць системи захисту.

1.2.9 Моделі, що збудовані з використанням теорії ігор.

В роботі [9] пропонується ігрова модель системи захисту інформації, яка використовується для вирішення проблеми оптимального вибору рішення, що забезпечує співвідношення між витратами на засоби захисту та зниженням ризику експлуатації системи. Тут досліджено стратегії одного гравця («захисника»), які полягатимуть у приведенні автоматизованої системи у відповідність до вимог певного класу захищеності, та стратегії іншого гравця («порушника»), які полягатимуть у реалізації загрози, що належить до певного класу загроз. Функція виграшу буде сумою витрат на реалізацію запропонованих заходів захисту та очікуваних втрат у разі реалізації загрози певного класу, за умови приведення системи у відповідність до вимог за класом захищеності.

Таким чином, якщо гра має рішення у чистих стратегіях, можна стверджувати, що для ІС знайдено оптимальний клас захищеності, з погляду мінімаксного критерію. Якщо рішення існує лише у змішаних стратегіях, то такий результат потребує додаткової інтерпретації.

Недоліком такого підходу є те, що необхідно знайти рішення у чистих стратегіях, що не завжди можливо, та описати поведінку зловмисника не завжди можна чистою стратегією, спрямованою на завдання максимальної шкоди. Наведена модель не розраховує ймовірність реалізації загрози, час реалізації і час виявлення атаки.

1.2.10 Моделі, що збудовані з використанням ентропійного підходу.

В роботі [10] пропонується модель системи забезпечення безпеки інформації з урахуванням ентропійного підходу. Нехай стан системи x_j характеризується деяким ресурсом (ефектом) $f(x_j)$. Під станом x_j розуміється

деякий і-й набір засобів захисту інформації. При цьому справедливе обмеження за формулою (1.1)

$$\sum_i p_i \cdot f(x_i) = E[f(x)] \le U,$$

(1.1)

де p_i – ймовірність стану x_i, U – обмеження на ресурс, або обмеження на корисний ефект.

Тоді задача пошуку оптимального розподілу величини x_i, формально записується у вигляді формул (1.2) – (1.4):

$$S \to \max,$$

(1.2)

$$\sum_i p_i \cdot f(x_i) = U,$$

(1.3)

$$\sum_i p_i = 1,$$

(1.4)

де $S = -\sum_i p_i \cdot \ln p_i$ – ентропія системи.

Для вирішення цього завдання використовується метод невизначених множників Лагранжа.

Таким чином, макростан системи забезпечення безпеки інформації можна задати рядом взаємопов'язаних характеристик (макропараметрів). Їх інтерпретація залежить від постановки задачі, що вирішується, а також від особливостей конкретної досліджуваної системи. Для практичного застосування запропонованих ентропійних методів моделювання необхідно ув'язати макропараметри системи з конкретними характеристиками окремих її підсистем та елементів, що може виконати експерт–аналітик.

Представлена модель має наступні переваги і недоліки. До переваг можна віднести гнучкість моделі, так як параметри моделі можуть використовуватися

різні величини і, відповідно, можливо отримати такі параметри як ймовірність реалізації загрози, час реалізації і час виявлення атаки. З іншого боку практично вкрай складно підігнати цю модель під реальну ІС і виділити основні параметри.

1.2.11 Порівняльний аналіз моделей систем захисту інформації.

Для проведення порівняльного аналізу визначаються критерії порівняння, за якими проводиться оцінка моделей. При визначенні набору критеріїв до уваги бралися такі практичні міркування:

– з практичної точки зору для оцінки ефективності СЗІ необхідно знати такі параметри як ймовірність реалізації тієї чи іншої загрози та ризики, пов'язані з нею;

– при функціонуванні ІС та при атаках на неї можливі ситуації, коли на певному етапі завдяки наявності системи виявлення вторгнень або певним регламентованим діям персоналу спроба атаки розкривається і відповідно атака може бути заблокована. Відповідно необхідно знати середній час, який минає від початку атаки до її виявлення і відповідно блокування;

– термін атака на ІВ передбачає послідовність уразливостей СЗІ ІС, які експлуатуються під час спроби реалізації загрози. Відповідно процес реалізації загрози зручно описувати саме з погляду вразливостей СЗІ, що використовуються;

– модель може використовувати різні дані як вихідні параметри, при цьому можливості отримання тих чи інших даних можуть бути завданнями різного ступеня складності.

З урахуванням практичних міркувань виділяються вимоги до моделі СЗІ, які використовуються як критерії порівняння:

– можливість розрахувати ймовірність реалізації загрози в залежності від використовуваних засобів захисту, уразливостей у них та рівня підготовки та оснащеності зловмисника;

– можливість розрахувати час реалізації загрози залежно від засобів захисту, уразливостей у них та рівня підготовки та оснащеності зловмисника;

– можливість розрахувати час виявлення атаки залежно від засобів захисту, вразливостей у них і рівня підготовки та оснащеності зловмисника;

– можливість розрахувати ризики інформаційної безпеки;

– практична застосовність принципу відображення процесу реалізації погрози;

– простота визначення вхідних параметрів моделі.

Аналіз підходів до моделювання систем захисту показав, що жодна з представлених моделей не задовольняє повною мірою основним критеріям. Результат аналізу представлено таблицю 1.1.

Таблиця 1.1 – Результати порівняльного аналізу підходів до моделювання системи захисту інформації щодо практичного застосування та простоти визначення вхідних параметрів.

Тип моделей	Практичне застосування	Простота визначення вхідних параметрів
1	2	3
Узагальнені моделі систем захисту	У зв'язку зі слабкою опрацьованістю формального боку моделей застосовність на практиці утруднена	Як параметри використовуються абстрактні величини. Їх визначення можливе лише із залученням експертів
Моделі, що побудовані з використанням теорії ймовірностей	Не враховуються різні шляхи подолання того чи іншого засобу захисту та залежності вибору шляху зловмисником від його підготовленості та оснащеності	Параметри складно отримати на практиці через недостатність статистичних даних та латентність успішних реалізацій загроз.
Моделі, що побудовані з використанням теорії випадкових процесів	Використовуються абстрактні стани процесів, що ускладнює застосування моделей до реальних систем.	У зв'язку з абстрактністю станів важко визначати такі параметри процесів як: щільність потоків, ймовірність переходів і час перебування в стані
Моделі, що побудовані з використанням теорії мереж Петрі	У моделі складно відобразити безліч шляхів подолання системи захисту, особливо великих систем	Параметри прості у визначенні
Моделі, що побудовані з використанням теорії автоматів	Модель, наведена в [4], добре відображає процес реалізації загрози.	Параметри визначаються просто. При цьому в [4] використовуються методи нейронних мереж.
Моделі, що побудовані з використанням теорії графів	Наочно демонструють усі можливі шляхи реалізації загрози.	Як параметри моделі використовуються списки вразливостей, також, можливе використання ймовірностей вибору шляху, успішності експлуатації вразливості та часу, що витрачається на використання вразливості.
Моделі, що побудовані з використанням теорії нечітких множин	Порівняно легко застосовувати практично.	Всі параметри щодо просто отримати на практиці

Моделі, що побудовані з використанням теорії катастроф	Модель має очевидну спрямованість на програмні засоби захисту.	Використовуються експертні оцінки, що з одного боку спрощує отримання вхідних даних, а з іншого ставить залежність коректність і повноту даних, що використовуються, від рівня підготовки експертів

Продовження таблиці 1.1

1	2	3
Моделі, що збудовані з використанням теорії ігор	Моделі не враховують залежності стратегій поведінки зловмисника від його підготовленості та оснащеності, також не враховується можливість здійснення загроз та заподіяння шкоди різними шляхами.	Параметри мають досить і складні у визначенні
Модель, що побудовані з використанням ентропійного підходу	У моделі використовується підхід, який не відображає особливостей функціонування СЗІ.	Вихідні дані для моделі дуже складно отримати.

Таким чином, результати порівняльного аналізу моделей СЗІ показали, що сфера застосування існуючих моделей – це в основному етапи експлуатації та супроводу ІС. Моделі не дозволяють отримати оцінки захищеності одночасно за всіма вимогами на більш ранніх етапах життєвого циклу ІС, а також не дозволяють вибирати оптимальні проекти СЗІ. Також класифікація моделей систем захисту інформації розглянуто у [11].

1.3 Деякі моделі оптимізації складу комплексу засобів захисту в комплексних системах захисту інформації

1.3.1 Підходи щодо формалізації завдання вибору засобів захисту інформації в інформаційній системи.

Можливі два підходи щодо формалізації завдання вибору та розподілу засобів захисту між різними функціями системи ЗІ. При першому підході, більш деталізованому, у процесі формалізації завдання розподілу засобів враховуються склад та кількість засобів забезпечення захисту інформації (ЗЗЗІ) та можливих заходів щодо ЗІ. Однак такий підхід, по-перше, передбачає наявність досить повної інформації про склад потенційно можливих ЗЗЗІ та заходів щодо ЗІ, і, по-друге, за досить великої кількості засобів та заходів (більше кількох десятків) розміри завдання, що виходить, часто не дозволяють вирішувати її за допомогою існуючих засобів обчислювальної техніки [12].

Другий підхід ґрунтується на більш узагальнених усереднених закономірностях зв'язку між вкладеними у процес забезпечення ЗІ засобами та ефективністю процесу забезпечення ЗІ. Отримані з урахуванням цього підходу

кінцеві результати мають менш точний характер, більше відбиваючи порядок результату. Однак цей підхід значною мірою позбавлений недоліків, які мають місце при першому підході. Кожен із описаних підходів може бути кращим за інший залежно від умов їх застосування. Зокрема, при проектуванні та плануванні процесів функціонування великих систем зазвичай краще другий підхід, а при проектуванні та плануванні процесів функціонування локальних компонентів автоматизованої системи обробки даних (АСОД) – перший. Нижче розглянуто обидва підходи до формалізації розглянутої задачі [12].

У роботі [13] описані різні методології теорії ігор, що включають проектування механізмів, аналіз стимулів, прийняття рішень в умовах неповної інформації та динамічні ігри, щоб забезпечити міцну основу науки про кібербезпеку. У цій роботі поєднуються різні класи ігор із різними наборами проблем безпеки. До першого класу відносяться Stackelberg та багаторівневі ігри для превентивного захисту, до другого – мережеві ігри для кіберфізичної безпеки, що займається захистом критичної інфраструктури та гарантії інформації, до третього – динамічні ігри для адаптивного захисту мережевої безпеки, до четвертого – теорія проектування механізмів для економіки мережевої безпеки, яка досліджує методології розподілу ресурсів та до п’ятого – теоретико–ігровий аналіз криптографічних концепцій, таких як абсолютна конфіденційність та автентифікація, проектування та забезпечення мережі та кількісне управління ризиками безпеки.

З погляду кібербезпеки у роботі [13] описані нещодавні застосування теорії ігор до кількох нових тем, таких як міжрівнева кіберфізична безпека, кіберобман, захист від рухомих цілей, захист критичної інфраструктури, вороже машинне навчання, інсайдерські загрози та управління кіберризиками.

1.3.2 Варіант моделі оцінювання ефективності розробки комплексної системи захисту інформації.

При впровадженні КСЗІ ставиться завдання мінімізації сумарних витрат шляхом змін капітальних та експлуатаційних витрат, що зводиться до оптимізації показника загальної ефективності заходів щодо забезпечення безпеки згідно формули (1.5) [14]:

$$E = \sum_{k=1}^{K} \left(Y_1^k - Y_2^k \right) - \sum_{b=1}^{B} \left(\Delta K_3 + \Delta E_3 \right)_b,$$

(1.5)

де E – ефективність розробки КСЗІ;

Y_1^k – можливі збитки k–го виду до впровадження КСЗІ;

Y_2^k – можливі збитки k–го виду після впровадження КСЗІ;

$\sum_{b=1}^{B} \left(\Delta K_3 + \Delta E_3 \right)_b$ – сумарні витрати на впровадження засобу безпеки b–го виду за рахунок змін капітальних (ΔK_3) та експлуатаційних (ΔE_3) витрат.

Ризик від реалізації загрози розраховується за формулою (1.6) [15]:

$$R = Y \cdot P,$$

(1.6)

де Y – можливі збитки від реалізації загрози;

P – ймовірність реалізації загрози порушником

Можна виділити три варіанти підвищення ефективності заходів щодо забезпечення комплексної безпеки об'єкта захисту, які описуються формулами (1.7) – (1.9) [15]:

$$\sum_{k=1}^{K} \left(Y_1^k - Y_2^k \right) \to \max, \ \sum_{b=1}^{B} \left(\Delta K_3 + \Delta E_3 \right)_b = \text{const},$$

(1.7)

$$\sum_{k=1}^{K} \left(Y_1^k - Y_2^k \right) = \text{const}, \ \sum_{b=1}^{B} \left(\Delta K_3 + \Delta E_3 \right)_b \to \min,$$

(1.8)

$$\sum_{k=1}^{K} \left(Y_1^k - Y_2^k \right) \to \max, \ \sum_{b=1}^{B} \left(\Delta K_3 + \Delta E_3 \right)_b \to \min,$$

(1.9)

Імовірні збитки від реалізації загрози визначаються згідно формули (1.10) [15]:

$$Y = Y^1 + Y^2 + Y^3 + Y^4 + Y^5 + Y^6 + Y^7, \quad (1.10)$$

де Y^1 – прямі втрати;

Y^2 – витрати на ліквідацію та розслідування;

Y^3 – соціально–економічні втрати;

Y^4 – непрямий збиток;

Y^5 – екологічні збитки;

Y^6 – втрати від вибуття трудових ресурсів;

Y^7 – збитки від втрати інформаційних ресурсів.

Усі потенційні загрози безпеці об'єкта захисту так чи інакше впливають на його економічний стан та на співвідношення «за витрати – збитки» під час управління безпекою. У зв'язку з цим доцільно таким чином формувати програму управління, щоб витрати на безпеку були адекватні потенційним загрозам. Подібна ситуація визначає необхідність оцінки ймовірності реалізації загрози [15].

Оцінка ймовірності реалізації загроз та пов'язана з цим оцінка можливих втрат – найскладніша та найвідповідальніша частина всього процесу забезпечення безпеки. Від того, наскільки, з одного боку, досить повно виявлені реальні та прогнозовані (потенційні) загрози, залежить зрештою ступінь захищеності об'єкта. З іншого боку, свідоме перевищення достатності при врахуванні тих загроз, вплив яких безпосередньо на функціонування об'єкта малоймовірний або локалізація яких неможлива або малоефективна, призведе до значного підвищення витрат на безпеку і може суттєво позначитися на реально досяжній економічній ефективності захисту [15].

1.3.3 Математична постановка задачі вибору засобів захисту інформації в інформаційних системах на основі моделі антагоністичної гри.

В роботі [16] розглянутий варіант задачі вибору засобів захисту інформації в інформаційних системах на основі моделі антагоністичної гри.

Вихідними даними для математичної постановки задачі будуть наступні параметри.

1) $A = \{a_1, a_2, \ldots, a_n\}$ – безліч можливих загроз безпеці або засобів проведення атак, якими може скористатися порушник, $N = \{1, 2, \ldots, n\}$ – безліч індексів цих загроз (засобів). Як можливі загрози тут можна розглядати конкретні технічні, програмні або організаційні засоби, які може задіяти сторона нападу.

2) $B = \{b_1, b_2, \ldots, b_n\}$ –множина засобів захисту інформації від загроз безпеки, $M = \{1, 2, \ldots, m\}$ – безліч індексів засобів захисту відповідно.

3) u_i, де $i \in N$ – середні збитки від незапобігання і-ої загрози за заданий період часу.

4) $c_i^{(н)} \geq 0$, де $i \in N$ – вартість реалізації і - ої загрози стороною нападу;

5) $c_j^{(з)} \geq 0$, де $j \in M$ – вартість j - го засобу захисту;

6) $u_{ij} \in [0,1]$, $i \in N, 0$, $j \in M$ – можливість, що описується в рамках теорії нечітких множин, або ймовірність (якщо є статистика) запобігання наслідків і - ої загрози за допомогою j - го засобу захисту, параметри утворюють матрицю $p = \|p_{ij}\|$ розмірності $n \times m$

Для опису показника якості введемо наступні змінні.

Для сторони захисту введемо змінну булеву $x_j \in \{0,1\}$, де $j \in M$. У змінної є два стани:

$$x_j = \begin{cases} 1, \text{якщо j – й засіб захисту використовується в АС} \\ 0, \text{в іншому випадку} \end{cases}$$

Тоді $\bar{X}$ – вектор булевих змінних x_j.

За аналогією для сторони нападу введемо булеву змінну y_i:

$$y_i = \begin{cases} 1, \text{якщо реалізовується і – а загроза в АС} \\ 0, \text{в іншому випадку} \end{cases}$$

Тоді $\bar{Y}$ – вектор булевих змінних y_i.

Збитки від реалізації атак без застосування засобів захисту для сторони захисту або максимально можлива збиток визначається згідно формули (1.11):

$$U^{(max)}(\bar{Y}) = \Sigma_{i \in N} u_i \cdot y_i,$$

(1.11)

При використанні засобів захисту можна буде уникнути частини збитку. Збиток, який можна уникнути, в загальному випадку можна описати формулою (1.12):

$$U^{(max)}(\bar{X}, \bar{Y}) = \Sigma_{i \in N} u_i \cdot y_i \cdot F_i(P, \bar{X}),$$

(1.12)

де $F_i(P, \bar{X})$, де $i \in N$ – функції, що визначають ступінь збитку, який можна запобігти, від кожної з загроз.

Такі функції будемо використовувати згідно формули (1.13):

$$F_i(P, \bar{X}) = \max_{j \in M}\left\{ p_{ij} \cdot x_j \right\}, \quad i \in N,$$

(1.13)

Змістовно функція задає те, що для запобігання збитку враховується лише один вибраний засіб захисту, що має максимальну можливість (імовірність) запобігання для і-ої загрози. У цій функції не враховується сумарний ефект від спільного використання двох або більше засобів захисту для запобігання загрозі. Тоді реальні збитки для сторони захисту визначається формулою (1.14):

$$U(\bar{X}, \bar{Y}) = U^{(max)}(\bar{Y}) - U^{(max)}(\bar{X}, \bar{Y}) = \Sigma_{i \in N} u_i \cdot y_i - \Sigma_{i \in N} u_i \cdot y_i \max_{j \in M}\left\{ p_{ij} \cdot x_j \right\}$$

,(1.14)

Цей показник визначає реально можливий збиток для захисту при використанні СЗІ. Сторона захисту намагається цю шкоду мінімізувати, а сторона нападу намагається максимізувати, таким чином, отримуємо гру двох гравців з нульовою сумою.

Далі розглянемо наступні обмеження. Вартість засобів захисту визначається за формулою (1.15):

$$C^{(з)}\left(\bar{X}\right) = \Sigma_{j\in M} c_j^{(з)} x_j, \quad (1.15)$$

При цьому сторона захисту обмежена у засобах, тобто $C_{max}^{(з)}$ та $C_{max}^{(н)}$ відповідно максимальна сума, яку можна витратити на захист інформації та максимальна сума, яку можна витратити на проведення атак. Тоді обмеження на максимальну вартість засобів захисту визначається нерівністю за формулою (1.16):

$$\Sigma_{j\in M} c_j^{(з)} x_j \le C_{max}^{(з)}, \quad (1.16)$$

За аналогією для сторони нападу введемо обмеження на максимальну вартість ресурсів, які використовуються для атак за формулою (1.17):

$$\Sigma_{i\in N} c_j^{(н)} y_i \le C_{max}^{(н)}, \quad (1.17)$$

Отже модель гри буде виглядати наступним чином. Сторона захисту або перший гравець вирішує задачу мінімізації показника (1.11) з обмеженнями (1.16):

$$U\left(\bar{X}, \bar{Y}\right) = \Sigma_{i\in N} u_i \cdot y_i - \Sigma_{i\in N} u_{i\cdot} \cdot y_i \max_{j\in M}\left\{ p_{ij} \cdot x_j \right\} \to \min_{\bar{X}\in\Delta_x^{(дод)}},$$

$$\Delta_x^{(дод)}: \Sigma_{j\in M} c_j^{(з)} x_j \le C_{max}^{(з)}, \quad (1.18)$$

де $\Delta_x^{(дод)}$ – безліч допустимих альтернатив (значень компонент невідомого вектора $\bar{X}$) для першого гравця. При фіксованих значеннях компонент вектора $\bar{Y}$ отримуємо завдання булевого програмування.

Сторона нападу або другий гравець вирішує завдання максимізації показника (1.11) з обмеженнями (1.17) [16]:

$$U\left(\bar{X},\bar{Y}\right)=\Sigma_{i\in N}u_i\cdot y_i-\Sigma_{i\in N}u_i\cdot y_i\max_{j\in M}\left\{p_{ij}\cdot x_j\right\}\rightarrow\max_{\bar{Y}\in\Delta_y^{(\text{дод})}}$$

, (1.19)

$$\Delta_y^{(\text{дод})}:\Sigma_{i\in N}c_j^{(\text{н})}y_i\leq C_{max}^{(\text{н})},$$

де $\Delta_y^{(\text{дод})}$ – безліч допустимих альтернатив (значень компонент невідомого вектора $\bar{Y}$) для першого гравця. При фіксованих значеннях компонент вектора $\bar{X}$ отримуємо завдання булевого програмування.

Надану модель гри можна звести до гри, що задана платіжною матрицею. Проблема полягає в тому, що розмірність цієї матриці може бути досить велика: число рядків дорівнює кількості допустимих значень вектора , що задовольняють обмеження (1.16), а число стовпців буде дорівнює кількості допустимих значень вектора, що задовольняють обмеження (1.17). У разі використання платіжної матриці часто шукають сідлову точку в чистих стратегіях або, якщо її не існує, у змішаних стратегіях. При великій розмірності платіжної матриці це завдання є скрутним.

2 АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ДЛЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

1. Загрози для інформаційних систем за ознаками

Загрози для інформаційних систем можуть класифікуватися за 9 ознаками [17].

1) За метою реалізації загрози:

– порушення конфіденційності інформації;

– порушення цілісності інформації (втрати від таких дій можуть бути набагато більшими, ніж при порушенні конфіденційності);

– порушення (часткове або повне) працездатності інформаційних систем (ІС).

2) За принципом впливу на інформаційну систему:

– з використанням доступу суб'єкту системи (користувача, процесу) до об'єкту (файлу даних, каналу зв'язку тощо);

– з використанням прихованих каналів.

Під прихованим каналом розуміється шлях передачі інформації, який дає змогу двом взаємодіючим процесам обмінюватися інформацією таким способом, що порушує системну політику безпеки.

Вплив, заснований на першому принципі, простіший, більш інформаційний, але від нього легше захиститись. Вплив на основі другого принципу відрізняється трудністю організації, меншою інформаційністю, складністю виявлення і усунення.

3) За характером впливу на ІС:

– активна загроза, що веде до зміни стану системи і може здійснюватися або з використанням доступу (наприклад, до набору даних), або як з використанням доступу, так і з використанням прихованих каналів;

– пасивна загроза, що здійснюється шляхом спостереження користувачем будь–яких побічних ефектів (наприклад, від роботи програми) та їх аналіз.

Прикладом пасивного впливу може бути прослуховування лінії зв'язку між двома вузлами мережі. Пасивний вплив не веде до зміни стану системи. Він завжди пов'язаний тільки з порушенням конфіденційності інформації в ІС.

4) За причиною використовуваної помилки захисту.

Така помилка може бути зумовлена однією з наступних причин:

– неадекватністю політики безпеки реальній ІС;

– помилками адміністративного управління, під якими розуміють некоректну реалізацію або підтримку прийнятої політики безпеки ІС;

– помилками в алгоритмах, у зв’язках між ними тощо, які виникають на етапі проектування програми або комплексу програм, у зв’язку з чим їх можна використовувати зовсім не так, як це описано в документації;

– помилками реалізації алгоритмів (помилками кодування), зв’язками між ними тощо, які виникають на етапі реалізації або впровадження і які також можуть бути джерелом не документованості.

5) За способом впливу на об’єкт атаки (при активному впливі):

– безпосередній вплив на об’єкт атаки, таким діям звичайно легко запобігти з допомогою засобів контролю доступу;

– вплив на систему управління доступом (в тому числі загарбання привілеїв);

– опосередкований вплив (через інших користувачів);

– «маскарад», у цьому разі користувач присвоює собі повноваження іншого користувача, видаючи себе за нього;

– «користувач наосліп» – коли один користувач змушує іншого виконувати необхідні дії, причому останній про них може і не підозрювати; для цього може використовуватися вірус (він виконує необхідні дії та повідомляє тому, хто його впровадив, про результат).

6) За способом впливу на ІС:

– в інтерактивному режимі;

– в пакетному режимі.

7) За об’єктом атаки.

Впливам можуть піддаватися такі компоненти ІС:

– ІС в цілому (проникнення в систему), для цього, як правило, використовують метод «маскараду», перехоплення або підробки пароля, «злом» та доступ до ІС через мережу;

– об’єкти ІС – дані або програми, самі пристрої системи, канали передачі даних;

– суб’єкти ІС – процеси і підпроцеси користувачів, частим випадком такого впливу є введення зловмисником вірусу в середовище другого процесу і його виконання від імені цього процесу;

– канали передачі даних – пакети даних, які передаються каналами зв’язку і власне канали, прослуховування каналу і аналіз трафіка (потоку повідомлень,

підміна або модифікація повідомлень у каналах зв’язку і на вузлах ретрансляторах, зміна топології та характеристик мережі).

8) За використовуваними засобами атаки (використовується або стандартне програмне забезпечення (ПЗ), або спеціально розроблені програми).

9) За станом об’єкта атаки.

Об’єкт атаки може знаходитись в одному із трьох станів:

– збереження – вплив на об’єкт, як правило, здійснюється з використанням доступу;

– передачі – вплив передбачає або доступ до фрагментів інформації, що передається, або просто прослуховування з використанням прихованих каналів;

– обробки – об’єктом атаки є процес користувача.

Серед найпоширеніших загроз є несанкціонований доступ (НСД). Він полягає в отриманні користувачем доступу до об’єкта, до якого у нього немає доступу відповідно до прийнятої організації політики безпеки.

Для того, щоб зменшити ризик від НСД, більшість систем захисту реалізує необхідні функції за допомогою відповідного набору привілеїв. Незаконне захоплення привілеїв можливе або при наявності помилок у самій системі захисту, або через халатність при управлінні системою і привілеями.

Небезпечні дії, що можуть призвести до порушення конфіденційності, цілісності та доступності певних компонентів і ресурсів ІС , можна згрупувати наступним чином:

– стихійні лиха;

– зовнішні впливи (підключення до мережі, інтерактивна робота, діяння зловмисників);

– навмисні порушення;

– ненавмисні помилки (введення помилкової команди, даних, використання несправних пристроїв, носіїв, а також нехтування деякими правилами безпеки).

Види загроз, які можуть з’явитися в результаті небезпечних дій.

1) Розкриття (витік) інформації. Для даного виду загрози об’єктами дій є устаткування (крадіжка носіїв, несанкціоноване підключення, несанкціоноване використання ресурсів), програми (несанкціоноване копіювання, перехоплення), дані (крадіжка, копіювання, перехоплення), персонал (передача відомостей про захист, розголошення, халатність).

2) Порушення цілісності інформації: устаткування (підключення, модифікація, спеціальні вкладення, зміна режимів, несанкціоноване використання

ресурсів), програми (впровадження «троянських коней» та «жучків»), дані (спотворення, модифікація), персонал (вербування, підкуп персоналу, «маскарад»).

3) порушення працездатності системи: устаткування (зміна режимів, виведення з ладу, руйнування), програми (спотворення, вилучення, підміна), дані (видалення, спотворення).

Підводячи підсумок з вищезгаданих ознак можна зазначити наступне.

Аналізуючи мету реалізації загроз можна побачити, що порушення працездатності може бути як найнебезпечніше, так і навпаки. Така ситуація склалася через те, що часткове порушення працездатності в компоненті ІС може бути виправлено швидко і нанесений збиток може бути мінімальний, набагато менший, ніж при порушенні конфіденційності. Але у разі порушення працездатності всієї ІС відновлення може зайняти багато часу, отже розмір збитку буде величезний.

Аналізуючи принципи впливу на інформаційну систему можна побачити, що приховані канали є більш небезпечними, бо витік через них може відбуватися довше і втрачена інформація, яка окремо може не представляти небезпеку і бути нецікавою, в сукупності може нанести великий збиток.

Дивлячись на характер впливу на інформаційну систему важливо зазначити що, хоч пасивні загрози і впливають лише на витік конфіденційної інформації і є безперечно менш небезпечними для ІС, але неможна їх недооцінювати. Ці загрози можуть бути дуже вагомими, наприклад, для конкурентів. Така інформація може бути використана для нанесення збитку іншими методами, отже пасивні загрози будуть найдоречніші як допоміжний засіб впливу на ІС.

Серед помилок захисту кожна з них може бути причиною значного збитку. Тут є впливовим людський фактор, тому відсутності цих причин можна мінімізувати, але не уникнути. Неадекватність політики безпеки є найскладнішою, не тільки через те що розповсюджується на всю ІС, а й через складність її виправлення. Некоректне адміністративне управління є другою найвагомішою причиною цього виду помилок, бо навіть при правильно розробленій політиці безпеки, коректне її впровадження та/або підтримка є критично важливою, отже через складність виправлення можуть бути нанесені значні збитки. Помилки в створенні та реалізації алгоритмів, якщо їх розглядати без врахування людського фактору, є менш вагомими, тому що, хоч і можуть розповсюджуватися на всю ІС, швидкість та простота виправлення є на низькому рівні. Але, при врахуванні

людського фактору, можна зрозуміти, що розрахувати час, який буде затрачено на виправлення, складно, він може бути великим і тому збиток може бути несподіваним.

Спосіб впливу на об’єкт атаки буде детальніше характеризувати активні атаки. Серед видів такого впливу досить небезпечним є «маскарад», так як його важко виявити звичайному користувачу, але «користувач наосліп» є найнебезпечнішим видом з представлених так як особистість того, хто впроваджує його залишається невідомою.

Аналізуючи способи впливу на ІС, можна сказати що, в пакетному режимі користувач не має доступу до машинних ресурсів та вплив безперервний, то це дозволяє зменшити час, за який буде нанесений необхідний рівень збитку. А в інтерактивному режимі доступ до машинних ресурсів є, що дає можливість користувачеві безпосередньо впливати на ІС, перевагою цього методу є можливість контролювати та корегувати вплив на ІС в реальному часі. Отже обидва методи є ефективними в залежності від потреб зловмисника.

Аналізуючи об’єкти атак, можна зробити висновок, що окремі компоненти ІС представляють значно меншу загрозу і нанесений збиток, при впливі на окремий компонент ІС, буде значно менший, отже потрібно концентруватися на захисті ІС загалом.

Аналізуючи таку ознаку як засоби атаки, важливо зазначити що переваги є як у стандартного, так і спеціального програмного забезпечення. При використанні стандартного ПЗ можна заощадити час та кошти, але при наявності важких для атаки місць може погіршитися ефективність такого ПЗ. На відміну від цього, спеціальне ПЗ направлене на ІС саме для конкретної атаки, тому ефективність буде більшою за рахунок сконцентрованості на необхідних місцях під час атаки. Але у спеціального ПЗ недоліком є висока вартість та довгий час на розробку такого ПЗ. Отже слід вибирати ПЗ в залежності від місць з критичною інформацією та від можливостей під час захисту ІС.

За станом об’єкта атаки, найпростішим в реалізації є стан «обробки», тому що під час дій користувача проведення атаки може залишитись непомітним для звичайного користувача. Тоді як проведення атаки зі станом об’єкта «збереження» вимагає більш складних дій, які важко не помітити навіть звичайному користувачу.

Також важливо згадати про вплив небезпечних дій та загрози, які з’являються в їх результаті. Щодо небезпечних дій, то будь який вид таких дій

здатен нанести значний збиток інформаційній системі, але це залежить від швидкості відновлення та локалізації шкоди, які можуть суттєво відрізнятися. Отже і види загроз, які з’являються в їх результаті, відрізняються як цілями, з якими вони реалізовуються, так і об’єктами, на які вони націлені.

Підводячи підсумок з аналізу ознак загроз для систем захисту інформації, можна зазначити, що всі ознаки хоч і мають різну ступінь важливості, розповсюдженості та ймовірності реалізації, тому захист від загроз повинен бути обґрунтований на критичності компонентів системи, яким можуть бути нанесені збитки.

2.2 Загрози безпеці інформації в інформаційних системах

Загрози циркулюючої в ІС інформації, як правило, залежать від структури та конфігурації ІС, технології обробки інформації в ній, стану навколишнього фізичного середовища, дій персоналу і структури самої інформації [17].

З множини способів класифікації загроз інформації найбільш узагальненою (базовою) є їх класифікація за наслідками можливого впливу на інформацію:

– загрози порушення конфіденційності;

– загрози порушення цілісності;

– загрози порушення доступності.

Згідно Закону «Про доступ до публічної інформації» до конфіденційної інформації відноситься інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Загрози конфіденційності направлені на отримання доступу до інформації, до якої відсутні повноваження на такий доступу. У разі реалізації цих загроз інформація, до якої обмежений доступ стає відомою стороннім особам.

Також така інформація, згідно Закону «Про інформацію» належить до інформації з обмеженим доступом так саме як таємна та службова інформація.

Така загроза має місце щоразу, коли можливий несанкціонований доступ до інформації, що зберігається в комп'ютерній системі або передається від однієї системи до іншої.

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила її отримання.

Загрози цілісності інформації направлені на неправомірну її зміну або спотворення, що призводить до порушення або повного знищення. Цілісність інформації може бути порушена умисно, а також у результаті дій з боку середовища, що оточує систему. Ця загроза особливо актуальна для систем передачі інформації, комп'ютерних мереж і систем телекомунікацій. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (знищення).

Загрози доступності (відмова в обслуговуванні) направлені на створення таких ситуацій, коли певні умисні дії або ускладнюють працездатність ІС, або унеможливлюють доступ до деяких її ресурсів інформаційної системи.

Розрізняють наступні види комп’ютерних злочинів [17].

1) Несанкціонований доступ до інформації.

2) Підробка комп'ютерної інформації.

3) Введення у програмне забезпечення «логічних бомб» – невеликих програм, які спрацьовують з настанням певних умов і можуть призвести до часткового або повного виведення системи з ладу.

4) Розробка і поширення комп'ютерних вірусів.

5) Злочинна недбалість у розробці, виготовленні та експлуатації комп'ютерної техніки та програмного забезпечення.

6) Комп'ютерні злочини в мережі Інтернет.

До загроз безпеки в інформаційних системах також відносяться ненавмисні суб’єктивні погрози та навмисні погрози [18].

До ненавмисних суб’єктивних погроз слід віднести наступне.

1) Ненавмисні дії людей, персоналу, що приводять до часткового або повного виходу інформаційних систем з ладу.

2) Неправомірне використання устаткування або зміни режимів робіт цього устаткування.

3) Ненавмисне псування носіїв інформації.

4) Нелегальне використання неліцензійних програм і устаткування.

5) Порушення атрибутів, правил, розмежувань тощо.

6) Неправильне проектування архітектури системи, у яку заздалегідь закладені «люки», «лази» і «дірки» для стороннього порушника. Ігнорування сторонніх порушень.

7) Вхід у інформаційну систему в обхід установлених правил.

8) Введення помилкових даних та інші.

До основних навмисних погроз слід віднести наступні злочинні дії.

1) Фізичне руйнування системи.

3) Дезорганізація комп’ютерної або обчислювальної системи.

4) Впровадження в число персоналу «зацікавленої» людини.

5) Навмисна погроза: шантаж, погроза персоналу комп'ютерної системи.

6) Застосування засобів технічних розвідок: фотографування, підслуховування тощо.

7) Перехоплення побічних електромагнітних випромінювань і наведень.

8) Перехоплення переданих даних по каналу зв'язку тощо.

9) Розкрадання носіїв інформації.

10) Незаконне одержання правил і атрибутів розмежування доступу.

11) Незаконне використання терміналів законних користувачів з метою проникнення в систему під іменем санкціонованого користувача.

12) Розкриття шифрів криптозахисту санкціонованих користувачів.

13) Упровадження закладок типу «троянських коней», «жучків», «пасток» і т.д. з метою впровадження недекларованого програмного забезпечення санкціонованих користувачів.

14) Незаконне підключення до ліній передачі даних з метою роботи між рядків, видаючи себе за законного користувача та інші.

2.3 Види та схеми атак

Спрощена класифікація, яка відображає найбільш типові атаки, може бути може бути представлена таким чином [18].

1) Віддалене проникнення або віддалене керування комп’ютером через мережу. Використовуючи програми віддаленого доступу можна здійснювати управління та адміністрування віддаленого комп'ютера в реальному часі.

2) Локальне проникнення, отримання НСД до вузлів, на яких ініційовані атаки.

3) Віддалена відмова в обслуговуванні. Це саме мережева атака, яка спрямована на порушення, гальмування функціонування системи. Тобто головна мета зловмисників досягти перевантаження комп’ютера таким чином, щоб після цього він не зміг відповідати на запити користувачів.

4) Мережева розвідка, а саме – збір інформації про мережу за допомогою загальнодоступних даних і додатків. Тобто проводиться збір даних про ІС,

використовуючи сканування портів, запит DNS, перевірка захисту комп’ютера і перевірка системи. Таку розвідку проводять перед серйозною цілеспрямованої атакою.

5) Використання сканерів вразливостей. Вони призначені для пошуку вразливостей на локальних та віддалених комп’ютерах. Такі сканери системні адміністратори використовують як діагностичні інструменти.

6) Злам паролів – це процес відновлення паролів з даних, які були збережені або передані за допомогою ІС. Існує два підходи до реалізації цієї атаки. Перший, більш розповсюджений, підхід полягає в тому, щоб підбором вгадати пароль. Другий – в тому, щоб змінити пароль, який ви начебто забули.

7) Пасивне прослуховування мережі, під час якого здійснюється несанкціоноване прослуховуванні пакетів від протоколів маршрутизації. Пасивна атака спрямована на розкриття конфіденційних даних. Під час проведення такої атаки комп’ютер зловмисника повинен знаходитись в тій самій локальній мережі, що і комп’ютер, стосовно якого проводиться атака. У цьому випадку весь інформаційний обмін в мережі стає доступним для зловмисника.

З вищезазначеного видно, що види загрози безпеці інформації можна розділити на різні групи. Тому при побудові системи захисту та виборі засобів захисту важливо з’ясувати які групи загроз є більш пріоритетними та на які важливо звернути більшу увагу. Наприклад, загрози НСД з боку працівників або введення у програмне забезпечення «логічних бомб» є одними з найбільш небезпечних видів загроз. В той час, як фізичне руйнування системи, перехоплення побічних електромагнітних випромінювань і наведень або розкрадання носіїв інформації є зазвичай менш ефективне.

Також зі спрощеної класифікації атак видно, що деякі типові атаки не становлять велику загрозу та досить прості в запобіганні. Але зазвичай такі атаки використовують як допоміжний засіб при більш складних та небезпечних атаках. Але важливо не нехтувати ними при розгляді можливих атак та при виборі засобів захисту.

2.4 Тенденції кібератак, що взяті до уваги в 2023 році

Розглядаючи тенденції кібератак в 2023 році неможна не згадати про аналітичний звіт Держспецзв’язку «RUSSIA’S CYBER TACTICS H1’2023». В

цьому звіті можна побачити детальний аналіз за першу половину 2023 року та основні висновки щодо кібернападів Росії проти України.

Перше про що варто сказати – це цільові сектори атак, які представлено на рисунку 2.1 [19]. З цього переліку видно, що цілі при реалізації кібератак значно не змінились, порівняно з 2022 роком.

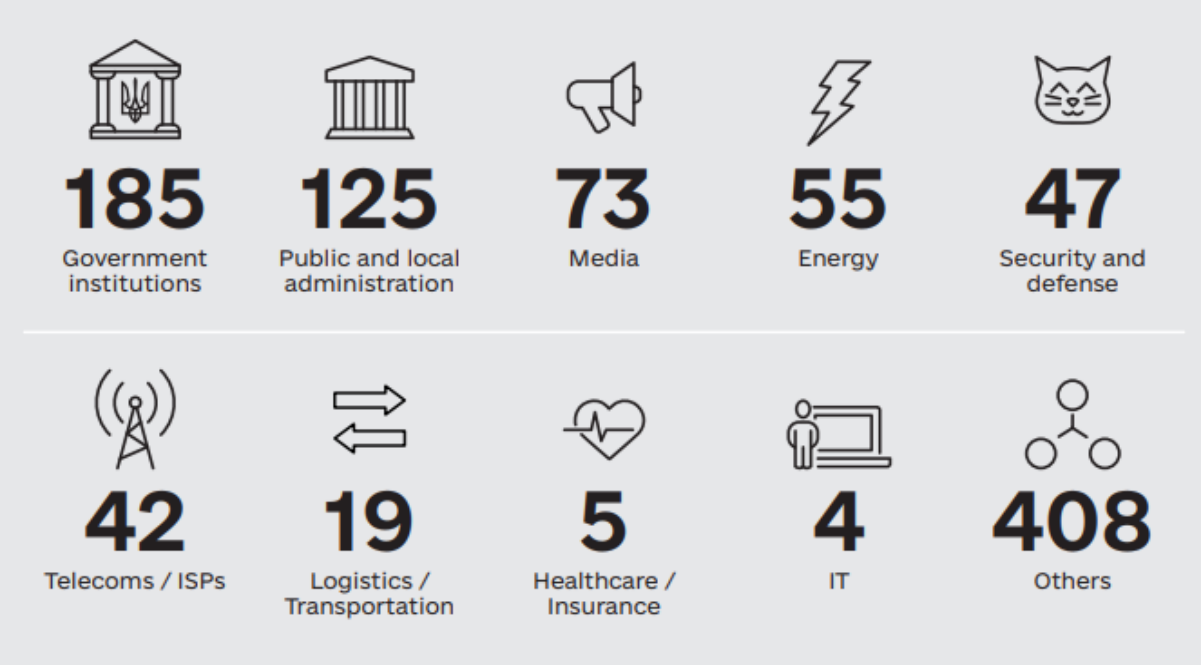

Рисунок 2.1 – Цільові сектори російських кібероперацій

Далі представлений перелік тенденцій в атаках на першу половину 2023 року з порівнянням даних за 2022 рік [19].

1) Перше про що варто сказати, це про зростання кількості зареєстрованих інцидентів у першій половині 2023 року. За даними звіту, у другому півріччі 2022 року було зареєстровано 342 кібератаки, у середньому 57 на місяць та 1 – 2 на день. А за 6 місяців у 1 півріччі 2023 року зареєстрованих кібернападів вже було 762, у середньому 128 на місяць, 4 – 5 на день.

2) Зростання кількості критичних інцидентів у 1 півріччі 2023 року. У 2 півріччі 2022 року зареєстровано 144 критичні інциденти, а в 1 півріччі 2022 року – 319 інцидентів. На відміну від цього за 1 півріччя 2023 року зареєстровано лише 27 критичних інцидентів.

3) Зниження рівня високих та критичних інцидентів у 1 півріччі 2023 року. Порівняно з другою половиною 2022 року (сталося 339 інцидентів високого та критичного рівня) та з першою половиною 2022 року (сталося 683 інцидентів

високого та критичного рівня) кількість таких інцидентів в першій половині 2023 року значно зменшилась і становить 183 інциденти високого та критичного рівня.

4) Зниження швидкості розповсюдження шкідливих програм електронною поштою. Показник становив 290 випадків у другій половині 2022 року, де домінувало зловмисне програмне забезпечення. А у першому півріччі 2023 року показник вже дорівнював 138 випадків, де домінував фішинг порівняно зі спробами поширення зловмисного програмного забезпечення.

5) Зниження рівня атак на енергетику та зменшення на 50 % випадків критичних інцидентів. У другій половині 2022 року відбувся 141 інцидент, з яких 16 є критичними із зареєстрованим впливом. А у першому півріччі 2023 року вже цей показних сягнув 55 інцидентів, з яких 8 є критичними із зареєстрованим впливом.

6) Зменшення кількості випадків з серйозним впливом. у і півріччі 2023 року. У другій половині 2022 року – 30 руйнівних спроб та 518 ефективних операцій, а у першій половині 2023 року – 34 руйнівні спроби та 267 ефективних операцій.

Узагальнюючи данні зі звіту Держспецзв'язку щодо кібератак в 2023 році, можна сказати, що хоч і зросла загальна кількість інцидентів, але в першій половині 2023 року ефективність проведених атак значно зменшилась, що свідчить про великий успіх і що є результатом посилення безпеки та зусиль CERT-UA.

Також говорячи про тенденції кібератак важливо розглянути наступні варіанти, як можливі атаки.

1) Атаки на 5G пристрої. Інфраструктура, створена провайдерами 5G, стане об'єктом кібератак. Такі пристрої сприятливі для DDoS атак, також технологія 5G базується на принципах SDN (від англ. Software-defined Networking), через що мережевий трафік легше контролювати та потенційно використовувати. Інша проблема безпеки полягає в тому, що використання 5G технологій багаторазового радіодоступу може створювати вразливості [20].

Щоб запобігти атакам такого виду необхідно не тільки перевіряти надійність прошивку, бо деякі виробники вбудовують у свої розробки не надійнішу прошивку, а й пам'ятати, що постачальники мережі повинні перевіряти як добре захищені їх мережі та чи належним чином зашифрований трафік. Також, щоб захиститися від цього, мережеві провайдери повинні переконатися, що їхні

мережі належним чином налаштовані та відстежуються на предмет будь-якої підозрілої активності [22].

2) Обхід одноразового пароля. Ця атака розроблена для подолання багатофакторної ідентифікації (або MFA) та вважається ефективною, бо може зупинити спроби неавторизованого входу до облікового запису. Зловмисники намагаються обійти MFA кількома методами. Наприклад, повторно використовуючи одноразовий пароль, використовуючи одноразовий пароль отриманий від іншого облікового запису, використовуючи викрадений одноразовий пароль та за допомогою переконання користувача у необхідності зміни паролю для подальшої його передачі [20].

Цей вид атаки орієнтований на недосвідчених користувачів, для запобігання цієї атаки в будь-якому її прояві необхідно дотримуватися правил використання одноразовим паролем та стандартів щодо їх реалізації, наприклад, RFC 1760 (S/Key), RFC 2289 (OTP), RFC 4226 (HOTP) та RFC 6238 (TOTP).

3) Атаки, приурочені до значних світовий подій. Злочинні групи хакерів усвідомлюють, що значні світові події та катастрофи можна монетизувати. Фішингові атаки, приурочені до значних подій, націлені на людей, які перебувають у стані стресу і через це стають менш уважними та обережними. Використовуючи методи соціальної інженерії, зловмисники вдаються до тактики викликання емоцій [20].

Тому потрібно бути особливо уважними до подібних спроб шахрайства та намагатися зберігати емоційну стабільність, а у разі якщо це неможливо, максимально обмежити свій доступ до речей через які зловмисники можуть мати негативний вплив.

4) Фішинг та його види, наприклад смішинг. Наразі смішинг приходить на зміну фішингу. Бази даних з номерами можна купити онлайн, тому зловмисники цим користуються та створюють повідомлення, які викликають довіру.

Щоб уникнути ситуацій, необхідно критично обмірковувати та перевіряти будь-яку інформацію, як надходить з невідомих номерів, навіть якщо вони видають себе за відомих вам осіб.

5) Шкідливе програмне забезпечення саме для мобільних пристроїв [20]. Для попередження цього обов’язково потрібно переконатися, що встановлене мобільне антивірусне програмне забезпечення є надійним та ефективним, що воно зможе не тільки виявляти віруси, а й запобігати зараженню ними..

6) Удосконалений фішинг із використанням штучного інтелекту та машинного навчання. Зловмисники удосконалюють фішинг за допомогою штучного інтелекту та машинного навчання, тому тепер такі листи бездоганно виглядають, нічим не відрізняється від листів певної компанії та є персоналізованим, що збільшує процент користувачів, у яких такі листи викликають довіру [20].

Отже потрібно бути дуже уважними при отриманні листів, які мають особисту інформацію про вас та мають посилання, за якими в листі просять перейти, або файли, які просять завантажити.

2.5 Огляд ризиків безпеки

Інтерфейс прикладного програмування (від англ. API) допомагає пришвидшити розробку програмного забезпечення, яке в свою чергу використовується в ІС. Тому слід дослідити які є ризики безпеки при використанні API. Існує багато досліджень на цю тему, але найкращим рішенням є використання досліджень від OWASP.

Open Worldwide Application Security Project (OWASP) — некомерційна організація, яка працює над підвищенням безпеки програмного забезпечення. Такий інформаційний документ як «OWASP Top 10 API Security Risks» допоможе зосередитися на підвищенні обізнаності про загальні слабкі місця безпеки API [21]. Обізнаність в слабких місцях допоможе не тільки краще зрозуміти існуючі ризики, а й знайти краще рішення задля їх зменшення. Розглянутий перелік значно полегшує вивчення ризиків для подальшого їх аналізу та попередження.

Топ–10 ризиків безпеки API OWASP – 2023 [21].

API1:2023 – порушена авторизація на рівні об’єкта. API, як правило, розкривають кінцеві точки, які обробляють ідентифікатори об’єктів, створюючи широку поверхню для атаки проблем із керуванням доступом на рівні об’єктів. Перевірки авторизації на рівні об’єкта слід враховувати в кожній функції, яка отримує доступ до джерела даних за допомогою ідентифікатора користувача.

API2:2023 – порушена автентифікація. Механізми автентифікації часто реалізуються неправильно, що дозволяє зловмисникам скомпрометувати токени автентифікації або використовувати недоліки реалізації, щоб тимчасово або назавжди присвоїти ідентифікаційні дані інших користувачів. Порушення

здатності системи ідентифікувати клієнта/користувача порушує загальну безпеку API.

API3:2023 – авторизація на рівні властивості зламаного об’єкта. Ця категорія об’єднує API3:2019 Excessive Data Exposure та API6:2019 – Mass Assignment, зосереджуючись на першопричині: відсутність або неправильна перевірка авторизації на рівні властивості об’єкта. Це призводить до викриття інформації або маніпулювання неавторизованими сторонами.

API4:2023 – необмежене споживання ресурсів. Для задоволення запитів API потрібні такі ресурси, як пропускна здатність мережі, ЦП, пам’ять і сховище. Інші ресурси, такі як електронні листи/SMS/телефонні дзвінки чи перевірка біометричних даних, надаються постачальниками послуг через інтеграцію API та оплачуються за запит. Успішні атаки можуть призвести до відмови в обслуговуванні або збільшення операційних витрат.

API5:2023 – порушена авторизація на рівні функції. Складні політики контролю доступу з різними ієрархіями, групами та ролями, а також нечітким розподілом між адміністративними та звичайними функціями, як правило, призводять до помилок авторизації. Використовуючи ці проблеми, зловмисники можуть отримати доступ до ресурсів інших користувачів і/або адміністративних функцій.

API6:2023 – необмежений доступ до конфіденційних бізнес–потоків. API, уразливі до цього ризику, піддають бізнес–потоку, як–от купівля квитка чи публікація коментаря, не компенсуючи того, як ці функції можуть зашкодити бізнесу, якщо їх надмірно використовувати в автоматизованому режимі. Це не обов’язково відбувається через помилки реалізації.

API7:2023 – підробка запитів на стороні сервера. Підробка запитів на стороні сервера (SSRF) може виникати, коли API отримує віддалений ресурс без перевірки наданого користувачем URI. Це дозволяє зловмиснику змусити програму надіслати створений запит до несподіваного пункту призначення, навіть якщо він захищений брандмауером або VPN.

API8:2023 – неправильна конфігурація безпеки. API та системи, які їх підтримують, зазвичай містять складні конфігурації, призначені для того, щоб зробити API більш настроюваними. Інженери програмного забезпечення та DevOps можуть пропустити ці конфігурації або не дотримуватися найкращих практик безпеки, коли йдеться про конфігурацію, відкриваючи двері для різних типів атак.

API9:2023 – неналежне управління запасами. API, як правило, відкривають більше кінцевих точок, ніж традиційні веб–додатки, що робить правильну й оновлену документацію надзвичайно важливою. Правильна інвентаризація хостів і розгорнутих версій API також важлива для пом’якшення таких проблем, як застарілі версії API та відкриті кінцеві точки налагодження.

API10:2023 – небезпечне використання API. Розробники, як правило, більше довіряють даним, отриманим від сторонніх API, ніж введеним користувачами, тому, як правило, застосовують слабкіші стандарти безпеки. Щоб скомпрометувати API, зловмисники шукають інтегровані сторонні служби замість того, щоб намагатися скомпрометувати цільовий API безпосередньо.

Аналізуючи ці ризики безпеки, видно, що лише один з них, а саме API4,має середню можливість використання на відміну від інших, у яких вона проста. Далі для порівняння їх між собою можна розглянути їх ступінь виявлення та розповсюдженість, у більшості ступінь виявлення – легкий, окрім API6, API9 та API10 у яких він – середній. Щодо розповсюдженості, то половина ризиків відноситься до поширених, а інші до широко поширених. Також розглядаючи технічну специфічність то половині ризиків присвоєний помірний рівень, а іншій половині серйозний.

2.6 Види загроз для комп'ютерних мереж

Основні види порушень інформаційної безпеки надані в таблиці 2.1 та в таблиці 2.2 [26].

Таблиця 2.1 – Найрозповсюдженіші джерела атак

Джерело атак (назва)	Джерело атак (%)
Недобросовісні співробітники	81
Хакери	77
Конкуренти	44
Зарубіжні компанії	26
Зарубіжні уряди	21

Таблиця 2.2 – Найрозповсюдженіші типи атак

Тип атаки	Частота виявлення (%)
Віруси	85

Зловживання в Інтернеті із боку співробітників	79
Несанкціонований доступ з боку співробітників	71
Відмова в обслуговуванні	27
Атаки зовнішніх зловмисників	25
Крадіжка конфіденційної інформації	20
Саботаж	17
Фінансові шахрайства	11
Шахрайства з телекомунікаційними пристроями	11

Для запобігання атак, пов’язаних з діями недобросовісних співробітників, необхідно, по-перше, запобігати можливість таких дій для співробітників, в тому числі для нових співробітників, які не мають позитивної репутації та не викликали довіри в їх добросовісності. Це можна досягти розмежовуючи доступ таких співробітників до інтернет ресурсів, інформації з обмеженим доступом (ІзОД), приміщень, де зберігається та оброблюється ІзОД за допомогою персональних перепусток тощо. Для запобігання атак з зовнішньої сторони, необхідно, по-перше, вибрати оптимальний комплекс засобів захисту (КЗЗ), який буде запобігати та виявляти можливі атаки, з урахуванням діяльності підприємства. По-друге, КЗЗ повинно складатися з засобів, для яких не припинено підтримку від виробника.

Основні загрози.

– потрапляння в інформаційну систему шкідливого програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем [23];

– атаки хакерів (кібератака) – спрямовані дії в кіберпросторі з утручанням у роботу інформаційно–телекомунікаційних систем з метою порушення конфіденційності, цілісності, доступності, авторства інформації; або контролю, зміни в роботі, вимкнення, знищення обчислювальних механізмів чи інфраструктури [24];

– BotNet – це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами – автономним програмним забезпеченням [23];

– DdoS – атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні – напад на інформаційну систему з наміром зробити комп'ютерні

ресурси недоступними користувачам, для яких інформаційна система була призначена [23];

– фішинг та його види – вид шахрайства, метою якого є виманювання персональних даних у клієнтів онлайн–аукціонів, сервісів з переказу або обміну валюти, інтернет–магазинів тощо [23];

– крадіжка коштів – використання можливостей несанкціонованого доступу до платіжних даних (реквізитів платіжних карток, паролів та ключів доступу до інтернет–банкінгу) або повного доступу до комп'ютеру (за рахунок його зараження шкідливим програмним забезпеченням) для проведення фінансових операцій [25];

– «крадіжка особистості» (Identity Theft) – несанкціоноване заволодіння персональними даними особи, що дозволяє зловмиснику здійснювати діяльність (підписувати документи, отримувати доступ до ресурсів, користуватися послугами тощо) від її імені (як один із механізмів підтвердження автентичності особи може використовуватись електронний цифровий підпис) [25].

Наразі великий відсоток атак проводиться успішно, саме через недбалість, необізнаність або недобросовісність персоналу. Для запобігання багатьох атак, буде достатньо регулярно проводити навчання співробітників щодо інформаційної безпеки з метою інформування про нові види атак та про методи їх ідентифікації та запобігання.

Комп'ютерні злочини за способом їх здійснення поділяються на [26]:

– методи перехоплення;

– методи несанкціонованого доступу;

– методи маніпуляції.

Комп'ютер є об'єктом правопорушення, коли мета злочинця – викрасти інформацію або завдати шкоди системі, що цікавить його. З комп'ютером як з об'єктом пов'язані такі види злочинів [26]:

– вилучення засобів комп'ютерної техніки;

– розкрадання інформації;

– розкрадання послуг;

– пошкодження системи;

– уівинг (заплутування слідів, коли метою атаки є прагнення приховати своє ім'я і місцезнаходження).

Зарубіжними фахівцями розроблені різні класифікації способів учинення комп'ютерних злочинів. Нижче наведено назви способів учинення подібних

злочинів, відповідних кодифікатору Генерального Секретаріату Інтерполу. Всі коди, які характеризують комп'ютерні злочини, мають ідентифікатор, що починається з літери Q. Для характеристики злочинів можуть використовуватися до п'яти кодів, розташованих у порядку убування значущості [26].

1) QA – несанкціонований доступ і перехоплення: QAH – комп'ютерний абордаж, QAI – перехоплення, QAT – крадіжка часу, QAZ – інші види несанкціонованого доступу і перехоплення.

2) QD – зміна комп'ютерних даних: QDL – логічна бомба, QDT – троянський кінь, QDV – комп'ютерний вірус, QDW – комп'ютерний черв'як, QDZ – інші види зміни даних.

3) QF – комп'ютерне шахрайство: QFC – шахрайство з банкоматами, QFF – комп'ютерна підробка, QFG – шахрайство з ігровими автоматами, QFM – маніпуляції з програмами введення–виводу, QFP – шахрайства з платіжними засобами, QFT – телефонне шахрайство, QFZ – інші комп'ютерні шахрайства.

4) QR – незаконне копіювання: QRG – комп'ютерні ігри, QRS – інше програмне забезпечення, QRT – топографія напівпровідникових виробів, QRZ – інше незаконне копіювання.

5) QS – комп'ютерний саботаж: QSH – з апаратним забезпеченням, QSS – з програмним забезпеченням, QSZ – інші види саботажу.

6) QZ – інші комп'ютерні злочини: QZB – з використанням комп'ютерних дошок об'яв, QZE – розкрадання інформації, що складають комерційну таємницю, QZS – передача інформації конфіденційного характеру, QZZ – інші комп'ютерні злочини.

Наявність такої кодифікації спрощує характеристику злочинів, при комунікації спеціалістів в сфері кіберзлочинності, до того ж така кодифікація є міжнародною. Набагато легше при спілкуванні та повідомленні інформації щодо злочинів вказати лише його код, ніж писати повністю назву, тому таку кодифікацію бажано використовувати всім спеціалістам у сфері кіберзлочинів.

3 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВІД ЗАГРОЗ БЕЗПЕКИ ДЛЯ ІНФОРМАЦІЙНИХ СИСТЕМ

3.1 Аналіз типової інформаційної системи на прикладі корпоративної комп’ютерної мережі

Сучасний підхід до вибору засобів захисту для типової комп'ютерної мережі передбачає обов'язкове створення моделі загроз. Така модель створюється на основі даних про ресурси комп'ютерної мережі та аналізу її вразливостей і являє собою абстрактний структурований опис загроз, притаманних певній системі [27].

3.1.1 Узагальнена схема типової інформаційної системи.

Почнемо з опису типової корпоративної комп’ютерної мережі, схема якої зображена на рисунку 3.1.

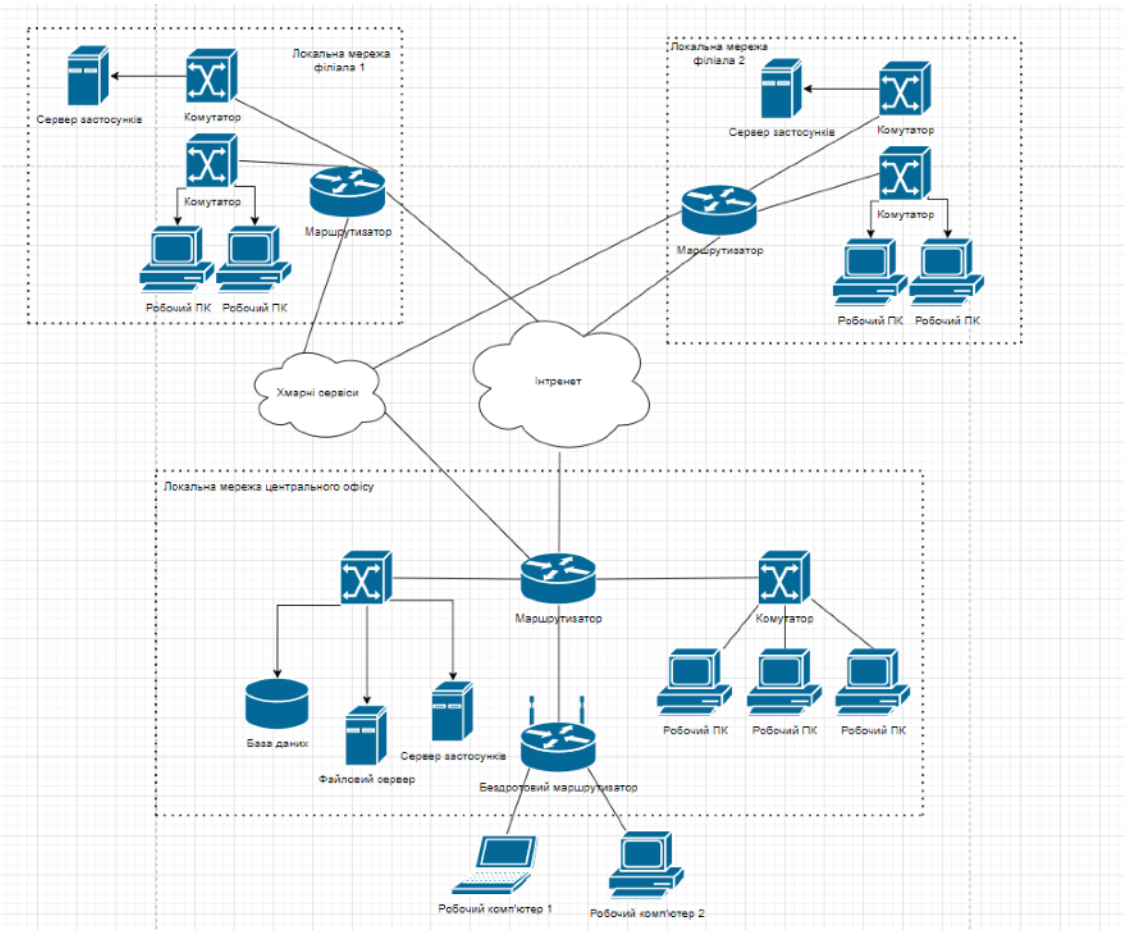

Рисунок 3.1 – Схема типової корпоративної комп’ютерної мережі

На схемі видно, що мережа, що розглядається складається з декількох частин.

1) Локальної мережі центрального офісу:

– файловий сервер;

– база даних;

– сервер застосунків;

– маршрутизатор;

– декілька комутаторів;

– комп’ютери користувачів.

2) Декількох 2 – 5 локальних мереж філіалів (їхня структура повторює центральну мережу за виключенням відсутності бази даних та файлового серверу).

3) Хмарних сервісів (зазвичай це програмні комплекси та віртуальні машини).

Слід зазначити, що на даному етапі розглядаються лише ресурси мережі, тому на схемі відсутні типові засоби захисту, такі як мережеві екрани.

Після опису складових інформаційної системи, слід також створити модель цінності інформаційних ресурсів. Цінність інформації залежить від декількох факторів. Перший – це час, так як з часом цінність інформації може зменшуватися та навіть стати від’ємною, тобто факт існування такої інформації буде шкідливим. Також цінність інформації залежить від таких класичних властивостей інформації як, цілісність, доступність та конфіденційність. Тож другий фактор – цілісність інформації, звісно якщо дані пошкоджені вони втрачають свою цінність. Конфіденційність та доступність інформації також можуть впливати на її цінність. У комп’ютерній системі яку ми розглядаємо найбільшу цінність має інформація, що міститься у базі даних та на файловому сервері центральної комп’ютерної мережі, оскільки там можуть міститися особисті дані клієнтів, яких обслуговує організація.

3.1.2 Аналіз ресурсів інформаційної системи.

Інформаційна система є деякою кількістю взаємодіючих ресурсів, кожен з яких може стати об'єктом атаки або зазнати впливу при атаці на інший ресурс ІС.

Класифікація ресурсів інформаційної системи представлена на рисунку 3.2.

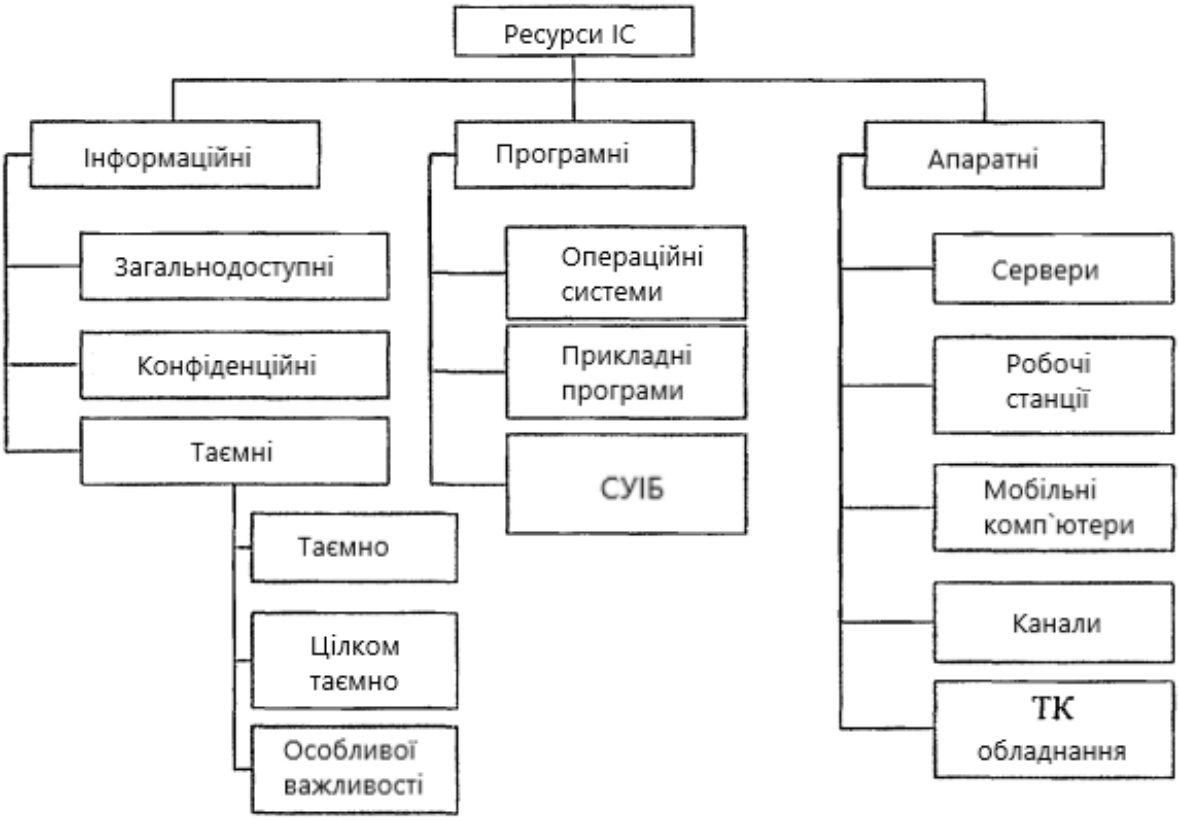

Рисунок 3.2 – Класифікація ресурсів інформаційної системи

Ресурси інформаційної системи поділяються на [28]:

– інформаційні ресурси – окремі документи та окремі масиви документів, документи та масиви документів в інформаційних системах;

– програмне забезпечення – операційні системи (ОС) та прикладні програми, що функціонують в ІВ;

– технічні засоби – файлові сервери, робочі станції, комутатори, маршрутизатори тощо.

Ця модель повною мірою розкриває безліч ресурсів ІС. До недоліків моделі відноситься те, що в ній не розглядаються бізнес-процеси ІС та зв'язок ресурсів з цими процесами, а також не вказуються зв'язки між ресурсами. У ній не виявляється, у яких апаратних складових ІС зберігається інформація, що це за інформація, якими каналами вона передається, з використанням яких програм обробляється тощо. Таким чином, неможливо визначити як, вплив на певний ресурс ІС вплине на безпеку інших ресурсів та бізнес-процесів, що підтримуються ІС в цілому.

3.2 Модель загроз та вразливостей типової інформаційної системи

Тут слід детальніше зупинитися на різниці між поняттями «загроза» та «вразливість».

Вразливість – це властиві об’єкту інформатизації причини, які призводять до порушення безпеки інформації на конкретному об’єкті та зумовлені вадами процесу функціонування об’єкта інформатизації, властивостями архітектури інформаційно-телекомунікаційної системи, протоколами обміну та інтерфейсами, що застосовуються програмним забезпеченням і апаратними засобами, умовами експлуатації [29].

Загроза – це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об’єкта захисту (інформаційних ресурсів), яке наносить збиток власнику або користувачу, що проявляється як небезпека спотворення або втрати інформації [29]. Тобто, підсумовуючи наведені вище визначення, можна сказати, що вразливість це недосконаліть у системі, а загроза – це вразливість, що потенційно може бути використана для реалізації атаки.

На наступному етапі модель загроз використовується для створення моделі порушника – опису потенційного зловмисника та загроз які він може використати для атаки, враховуючи його можливості та бюджет. Нарешті, на основі моделі порушника та визначеної для даної системи цінності інформаційних ресурсів обтираються технічні та програмні засоби безпеки інформації, що мають бути використані в комп’ютерній мережі.

Далі, проаналізуємо основні вразливості такої комп’ютерної мережі. Загалом їх можна розділити на вразливості у програмному забезпечені та вразливості апаратного забезпечення.

У свою чергу програмні вразливості можна розділити на вразливості мережевих протоколів зв’язку, вразливості кінцевих точок, а також вразливості хмарних сервісів. Проте, перш ніж скористатися останніми зловмисник має потрапити на робочу станцію або сервер. Для аналізу найбільш поширених вразливостей мережних протоколів будемо використовувати мережеву модель OSI, яка представлена на рисунку 3.3.

Рисунок 3.3 – Модель взаємодії відкритих систем

На канальному рівні, є протокол протокол визначення адрес (ARP) (від англ. Address Resolution Protocol), що слугує для визначення MAC-адрес всередині локальної мережі. Вразливість полягає в тому, що хост не може перевірити від якого хоста надійшов мережевий пакет. Це створює можливості для підміни ARP.

Суттєві вразливості має і протокол передавання файлів прикладного рівня (FTP) (від англ. File Transfer Protocol), він призначений для віддаленої передачі файлів. Не шифрує дані, тобто імена та паролі користувачів передаються у вигляді відкритого тексту. Таку саму вразливість має і протокол Telnet.

Свої вразливості мають і протоколи управління передачею транспортного рівня (TCP) (від англ. Transmission Control Protocol) та датаграм користувача (UDP) (від англ. User Datagram Protocol). Однією з вразливостей TCP є можливість появи так званих «напіввідкритих з'єднань», що може бути використано для переповнення черги на підключення на сервері. У свою чергу UDP також за замовчуванням не шифрується.

Вразливості кінцевих точок розділимо за місцем їх появи у системі:

– операційна система;

– прикладні програми;

– сервісні утиліти.

Навіть у типовій інформаційній системі, що розглядається, можна виділити дуже велику кількість вразливостей, тому всеохоплюючий аналіз вразливостей, і відповідно модель загроз, не є доцільними. Виділимо кілька поширених

вразливостей кінцевих точок. Для цього будемо використовувати класифікацію CWE (від англ. Common Weaknees Enumeration), вона являє собою список слабких місць програмного забезпечення, що підтримується корпорацією MITRE.

CWE-89 – SQL ін'єкція, вразливість, яка дозволяє зловмиснику за допомогою специфічних запитів отримувати доступ до конфіденційних даних у базі. Одна з найпоширеніших вразливостей реляційних баз даних.

CWE-121 – переповнення буфера: як зрозуміло з назви, ця вразливість виникає коли у буфер записується більше даних ніж він може вмістити. Часто це дозволяє зловмиснику виконувати довільний код.

CWE-434 с завантаження файлу з небезпечним розширенням. Завантаження потенційно небажаних файлів, як правило з розширенням «.exe» або «.bat», очевидно, що деякі користувачі можуть запускати такі файли, чим і користуються зловмисники під час фішингових атак.

CWE-362 – «Race Conditions». Ця вразливість виникає при спільному доступі до ресурсів, наприклад одного запису у базі даних. Може бути критичною коли синхронізація відсутня у критично важливому коді, наприклад такому, що відповідає за аутентифікацію.

CWE-798 – «хардкодинг» конфіденційних даних. Програмний код продукту містить задані прямо у коді дані. Це може бути, наприклад пароль адміністратора чи криптографічний ключ. Цю, здавлося б, тривіальну проблему іноді буває досить складно знайти у великих продуктах з десятками тисяч рядків коду.

Вразливості хмарних технологій є окремою великою темою, проте зазвичай основним недоліком їх використання з точки зору безпеки інформації є необхідність беззаперечної довіри до третьої сторони, тобто надавача ресурсів, якому доступні дані, які зберігаються у хмарі.

Проаналізувавши наявні вразливості та визначивши найбільш цінні інформаційні ресурси, можна перейти до моделі загроз. У Додатку до НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі», рекомендується наступна структура опису загрози:

– властивості інформації або АС, на порушення яких спрямована загроза;

– джерела виникнення загрози (зовнішні або внутрішні суб'єкти);

– можливі способи реалізації загрози.

Використовуючи таку структуру опису загроз та врахувавши аналіз вразливостей та цінність інформаційних ресурсів що наведені вище, опишемо модель загроз для типової корпоративної комп'ютерної мережі. Також важливо

зазначити, що це буде дуже обмежена модель, оскільки побудова всеосяжної моделі загроз такої системи – дуже складна, комплексна задача. Тому тут наведені приклади опису загроз, лише згідно з розглянутими попередньо вразливостями.

1) Несанкціонований доступ зловмисника до бази даних. Ця загроза може бути спрямована на порушення цілісності конфіденційності та доступності. Джерелами цієї загрози як правило є зовнішні відносно інформаційної системи суб'єкти. Для реалізації загрози зловмисники можуть використовувати вразливості CWE-89 (конфіденційність, цілісність) та CWE-362 (доступність). Загроза може бути реалізована зокрема шляхом формування специфічних засобів до реляційної бази даних або ж підробкою інформації у базі даних під час «Race Conditions».

2) Віддалене виконання шкідливого коду всередині локальної мережі. Ця загроза також може бути спрямована на порушення цілісності конфіденційності та доступності інформації, а також спостережності та керованості інформаційної системи в цілому. Джерелами цієї загрози можуть бути як внутрішні так і зовнішні суб'єкти інформаційної мережі. Для реалізації такої загрози може використовуватися зокрема CWE-434 в комбінації з «Code Injection».

3) Перевантаження мережі. Спрямована передусім на порушення доступності інформації та керованості інформаційної системи. Джерелами цієї загрози є зовнішні відносно інформаційної системи суб'єкти. Може бути реалізована за допомогою надсилання великої кількості запитів для перевантаження каналів зв'язку. Також для реалізації цієї загрози можуть використовуватися протоколи транспортного рівня, в якості прикладу можна навести атаку SYN flood.

Тепер можна перейти до моделі порушника. Власне, всіх порушників, можна розділити на зовнішніх та внутрішніх. Очевидно, що внутрішні порушники, або «інсайдери» є набагато небезпечнішими для інформаційної системи, оскільки можуть мати у системі права адміністратора та не потребують отримання доступу до мережі ззовні.

Згідно [27] модель порушника – абстрактний формалізований чи неформалізований опис порушника. Моделі загроз і порушника є вихідною інформацією для розроблення політики безпеки і проектування будь-яких систем захисту. При її створенні слід врахувати модель загроз, та визначити, які з описаних загроз порушник з більшою вірогідністю буде використовувати для реалізації атаки. У НД ТЗІ 1.4-001-2000 рекомендується така структура для опису моделі порушника:

– категорія осіб, до якої може належати порушник;

– мета порушника;

– повноваження порушника в системі;

– технічна оснащеність порушника;

– кваліфікація порушника.

На основі цієї структури опишемо модель потенційного порушника у нашій мережі.

Скоріше за все, це буде людина, що не має відношення до організації, тобто зовнішній порушник. Втім, не слід цілком виключати і співробітників. Метою порушника може бути викрадення даних з бази даних, порушення роботи мережі з метою шантажу або несанкціонована зміна даних у мережі. У випадку якщо порушник зовнішній, він буде мати дуже обмежені права у системі, якщо порушник це співробітник, він може мати адміністративні права в системі. Організація, яку ми розглядаємо невелика за розміром, тож навряд чи метою порушника є фінансова вигода. Скоріше за все він має невеликий бюджет, тому буде використовувати лише найпоширеніші безкоштовні програмні засоби. Однак кваліфікація порушника за замовчуванням завжди вважається високою. Враховуючи написану для інформаційної системи модель загроз зловмисник скоріше за все буде використовувати загрозу, що пов’язана з несанкціонованим доступом до бази даних, для реалізації загрози буде використовувати вразливість типу SQL-ін’єкція, оскільки має для цього достатню кваліфікацію.

Таким чином можна помітити, що на кожному етапі такого аналізу множина найбільш вірогідних атак на мережу зменшується. Це дає можливість обрати засоби інформаційного захисту, які будуть найбільш доцільними та оптимальними за ціною для конкретної мережі, що є однозначною перевагою даного методу.

Однак, звісно у такого підходу присутні свої недоліки, зокрема його недостатня формалізованість, адже висновки про те, які вразливості є загрозами та які з них зловмисник з найбільшою вірогідністю використає для атаки визначаються аналітичним методом, тобто якість цієї оцінки залежить від кваліфікації спеціаліста з інформаційної безпеки. Другий недолік – модель загроз, створюється для конкретної системи, тому вона не є гнучкою, не може швидко змінюватись. У сучасній інформаційній безпеці, коли методи атак на інформаційні системи швидко змінюються, гнучкість моделі стає не перевагою, а необхідністю. Проте, цей недолік відноситься до концепції КСЗІ в цілому.

3.3 Аналіз методів та засобів захисту інформації

Сучасні засоби та методи для забезпечення інформаційної безпеки організації, можна умовно розділити на 4 основних групи (рис. 3.4).

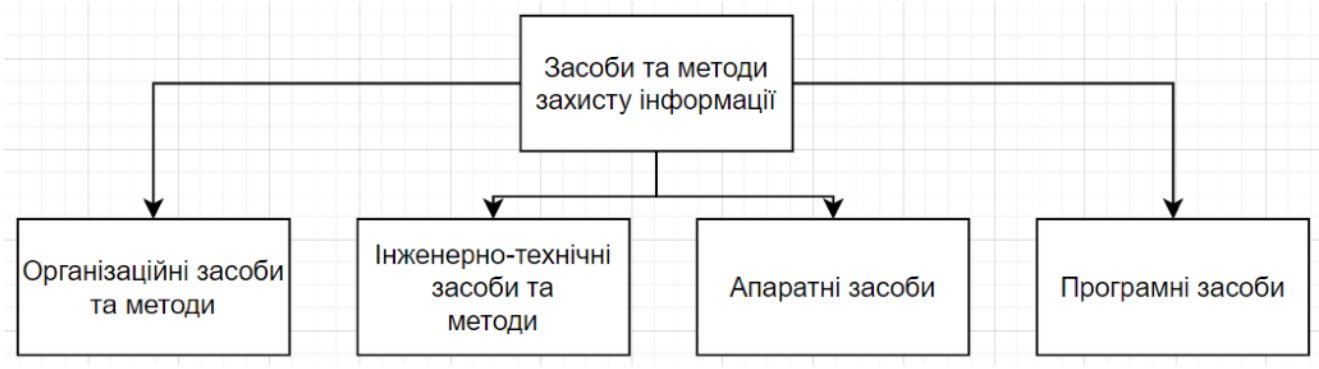

Рисунок 3.4 – Види засобів та методів захисту інформації

Перша група – організаційні засоби та методи. Під цим розуміється передусім політика безпеки компанії. Друга група – інженерно-технічні засоби та методи. Також важливими для забезпечення інформаційної безпеки є апаратні засоби, наприклад генератори завад, системи відеоспостереження та інші пристрої з ТЗІ. Проте, наразі дуже важливу роль у захисті інформації мають програмні засоби, вони досягли чи не найбільшого різноманіття, оскільки атаки зі спробою викрадення спотворення або знищення інформації сьогодні відбуваються здебільш саме через мережу. До цієї підгрупи належать антивіруси, системи EDR SIEM, IDS/IPS, DLP та багато інших

Основні властивості методів та засобів організаційного захисту [30]:

– забезпечення перекриття каналів витоку інформації;

– об'єднання всіх засобів у цілісний механізм захисту інформації:

Методи та засоби організаційного захисту інформації включають:

– розмежування фізичного доступу до об'єктів інформаційної системи;

– обмеження можливості перехоплення побічних електромагнітних випромінювань і наведень;

– розмежування доступу до інформаційних ресурсів та процесів інформаційної системи;

– резервне копіювання необхідної інформації;

– запобігання інфікування комп'ютерів вірусами.

Для проведення організаційних заходів за основу беруть використання та підготовку законодавчих та нормативних документів у галузі інформаційної безпеки, які на правовому рівні мають регулювати доступ до інформації з боку споживачів. Такими нормативними документами є не тільки нормативні документи на рівні держави, а й внутрішні нормативі документи, які створюються та використовуються лише в межах організації та виключно для задоволення потреб організації.

Під інженерно-технічними засобами захисту розуміють фізичні об'єкти, механічні, електричні та електронні пристрої, елементи конструкції будівель, засоби пожежогасіння та інші засоби, що забезпечують:

– захист території та приміщень від НСД зовнішніх порушників;

– захист апаратних засобів та носіїв інформації;

– запобігання можливості віддаленого доступу до технічних засобів ІС;

– запобігання можливості перехоплення побічних електромагнітних випромінювань і наведень;

– розмежування доступу співробітників;

– перевірку режиму роботи персоналу ІС;

– перевірку переміщень співробітників ІС у різних виробничих зонах;

– протипожежний захист приміщень ІС;

– мінімізацію матеріальних збитків від втрат інформації, що виникли внаслідок стихійних лих та техногенних аварій.

Важливість реалізації захисту інженерно-технічними засобами є досить високою, бо такі засоби захисту є першою фізичною лінією захисту.

До апаратних засобів захисту інформації відносяться електронні та електронно-механічні пристрої, що включаються до складу технічних засобів ІС та виконують деякі функції забезпечення інформаційної безпеки. Критерієм віднесення пристрою до апаратних, а не інженерно-технічних засобів захисту є обов'язкове включення до складу технічних засобів ІС.

Під програмними засобами захисту розуміють спеціальні програми, що включаються до складу програмного забезпечення ІС виключно для виконання захисних функцій.

Перед тим як проводити аналіз та вирішувати завдання вибору оптимального засобу захисту інформаційної системи, необхідно розглянути всі можливі засоби захисту та їх призначення. Це допоможе з множини засобів захисту вибрати ті, які будуть піддаватися подальшому аналізу. Цей огляд

проводиться з метою визначення таких засобів захисту, чиї функції в поєднанні будуть доповнювати один одного та полегшувати управління безпекою в комп’ютерній мережі.

Огляду будуть піддаватись наступні загальні, програмні та апаратні засоби захисту, які найчастіше використовуються для забезпечення безпеки в інформаційних системах: антивірусне програмне забезпечення, проксі-сервер, міжмережевий екран, VPN, SIEM системи, IPS/IDS та програми для моніторингу мережі.

Антивірусна програма (антивірус, антивірусне програмне забезпечення) – спеціалізована програма для виявлення комп'ютерних вірусів, а також шкідливих програм, та відновлення заражених файлів, а також задля запобігання зараженню файлів чи операційної системи шкідливим кодом. Основні завдання: сканування файлів і програм в режимі реального часу, сканування комп'ютера за потребою, сканування інтернет-трафіку, сканування електронної пошти, захист від атак ворожих веб-вузлів та відновлення пошкоджених файлів [31].

Проксі-сервер – сервер в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі, через посередництво проксі-сервера, запити до мережевих сервісів. Найчастіше проксі-сервери застосовуються для [32]:

– забезпечення доступу з комп'ютерів локальної мережі в інтернет;

– хешування даних, стиснення даних;

– захист локальної мережі від зовнішнього доступу;

– обмеження доступу з локальної мережі до зовнішньої;

– анонімізації доступу до різних ресурсів.

Міжмережевий екран (брандмауер, фаєрвол) – узагальнена назва системи на основі апаратного чи програмного забезпечення, яка взаємодіє з мережевим трафіком згідно з набором правил безпеки. Головна функція брандмауера – фільтрація шкідливого та потенційно небезпечного контенту та з’єднань.

Існує чотири типи брандмауерів із різними видами фільтрування трафіку. Брандмауер першого покоління працює як пакетний фільтр, порівнюючи основну інформацію; друге покоління брандмауера містить ще один параметр для налаштувань фільтра – стан з'єднання; брандмауери третього покоління побудовані для фільтрування інформації за допомогою усіх рівнів моделі OSI, зокрема і прикладного рівня; нові фаєрволи все ще належать до третього покоління, однак їх часто називають «наступним поколінням» або NGFW, так як

даний вид поєднує всі раніше використані підходи з поглибленим оглядом відфільтрованого контенту [33].

VPN (Virtual Private Network) – це віртуальна приватна мережа, яка забезпечує шифрування трафіку між клієнтом та VPN-сервером і зміну IP-адреси. При підключенні до VPN створюється захищений канал між комп'ютером користувача і VPN-сервером. Доцільно використовувати VPN в наступних випадках [34]:

– під час користування незахищеними загальнодоступними мережами Wi-Fi, щоб захистити свої дані;

– коли необхідний захищений доступ до інтернет-мережі та систем під час організації віддаленої роботи;

– щоб захистити себе від веб - сайтів, програм і сервісів, які хочуть відстежувати ваші дії;

– щоб оператор або провайдер не міг відслідковувати ваших дій в інтернеті;

– щоб отримати доступ до заблокованих інформаційних ресурсів.

SIEM (від англ. Security information and event management) у комп'ютерній безпеці є програмними продуктами, які об'єднують управління інформаційною безпекою та управління подіями [35].

Технологія SIEM забезпечує управління журналами даних, сповіщення про поточні проблеми, відображення діаграм, які допомагають ідентифікувати випадки, що відмінні від стандартної поведінки, зберігання даних та можливість подальшого пошуку серед збережених даних [35].

Система виявлення вторгнень (від англ. Intrusion Detection System, IDS) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет [36].

Система запобігання вторгненням (англ. Intrusion Prevention System, IPS) – програмна або апаратна система мережевої та комп'ютерної безпеки, яка виявляє вторгнення або порушення безпеки і автоматично захищає від них. Системи IPS можна розглядати як розширення систем виявлення вторгнень (IDS), так як завдання відстеження атак залишається однаковою. Однак, вони відрізняються в тому, що IPS повинна відслідковувати активність в реальному часі і швидко реалізовувати дії щодо запобігання атак [36].

Програми для моніторингу мережі – це програми, які дозволяють оперативно реагувати на аномальну діяльність в межах локальної мережі, бути в

курсі всіх мережевих процесів і, таким чином, автоматизувати частину рутинної діяльності адміністратора [37].

Отже, аналізуючи функції та призначення вищезазначених засобів захисту, можна зробити висновок, що найдоцільніше використовувати наступне:

– антивірусне програмне забезпечення;

– проксі-сервер;

– SIEM системи;

– програми для моніторингу мережі;

– брандмауери.

Аналізуючи конкретні рішення антивірусних програм, можна побачити, що в деяких програмах вже є вбудований VPN, тому прийнято рішення для подальшого аналізу VPN не використовувати. Аналогічна ситуація з вбудованою IPS/IDS в SIEM системи, тому IPS/IDS теж не буде розглядатися в подальшому аналізі. Але важливо було зазначити, про можливість використання таких засобів захисту. Це зазначено для розуміння того, що у разі потреби є можливість їх роздільного використання.

Прийнято рішення зупинитися на таких засобах захисту як, антивіруси, SIEM системи, програми для моніторингу мережі та брандмауери.

Для вибору конкретних рішень для кожного виду засобів захисту був проведений аналіз представлених рішень у джерелах [37 - 41] та вибрані деякі з них.

Для аналізу програм антивірусного захисту були вибрані наступні рішення: Norton, TotalAV, McAfee, Intego, Bitdefender, Panda та Avira [38].

Продукти Norton від компанії Gen Digital обрані для аналізу, бо ~~що~~ вони є досить різноманітними як за функціями, так і за вартістю. Тому в залежності від функціоналу, який необхідний в якості антивірусного програмного забезпечення, є можливість вибрати рішення від Norton саме таке, яке підійде і за ціною, і за можливостями.

Другим рішенням для порівняльного аналізу є TotalAV. Він має вже не так багато варіантів рішень, як попередній, але має в своєму функціоналі досить важливі та корисні функції, а саме, функції захисту у реальному часі, налаштування інтелектуальних сканувань, тощо. Також великою перевагою є його вартість, яка відносно попереднього є майже у двічі меншою.

Третім рішенням для порівняльного аналізу є McAfee. Це глобальний лідер у сфері захисту в Інтернеті. Ця компанія орієнтована на захист пристроїв,

враховуючи та адаптуючись до потреб клієнтів. Кількість можливих рішень, які можуть бути використані як антивірусне програмне забезпечення також не є великою, але якщо розглядати вартість цих рішень, то вона стоїть на одному рівні з вартістю деяких рішень від Norton.

Наступним рішенням для порівняльного аналізу є Intego. Тут різноманітність рішень не така велика, як в попередніх варіантах, але перевагою є наявність рішень для macOS. Вартість порівняно з попередніми рішеннями є нижчою, але не дивлячись на це, кількість функцій не є значно меншою, що робить його конкурентоспроможним при виборі оптимального антивірусного програмного забезпечення.

Розглядаючи такі рішення як Bitdefender, ~~то~~ важливо зазначити, що також присутні рішення для організацій різного масштабу. Корисною функцією є аналіз людських ризиків, тому, що розмістивши аспект людського фактору у центрі стратегії аналізу ризиків, зробити систему більш стійкою до можливих порушень та атак стає легше. Відмінною рисою є його вплив на продуктивність, який є низьким в порівнянні з іншими рішеннями.

Таке антивірусне рішення, як Panda, підійде далеко не для всіх, тому що діяльність цієї системи ґрунтується на принципі повного перенесення процесів виявлення та сканування шкідливого програмного забезпечення в "хмару". Але головною перевагою Panda є те, що він є безкоштовним, але водночас його функціонал досить обмежений через принцип його роботи.

Останнє рішення це Avira, головною перевагою якого є вбудований веб-захист та розширений захист від програм-вимагачів та вартість, яка не є високою, порівнюючи з іншими представниками антивірусного програмного забезпечення. Але кількість можливих рішень досить обмежена, так само як і функціонал багатьох рішень.

Для порівняльного аналізу вибрані наступні 8 критеріїв: виявлення шкідливих програм через сканування, захист від вірусів в реальному часі, наявність VPN, настроюваний брандмауер, батьківський контроль, кількість пристроїв, найкраща ціна, гарантія повернення коштів. Вибрані критерії є ключовими при виборі найкращого рішення серед програм антивірусного захисту.

Для аналізу SIEM систем були вибрані наступні рішення: IBM Security QRadar SIEM, Splunk Enterprise, McAfee, FIREEYE Helix Security Platform та Rapid7 InsightIDR [40, 41].

Першим рішенням для аналізу SIEM систем є IBM Security QRadar SIEM. До можливостей цього рішення відноситься відстеження та кореляція даних про загрози, мережу та аномалії поведінки користувачів, щоб визначити пріоритетність сповіщень високої точності. Це рішення має багато переваг, наприклад, управління інцидентами та їх усунення та проведення розслідувань тощо. Функціонал даного рішення є доволі різноманітним, тому при порівнянні SIEM систем не можна не розглядати саме це рішення.

Друге рішення від компанії Splunk. Ця компанія входить в перелік лідерів розробки програмного забезпечення. Рішення Splunk Enterprise дозволяє фахівцям з безпеки ефективно виявляти внутрішні та зовнішні атаки та оперативно вживати заходів у відповідь на них. Це спрощує процеси забезпечення захисту від загроз, зменшує ризики та забезпечує безпеку бізнес-процесів.

Наступне рішення від компанії McAfee. Дане рішення підійде найкраще для клієнтів, які працюють з великими обсягами даних. Перевагою цього рішення є висока продуктивність та можливість надання інформації для вжиття необхідних заходів, що полегшує та прискорює реагування на загрози.

Таке рішення, як FIREEYE Helix Security Platform добре підійде саме для тих організацій, які орієнтуються на безпеці в «хмарі». Так як це хмарна платформа операцій безпеки, яка дозволяє організаціям контролювати будь-які інциденти від попередження до виправлення. Але є негативний момент, такий як управління логами. Але це не є критичним, тому це рішення теж є конкурентоспроможним для порівняння.

І останнє рішення серед SIEM систем це Rapid7 InsightIDR. Перевагою цього рішення є легкість встановлення та автоматизація процесів, що полегшує взаємодію з користувачем.

Для порівняльного аналізу вибрані наступні 16 критеріїв: можливість налаштовувати звіти, управління логами, застосування правил кореляції у часі, резервування конфігурації системи, агрегація подій за типом, використання алгоритмів машинного навчання, проведення розслідувань, управління інцидентами та їх усунення, підтримка хмарних сервісів, виявлення аномалій з урахуванням поведінки, автоматизовані робочі процеси, сповіщення та попередження у реальному часі, розширене виявлення погроз, виявлення інсайдерських загроз та пробний період. Вибрані критерії є ключовими при виборі найкращого рішення серед SIEM систем.

Для аналізу програм для моніторингу мережі були вибрані наступні рішення: Nagios, PRTG Network Monitor, Kismet, WireShark та Zabbix [38].

Перше що слід розглянути це Nagios. Це рішення для моніторингу з відкритим вихідним кодом. Це один з інструментів моніторингу та оповіщення за допомогою гнучкої та розширюваної архітектури моніторингу. Великою перевагою цього рішення це зрозумілість інтерфейсу, що значно полегшує експлуатацію для недосвідчених користувачів.

Друге рішення – PRTG Network Monitor, має кілька варіантів з різною конфігурацією, тому є можливість обрати більш доречнішу та ефективнішу. Також великою перевагою є вартість та можливість використання для великих організацій.

Ще одним варіантом є Kismet. Важливо зазначити що цей інструмент можна використовувати лише з Linux, що є великим мінусом, але водночас функціонал цього інструмента є доволі корисним тому в окремих випадках його використання буде доцільним.

Наступним рішенням є WireShark, що є досить популярним у використанні, активно розвивається та має багато нагород та відзнак. Однією з головних переваг є можливість аналізу різноманітних форматів файлів та підтримка багатьох платформ.

Останнє рішення серед програм для моніторингу мережі є Zabbix. Zabbix – це програмне забезпечення, яке відстежує різноманітні параметри мережі, стан серверів, віртуальних машин, програм, служб, баз даних, веб-сайтів, хмарних сервісів тощо. Ця система підтримує як опитування, так і перехоплення даних. Доступ до всіх звітів і статистики Zabbix, а також налаштування параметрів конфігурації, доступний через веб-інтерфейс. Головними перевагами є зручність інтерфейсу та те, що Zabbix є безкоштовним.

Для порівняльного аналізу вибрані наступні 6 критеріїв: підтримка різних систем, легкість встановлення, зрозумілість інтерфейсу, вартість, підходить для великих організацій та різноманітність функцій. Вибрані критерії є ключовими при виборі найкращого рішення серед програм для моніторингу мережі.

Для аналізу брандмауерів були вибрані наступні рішення: Kerio WinRoute, Forcepoint, Cisco, NordLayer, Fortinet та VMware NSX Distributed Firewall [41].

Перше рішення серед брандмауерів це Kerio WinRoute. Він призначений для захисту від зовнішніх атак та вірусів та дає можливість обмеження доступу до веб-сайтів, залежно від їхнього змісту. Також він дозволяє налаштовувати правила

для перевірки вхідного та вихідного трафіку з урахуванням стану протоколу та надає можливість сканування трафіку на наявність вірусів, що є його перевагою.

Брандмауери Check Point забезпечують гарний рівень безпеки, порівняно з іншими міжмережевими екранами нового покоління. Належність до міжмережевих екранів нового покоління є великою перевагою цих брандмауерів. Вони реалізовані як апаратні файерволи, що, разом з таким критерієм, як наявність вбудованої IDS/IPS, є показниками, які вирізняють ці міжмережеві екрани серед інших.

Другим рішенням є Forcepoint. Брандмауери цієї компанії є також міжмережевими екранами нового покоління, які мають вбудовану систему запобігання вторгненням, але також тут присутня можливість розгорнути за допомогою хмари, що є перевагою цих брандмауерів перед іншими. Також потрібно згадати те, що це апаратні міжмережеві екрани, що може бути критерієм при аналізі та виборі найкращого рішення.

Наступним рішенням є Cisco. Це досить популярна компанії, тому їх брандмауери є розповсюдженими у використанні не тільки через відомість компанії, а й через наявність багатьох функцій. Однією з головних переваг є, окрім вищезазначених функцій в інших рішеннях, широкий вибір міжмережевих екранів та використання для локальної мережі. Також важливо зазначити, що міжмережеві екрани Cisco, як і попередні рішення, є апаратними рішеннями, що безумовно є перевагою.

Ще одне рішення це NordLayer. Це брандмауер призначений для хмарних мереж. Одні з переваг цього хмарного брандмауера – це запобігання або зменшення несанкціонованого доступу до приватних мереж та використання для локальної мережі, але відмінною рисою від попередніх рішень є те, що він не потребує апаратного забезпечення.

Рішення від компанії Fortinet це безумовно брандмауери, які варто розглянути, бо вони виконують захист хмарної інфраструктури, є брандмауерами наступного покоління, мають вбудовану IDS/IPS тощо. Але найбільшою їх перевагою є можливість широкого вибору продуктів.

Останнє рішення – це VMware NSX Distributed Firewall. Він, як і попередні, забезпечує захист в хмарі та має вбудовану IDS/IPS, а також включає спрощену роботу через консоль та проводить моніторинг зашифрованого трафіку, що є одними з його переваг.

Для порівняльного аналізу вибрані наступні 6 критеріїв: призначений для LAN, призначений для хмарних мереж, наявність вбудованої IDS/IPS, вартість, є рішення для різних видів організацій та належність до брандмауерів наступного покоління. Вибрані критерії є ключовими при виборі найкращого рішення серед брандмауерів.

Для аналізу платформ безпеки кінцевих точок були вибрані наступні рішення: Central Endpoint Intercept X, Microsoft Defender for Endpoint, McAfee та Symantec Endpoint Security Enterprise [43 - 46].

Першим рішенням для аналізу платформ безпеки кінцевих точок є Central Endpoint Intercept X від Sophos. Це рішення впроваджує інноваційні технології, такі як виявлення шкідливого трафіку через засоби розвідки в режимі реального часу, що сприяє запобіганню, виявленню та ліквідації потенційних загроз. Ключовою особливістю Intercept X є використання штучного інтелекту, який являє собою нейронну мережу з самонавчанням.

Друге рішення від компанії Microsoft. Ця компанія входить в перелік лідерів розробки програмного забезпечення. Рішення Microsoft Defender for Endpoint застосовує захист кінцевих точок на основі штучного інтелекту. Також у поєднанні з можливістю швидкого реагування на розширені атаки Microsoft Defender for Endpoint пропонує автоматичне розслідування та можливості виправлення, які допомагають зменшити кількість сповіщень за хвилини в масштабі.

Наступне рішення від компанії McAfee Endpoint Threat Defense and Response надає можливості безперервного збору інформації про все, що відбувається, що гарантує швидке виявлення випадків порушень безпеки і управляти всім циклом забезпечення захисту. Це рішення виявляє зловмисне програмне забезпечення, яке
можна знайти лише за допомогою динамічного аналізу поведінки.

Таке рішення, як Symantec Endpoint Security Enterprise добре підійде також і для тих організацій, які орієнтуються на безпеці в «хмарі». Так як це хмарна платформа операцій безпеки, яка дозволяє організаціям контролювати будь-які інциденти від попередження до виправлення. Такі функції як інтелектуальна автоматизація, управління політиками на основі штучного інтелекту та єдина консоль управління безпекою, надають перевагу серед інших рішень.

Для порівняльного аналізу вибрані наступні 5 критеріїв: простота використання, кросплатформеність, захист від шкідливих програм, виявлення та

нейтралізації атак та консоль управління безпекою. Вибрані критерії є ключовими при виборі найкращого рішення серед брандмауерів.

Таким чином, проведено детальний аналіз існуючих засобів захисту від загроз в комп’ютерних мережах.

4 РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ОПТИМАЛЬНОГО ВИБОРУ ЗАСОБІВ ЗАХИСТУ ДЛЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

4.1 Аналіз наявних підходів щодо вибору засобів захисту від загроз безпеки для інформаційних систем в Україні

Значущість визначення ефективності комплексних систем захисту інформації визнається в контексті нормативного підходу. Нормативний підхід вимагає впровадження політики безпеки інформаційних технологій державою, яка базується на нормативних актах. У цих документах потрібно чітко визначити вимоги до захисту інформації різних категорій конфіденційності та важливості.

Ці вимоги можуть включати перелік захисних механізмів, які повинні бути вбудовані в КСЗІ для відповідності конкретному рівню захисту. Використовуючи такі документи, можна оцінити ефективність КСЗІ, звертаючи увагу на її клас захищеності як критерій ефективності.

Однак нормативний підхід має свої недоліки. Недосконалістю є відсутність конкретної оцінки ефективності окремих механізмів захисту. Замість цього визначається лише наявність або відсутність цих механізмів. Цей недолік частково компенсується в деяких документах, які містять деталізовані вимоги до захисних механізмів. Не дивлячись на це, значною перевагою цього підходу є простота використання.

Далі необхідно розглянути що таке профіль захищеності інформаційної системи та яким чином він визначається. Для цього використовують такі НД ТЗІ як, НД ТЗІ 2.5-007-07 «Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу 1», НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» та НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу».

В [46] описані функціональні критерії, які розбиті на чотири групи. Вони описують вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів. Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, цей документ містить критерії гарантій,

що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

Для визначення профілю захищеності інформаційної системи необхідно з'ясувати деякі основні моменти. Насамперед, які є класи АС, що таке функціональний профіль захищеності, та як залежить вибір профілю захищеності від призначення АС.

Мета введення класифікації АС і стандартних функціональних профілів захищеності – полегшення задачі співставлення вимог до КЗЗ обчислювальної системи АС з характеристиками АС [47].

В [47] проведено класифікацію, згідно якої АС поділяються на 3 класи. У кожного з них є свої особливості та відмінні риси. Для подальшого розгляду вибрано розглядати АС класу “1”. Отже важливо зазначити, що при АС такого класу, система оброблення інформації складається лише з однієї машини для обробки інформації з одним обліковим записом, ступінь конфіденційності оброблювальної інформації на такі машині може бути різним. Але доступ до такої машини можуть мати декілька користувачів з однаковими правами.

Настуне що слід зазначити це поняття стандартного профілю захищеності АС. Стандартний функціональний профіль (СФП) захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС [47].

Наявність СФП захищеності ні в якому разі не вимагає їх використання, при необхідності можна створювати нові профілі захищеності. Але є єдина умова, якої слід обов'язково дотримуватися при створенні нових профілів захищеності - це додержання описаних в НД ТЗІ 2.5-004-99 необхідних умов для кожної із послуг, що включаються до профілю [47].

Також НД ТЗІ 2.5-005-99 дає на даний момент досить великий перелік стандартних профілів захищеності з яких можна вибрати вже готовий перелік послуг відповідно до класу АС та з урахуванням призначення АС, що значно полегшує управління інформаційною безпекою. В [47] СФП захищеності описані не лише за класами АС, а й за їх призначення, описані профілі захищеності для комп'ютерних систем, які входять до АС, а саме:

– КС, призначених для автоматизації діяльності органів державної влади;

– КС, які призначені для автоматизації банківської діяльності;

– КС, які призначені для керування технологічними процесами;

– КС, що входять до складу довідково-пошукових систем.

Також не можна не згадати про “Додаток А” до цього НД ТЗІ, який стане у нагоді, коли останнє питання вибору профілю захищеності так як описує основні загрози в АС в залежності від їх призначення та дає рекомендації щодо вибору профілю захищеності.

Отже, вибір профілю захищеності залежить не лише від класу АС, а від призначення такої системи.

Також при виборі профіля захищеності необхідно визначити вимоги щодо захисту секретної інформації в АС. Саме тому в нагоді стане такий документ, як НД ТЗІ 2.5-007-07. Він не тільки дає розуміння про вимоги щодо захисту секретної інформації, а й опис типові умови функціонування АС класу “1” з розподілення доступу користувачів до інформації.

Згідно з [48] вимогами щодо АС в яких може оброблятися секретна інформація є наступне:

– секретна інформація в процесі обробки в АС не підлягає неконтрольованому та несанкціонованому ознайомленню, розмноженню, розповсюдженню, копіюванню, відновленню, а також неконтрольованій та несанкціонованій модифікації;

– надання доступу до секретної інформації повинно здійснюватися за умови достовірного розпізнавання в АС користувачів АС з урахуванням наданих, згідно із службовою необхідністю, повноважень;

– АС повинна забезпечувати можливість своєчасного доступу зареєстрованих користувачів АС до секретної інформації;

– секретна інформація під час обробки в АС повинна мати атрибути з визначенням встановленого, відповідно до законодавства, ступеня її секретності;

– носії інформації (магнітні, оптичні, флеш, паперові тощо), на які виводиться секретна інформація, повинні мати встановлені, відповідно до порядку забезпечення режиму секретності, реквізити;

– АС повинна забезпечувати автоматизований облік дій всіх користувачів АС щодо обробки секретної інформації. В АС повинен здійснюватися періодичний контроль за всіма обліковими подіями;

– спроби порушення встановленого порядку доступу до секретної інформації підлягають реєстрації з видачою службі захисту інформації в АС

повідомлень. У цьому випадку повинна забезпечуватися можливість блокування доступу до секретної інформації.

Щодо опису функціонування АС, то важливими моментами є опис оброблювальної інформації та технологій її обробки. Оброблювальна інформація поділяється на наступні 5 груп [48]:

– дані та програмні коди які містять державну таємницю;

– бази даних захисту;

– дані з обмеженим доступом, які не містять відомостей, що становлять державну таємницю;

– дані, захищені ліцензійними умовами використання та розповсюдження, або такі, що належать деяким групам та окремим користувачам;

– дані загального користування.

Обробка таких даних повинна виконуватися згідно з експлуатаційною документацією з урахуванням вимог нормативних документів з питань охорони державної таємниці та згідно з вимогами нормативно-правових актів або розпорядчих документів власника АС. Ступінь секретності таких даних має бути не нижчим ступеня секретності інформації, що обробляється в АС.

Що стосується технологій обробки даних, то НД ТЗІ 2.5-007-07 пропонує дві технологій. Ці дві технології відрізняються одна від одної розмежуванням доступу користувачів до даних. Згідно першої технології усі користувачі мають однакові права на доступ до даних, а згідно другої – різні.

Спільним в технологіях обробки є наступне:

– секретні дані зберігаються на з’ємних та нез’ємних магнітних, оптичних та флеш носіях інформації;

– на носіях інформації зберігаються дані різних ступенів секретності. Гриф секретності носія інформації повинен відповідати вищому ступеню секретності даних, які на ньому зберігаються. Інформація, яка має гриф секретності “особливої важливості” зберігається тільки на з’ємних носіях інформації.

Також в [48] запропоновано СФП для кожної з двох технологій з зазначенням такої послугу як КО-0, яка не зустрічається в інших СФП. Ця послуга деталізує опис послуги КО-1 “Повторне використання об’єктів” та дає більш конкретне розуміння об'єктів на які розповсюджується ця послуга та необхідних заходів задля реалізації цієї послуги.

Також важливим моментом є визначення необхідного рівня гарантій. В [48] зазначено необхідний рівень гарантій для СФП в залежності від технології обробки інформації.

Метою роботи є визначення оптимального вибору засобів захисту в інформаційній системі. Для цього використовується метод ранжування альтернатив багатокритеріального вибору з використанням математичної моделі. Для цього потрібно проаналізувати існуючі методи вирішення задачі багатокритеріального вибору та сформувати алгоритм формування комплексу засобів захисту в контексті математичної моделі оптимального вибору засобів захисту інформації.

Данна робота може бути використана як основа для класифікації та аналізу методів моделювання комплексних систем захисту інформації

Призначенням розробки є дослідження методів моделювання комплексних систем захисту інформації.

Метою розробки є оптимізація вибору засобів захисту інформації при проектуванні комплексної системи захисту на об'єкті інформатизації.

Таким чином, на підставі проведеного порівняльного аналізу можливих загроз, засобів захисту та методів оптимізації, прийнято рішення щодо методу для порівняння та видів засобів захисту для порівняльного аналізу.

Далі важливо зазначити, що огляд математичної модель оптимального вибору розглянутий у роботах [49, 50].

4.2. Математична модель оптимального вибору засобів захисту інформації при проектуванні комплексної системи захисту на об'єкті інформатизації

У сучасний період однією з ключових викликів при побудові ефективної системи захисту інформації є вибір оптимального набору засобів серед великої кількості доступних варіантів. Цей вибір має забезпечити ефективну нейтралізацію всіх можливих інформаційних загроз з високою якістю та мінімальними ресурсами.

Відомо, що найбільш ефективні вибори засобів захисту інформації приймаються під час проектування комплексної системи захисту інформації (КСЗІ), коли оцінюються потенційні загрози та вибираються адекватні механізми для їхнього усунення.

На даний момент відсутні повні методичні рекомендації щодо вибору комплексу засобів захисту. Тому, розробка методичного забезпечення для оптимального вибору засобів захисту на етапі проектування КСЗІ є доволі актуальною задачею.

4.2.1 Чинні підходи до оцінки ефективності комплексної системи захисту інформації.

Ефективність системи – це властивість системи, що характеризує її здатність тією чи іншою мірою виконувати свою цільову функцію. Для оцінки ефективності системи необхідно визначити якісні та кількісні показники ефективності, а також необхідно визначити інтегральний показник ефективності системи в цілому [51].

Ефективність КСЗІ оцінюється як на етапі розробки, так і під час її експлуатації. При оцінці ефективності КСЗІ, залежно від використовуваних показників та методів їх отримання, можна виділити три підходи [51]:

– класичний;
– нормативний;
– експериментальний.

При класичному підході для оцінки ефективності КСЗІ та отримання критерію ефективності за умов використання деякої множини n показників використовують ряд методів.

1) Метод головного критерію. Сутність методу головного критерію полягає у виділенні головного критерію – такого, який значно перевершує за важливістю всі інші (на практиці втричі і більше разів) та розрахунку максимального аргументу за умови, що інші критерії не менші від деяких граничних значень.

2) Методи, що засновані на ранжируванні показників за важливістю. При порівнянні систем однойменні показники ефективності зіставляються в порядку зменшення їх важливості за певними алгоритмами. По суті, при використанні даного підходу, здійснюється скорочення числа альтернатив у вихідній множині, при якій виключаються свідомо погані альтернативи.

3) Мультиплікативні та адитивні методи отримання критеріїв ефективності, які ґрунтуються на об'єднанні всіх або частини показників за допомогою операцій множення або додавання до узагальнених показників.

4) Метод Парето: під час використання n показників ефективності системі від-повідає точка в n-мірному просторі. У n-вимірному просторі будується область

парето-оптимальних рішень, що містить незрівнянні рішення, для яких поліпшення будь-якого показника неможливе без погіршення інших показників ефективності. Вибір найкращого рішення з поміж парето-оптимальних може здійснюватися за різними правилами.

Незважаючи на певну кількість альтернативних методів, класичні підходи передбачають формування цільової функції F(X) та її максимізацію на просторі наявних альтернатив A:

$$\begin{gathered} F(X) \rightarrow \max \\ X \in A. \end{gathered} \tag{4.1}$$

Нормативний підхід не передбачає вирішення багатокритеріальних оптимізаційних задач і ґрунтується виключно на використанні нормативних документів та актів із питань побудови КСЗІ, де зазначаються вимоги до захищеності інформації різних категорій конфіденційності та важливості. Вимоги задаються переліком механізмів захисту інформації, які необхідно мати у КСЗІ, щоб вона відповідала певному стандартному функціональному профілю захищеності. Таким чином, критерієм ефективності КСЗІ є її клас захищеності. Безперечною перевагою такого нормативного підходу є простота використання. Його основним недоліком є те, що не визначається ефективність конкретного механізму захисту, а констатується лише факт його наявності чи відсутності. Крім того не враховується витрати на впровадження та експлуатацію засобів захисту. Цей недолік певною мірою компенсується завданням у деяких документах докладних вимог до цих механізмів захисту.

Під експериментальним підходом розуміється організація процесу визначення ефективності наявних засобів КСЗІ шляхом спроб подолання захисних механізмів системи фахівцями, які виступають у ролі зловмисників.

З огляду на те, що засоби безпеки мають обмежені можливості протидії загрозам, завжди існує ймовірність порушення захисту, навіть якщо під час тестування механізми безпеки не були обійдені або блоковані. Для оцінки цієї ймовірності мають проводитися додаткові дослідження.

У методичному плані визначення ефективності КСЗІ повинне полягати у виробленні судження щодо придатності способу дій персоналу чи пристосованості технічних засобів до досягнення мети захисту на основі вимірювання відповідних показників при функціональному тестуванні.

Ефективність оцінюється для вирішення таких задач:

- ухвалення рішення про допустимість практичного використання КСЗІ в конкретній ситуації;
- виявлення впливу різних факторів у досягнення мети;
- встановлення шляхів підвищення ефективності КСЗІ;
- порівняння альтернативних варіантів систем.

Вирішенням проблеми оцінювання ефективності КСЗІ може стати використання системного підходу, який дозволить ще на стадії проектування КСЗІ кількісно оцінити рівень безпеки та надати умови для ефективного управління ризиками. Однак цей шлях може бути реалізований за наявності відповідної системи показників та критеріїв.

Високий ступінь невизначеності вихідних даних при проектуванні КСЗІ є причиною того, що її ефективність не може бути адекватно виражена та описана детермінованими показниками. Тому, об'єктивною характеристикою якості КСЗІ може бути лише ймовірність, що характеризує ступінь відповідності системи, що оцінюється, своєму призначенню – досягненню необхідного рівня безпеки в умовах реального впливу випадкових факторів при заданому комплексі умов. Така характеристика називається ймовірністю виконання завдання системою. Ця ймовірність має бути покладена в основу комплексу показників та критеріїв оцінки ефективності КСЗІ. При цьому критеріями оцінки є поняття придатності та оптимальності. Придатність означає виконання всіх встановлених до КСЗІ вимог, а оптимальність – досягнення однієї з характеристик екстремального значення при дотриманні обмежень та умов інших властивостей системи. При виборі конкретного критерію необхідне його узгодження з метою КСЗІ

У ряді робіт, що присвячені питанням оцінки ефективності захисту інформації в якості показника ефективності, розглядається залишковий ризик — величина збитку R з урахуванням ймовірності реалізації події, що призводить до цієї збитку

$$R = \sum_i P_i \cdot C_i,$$

(4.2)

де P_i – ймовірність реалізації і-ї загрози після встановлення певного варіанту КЗЗ;

C_i – величина збитку від реалізації і-ї загрози.

Величини P_i та C_i визначаються методом експертних чи аналітичних оцінок. Розмір збитку є випадковою величиною з функцією розподілу F(C), де $C \in [0, \infty]$, а як міру збитку у виразі (4.2) приймають математичне очікування величини збитку.

Часто при визначенні ризику враховують витрати на реалізацію захисних заходів – S. У цьому випадку вираз (4.2) перетворюється у такий вигляд:

$$R = \sum_i P_i \cdot (C_i + S_i),$$

(4.3)

де Si, – вартість реалізації захисних механізмів від тієї ж загрози.

Однак за такого підходу витрати на впровадження та експлуатацію засобів захисту прирівнюються до збитків від реалізації загрози, що не завжди є коректним.

У роботі [14], як показник ефективності розробки КСЗІ використовується величина, яка дорівнює різниці між збитками, які вдалося запобігти та витратами на впровадження та експлуатацію засобів безпеки:

$$E = \sum_{i=1}^{K} \left(C_i - C_i^*\right) - \sum_{b=1}^{B} \left(S_b^{вп} + S_b^{ек}\right),$$

(4.4)

де E – ефективність розробки КСЗІ;

K – кількість загроз;

C_i – величина збитків від реалізації і-ї загрози до впровадження КСЗІ;

C_i^* – величина збитків від реалізації і-ї загрози після впровадження КСЗІ;

B – кількість засобів захисту;

$S_b^{вп}$ – витрати на впровадження b-го засобу захисту;

$S_b^{ек}$ – витрати на експлуатацію b-го засобу захисту.

Аналіз показав, що за такого підходу не враховуються ймовірності реалізації загроз, що не дозволяє оптимальним чином вибрати адекватні методи і засоби захисту. Доцільно таким чином формувати КЗЗ, щоб витрати на безпеку були адекватні потенційним загрозам. Подібна ситуація визначає необхідність оцінювання та врахування ймовірностей реалізації загроз.

4.2.2 Визначення показника ефективності та критерія оптимальності комплексної системи захисту інформації.

Оцінювання ймовірності реалізації загроз та пов'язана з цим оцінка можливих втрат – найскладніша та найвідповідальніша частина всього процесу забезпечення безпеки. Від того, наскільки повно виявлені реальні та прогнозовані (потенційні) загрози, залежить ступінь захищеності об'єкта. З іншого боку, свідоме перевищення достатності при врахуванні тих загроз, вплив яких безпосередньо на функціонування об'єкта малоймовірний або локалізація яких неможлива або малоефективна, призведе до значного підвищення витрат на безпеку і може суттєво позначитися на реально досягненій економічній ефективності захисту.

Звідси постає завдання оптимізації рівня захищеності об'єкта від загроз, що дозволяє досягти максимальної ефективності обраного варіанта комплексу захисних заходів. При цьому необхідно враховувати дуже важливе обмеження: незважаючи на видиму пряму залежність між обсягом ресурсів, виділених на захист і ефективністю захисту, існує максимально припустима величина витрат, що визначається прибутковістю проектованої системи захисту – нормою прибутку на інвестовані в неї кошти.

Підвищення рентабельності захисту можливе як завдяки обґрунтованій економії витрат на його організацію і експлуатацію, так і завдяки їхньому оптимальному розподілу в просторі загроз.

Що стосується комп'ютерних мереж, то їхня вразливість суттєво перевищує вразливість автономних комп'ютерів. Це пов'язано, перш за все, з відкритістю, масштабністю та неоднорідністю самих комп'ютерних мереж. Існує чимало способів атак на сучасні комп'ютерні мережі [27] та [52 – 57]. При цьому кількість загроз інформаційній комп'ютерній безпеці та способів їхньої реалізації постійно збільшується. Основними причинами тут є недоліки сучасних інформаційних технологій, а також неухильне зростання складності програмно-апаратних засобів.

Для ефективного вирішення завдання захисту інформації в комп'ютерній мережі необхідний ретельний аналіз усіх можливих загроз інформаційної безпеки, що дозволить своєчасно прийняти заходи протидії загрозам. При аналізі загрози необхідно оцінити можливість її прояву, а також збитки, які будуть завдано підприємству в разі незапобігання загрози.

Для протидії одній і тій самій загрозі зазвичай існує кілька засобів захисту, які випускаються різними виробниками, розрізняються за вартістю реалізації та забезпечують різну можливість запобігання загрозам. У найпростішому випадку можна було б припустити, що кожен засіб захищає від однієї загрози. Але в реальних умовах ринок засобів інформаційної безпеки надає засоби захисту, які протидіють довільній кількості загроз, причому можливість запобігання кожній загрозі різна.

Математична модель оптимального вибору методів та засобів захисту від загроз для кожного інформаційного ресурсу на ОІ надає можливість економічно обґрунтувати склад комплексу спеціальних технічних засобів для КСЗІ в цілому. Критерієм оптимальності цієї композиції може бути обрана сума середніх втрат від реалізації загроз та витрат на систему захисту.

Припустимо, що на ОІ виявлено М критичних інформаційних ресурсів. Для кожного ресурсу визначені загрози та вразливості та існує набір засобів захисту $X = \{X_1, X_2, \ldots, X_i\}$. Задача полягає в виборі складу засобів захисту відповідно до певного критерію оптимальності.

Позначимо ймовірність реалізації і-ї загрози щодо m-го ресурсу у випадку, якщо не використовуються засоби захисту, як P_{im}, і збиток компанії від її реалізації – C_{im}. Тоді ризик від реалізації і-ї загрози (R_{im}) дорівнює:

$$R_{im}=P_{im} \cdot C_{im},$$

(4.5)

Після впровадження засобу захисту X_i величина ризику стане рівною

$$R_{im}(X_i) = P_{im}(X_i) \cdot C_{im},$$

(4.6)

Якщо захисні характеристики засобів задаються можливостями запобігання загрозі, то ймовірність реалізації загрози при впровадженому засобу захисту буде визначатися сумісною ймовірністю:

$$P_{im}(X_i) = P_{im} \cdot (1 - U_{im}(X_i)),$$

(4.7)

де $U_{im}(X_i) = \{0,\ldots,1\}$ – можливість запобігання загрози, яка забезпечується засобом X_i. Тобто, якщо засіб не забезпечує запобігання загрози $U_{im}(X_i) = 0$, то ймовірність її реалізації не змінюється. І навпаки, якщо засіб гарантує абсолютне запобігання загрози ($U_{im}(X_i) = 1$), то ймовірність реалізації цієї загрози дорівнює 0.

З урахуванням вартості цього засобу захисту S_i пропонується використовувати наступний показник ефективності:

$$E_{im}(X_i)[\%] = \left(\frac{R_{im} - R_{im}(X_i)}{R_{im}} \cdot 100)\right) - \left(\frac{S_i}{R_{im}} \cdot 100\right)$$

(4.8)

Цей показник відображає зменшення ризику для m-го інформаційного ресурсу (у грошовому еквіваленті) завдяки використанню засобу захисту в разі реалізації і-ї загрози відносно ресурсу, що захищається, з урахуванням вартості заходу щодо захисту (з урахуванням вартості обладнання, його встановлення та експлуатації).

Однак тут не враховується те, що один і той самий засіб може забезпечувати захист інформації відразу від кількох загроз. Але це можна врахувати при обчисленні параметру $E_{im}(X_i)$ таким чином:

$$E_{im}(X_i)[\%] = \left(\frac{R_{im} - R_{im}(X_i)}{R_{im}} \cdot 100)\right) - \left(\frac{S_i \cdot A_{im}}{R_{im}} \cdot 100\right)$$

, (4.9)

де A_{im}– булева змінна, яка вказує на повторне використання засобу захисту X_i. Якщо $A_{im}=1$, то засіб захисту вибирається першій раз, інакше $A_{im}=0$. Результатом цього буде підвищення значення параметру $E_{im}(X_i)$.

Завданням оптимізації є вибір такого засобу захисту із множини $X=\{X_1, X_2, \ldots, X_i\}$, для якого виконується умова:

$$X_{im}^{opt} = \text{argmax}E_{im}(X_i),$$

(4.10)

де X_{im}^{opt} – оптимальний засіб захисту інформації при реалізації і-ї загрози щодо m-го ресурсу, що захищається, $E_{im}(X_i)$ – ефективність засобу захисту (X_i) при реалізації і-ї загрози щодо m-го ресурсу, що захищається.

Іншими словами, цей засіб повинен забезпечувати максимальне зменшення ризику при мінімальних витратах. У деяких випадках максимальне значення параметра $E_{im}(X_i)$ може приймати значення близькі до нуля, що є прийнятним. Однак, якщо максимальне значення параметра оптимізації набуває негативних значень, це свідчить про перевищення витрат і необхідність використання більш дешевих засобів та методів захисту.

Загалом для комплексу засобів захисту M інформаційних ресурсів, які виявлені на ОІ в ході попереднього обстеження (інвентаризації) для множини загроз Y вираз для параметра ефективності можна записати в наступному вигляді:

$$E(X) = \sum_{m=1}^{M} \sum_{i=1}^{Y} E_{im}(X_i),$$

(4.11)

Рішенням оптимізаційної задачі для КСЗІ буде знаходження складу комплексу засобів захисту $X_{opt}=\{X_1, X_2, \ldots, X_i\}$, для якого буде виконуватись умова:

$$X_{opt} = \text{argmax}E(X, Y, P, C, S),$$

(4.12)

де $Y=\{Y_1, Y_2, \ldots, Y_i\}$ – множина загроз, $P=\{P_1, P_2, \ldots, P_i\}$ – ймовірності реалізації загроз, $C=\{C_1, C_2, \ldots, C_i\}$ – збитки від реалізації загроз, $S=\{S_1, S_2, \ldots, S_i\}$ – вартості реалізації засобів захисту.

Згідно з цим критерієм, оптимальний КЗЗ повинен забезпечувати максимальне зменшення ризику при мінімальних витратах на його впровадження та експлуатацію.

4.2.3 Алгоритм оптимального вибору засобів захисту інформації.

Алгоритм оптимізації складу КЗЗ відповідно до запропонованої математичної моделі наданий у вигляді блок-схеми на рисунку 4.1.

Принцип дії алгоритму полягає в наступному:

- на кроці 2 визначаються інформаційні ресурси на ОІ, що підлягають захисту;
- на кроці 3 визначаються доступні засоби захисту та вартість їх впровадження та експлуатації;
- на кроці 4 визначаються наявні загрози для кожного ресурсу, ймовірності їх реалізації P_{im} та можливі збитки C_{im} від їхньої реалізації;
- на кроці 5 вибирається один із інформаційних ресурсів m, що є на ОІ;
- на кроці 6 вибирається одна із загроз для ресурсу m, ймовірність її реалізації P_{im} та можливі збитки C_{im} від її реалізації;
- на кроці 7 розраховується ризик R_{im} за виразом (4.5);
- на кроці 8 вибирається один із доступних засобів захисту інформації X_i із відповідній йому вартістю впровадження та експлуатації S_i для запобігання і-ї загрози для ресурсу m;
- на кроці 9 розраховується показник ефективності $E_{im}(X_i)$ для вибраного засобу захисту за виразом (4.9);

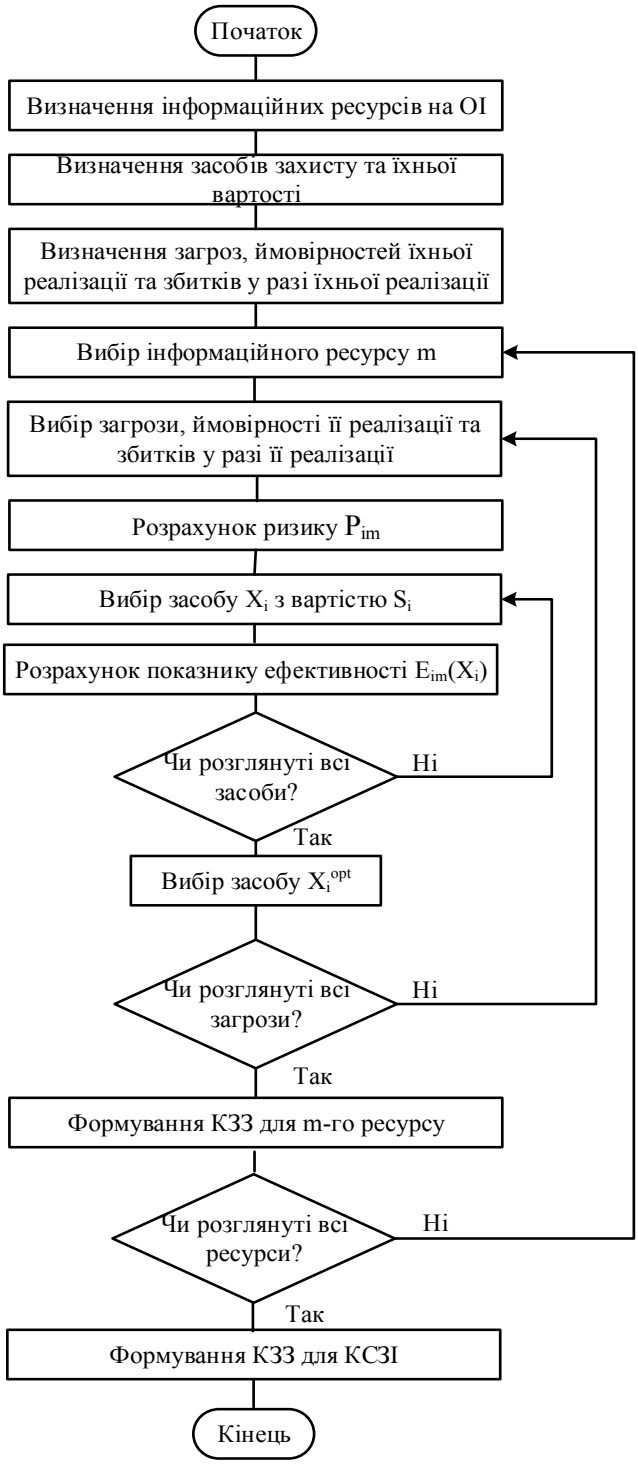

Рисунок 4.1 – Блок-схема алгоритму формування комплексу засобів захисту

- на кроці 10 циклічно перевіряється наявність альтернативних засобів захисту для запобігання тієї ж загрози. При їх наявності для кожного засобу розраховується показник ефективності $E_{im}(X_i)$;
- на кроці 11 із наявних засобів захисту вибирається той, що відповідає критерію оптимальності (4.10);

- на кроці 12 здійснюється перехід до інших загроз безпеці інформації для того ж ресурсу m, і таким чином обираються оптимальні засоби захисту для запобігання цим загрозам;
- на кроці 13 здійснюється формування оптимального комплексу засобів захисту для запобігання загроз безпеки для ресурсу m;
- на кроці 14 здійснюється перехід до інших інформаційних ресурсів для кожного з яких вибираються засоби захисту відповідно до критерія оптимальності (4.10). Для кожного з них формується КЗЗ для запобігання всім загрозам безпеки.

Якщо процедурою формування КЗЗ були охоплені усі інформаційні ресурси, що були виявлені на ОІ, то на кроці 15 остаточно формується КЗЗ для КСЗІ на ОІ. Оптимальність складу КЗЗ перевіряється за критерієм (4.12).

4.2.4 Приклад оптимального вибору складу засобів захисту від загроз безпеки у комп'ютерній мережі підприємства.

Для демонстрації використання запропонованої математичної моделі розглянемо невеликий приклад, що показує її практичне застосування. В якості об'єкту інформатизації в даному випадку візьмемо комп'ютерну мережу підприємства на періоді її функціонування T = 1 рік. Для прикладу розглянемо три загрози безпеки та п'ять засобів захисту. У реальних системах кількість загроз та можливих для їх запобігання засобів захисту може досягати кількох десятків, і більше.

У табл. 4.1 наведено три типові загрози для комп'ютерної мережі підприємства (реально їх набагато більше). Можливості прояву загроз вибрано на основі статистичних досліджень. Дані про середні збитки від можливого запобігання загрозам безпеці сильно залежать від специфіки діяльності компанії та обрані на основі деяких середніх показників для типового підприємства.

У табл. 4.2 наведено п'ять засобів захисту від загроз безпеці. Вартість реалізації засобів захисту вибрано на основі припущення про наявність у компанії 200 робочих станцій та 5 файлових серверів. Можливість запобігання загроз вибрана на основі експертних оцінок.

Таблиця 4.1 – Можливі загрози безпеці та можливі збитки від їхньої реалізації на інтервалі часу один рік

Загроза	Ймовірність реалізації	Можливі збитки від реалізації, грн.	Ризик від реалізації, грн.
Несанкціоноване вторгнення в мережу (загроза 1)	0,6	2000000	1200000
Вірусна атака (загроза 2)	0,9	400000	360000
Витік конфіденційної інформації (загроза 3)	0,8	3000000	2400000

Таблиця 4.2 – Засоби захисту від загроз безпеки, вартості їхньої реалізації та можливості запобігання загрозам на інтервалі часу один рік

Засіб захисту	Вартість реалізації, грн.	Можливість запобігання загрозі		
		несанкціонованого вторгнення в мережу	вірусної атаки	витоку конфіденційної інформації
ESET NOD32 Antivirus (засіб 1)	325680	0	0,8	0
Fortinet FortiGate 100F (засіб 2)	258375	0,7	0,4	0
Symantec Antivirus Enterprise (засіб 3)	580000	0	0,9	0,7
Outpost Network Security (засіб 4)	364122	0,8	0,5	0,6
Kerio WinRoute Firewall (засіб 5)	158000	0,7	0,3	0,7

Таблиця 4.3 – Результати розрахунків для загрози 1 (C=2000000 грн.)

Засіб захисту	S(X), грн.	U(X)	P_1	$P_1(X)$	R_1,грн.	$R_1(X)$,грн.	$E_1(X)$,%
Засіб 1	325680	0	0,6	0,6	1200000	1200000	-27,14
Засіб 2	258375	0,7	0,6	0,18	1200000	360000	48,469
Засіб 3	580000	0	0,6	0,6	1200000	1200000	-48,333
Засіб 4	364122	0,8	0,6	0,12	1200000	240000	49,657

Засіб 5	158000	0,7	0,6	0,18	1200000	360000	56,833

Таблиця 4.4 – Результати розрахунків для загрози 2 (С=400000 грн.)

Засіб захисту	S(X), грн.	U(X)	P_2	$P_2(X)$	R_2,грн.	$R_2(X)$,грн.	$E_2(X)$,%
Засіб 1	325680	0,8	0,9	0,18	360000	72000	-10,467
Засіб 2	258375	0,4	0,9	0,54	360000	216000	-31,771
Засіб 3	580000	0,9	0,9	0,09	360000	36000	-71,111
Засіб 4	364122	0,5	0,9	0,45	360000	180000	-51,145
Засіб 5	158000	0,3	0,9	0,63	360000	252000	-13,889

Таблиця 4.5 – Результати розрахунків для загрози 3 (С=3000000 грн.)

Засіб захисту	S(X), грн.	U(X)	P_3	$P_3(X)$	R_3,грн.	$R_3(X)$,грн.	$E_3(X)$,%
Засіб 1	325680	0	0,8	0,8	2400000	2400000	-13,57
Засіб 2	258375	0	0,8	0,8	2400000	2400000	-10,766
Засіб 3	580000	0,7	0,8	0,24	2400000	720000	45,833
Засіб 4	364122	0,6	0,8	0,32	2400000	960000	44,828
Засіб 5	158000	0,7	0,8	0,24	2400000	720000	63,417

Аналіз результатів розрахунків (табл. 4.3) показує, що для запобігання першої загрози оптимальним є засіб захисту 5. Із таблиці 4.4 видно, що для другої загрози показники ефективності для всіх наявних засобів мають негативні значення. Це говорить про перевищення витрат на засоби захисту для запобігання цій загрозі та необхідності пошуку більш дешевших засобів. Тим не менш, серед наявних засобів оптимальним є засіб захисту 1. Із таблиці 4.5 видно, що для запобігання загрози 3 оптимальним є засіб захисту 5. Таким чином, даний засіб захисту є оптимальним для запобігання відразу двох загроз – загрози 1 і загрози 3.

Це враховується при розрахунку інтегрального показника ефективності КЗЗ (4.11). Вартість засобу 3 згідно з (4.8) повторно не враховується (A_3 = 0). Інтегральний показник ефективності (4.11) для КЗЗ, що складається з двох засобів (засіб 1 і засіб 5) приймає максимальне значення і дорівнює E(X) = 116,366 %.

4.3 Аналіз методів багатокритеріальної оптимізації щодо оптимального вибору засобів захисту інформаційних систем

Математична модель задачі багатокритеріальної оптимізації це задача прийняття рішень, коли відбувається процес одночасної оптимізації двох або більше конфліктуючих цільових функцій в заданій області визначення. Будемо розглядати скінченновимірні задачі багатокритеріальної максимізації, які описуються виразами (4.12) [57]:

$$f(x) \to \max \qquad (4.13)$$
$$x \in D,$$

де $D \in \mathbb{R}^n$ – допустима область;

$X = (x_1, \ldots, x_n)$ – множини D називаються допустимими розв'язками або альтернативами;

$f(X) = (f(X_1), \ldots, f(X_n))$ – вектор-функція часткових критеріїв $fi : D \to \mathbb{R}^1$, $i = \overline{1,m}$.

У таких задачах допустима множина D найчастіше задається у вигляді нерівностей:

$$D = \{X \in \mathbb{R}^n \ \ g_j(X) \le b_j, \ j = \overline{1,n}\}. \qquad (4.14)$$

Основні, найбільш поширені методи розв'язання задач багатокритеріальної оптимізації представлені на рисунку (4.2) [57].

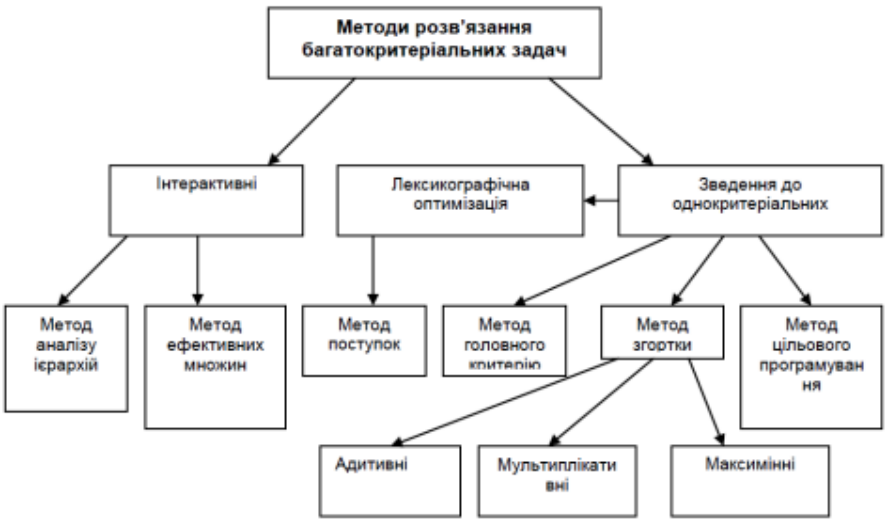

Рисунок 4.2 – Класифікація методів багатокритеріальної оптимізації

Найбільш поширені методи: згортання часткових критеріїв, головного часткового критерію, послідовних поступок, цільового програмування [57].

Основною метою методів згортки є об'єднання множини часткових критеріїв в єдиний головний критерій, таким чином задачу вибору з багатьох критеріїв спрощують задачі вибору з одним критерієм, зокрема, до вирішення завдання максимізації цього критерію.

Загальний вигляд методу згортки приватних критеріїв можна представити у вигляді функції з набору змінних, кількість яких відповідає кількості приватних критеріїв.

Виходячи з цього можна сказати, що задача багатокритеріальної оптимізації скорочується до завдання максимізації або мінімізації головного критерію f(x) на множині D, отриманого завдяки згортці приватних критеріїв.

Несприятливою рисою методів згортки є суб'єктивний вибір вагових коефіцієнтів для кожного критерію. Це завдання є складним і суб'єктивним, оскільки воно базується на пріоритетах користувача, що може призводити до неоднозначних результатів.

Розрізняють такі методи згортки: адитивна, мультиплікативна та максимінна згортка [57].

Розрахунки методом адитивної згортки проводяться відповідно до формули (4.15).

$$K(x) = \sum_{j=1}^{n} a_j \cdot K_j(x), \qquad (4.15)$$

де K(x) – підсумковий узагальнений критерій для сукупності альтернатив;

$K_j(x)$ – набір приватних критеріїв;

n – число приватних критеріїв;

a_j – відносна вага (важливість приватного критерію), причому сума цих показників для кожного критерію повинна дорівнювати 1.

Найкраще рішення можна описати виразом (4.16).

$$x^* = \operatorname{argmax} K(x) \qquad (4.16)$$

$$x \in X$$

Розрахунки методом мультиплікативної згортки проводяться відповідно до формули (4.17).

$$K(x) = \prod_{j=1}^{n} a_j \cdot K_j(x), \qquad (4.17)$$

де K(x) – підсумковий узагальнений критерій для сукупності альтернатив;

$K_j(x)$ – набір приватних критеріїв;

n – число приватних критеріїв;

a_j – відносна вага (важливість приватного критерію), причому сума цих показників для кожного критерію повинна дорівнювати 1.

Найкраще рішення можна описати виразом (4.16).

Розрахунки методом максимінної згортки проводяться відповідно до формули (4.18).

$$K(x) = \min_{j}(a_j \cdot K_j(x)), \qquad (4.18)$$

де K(x) – підсумковий узагальнений критерій для сукупності альтернатив;

$K_j(x)$ – набір приватних критеріїв;

n – число приватних критеріїв;

a_j – відносна вага (важливість приватного критерію), причому сума цих показників для кожного критерію повинна дорівнювати 1.

Найкраще рішення можна описати виразом (4.19) з урахуванням виразу (4.18).

$$x^* = \underset{x \in X}{\operatorname{argmax}} \min_{j}(a_j \cdot K_j(x)) \qquad (4.19)$$

Для аналізу засобів захисту інформаційних систем буде використовуватися саме методи згортки, котрий є методом зведення багатокритеріальних задач до єдиного критерію [57]. Ці методи найкраще підходять для вирішення поставленої задачі, бо детально описують та відображають вагомість кожного критерію засобів захисту та їх важливість відносно інших засобів захисту при виборі оптимального засобу захисту.

4.4 Вирішення завдань вибору оптимального засобу захисту методами згортки

В цьому пункті проведено порівняльний аналіз засобів захисту. Для кожного виду засобів захисту вибрані різні критерії для порівняння. Також для більшої зручності аналіз кожного виду засобів захисту виконано в рамках різних завдань. Завдання 4.1 відповідно для вибору оптимального засобу захисту програм антивірусного захисту, аналогічно завдання 4.2 – програм управління інформаційною безпекою, завдання 4.3 – програм для моніторингу мережі, завдання 4.4 – брандмауерів, завдання 4.5 – платформ безпеки кінцевих точок.

Оцінка критеріїв та вага критеріїв вибрані на основі експертних оцінок. Визначати найкращий варіант будемо: методом адитивної згортки, методом мультиплікативної згортки та методом максимінної згортки.

Завдання 4.1: При виборі найкращого антивіруса представлені 6 варіантів. Нормовані за 100-бальною шкалою. Результати критеріїв та їх відповідні ваги представлені в таблиці 4.6.

Таблиця 4.6 – Вихідні дані

	Критерій 1		Критерій 2		Критерій 3		Критерій 4	
	Виявлення шкідливих програм через сканування	Вага критерію	Захист від вірусів в реальному часі	Вага критерію	VPN	Вага критерію	Настроюваний брандмауер	Вага критерію
Norton	100	0,23	90	0,26	70	0,17	80	0,14
TotalAV	60		40		80		50	
McAfee	90		70		50		100	
Intego	50		60		40		60	
Bitdefender	80		100		90		90	
Panda	40		50		60		70	
Avira	70		80		100		40	
	Критерій 5		Критерій 6		Критерій 7		Критерій 8	

	Батьківський контроль	Вага критерію	Кількість пристроїв	Вага критерію	Найкраща ціна	Вага критерію	Гарантія повернення коштів	Вага критерію
Norton	100	0,1	70	0,025	100	0,05	100	0,025
TotalAV	60		50		90		70	
McAfee	90		90		40		60	
Intego	40		80		70		50	
Bitdefender	70		100		50		40	
Panda	80		60		80		80	
Avira	50		40		60		90	

Для проведення розрахунків методом адитивної згортки, будемо використовувати вирази (4.15) та (4.16). Для проведення розрахунків методом мультиплікативної згортки, будемо використовувати вирази (4.16) та (4.17). Для проведення розрахунків методом максимінної згортки, будемо використовувати вирази (4.18) та (4.19). Помаранчевим кольором виділено числові значення критеріїв, які мають найменше значення для кожного альтернативного рішення.

Результат розрахунків методом адитивної згортки представлений у табл. 4.7, результат розрахунків методом мультиплікативної згортки представлені у табл. 4.8. та результат розрахунків методом максимінної згортки представлені у табл. 4.9.

Таблиця 4.7 – Метод адитивної згортки

	Результат
Norton	100*0,23+90*0,26+70*0,17+80* 0,14*100*0,1+70*0,025+100*0,05+100*0,025= 88,75
TotalAV	58,3
McAfee	76,15
Intego	53,05
Bitdefender	85,3
Panda	57,7
Avira	70,75

Таблиця 4.8 – Метод мультиплікативної згортки

	Результат
Norton	100*0,23*90*0,26*70*0,17*80* 0,14*100*0,1*70*0,025*100*0,05*100*0,025= 156,91221*10^5
TotalAV	8,069771*10^5
McAfee	27,23548*10^5
Intego	3,586565*10^5
Bitdefender	40,34885*10^5
Panda	11,47701*10^5
Avira	10,75969*10^5

Таблиця 4.9 – Метод максимінної згортки

	Критерій 1	Критерій 2	Критерій 3	Критерій 4	Критерій 5	Критерій 6	Критерій 7	Критерій 8
Norton	23	23,4	11,9	11,2	10	1,75	5	2,5
TotalAV	13,8	10,4	13,6	7	6	1,25	4,5	1,75
McAfee	20,7	18,2	8,5	14	9	2,25	2	1,5
Intego	11,5	15,6	6,8	8,4	4	2	3,5	1,25
Bitdefender	18,4	26	15,3	12,6	7	2,5	2,5	1
Panda	9,2	13	10,2	9,8	8	1,5	4	2
Avira	16,1	20,8	17	5,6	5	1	3	2,25

Отже, шляхом вирішення задач методами згортки, визначили, що Norton є оптимальним під час вибору, тобто він найкращий антивірус для використання.

Завдання 4.2: При виборі найкращої SIEM системи представлені 4 варіанти та розглянутий у цьому порівнянні одне рішення, яке не є SIEM системою, але має схожий функціонал. Саме тому прийнято рішення розглядати цей варіант серед SIEM систем. Нормовані за 100-бальною шкалою результати критеріїв та їх відповідні вади представлені в таблиці 4.10.

Таблиця 4.10 – Вихідні дані

	Критерій 1		Критерій 2		Критерій 3		Критерій 4	
	Налаштовані звіти	Вага критерію	Управління логами	Вага критерію	Правила кореляції	Вага критерію	Застосування правил кореляції у часі	Вага критерію
1	2	3	4	5	6	7	8	9
IBM Security QRadar SIEM	90	0,035	100	0,045	100	0,055	100	0,05
Splunk Enterprise	80		90		80		80	
McAfee	60		80		90		90	

FIREEYE Helix Security Platform	100		60		70		70	
Rapid7 InsightIDR	60		70		60		60	

Продовження таблиці 4.10

1	2	3	4	5	6	7	8	9
	Критерій 5		Критерій 6		Критерій 7		Критерій 8	
	Резервування конфігурації системи	Вага критерію	Агрегація подій за типом	Вага критерію	Використання алгоритмів машинного навчання	Вага критерію	Проведення розслідувань	Вага критерію
IBM Security QRadar SIEM	100	0,035	100	0,047	70	0,075	100	0,06
Splunk Enterprise	80		70		60		80	
FIREEYE Helix Security Platform	70		60		100		60	
Rapid7 InsightIDR	60		80		80		90	
	Критерій 9		Критерій 10		Критерій 11		Критерій 12	
	Управління інцидентами та їх усунення	Вага критерію	Підтримка хмарних сервісів	Вага критерію	Виявлення аномалій з урахуванням поведінки	Вага критерію	Автоматизовані робочі процеси	Вага критерію
IBM Security QRadar SIEM	100	0,068	80	0,073	80	0,082	60	0,07
Splunk Enterprise	80		70		90		70	
McAfee	90		90		70		90	

FIREEYE Helix Security Platform	70		100		100		100	
Rapid7 InsightIDR	60	0,068	60	0,073	60	0,08	80	0,07

Продовження таблиці 4.10

1	2	3	4	5	6	7	8	9
	Критерій 13		Критерій 14		Критерій 15		Критерій 16	
	Сповіщення та попередження у реальному часі	Вага критерію	Розширене виявлення погроз	Вага критерію	Виявлення інсайдерських загроз	Вага критерію	Пробний період	Вага критерію
IBM Security QRadar SIEM	100	0,085	90	0,075	90	0,092	100	0,053
Splunk Enterprise	60		70		70		80	
McAfee	90		60		60		70	
FIREEYE Helix Security Platform	70		100		100		60	
Rapid7 InsightIDR	80		80		80		90	

Рішення: Результати розрахунків методом адитивної згортки представлені у табл. 4.11. Результати розрахунків методом мультиплікативної згортки представлені у табл. 4.12. Результати розрахунків методом максимінної згортки представлені у табл. 4.13.

Таблиця 4.11 – Метод адитивної згортки

	Результат
IBM Security QRadar SIEM	90*0,035+100*0,045+100*0,055+100* 0,05+100*0,035+100*0,047+70*0,075+100* 0,06+100*0,068+80*0,073+80*0,082+60*0,07+100*0,085+90*0,075+90*0,092+100* 0,053= 89,83
Splunk Enterprise	74,5
McAfee	79,59

FIREEYE Helix Security Platform	83,01
Rapid7 InsightIDR	72,72

Таблиця 4.12 – Метод мультиплікативної згортки

	Результат
IBM Security QRadar SIEM	90*0,035*100*0,045*100*0,055*100*0,05*100*0,035*100*0,047*70*0,075*100*0,06*100*0,068*80*0,073*80*0,082*60*0,07*100*0,085*90*0,075*90*0,092*100* 0,053=5,564626402*10^11
Splunk Enterprise	0,291868246*10^11
McAfee	0,652078172*10^11
FIREEYE Helix Security Platform	0,618549444*10^11
Rapid7 InsightIDR	0,118157407*10^11

Таблиця 4.13 – Метод максимінної згортки

	IBM Security QRadar SIEM	Splunk Enterprise	McAfee	FIREEYE Helix Security Platform	Rapid7 InsightIDR
1	2	3	4	5	6
Критерій 1	3,15	2,8	2,1	3,5	2,1
Критерій 2	4,5	4,05	3,6	2,7	3,15
Критерій 3	5,5	4,4	4,95	3,85	3,3
Критерій 4	5	4	4,5	3,5	3
Критерій 5	3,5	2,8	3,15	2,45	2,1
Критерій 6	4,7	3,29	4,23	2,82	3,76
Критерій 7	5,25	4,5	6,75	7,5	6
Критерій 8	6	4,8	4,2	3,6	5,4
Критерій 9	6,8	5,44	6,12	4,76	4,08
Критерій 10	5,84	5,11	6,57	7,3	4,38
Критерій 11	6,56	7,38	5,74	8?2	4,92
Критерій 12	4,2	4,49	6,3	7	5,6
Критерій 13	8,5	5,1	7,65	5,95	6,8
Критерій 14	6,75	5,25	4,5	7,5	6
Критерій 15	8,28	6,44	5,52	9,2	7,36

Критерій 16	5,3	4,24	3,71	3,18	4,77

Отже, шляхом вирішення задач методами згортки, визначили, що IBM Security QRadar SIEM є оптимальною під час вибору SIEM системою..

Завдання 4.3: При виборі найкращої програми для моніторингу мережі представлені 5 варіантів. Нормовані за 100-бальною шкалою результати критеріїв та їх відповідні вади представлені в таблиці 4.14.

Таблиця 4.14 – Вихідні дані

	Критерій 1		Критерій 2		Критерій 3	
	Підтримка різних систем	Вага критерію	Легкість встановлення	Вага критерію	Зрозумілість інтерфейсу	Вага критерію
1	2	3	4	5	6	7
Nagios	70	0,2	60	0,17	90	0,12
PRTG Network Monitor	50		80		60	
Kismet	80		70		70	
WireShark	100		90		80	
Zabbix	90		100		100	
	Критерій 4		Критерій 5		Критерій 6	
	Вартість	Вага критерію	Підходить для великих організацій	Вага критерію	Різноманітність функцій	Вага критерію
Nagios	80	0,11	70	0,18	80	0,22
PRTG Network Monitor	100		100		70	
Kismet	80	0,11	60	0,18	60	0,22
WireShark	70		80		90	
Zabbix	90		90		100	

Результати розрахунків методом адитивної згортки представлені у табл. 4.15. Результати розрахунків методом мультиплікативної згортки представлені у табл.

4.16. Результати розрахунків методом максимальної згортки представлені у табл. 4.17.

Таблиця 4.15 – Метод адитивної згортки

	Результат
Nagios	70*0,2+60*0,17+90*0,12+80* 0,11+70*0,18+80*0,22 = 74
PRTG Network Monitor	75,2
Kismet	69,1
WireShark	86,8
Zabbix	95,1

Таблиця 4.16 – Метод мультиплікативної згортки

	Результат
Nagios	70*0,2*60*0,17*90*0,12*80* 0,11*70*0,18*80*0,22 = 3,009662853*10^6
PRTG Network Monitor	2,98577664*10^6
Kismet	2,006441902*10^6
WireShark	6,449277542*10^6
Zabbix	12,95613792*10^6

Таблиця 4.17 – Метод максимінної згортки

	Критерій 1	Критерій 2	Критерій 3	Критерій 4	Критерій 5	Критерій 6
Nagios	14	10,2	10,8	8,8	12,6	17,6
PRTG Network Monitor	10	13,6	7,2	11	18	15,4
Kismet	16	11,9	8,4	8,8	10,8	13,2
WireShark	20	15,3	9,6	7,7	14,4	19,8
Zabbix	18	17	12	9,9	16,2	22

Отже, шляхом вирішення задач методами згортки, визначили, що Zabbix є оптимальним під час вибору, тобто він найкраща програма для моніторингу мережі для використання.

Завдання 4.4: При виборі найкращого брандмауерів представлені 6 варіантів. Нормовані за 100-бальною шкалою результати критеріїв та їх відповідні вади представлені в таблиці 4.18.

Таблиця 4.18 – Вихідні дані

	Критерій 1		Критерій 2		Критерій 3	
	Призначений для LAN	Вага критерію	Призначений для хмарних мереж	Вага критерію	Наявність вбудованої IDS/IPS	Вага критерію
1	2	3	4	5	6	7
Kerio WinRoute	70		90		90	

Forcepoint	60	0,23	50	0,11	70	0,19
Cisco	100		60		80	
NordLayer	90		100		60	
Fortinet	50	0,23	80	0,11	50	0,19
VMware	80		90		100	

Продовження таблиці 4.18

1	2	3	4	5	6	7
	Критерій 4		Критерій 5		Критерій 6	
	Вартість	Вага критерію	Є рішення для різних видів організацій	Вага критерію	Належність до брандмауерів наступного покоління	Вага критерію
Kerio WinRoute	60	0,08	50	0,25	80	0,14
Forcepoint	100		70		90	
Cisco	50		100		60	
NordLayer	80	0,08	60	0,25	50	0,14
Fortinet	70		90		100	
VMware	90		80		70	

Результати розрахунків методом адитивної згортки представлені у табл. 4.19. Результати розрахунків методом мультиплікативної згортки представлені у табл. 4.20. Результати розрахунків методом максимальної згортки представлені у табл. 4.21.

Таблиця 4.19 – Метод адитивної згортки

	Результат
Kerio WinRoute	70*0,23+90*0,11+90*0,19+60*0,08+50*0,25+80*0,14 = 71,6
Forcepoint	70,7
Cisco	82,2
NordLayer	71,5
Fortinet	71,9

VMware	84,3

Таблиця 4.20 – Метод мультиплікативної згортки

	Результат
Kerio WinRoute	70*0,23*90*0,11*90*0,19*60*0,08*50*0,25*80*0,14 = 1,831582368*10^6
Forcepoint	1,78070508*10^6
Cisco	1,9381824*10^6
NordLayer	1,74436416*10^6
Fortinet	1,6959096*10^6
VMware	4,884219648*10^6

Таблиця 4.21 – Метод максимінної згортки

	Критерій 1	Критерій 2	Критерій 3	Критерій 4	Критерій 5	Критерій 6
Kerio WinRoute	16,1	9,9	17,1	4,8	12,5	11,2
Forcepoint	13,8	5,5	13,3	8	17,5	12,6
Cisco	23	6,6	15,2	4	25	8,4
NordLayer	20,7	11	11,4	6,4	15	7
Fortinet	11,5	8,8	9,5	5,6	22,5	14
VMware	18,4	9,9	19	7,2	20	9,8

Отже, шляхом вирішення задач методами згортки, визначили, що VMware є оптимальним під час вибору, тобто він найкращий брандмауер для використання.

В цьому розділі було розглянуто такі засоби захисту як антивірус, програми управління інформаційною безпекою, програми для моніторингу мережі та брандмауери. Проведений порівняльний аналіз конкретних рішень серед кожного виду засобів захисту та запропоновані оптимальні рішення серед них.

Завдання 4.5: При виборі найкращої платформи безпеки кінцевих точок представлені 6 варіантів. Нормовані за 100-бальною шкалою результати критеріїв та їх відповідні вади представлені в таблиці 4.22.

Таблиця 4.22 – Вихідні дані

	Критерій 1		Критерій 2		Критерій 3	
	Простота використання	Вага критерію	Виявлення та нейтралізації атак	Вага критерію	Кросплатформеність	Вага критерію
1	2	3	4	5	6	7
Central Endpoint Intercept X	100		70		70	
Microsoft Defender	80		80		80	
McAfee	70	0,15	100	0,12	90	0,23

Symantec Endpoint Security Enterprise	90		90		100	

Продовження таблиці 4.22

1	2	3	4	5	6	7
	Критерій 4		Критерій 5		Критерій 6	
	Захист від шкідливих програм	Вага критерію	Призначений для хмарних мереж	Вага критерію	Консоль управління безпекою	Вага критерію
Central Endpoint Intercept X	70	0,14	80	0,19	90	0,17
Microsoft Defender	90		90		70	
McAfee	100		70		80	
Symantec Endpoint Security Enterprise	80		100		100	

Результати розрахунків методом адитивної згортки представлені у табл. 4.23. Результати розрахунків методом мультиплікативної згортки представлені у табл. 4.24. Результати розрахунків методом максимальної згортки представлені у табл. 4.25.

Таблиця 4.23 – Метод адитивної згортки

	Результат
Central Endpoint Intercept X	100*0,15+70*0,12+70*0,23+70*0,14+80*0,19+90*0,17 = 79,8
Microsoft Defender	81,6
McAfee	84,1
Symantec Endpoint Security Enterprise	94,5

Таблиця 4.24 – Метод мультиплікативної згортки

	Результат

Central Endpoint Intercept X	100*0,15*70*0,12*70*0,23*70*0,14*80*0,19*90*0,17 = 4,623357917*10^6
Microsoft Defender	5,434804408*10^6
McAfee	6,604797024*10^6
Symantec Endpoint Security Enterprise	12,13125984*10^6

Таблиця 4.25 – Метод максимінної згортки

	Критерій 1	Критерій 2	Критерій 3	Критерій 4	Критерій 5
Central Endpoint Intercept X	15	8,4	16,1	9,8	15,2
Microsoft Defender	12	9,6	18,4	12,6	17,1
McAfee	10,5	12	20,7	14	13,3
Symantec Endpoint Security Enterprise	13,5	10,8	23	11,2	19

Отже, шляхом вирішення задач методами згортки, визначили, що Symantec Endpoint Security Enterprise є оптимальним, тобто він найкращий брандмауер для використання.

4.5 Основні висновки щодо оптимального вибору засобу захисту

Для проведення аналізу та для оптимального вибору засобів захисту було проведено дослідження методів вирішення багатокритеріальних здач. Вибрано для проведення подальшого аналізу методи згортки, так як ці методи найкраще підходять для поставленої задачі та більш повноцінно відображають кількісну характеристику вибраних засобів захисту. Кількісна характеристика критеріїв засобів захисту вибрана на основі експертних оцінок. Вибір засобів захисту та рішень в кожному виді, зроблено на основі проведеного дослідження та аналізу існуючих програмних та апаратних засобів захисту та їх функціоналу.

Після проведеного порівняльного аналізу конкретних рішень серед кожного виду засобів захисту запропоновані оптимальні рішення серед них. З цих розрахунків можна зробити висновок, що найкращими засобами захисту є антивірусне програмне забезпечення Norton, IBM Security QRadar SIEM, Symantec Endpoint Security Enterprise, програма для моніторингу мережі Zabbix та брандмауер VMware.

Запропонована математична модель оптимального вибору засобів захисту інформації враховує підходити до оцінки ефективності КСЗІ, визначення показника ефективності та має в своєму складі приклад оптимального вибору складу засобів захисту. Також важливим досягненням є розробка алгоритму оптимального вибору засобів захисту інформації. Такий алгоритм є актуальним та новаторським, так як враховує такий показник, як показник ефективності.

ВИСНОВКИ

В даній магістерській роботі представлені результати досліджень за напрямом, що є актуальним у кібербезпеці, а саме – вирішення задачі оптимізації складу комплексу засобів захисту від загроз безпеки в інформаційних системах.

У роботі представлена математична модель, яка базується на показнику, який відображає зменшення ризику для певного інформаційного ресурсу (у грошовому еквіваленті) завдяки використанню засобу захисту в разі реалізації певної загрози відносно ресурсу, що захищається, з урахуванням вартості заходу щодо захисту.

Також, на основі цієї моделі розроблено алгоритм оптимального вибору КЗЗ для побудови КСЗІ, який також є важливим досягненням. Для розробки такої моделі попередньо було детально проаналізовано процес побудови КСЗІ, різні види сучасних засобів захисту з прикладами конкретних продуктів, а також різноманітні сучасні атаки на КС. Наведено приклад побудови моделі загроз та моделі порушника для типової КС, оскільки ці поняття є принциповими для побудови КСЗІ.

Після цього було проведено огляд наявних методів вибору засобів захисту, що використовуються в Україні, основним з яких є нормативний підхід. Виділені його недоліки, головний з яких є відсутність конкретної оцінки для окремих механізмів захисту інформації, однак до переваг можна віднести простоту використання.

Далі, наведено приклад використання розробленої математичної моделі, для гіпотетичної комп’ютерної системи, яка функціонує 1 рік, для трьох загроз та п’яти різних ЗЗЗІ. Продемонстровано адекватність моделі та зручність її використання.

Однозначною перевагою моделі є наявність кількісного критерію оцінки захищеності КС, що враховує бюджет на впровадження КСЗІ. Водночас, недоліком моделі є те, що для розрахунків використовуються величини, визначені експертним методом, що знижує точність такої моделі.

Недостатня формалізація є проблемою інформаційної безпеки в цілому, оскільки на даний момент не існує критеріїв, що були б визначені суто математично, виходячи з даних про ресурси системи, моделі загроз та порушника. Однак моделі, подібні до розробленої у даній роботі наближають фахівців з

інформаційної безпеки до появи таких критеріїв. Ця робота може бути використана у подальших дослідженнях на теми моделювання КСЗІ, формалізації підходів до вибору засобів захисту інформації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Цыбулин А.М., Арьков П.А. Модели, безопасности информационных систем. *Проблемы современного этапа реформ России: федеральный и региональный аспекты*: материалы конф. ГОУ ВП0 ВАГС. Волгоград, 2005

2. Борисов Р. Обзор математических моделей для модели оптимизации комплексной системы защиты информации в современных автоматизированных системах обработки данных. *Международный журнал прикладных наук и технологий «Integral»*. 2019. Вип. 2, ч. 2. С. 211 – 218.

3. Тищенко Е.Н., Строкачева О.А. Вероятностные методы анализа защищенности систем электронной коммерции. *Информационная безопасность* : материалы VIII науч.–практ. Конф. Часть 1 – Таганрог: ТРТУ, 2006. С. 204 – 207

4. Тумоян Е.П. Метод моделирования компьютерных атак на основе вероятностных автоматов. *Информационная безопасность* : материалы VIII науч.–практ. Конф. Часть 1 – Таганрог: Изд–во ТТИ ЮФУ, 2008 – С. 190 – 194

5. Колегов Д.Н. Проблемы анализа и синтеза графов URL: http://www.securitylab.ru/contest/299868.php (дата звернення: 23.11.2023)

6. Курилов, Ф. М. Моделирование систем защиты информации. Приложение теории графов. *Технические науки: теория и практика* : материалы III Междунар. науч. конф. Чита : Издательство Молодой ученый, 2016. — С. 6 – 9. URL: https://moluch.ru/conf/tech/archive/165/9766/ (дата обращения: 23.11.2023).

7. Кудрявцева Р.Т., Савина И.А., Шарипова И.И. Алгоритм расчета рисков при оценке защищенности организации *Информационная безопасность* : Материалы VIII науч.–практ. Конф. Часть 1 – Таганрог: ТРТУ, 2006. С. 95 – 98

8. Иванов В.П. Математическая оценка защищенности информации от несанкционированного доступа. *Специальная техника.* 2004. №1.

9. Козлов В.Н., Нестеров В.А. Использование игровой модели при проектировании комплекса средств защиты информации в автоматизированной системе. *«Методы и технические средства обеспечения безопасности информации»* : тезисы докладов. СПб.: Изд-во СПбГТУ, 2000. С. 42 – 43.

10. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Горячая линия – Телеком. М., 2004. 280 с.

11. Клочкова Д.Ю., Пшеничних С.В. Класифікація моделей систем захисту інформації. Матеріали дев'ятої Міжнародної науково-технічної конференції «Інформаційно-комунікаційні технології та кібербезпека» (ІКТК-2023). Харків, ХНУРЕ, 2023, С. 196-197. URL: https://ice.nure.ua/wp-content/uploads/2024/01/59_Klochkova-D.Iu.-Pshenychnykh-S.V._2._Str.196-197.pdf (дата звернення: 01.01.2024).

12. Белов С. В. Формализация задачи распределения ресурсов между различными функциями обеспечения защиты информации. *Вестник Астраханского гос. технического ун-та.*. 2012. № 1. с. 112 – 116.

13. Zhu Q. Game theory meets network security: A tutorial / Q. Zhu, S. Rass // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. – January 2018. – P. 2163 – 2165.

14. Домарев В. В. Безопасность информационных технологий. Системный подход. Киев: ООО «ТИД», 2004, 912 с

15. Еременко В. Т., Рытов М. Ю., Голембиовская О. М., Рязанцев П. Н. – Комплексные системы защиты информации предприятия: учебное пособие. Орел : ФГБОУ ВО «Орловский гос. ун-т им. И.С. Тургенева», 2016. 116 с.

16. Быков А. Ю., Алтухов Н. О., Сосенко А. С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры. *Инженерный весник*. 2014. 4 апреля. С. 525 – 542

17. Карачка А. Ф. Технології захисту інформації: курс лекцій. Тернопіль: ТНЕУ, 2017. 86 с.

18. Гапак О. М. Захист інформації в інформаційних системах: підручник для студентів інженерно–технічного факультету ДВНЗ «УжНУ», Ужгород: УжНУ, 2021. 184 с.

19. Аналітичний звіт Державної служби спеціального зв'язку та захисту інформації України «Російські Кібероперації». URL: https://armyinform.com.ua/2023/10/31/derzhspeczzvyazku-pidgotuvala-analitychnyj-zvit/ (дата звернення: 13.12.2023).

20. Які тенденції кібератак взяти до уваги в 2023 році? URL: https://www.kliksolutions.com.ua/great-info/yaki-tendencziyi-kiberatak-vzyaty-do-uvagy-v-2023-roczi/ (дата звернення: 24.11.2023).

21. OWASP Top 10 API Security Risks – 2023. URL:https://owasp.org/API–Security/editions/2023/en/0x11–t10/ (дата звернення: 13.12.2023).

22. Наслідки технології 5G для безпеки. URL: https://ts2.space/uk/sc.tab=0 (дата звернення: 13.12.2023).

23. Інформаційна безпека. Загрози при роботі в Інтернеті і їх уникнення: URL: https://www.miyklas.com.ua/p/informatica/10-klas/informatciini-tekhnologiyi-v-suspilstvi-322205/informatciina-bezpeka-navchannia-v-interneti-321523/re-0cf3c5d6-6a11-458b-b39d-889f102e9e71 (дата звернення: 29.11.2023).

24. Кібератака: веб–сайт. URL: https://vue.gov.ua/ (дата звернення: 29.11.2023).

25. Найбільш розповсюджені види сучасних комп'ютерних загроз: URL: https://ema.com.ua/wpcontent/uploads/2018/08/material_02_10_2014_recent_fraud_scheme.pdf (дата звернення: 29.11.2023).

26. Іванов В. Г., Іванов С. М., Карасюк В. В. та ін. Правова інформація та комп'ютерні технології в юридичній діяльності: навч. посіб. / за заг. ред. В.Г. Іванова. Харків : Право, 2010. 240 с.

27. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. Київ : Видавнича група BHV, 2009. 608 с.

28. Протасов И.Д. Теория игр и исследование операций: учеб. пособ. Москва : Гелиос АРВ, 2003. 368 с.

29. Богуш В. М. Кіберпростір: основи кібербезпеки та кіберзахисту: Навч. посіб. у 3-х част. Ч. 3: Основи кіберзахисту / В. М. Богуш, В. Д. Бровко, В. П. Настрадін Київ : нац. акад. СБУ, 2020. 272 с.

30. Хорев П. Б. Методы и средства защиты информации в компьютерных, системах. Москва : издательский центр «Академия», 2005. 256 с.

31. Антивірусна програма. URL: https://uk.wikipedia.org/wiki/ (дата звернення: 01.01.2024).

32. Проксі-сервер. URL: https://uk.wikipedia.org/wiki/ (дата звернення: 01.01.2024).

33. Брандмауер. URL: https://www.eset.com/uaru/support/information/entsiklopediya-ugroz/brandmauer/ (дата звернення: 01.01.2024).

34. Що таке VPN, і як ним безпечно користуватись. URL: https://cip.gov.ua/ua/news/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis (дата звернення: 01.01.2024).

35. SIEM. URL: https://uk.wikipedia.org/wiki/SIEM (дата звернення: 01.01.2024).

36. Система запобігання вторгнень. URL: https://cloudnetworks.ru/inf-bezopasnost/ids-ips/

37. Топ 10 кращих програм для моніторингу мереж у 2023. URL: https://www.softinventive.ru/best-network-monitoring-tools (дата звернення: 16.12.2023).

38. Рейтинг найкращих антивірусів – ТОП-10 програм. URL: https://itc.ua/articles/rejting-antivirusov/ (дата звернення: 16.12.2023).

39. Обзор решений SIEM (Security information and event management). URL: https://habr.com/ru/companies/roi4cio/articles/528770/ (дата звернення: 16.12.2023).

40. B2B platform for IT buyers, vendors and suppliers. URL: https://roi4cio.com/ (дата звернення: 01.01.2024).

41. The Top 11 Network Firewall Solutions. URL: https://expertinsights.com/insights/the-top-11-network-firewalls/ (дата звернення: 16.12.2023).

42. Sophos Central Intercept X. URL: https://www.softkey.ua/catalog/data_protection/sophos-central-endpoint-advanced/ (дата звернення: 13.01.2024).

43. Microsoft Defender для кінцевої точки. URL: https://learn.microsoft.com/ru-ru/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection (дата звер-нення: 13.01.2024).

44. McAfee Endpoint Threat Defense and Response Family. URL: https://www.pugh.co.uk/wp-content/uploads/2017/08/mcafee-endpoint-threat-defense.pdf (дата звернення: 13.01.2024).

45. Symantec Endpoint Security Enterprise. URL: https://www.fortsoft.com.ua/ua/catalog/zashchita-informatsii/symantec-endpoint-security.html (дата звернення: 13.01.2024).

46. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Чинний від. 28.12.2012. Київ : Державна служба спеціального зв'язку України, 1999. 60 с.

47. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Чинний від 01.07.1999. Київ : Державна служба спеціального зв'язку України, 1999. 18 с.

48. НД ТЗІ 2.5-007-07. Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу 1. Чинний від 21.09.2007. Вид. офіц. Київ : Державна служба спеціального зв'язку України, 2007. 9 с.

49. Клочкова Д.Ю., Пшеничних С.В. Математична постановка задачі оптимального вибору засобів захисту при проектуванні комплексної системи захисту інформації. Матеріали дев'ятої Міжнародної науково-технічної конференції «Інформаційно-комунікаційні технології та кібербезпека» (ІКТК-2023). Харків, ХНУРЕ, 2023, С. 194 – 195. URL: https://ice.nure.ua/wp-content/uploads/2024/01/58_Klochkova-D.Iu.-Pshenychnykh-S.V._1_Str.194-195.pdf (дата звернення: 01.01.2024).

50. Пшеничних С.В, Добринін І.С., Клочкова Д.Ю. Математична модель оптимального вибору засобів захисту інформації в інформаційній системі. Матеріали дев'ятої Міжнародної науково-технічної конференції «Інформаційно-комунікаційні технології та кібербезпека» (ІКТК-2023). Харків, ХНУРЕ, 2023, С. 198 – 199. URL: https://ice.nure.ua/wp-content/uploads/2024/01/60_Pshenychnykh-S.V-Dobrynin-I.S.-Klochkova-D.Iu._Str.198-199.pdf (дата звернення: 01.01.2024).

51. Пшеничних С.В, Добринін І.С., Клочкова Д.Ю. Математична модель оптимального вибору засобів захисту інформації при проектуванні комплексної системи захисту на об'єкті інформатизації. *Проблеми телекомунікацій*, 2023. № 1(32). С. 3 – 16.

52. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Усов Я. Ю. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. Ніжин : ТПК «Орхідея», 2019. 144 с.

53. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Комплексні системи захисту інформації : навч. посіб. Вінниця : ВНТУ, 2018. 118 с.

54. Богуш В. М. Теоретичні основи захищених інформаційних технологій: навч. посіб. / Б. М. Богуш, О. А. Довидьков, В. Г. Кривуца. Київ : ДУІКТ, 2010. 454 с.

55. Юдін О. К. Захист інформації в мережах передачі даних / О. К. Юдін, О. Г. Корченко, Г. Ф. Конахович. Київ : Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. 716 с.

56. Отчет «Понимание кибер-угроз 2020». URL: https://iitd.com.ua/wp-content/uploads/2020/05/pandalabs-threat-insights-2020.pdf (дата звернення: 22.01.2024).

57. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів : «Новий Світ-2000», 2020. 678 с.

58. Методи розв'язування задач багатокритеріальної оптимізації: методичні вказівки та завдання до самостійної роботи для студентів IV курсу денної форми

навчання напрямів підготовки 6.040301 Прикладна математика та 6.040201 Математика / О. Б. Васильєв, Н. С. Васильєва, О. Д. Кічмаренко. Одеса : Одеський нац. ун-т ім. І. І. Мечникова, 2017. 48 с.