Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Стативи Богдана Олександровича*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *кібербезпека*

на тему *Вдосконалення методу захисту хмарних даних із контролем ліній зв'язку інформаційно-комунікаційних систем*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н.,проф. Корнієнко В. І.			
розділів:				
спеціальний	д.т.н.,проф. Корнієнко В. І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Стативи Богдану Олександровичу* **академічної групи** *125м-20-2*

(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

(код і назва спеціальності)

на тему *Вдосконалення методу захисту хмарних даних із контролем ліній зв'язку інформаційно-комунікаційних систем*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.21 №1036-е

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз загроз, що впливають на стан захисту даних в ІКС. Аналіз вимог інформаційної безпеки та антивірусного захисту в ІКС. Засоби та методи забезпечення заданих вимог.	22.11.2021
Розділ 2	Алгоритм формування множин маршрутів передачі метаданих. Алгоритм пошуку найкоротших шляхів в ІКС. Алгоритм безпечної маршрутизації на базовій безлічі шляхів. Оцінка ефективності методу захисту хмарних даних. Практичні рекомендації.	20.12.2021
Розділ 3	Техніко-економічне обґрунтування доцільності запровадження запропонованих в роботі рішень.	10.01.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі:

Дата подання до екзаменаційної комісії:

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 91 с., 19 рис., 4 табл., 4 додатків, 36 джерела.

Об'єкт дослідження: забезпечення інформаційної безпеки під загрозою впливів комп'ютерних вірусів.

Предмет дослідження: метод антивірусного захисту даних в ІКС.

Метою кваліфікаційної роботи є: дослідження та вдосконалення методу антивірусного захисту даних в ІКС з використанням сучасних хмарних обчислювальних систем.

У першому розділі кваліфікаційної роботи проводиться аналіз загроз, що впливають на стан захисту даних в ІКС, аналізи вимог інформаційної безпеки та вимоги антивірусного захисту в ІКС. Приводяться до розгляду засоби та методи забезпечення заданих вимог, та обгрунтування вибору напрямку дослідження.

У другому розділі кваліфікаційної роботи запропоновані алгоритми формування множин маршрутів передачі метаданих, з використанням алгоритмів пошуку найкоротших шляхів, формування базової множини маршрутів та безпечної маршрутизації. Представлені методи контролю ліній зв'язку ІКС та модель системи нейромережевих експертів безпечної маршрутизації. Також дана оцінка ефективності методу та практичні рекомендації щодо застосування.

У третьому розділі кваліфікаційної роботи розраховані капітальні витрати на придбання нового програмного забезпечення та її модернізація, витрати на її експлуатацію та щорічну підтримку. Також розрахована оцінка можливого збитку й аналіз економічної ефективності системи. Доведена економічна доцільність запропонованого методу щодо розглянутого підприємства ТОВ «Машина».

АНТИВІРУСНИЙ ЗАХИСТ, ХМАРНІ ОБЧИСЛЮВАЛЬНІ ТЕХНОЛОГІЇ, МНОЖИНА МАРШРУТІВ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕА, НЕЙРОМЕРЕЖЕВІ ЕКСПЕРТИ.

РЕФЕРАТ

Пояснительная записка: 91 с., 19 рис., 4 табл., 4 приложений, 36 источника.

Объект исследования: обеспечение информационной сохранности под опасностью действий компьютерных вирусов.

Предмет исследования: метод антивирусной защиты данных в ИКС.

Целью квалификационной работы является: исследование и усовершенствование метода антивирусной защиты данных в ИКС с использованием современных облачных вычислительных систем.

В первом разделе квалификационной работы проводится анализ угроз, влияющих на состояние защиты данных в ИКС, анализ требований информационной безопасности и требования антивирусной защиты в ИКС. Приводятся к рассмотрению средства и методы обеспечения заданных требований и обоснование выбора направления исследования.

Во втором разделе квалификационной работы предложены алгоритмы формирования множества маршрутов передачи метаданных, с использованием алгоритмов поиска кратчайших путей, формирования базового множества маршрутов и безопасной маршрутизации. Представлены методы контроля линий связи ИКС и модель системы нейросетевых экспертов безопасной маршрутизации. Дана оценка эффективности метода.

В третьем разделе квалификационной работы рассчитаны капитальные затраты на приобретение нового программного обеспечения и его модернизация, затраты на его эксплуатацию и ежегодную поддержку. Также рассчитана оценка возможного ущерба и анализ экономической эффективности системы. Доказана экономическая целесообразность предлагаемого метода рассмотренного предприятия ООО «Машина».

АНТИВИРУСНАЯ ЗАЩИТА, ОБЛАЧНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ ТЕХНОЛОГИИ, МНОЖЕСТВО МАРШРУТОВ, ИНФОРМАЦИОННО-КОММУНИКАЦИОННАЯ СИСТЕА, НЕЙРОСЕТЕВЫЕ ЭКСПЕРТЫ.

ABSTRACT

Explanatory note: 91 pages, 19 figures, 4 tables, 4 applications, 36 sources.

Object of study: ensuring information security under the threat of computer viruses.

Research subject: method of anti-virus data protection in the ICS.

The purpose of the qualification work: is research and improvement of the method of anti-virus data protection in the ICS using modern cloud computing systems.

The first section of the qualification project analyzes threats that affect the state of data protection in the ICS, the analysis of information security requirements and the requirements of antivirus protection in the ICS. The means and methods of ensuring the specified requirements and justification of the choice of research direction are considered.

In the second section of the qualification project algorithms of forming set of routes of metadata transfer, using algorithms of shortest path search, formation of basic set of routes and secure routing are proposed. It presents methods of control of ICS communication lines and a model of neural network expert system of secure routing. The effectiveness of the method and practical recommendations for stasis are also evaluated.

The third section of the qualification project calculates the capital cost of purchasing new software and upgrading it, the cost of its operation and annual support. It also calculated the assessment of the possible damage and cost-effectiveness analysis of the system. The economic feasibility of the proposed method of the considered enterprise LLC "Machine" is proved.

ANTIVIRUS PROTECTION, CLOUD COMPUTING, MULTIPLE ROUTES, INFORMATION AND COMMUNICATION SYSTEM, NEURAL NETWORK EXPERTS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВПС – вузол програмного серверу;

ВОЛЗ – волоконо-оптична лінія зв'язку;

ЗУ – закон України;

ІБ – інформаційна безпека;

ІКС – інформаційно-комунікаційна система;

ІКТ – інформаційно-комунікаційна технологія;

ІзОД – інформація з обмеженим доступом;

НСД – несанкціонований доступ;

НД ТЗІ – нормативний документ в галузі технічний захист інформації;

ХОС – хмарні обчислювальні системи;

ОС – обчислювальна система;

ОІД – об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ТОВ – товариство з обмеженою відповідальністю;

ISO – International Organization for Standardization.

ЗМІСТ

ВСТУП

За останні роки інформаційно-комунікаційні технології перебувають у постійному розвитку та вдосконаленні. Цей інтенсивний розвиток нових інформаційних та телекомунікаційних технологій надає потенційно нову якість інформаційного обігу та стає рушійною силою в таких сферах життя, як економічна, соціальна, наукова, військова та світова загалом, тощо.

Інформаційно-комунікаційні технології надають можливість представляти будь-яку інформацію (числову, текстову, звукову, зображення і т. д.) в цифровому форматі, що є придатним для зберігання, обробки, передачі на комп'ютері. Можливість передачі інформації між комп'ютерними системами за допомогою глобальної мережі Інтернет, який забезпечує доступ до світового інформаційного простору користувачеві. Але слід зауважити, що дані технології мають ряд вразливостей та можуть представляти потенційну загрозу, як окремому користувачу, так і цілій державі. Так як зловмисники зацікавлені в отриманні вигоди від різного роду інформації, що передається, обробляється та зберігається, дані процеси необхідно контролювати, ідентифікувати загрози інформаційній безпеці та ліквідувати її.

Як і десятиріччя тому, сьогодні шкідливе програмне забезпечення (комп'ютерні віруси) є головною зброєю зловмисників, яка розвивається швидкими темпами, та становить одну з головних загроз інформаційній безпеці. Тому розвиток систем, комплексів та засобів захисту інформації має бути на шаг попереду, тож існують різні підходи та засоби забезпечення захищеності інформації. Виходячи з цього, основним засобом боротьби з комп'ютерними вірусами на сьогодні є – антивірусний захист даних. В даній роботі наведені різні методи антивірусного захисту (сигнатурні та евристичні) та проводяться аналізи, дослідження цих методів, а також використання сучасних хмарних технологій.

Таким чином, для підвищення надійності, захищеності даних, своєчасної локалізації комп'ютерних вірусів та інших дій зловмисників постає

необхідність у вдосконаленні вже існуючих антивірусних засобів захисту в інформаційно-комунікаційних системах з використанням хмарних обчислювальних систем.

Метою роботи та завданням дослідження є:

1. Проаналізувати вимоги інформаційної безпеки та антивірусного захисту;
2. Вдосконалення методу контролю ліній зв'язку ІКС;
3. Вдосконалення моделі системи нейромережевих експертів безпечної маршрутизації;
4. На основі отриманих даних вдосконалити метод антивірусного захисту в ІКС;
5. Оцінка ефективності методу та економічна доцільність впровадження методу.

Об'єктом дослідження є вдосконалення методу забезпечення інформаційної безпеки від комп'ютерних вірусів.

Предметом дослідження є метод антивірусного захисту в ІКС.

Практична цінність отриманих результатів полягає у дослідженні та вдосконаленні методу антивірусного захисту в ІКС та у вдосконаленні алгоритму передачі метаданих в хмарні антивірусні системи

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

У цьому розділі аналізуються основні загрози, що впливають на стан захисту даних в інформаційно-комунікаційних системах (ІКС), вимоги до інформаційної безпеки та антивірусного захисту в ІКС, розглядаються засоби та методи забезпечення заданих вимог, обґрунтовування вибору напрямку дослідження та формування задачі вдосконалення методу антивірусного захисту даних з використанням хмарних обчислювальних технологій.

1.1 Аналіз загроз, що впливають на стан захисту даних в ІКС

Інформаційно-комунікаційні технології (ІКТ) – це загальний термін, що включає в себе всі технології передачі інформації [5]. Термін можна визначити, як комплекс дій, які пов'язані з обробкою, зберіганням та інтерпретацією інформації, відповідно з чим вона видозмінюється до потреб конкретного суб'єкта.

Стрибок в інформаційних технологій дуже швидко перетворився на життєве важливий стимул розвитку світової економіки, політики, військової сфери й майже всіх сфер людської діяльності. Сьогодні сучасне суспільство переповнене потоками інформації, які безумовно потребують обробки. Підприємства вимушені постійно модернізувати моделі та технології управління з урахуванням сучасних ІКТ, щоб покращити організацію бізнес ланцюгів підприємства та успішно реалізувати стратегію і тактику в конкурентному середовищі. Тому фактор безпеки інформаційних ресурсів і послуг при розробці та експлуатації сучасних ІКС відіграє першорядну роль.

Під загрозою безпеки інформаційним ресурсам [6] мають на увазі дії, які можуть призвести до модифікації, несанкціонованого використання або знищення інформаційних ресурсів керованої системи, а також програмних та апаратних засобів, що становить найбільшу небезпеку в політичній, економічній, оборонній і інших сферах діяльності держави (рис. 1.2).

Загрози інформаційним ресурсам можна класифікувати за наступними критеріями (рис. 1.1):

1. Інформаційної безпеки (загрози конфіденційності даних; загрози цілісності даних, програм, апаратури; загрози доступності даних; загрози відмови від виконання операцій).

2. Компоненти інформаційних систем, на які загрози націлені (інформаційні ресурси та послуги, персональні дані, програмні засоби, апаратні засоби, програмно-апаратні засоби;);

3. Способом здійснення (випадкові, навмисні дії природного та техногенного характеру);

4. Розташуванням джерела загроз (внутрішні та зовнішні.).

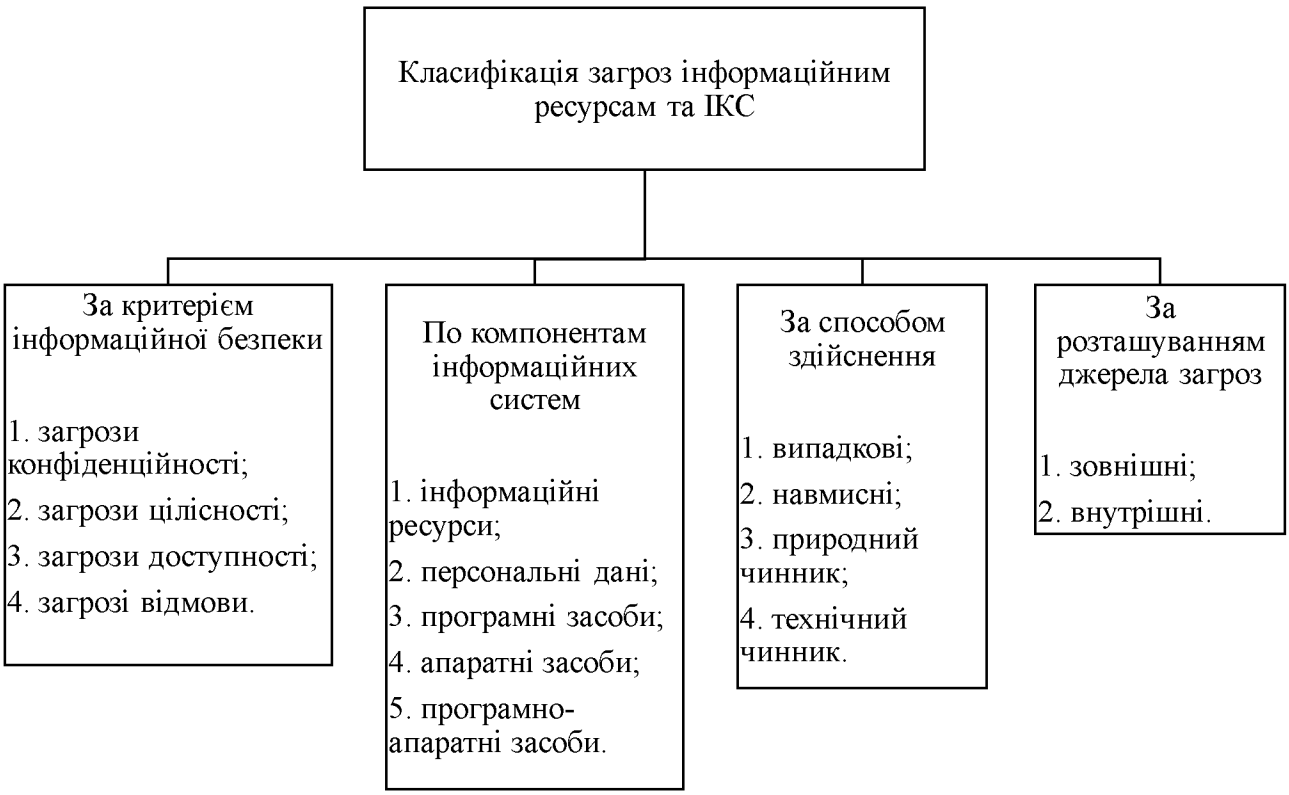

Рисунок 1.1 – Класифікація базових загроз інформаційним ресурсам та ІКС

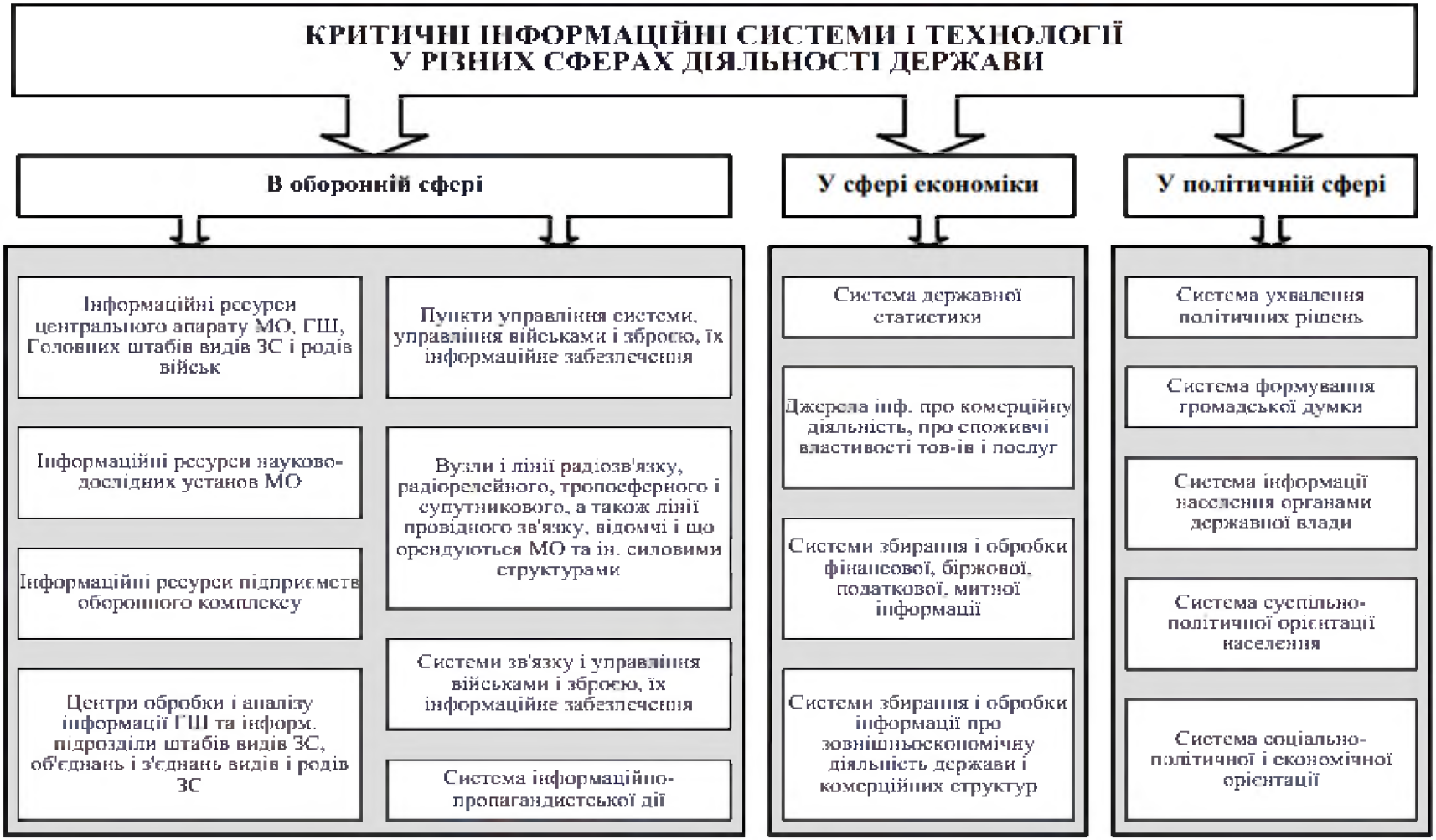

Рисунок 1.2 – Критичні інформаційні системи і технології в різних сферах

Таким чином, слід зазначити, що можливості реалізації умисних загроз останнім часом різко зросли. Це пояснюється збільшенням обчислювальної потужності комп'ютерних засобів, що знаходяться в руках зловмисників, різноманітністю програмного забезпечення, що дозволяє відтворювати програмні загрози. Реалізація умисних загроз може призвести до тяжких наслідків в обороні, промисловості, економіці, банківській сфері та інших галузях господарської діяльності, екології, житті і здоров'ї населення.

З цього можна зробити один важливий висновок – без застосування спеціальних заходів захисту існує ймовірність пошкодження ІКС, що можуть призвести до небажаних втрат або тимчасової недоступності важливих даних. Зрештою, будь-яка нова технологія приховує небезпеку, яка не завжди очевидна. Отже, задачі захисту інформації в ІКС є суперпозицією задач двох головних напрямів:

1. Захист важливої інформації, зокрема державної, військової або комерційної таємниці, від цілеспрямованих дій порушників.

2. Захист інформації від негативного впливу програмного забезпечення, некоректного функціонування комп’ютерної системи через відмову обладнання, помилки програмного забезпечення або реалізації апаратних, програмних засобів.

Також можна виділити ненавмисні дії користувачів та аварії, стихійні лиха, що становлять особливу небезпеку для комп'ютерних систем, оскільки вони спричиняють найбільш негативні наслідки. Внаслідок фізичного руйнування систем інформація стає недоступною, або втрачається зовсім.

Проаналізуємо існуючі послуги і механізми захисту інформації, розглянемо можливі підходи до забезпечення безпеки інформаційних систем і технологій.

1.2 Аналіз вимог інформаційної безпеки в ІКС

Дана тема забезпечення інформаційної безпеки знайшла своє відображення в працях таких авторів як Герасименко В О, Зегжда П. Д., Ліпаєва В. В., Стенг Д. І. та інших. Математичні методи ті інструментарій економіко-математичного моделювання в ризикології представлені в роботах Верченко П. І., Вітінського В. В., Галіцина В. К., Клебнової Т. С., Клейнера Г. Б., Матвійчука А. В. та інших [7 - 11].

Найбільша увага науковців приділяється розвитку механізмів забезпечення інформаційної безпеки, що ґрунтується на використанні апаратних, програмних та криптографічних засобів захисту.

Автори відомих праць [7 - 11] керуються такими стандартами як ISO 15408 "Загальні критерії оцінки безпеки інформаційних технологій" і даних аналізу ризиків ISO 17799 "Стандарт побудови ефективної системи безпеки". Ці стандарти відповідають спеціальним нормативним документам із гарантування інформаційної безпеки, прийнятих в Україні.

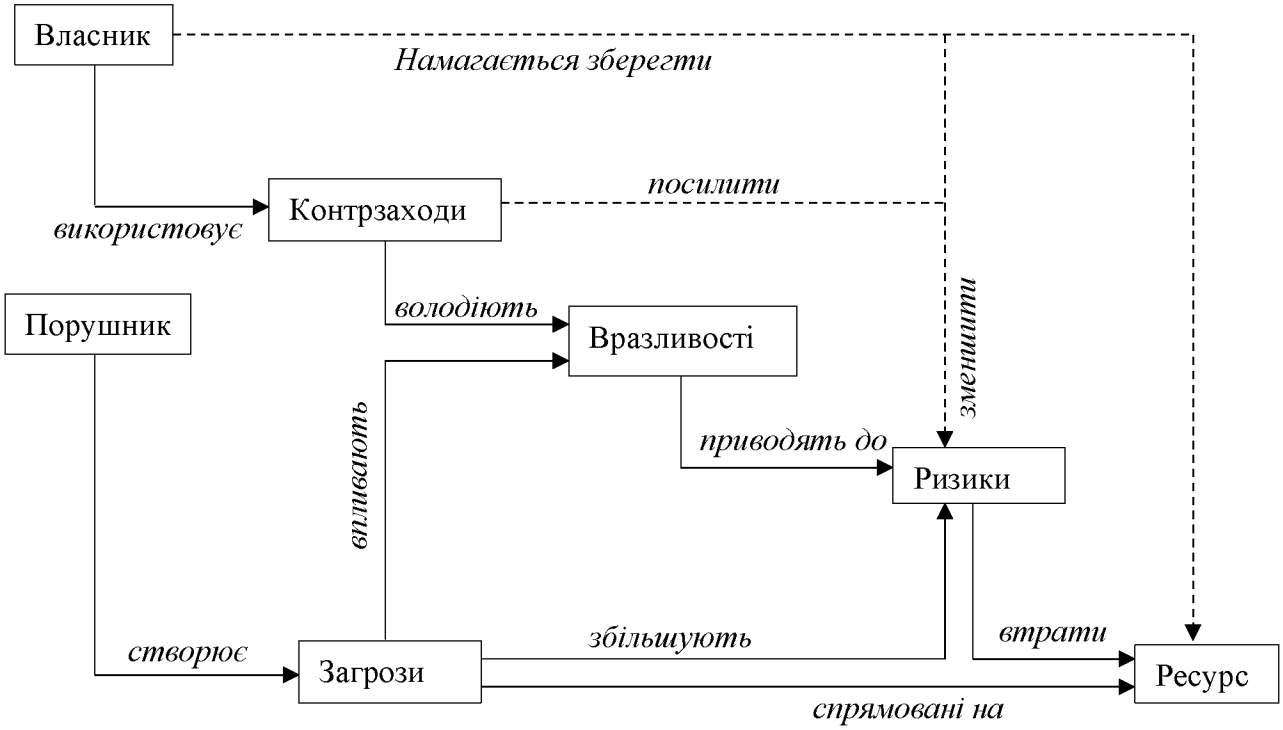

Рисунок 1.3 – Модель системи безпеки в інформаційній сфері

У попередньому розділі докладно описано ті властивості ІКС, що роблять їх уразливими до реалізації багатьох загроз. По-перше, захист системи не є головною метою, важливо досягти розумного компромісу між захищеністю, функціональністю, зручністю у використанні та вартістю системи. По-друге, сучасні технології програмування не дають змоги повністю виключити можливість виникнення помилок. Використання технологій, які зменшують імовірність виникнення помилок, призводить до значного зростання вартості розроблення програмного забезпечення, не гарантуючи повної відсутності помилок.

На рисунку 1.3 модель інформаційної безпеки, що відображає сукупність об'єктивних зовнішніх і внутрішніх чинників та їх вплив на стан інформаційної безпеки на об'єкті і на збереження матеріальних або інформаційних ресурсів. Чинники безпеки можна поділити на такі категорії, як технологічні, технічні й організаційні.

Дана методика (Рис. 1.3) дає змогу проаналізувати вимоги щодо гарантування інформаційної безпеки підприємства. Для досягнення поставленої мети необхідне вирішення певних завдань:

1. розподілення інформації за рівнями доступу;
2. прогнозування і своєчасне виявлення загроз безпеці інформаційних ресурсів;
3. створення умов, при яких найменш вірогідна загроза безпеці інформаційних ресурсів;
4. створення механізму і умов оперативного реагування на загрози інформаційній безпеці, забезпечення проведення робіт в короткі терміни;
5. створення механізму і умов для максимально можливого відшкодування і локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб;

6. забезпечення оптимального вибору заходів протидії;

7. оцінити ефективність контрзаходів, порівняти різні їх варіанти.

На основі побудованої моделі можна обґрунтовано вибрати систему контрзаходів, які здатні знизити ризики до допустимих рівнів. Обов'язковим елементом контрзаходів повинна бути регулярна перевірка ефективності системи, перевірка відповідності існуючого режиму інформаційної безпеки політиці безпеки, перевірка відповідності сертифікації інформаційної системи (технології) на відповідність вимогам певного стандарту безпеки.

Також ефективність програмних засобів захисту залежить від правильності дій користувача, які можуть бути виконані помилково або зі злим умислом. Тому необхідні наступні організаційні вимоги захисту:

1. Загальне регулювання доступу, що включає систему паролів і сегментацію вінчестера;

2. Навчання персоналу технології захисту;

3. Забезпечення фізичної безпеки комп'ютера і магнітних носіїв;

4. Вироблення правил архівування;

5. Зберігання окремих файлів в зашифрованому вигляді;

6. Створення плану відновлення диску (вінчестера) і зіпсованої інформації на неї.

Отримані дані з провідних авторів даної теми [7 – 11] показують, що один з найрозповсюдженішими і небезпечними процесами є саме впровадження шкідливих програмних засобів зловмисником. Виходячи з цього, в рамках кваліфікаційної роботи основним напрямком обрано – антивірусний захист даних.

Отже, проведемо аналіз вимог до антивірусного захисту даних в ІКС.

1.3 Аналіз вимог антивірусного захисту в ІКС

Мета створення системи антивірусного захисту – забезпечення захисту робочих станцій та серверів локальних обчислювальних мереж від деструктивного впливу комп’ютерних вірусів за мінімальних видатків на адміністрування, ресурси обчислювальної техніки та телекомунікаційне устаткування.

Механізм роботи сучасних антивірусів складається з конкретних модулів. Сучасний антивірус є складним програмним засобом, який має забезпечити надійний захист комп'ютерного пристрою (комп'ютера, кишенькового комп'ютера або нетбука) від різних вірусів (шкідливих програм). Загальна схема антивіруса представлена на рисунку 1.4:

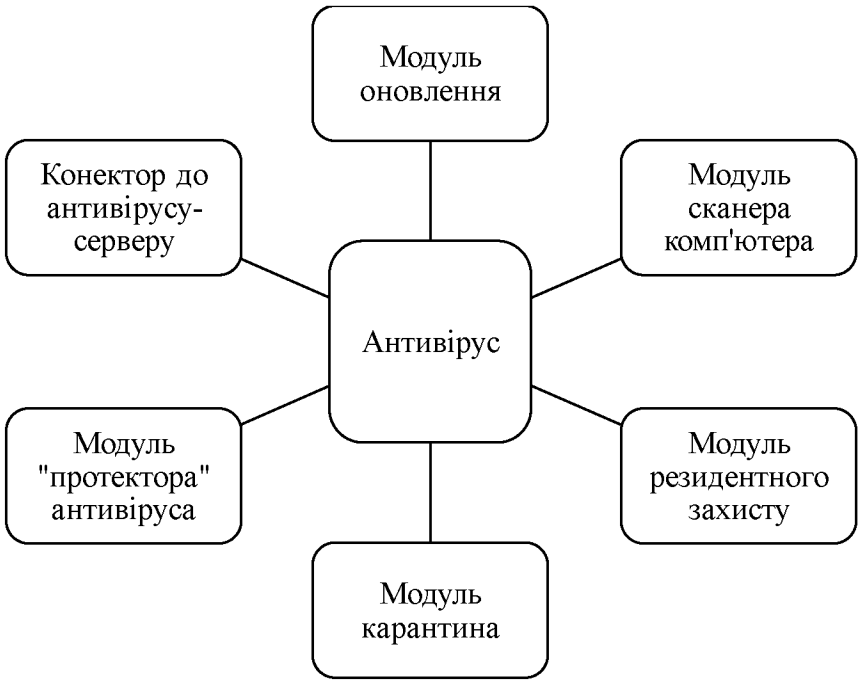

Рисунок 1.4 – Механізм роботи сучасних антивірусів

Можна виділити основні вимоги до антивірусних програм. Кількість і різноманітність вірусів велике, і щоб їх швидко і ефективно виявити, антивірусна програма повинна відповідати деяким параметрам.

Стабільність і надійність роботи. Цей параметр, без сумніву, є визначальним - навіть найкращий антивірус виявиться абсолютно марним, якщо він не зможе нормально функціонувати на вашому комп'ютері, якщо в результаті якого збою в роботі програми процес перевірки комп'ютера не пройде до кінця. Тоді завжди є ймовірність того, що у системі залишиться заражені або шкідливі файли.

Розміри вірусної бази програми (кількість вірусів, які правильно визначаються програмою). З урахуванням постійної появи нових вірусів база даних повинна регулярно оновлюватися. Сюди ж слід віднести і можливість програми визначати різноманітні типи вірусів, і вміння працювати з файлами різних типів (архіви, документи). Важливим також є наявність резидентного монітора, здійснює перевірку всіх нових файлів автоматично, по мірі їх запису на диск. Швидкість роботи програми, наявність додаткових можливостей типу алгоритмів визначення навіть невідомих програмі вірусів (евристичне сканування). Сюди ж слід віднести можливість відновлювати заражені файли, не стираючи їх з жорсткого диска, а лише видаливши з них віруси. Немаловажним є також відсоток помилкових спрацьовувань програми.

Наявність версій програми під різні операційні системи. Звичайно, якщо антивірус використовується тільки вдома, на одному комп'ютері, то цей параметр не має великого значення. Але ось антивірус для великої організації просто зобов'язаний підтримувати всі поширені операційні системи. Крім того, при роботі в мережі немаловажним є наявність серверних функцій, призначених для адміністративної роботи, а також можливість роботи з різними видами серверів.

При комплексному захисті локальної мережі необхідно приділити увагу всім можливим точкам проникнення вірусів ззовні. На рисунку 1.5 наведено загальну структуру антивірусного захисту локальної мережі. На першому рівні захищають підключення до Інтернету чи мережу постачальника послуг зв'язку - це міжмережевий екран та поштові шлюзи, оскільки за статистикою саме звідти

потрапляє близько 80% вірусів. Необхідно відзначити, що таким чином буде виявлено не більше 30% вірусів, так як 70%, що залишилися, будуть виявлені тільки в процесі виконання.

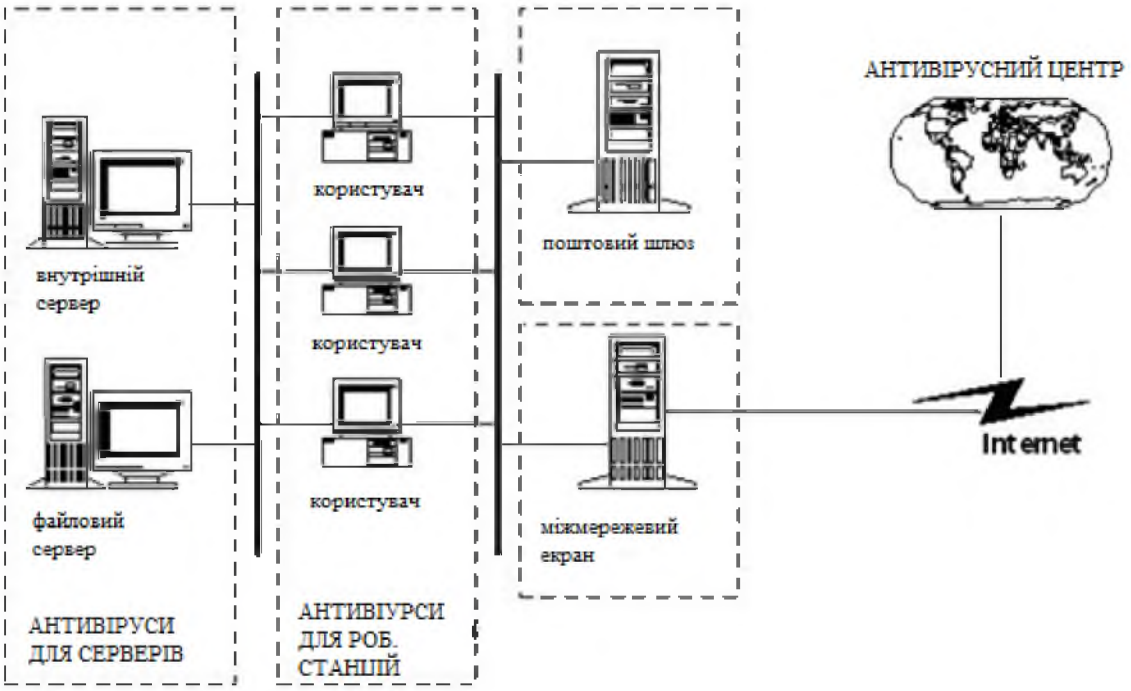

Рисунок 1.5 – Загальну структуру антивірусного захисту

Антивірусному захисту підлягають усі компоненти інформаційної системи, що беруть участь у транспортуванні інформації та/або її зберіганні: файл-сервери, робочі станції, робочі станції мобільних користувачів, сервер резервного копіювання, поштові сервери.

Дослідження праць провідних авторів з даної теми [19 - 22] дозволив сформулювати ряд тимчасових вимог до процесу виявлення шкідливого програмного забезпечення (комп'ютерних вірусів) і подати їх у вигляді таблиці 1.1. Був проведених аналіз таких моделей: SI (Suspected-Infected), SIR(Suspected-Infected-Recovered), PSIDR (Progressive Suspected-Infected-Detected-Recovered), PSIDDR (Progressive Suspected Infected Detected Death Recovered).

Таблиця 1.1 – Вимоги до часу виявлення комп'ютерних вірусів

Час функціонування системи (с)	Час розповсюдження вірусу (с)			
	SI	SIR	PSIDR	PSODDR
5	10	11	1	2
10	13	15	2	7
15	15	17	2	10
20	19	24	3	20
25	23	30	3	29
50	25	35	4	34
75	30	50	11	48
100	33	-	-	60

За цими результатами моделювання дослідників показала складність забезпечення необхідних тимчасових показників та дала відповідь щодо доцільності використання сучасних методів та засобів антивірусного захисту даних.

З усіх методів антивірусного захисту можна виділити дві основні групи: сигнатурні та евристичні методи [23 - 25].

Сигнатурні методи – точні методи виявлення вірусів, засновані на порівнянні файлу з відомими зразками вірусів.

Сигнатурний аналіз є найбільш відомим методом виявлення вірусів та використовується практично у всіх сучасних антивірусах. Сигнатурний аналіз полягає у виявленні характерних ідентифікуючих рис кожного вірусу та пошуку вірусів шляхом порівняння файлів із виявленими рисами.

Сигнатурою вірусу вважатиметься сукупність характеристик, що дозволяють однозначно ідентифікувати наявність вірусу у файлі (включаючи

випадки, коли файл цілком є вірусом). Усі разом сигнатури відомих вірусів становлять антивірусну основу. Завдання виділення сигнатур, як правило, вирішують люди - експерти в галузі комп'ютерної вірусології, здатні виділити код вірусу з коду програми та сформулювати його характерні риси у формі, найбільш зручній для пошуку.

Інша важлива, але негативна властивість – для отримання сигнатури необхідно мати зразок вірусу. Отже, сигнатурний метод непридатний захисту від нових вірусів, т. до. доки вірус не потрапив на аналіз до експертів, створити його сигнатуру неможливо. Саме тому всі найбільші епідемії викликаються новими вірусами. З моменту появи вірусу в Інтернеті до випуску перших сигнатур зазвичай проходить кілька годин, і весь цей час вірус здатний заражати комп'ютери майже безперешкодно. Майже тому, що в захисті від нових вірусів допомагають додаткові засоби захисту, розглянуті раніше, а також евристичні методи, що використовуються в антивірусних програмах.

Евристичні методи - приблизні методи виявлення, які дозволяють певною мірою припустити, що файл заражений.

Якщо сигнатурний метод виділяє ознаки вірусу і пошуку цих ознак у файлах, що перевіряються, то евристичний аналіз ґрунтується на припущенні, що нові віруси часто виявляються схожі на якісь вже відомі. Постфактум таке припущення виправдовується наявністю в антивірусних базах сигнатур визначення не одного, а відразу кількох вірусів. Засноване на такому припущенні евристичний метод полягає у пошуку файлів, які не повністю, але дуже близько відповідають сигнатурам відомих вірусів.

Позитивним ефектом від цього методу є можливість виявити нові віруси ще до того, як для них будуть виділені сигнатури але й негативні сторони це те, що є імовірність помилково визначити наявність у файлі вірусу, коли насправді файл чистий – такі події називаються хибними спрацьовуваннями. Також неможливість лікування – і через можливі помилкові спрацьовування, і через

можливе неточне визначення типу вірусу, спроба лікування може призвести до більших втрат інформації, ніж сам вірус, що не можна припускати.

Але головний недолік методів антивірусних систем зв'язаний з необхідністю постійного оновлення антивірусної бази даних, який провідні розробники намагаються подолати за допомогою хмарних обчислювальних систем. Такі системи називаються хмарні антивірусні технології, що користуються широким визнанням, але також не позбавлені недоліків. Всі онлайн-антивіруси мають одне суттєве обмеження – вони не здатні працювати у фоновому режимі. Важливість фонового сканування не можна недооцінювати. Крім того, захист одного підприємства лежить у руках іншого. Якщо компанія-постачальник раптово стане банкрутом, обслуговування серверів припиниться. У цьому випадку про повну незалежність нема чого й говорити.

Отже, можна зробити висновок, що оптимальний рівень захисту перебуває на стику двох підходів, хмарних технологій та стаціонарних.

1.4 Засоби та методи забезпечення заданих вимог

Сьогодні зростання шкідливого програмного забезпечення стає лавиноподібним майже 70 000 екземплярів на день. Як повідомляє відомий статистичний американський ресурс з кібербезпеки AV-TEST - The Independent IT-Security Institute, спираючись на дослідження у науковій літературі, були проаналізовані основні загрози інформаційної безпеки у сфері інформаційних технологій: загальна кількість заражень шкідливим програмним забезпеченням зросла за останні 10 років у 20 разів (рис. 1.6). Дослідження ґрунтувалося на кількісних та якісних результатах, одержаних при тестуванні незалежною тестовою лабораторією AV-Comparatives. Все це сприяє тому, що традиційних засобів антивірусного захисту, таких як евристичний захист та сигнатурний аналіз стає недостатньо для забезпечення безпеки.

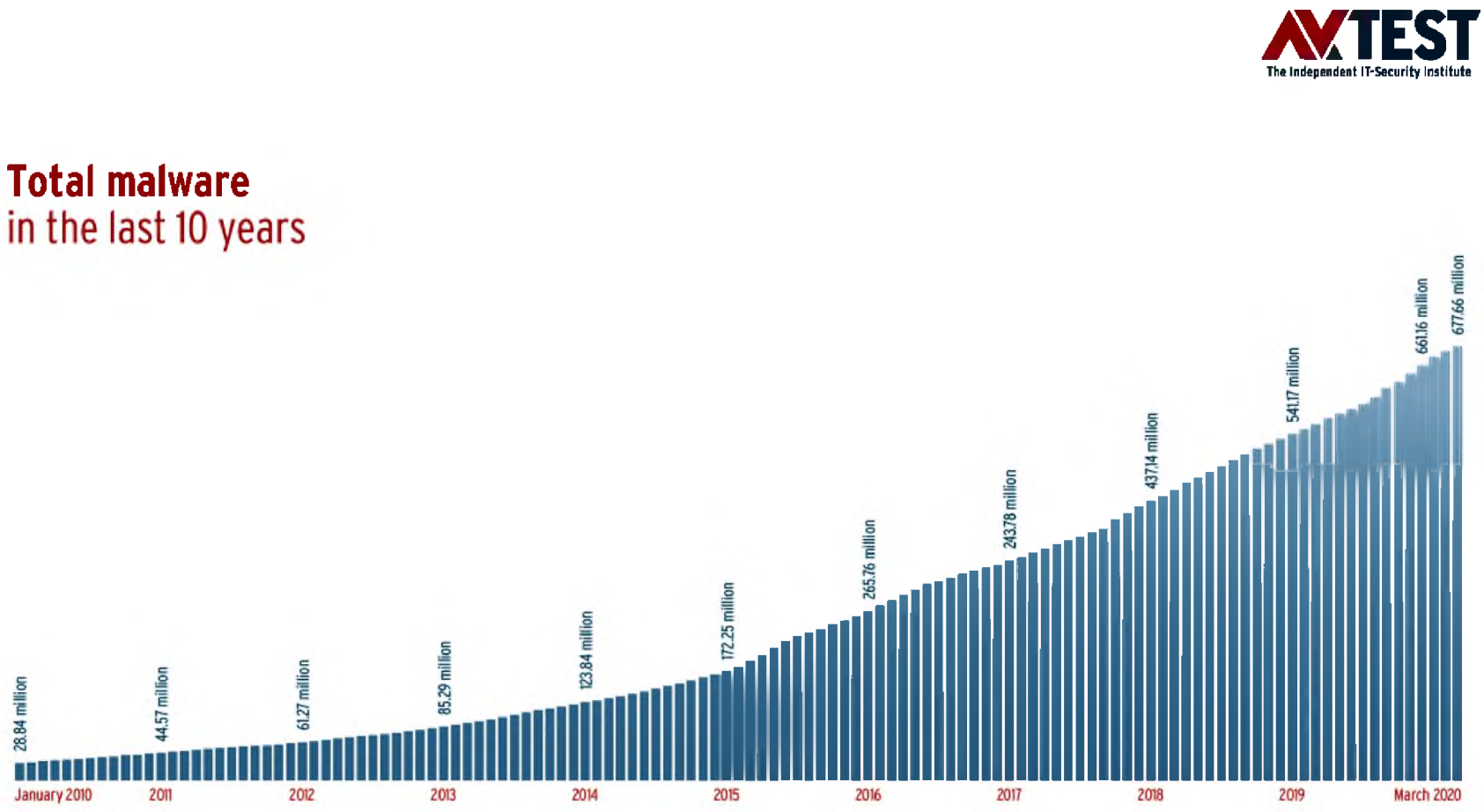

Рисунок 1.6 – Загальна кількість заражень шкідливим ПО

З попереднього аналізу дізналися про методи, при яких від постраждалого користувача або з іншого джерела до лабораторії надсилався зразок шкідливого коду, і після проведення всебічного аналізу антивірусна лабораторія випускала оновлення баз сигнатур разом із рецептом видалення вірусів. Усі клієнти завантажували це оновлення та отримували відповідний захист. Звичайно, хтось заражався раніше, ніж отримував «ліки». Але таких було не так багато. Проте йшов час, кількість загроз зростала. Виробникам антивірусного програмного забезпечення довелося максимально автоматизувати процес аналізу нових загроз, використовуючи евристичні механізми, і навіть вбудувати подібні механізми в клієнтські антивіруси. Ці технології набули широкого поширення, але проблеми вирішити не змогли. Найкращі приклади реалізації евристичного аналізу забезпечують рівень виявлення в межах 50-70% для знайомих сімейств вірусів і абсолютно безсильні перед новими видами атак.

У таких умовах необхідний якісний стрибок у промисловості безпеки. Його забезпечили «хмарні» технології захисту. Сьогодні до складу багатьох антивірусів входить «хмарна» складова. Перехід до «хмарних» технологій дозволяє спростити архітектуру продукту, який користувач ставить на свій комп'ютер, адже тепер для кожного підозрілого ресурсу надається невелике за обсягом оновлення, яке індивідуально завантажується з «хмари» практично в реальному часі. До того ж такий підхід дозволяє стандартизувати ПЗ, навіть якщо на комп'ютерах підприємства встановлені різні операційні системи (Windows, Linux, MacOS тощо).

За даними дослідження, проведеного у другому кварталі 2010 року компанією NSS Labs, час, необхідний антивірусним компаніям для блокування веб-загроз, становить від 4,62 до 92,48 годин. Подальше принципове збільшення максимальної швидкості реакції на загрози за допомогою звичайних антивірусних оновлень неможливе.

Також слід зауважити, що моделі розгортання хмари поділяють на приватні, загальнодоступні (публічні) та гібридні. Тож треба зрозуміти, під яку ситуацію або критерії буде використовуватися технологія, щоб забезпечити найвищу ефективність та надійність на підприємстві або в будь якій структурі, що використовує ІКС.

Приватні хмарні технології – це внутрішні хмарні інфраструктури або підприємства. Ці хмарні технології знаходяться у межах корпоративної мережі. Організація може керувати приватною хмарою самостійно або доручити це завдання зовнішній компанії постачальнику. Інфраструктура може розміщуватися або у приміщеннях замовника, або у зовнішнього оператора, або частково у замовника та частково у оператора. Ідеальний варіант приватної хмари – хмара, розгорнута на території організації, яка обслуговується та контролюється її співробітниками.

Приватні хмарні технології мають схожі переваги, що й загальнодоступні, але з однією важливою особливістю: підприємство саме займається встановленням та підтримкою технології. Складність та вартість створення внутрішньої хмари можуть бути дуже високі, а витрати на її експлуатацію можуть перевищувати вартість використання загальнодоступних хмарних технологій.

Загальнодоступні (публічні) хмарні технології – це хмарні послуги, які надає постачальник. Вони за межами корпоративної мережі. Користувачі цих хмар не мають можливості керувати цією хмарою або обслуговувати її, вся відповідальність покладена на власника цієї хмари. Постачальник хмарних послуг бере на себе обов'язки щодо встановлення, управління, надання та обслуговування програмного забезпечення, інфраструктури додатків або фізичної інфраструктури. Клієнти платять лише за ресурси, які вони використовують.

Гібридні хмарні технології є поєднанням загальнодоступних і приватних хмарних технологій. Зазвичай вони створюються підприємством, а обов'язки з

управління ними розподіляються між підприємством та постачальником загальнодоступної хмари. Гібридна хмара надає послуги, частина яких належить до загальнодоступних, а частина – приватних. Добре продумана гібридна хмара може обслуговувати як критичні важливі процеси, що вимагають безпеки, такі як отримання платежів від клієнтів, так і більш другорядні.

Отже, можна зробити висновок про необхідність вдосконалення та практичного використання нових механізмів, методів та засобів антивірусного захисту даних з використанням хмарних обчислювальних технологій.

1.5 Обґрунтування вибору напрямку дослідження

Проведені роботи з дослідження даної теми авторів видань [19 - 25] та аналіз методів та засобів антивірусного захисту даних показали, що існує широкий спектр варіантів побудови та використання методів, та засобів забезпечення інформаційної безпеки в ІКС. Ці варіанти можуть суттєво відрізнятися технологічними впровадженням, топологічними структурами, методологічними, тактико-технічними (та іншими) характеристиками окремих елементів, вартістю розробки або вдосконалення та іншим. Також дослідження та аналізи, що описані у попередніх пунктах даного розділу, показали про необхідність враховувати низку негативних факторів, що впливають на безпеку інформації, при проектуванні та реалізації методів та засобів антивірусного захисту даних.

Мета роботи полягає в підвищенні рівня антивірусного захисту даних в ІКС за рахунок використання можливостей сучасних хмарних обчислювальних технологій. Відповідно до мети роботи необхідно вирішити задачу вдосконалення методу антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих в хмарні обчислювальні системи (ХОС). Для вирішення поставленої задачі необхідно мати план дій, що буде описувати кожний етап роботи.

Тож для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Виконати аналіз вимог інформаційної безпеки, методів та засобів антивірусного захисту даних в ІКС та обґрунтувати напрямок обраного дослідження.

2. Вдосконалити метод контролю ліній зв'язку ІКС шляхом використанням процедури врахування «скомпрометованих» біт даних спеціальних сигнатур, які передані в хмарні антивірусні системи.

3. Розробити модель системи нейромережевих експертів безпечної маршрутизації з комплексним використанням нейронних мереж різного типу й конфігурації.

4. На основі алгоритмів формування множини маршрутів передачі метаданих, контролю ліній зв'язку ІКС та моделі системи нейромережевих експертів безпечної маршрутизації оцінити ефективність вдосконаленого методу антивірусного захисту даних в ІКС.

5. Оцінити економічну доцільність вдосконаленого методу захисту. Техніко-економічне обґрунтування, щодо запровадження запропонованих рішень.

При розробці методу антивірусного захисту даних у ІКС за рахунок безпечної маршрутизації метаданих у хмарні антивірусні системи виникає потреба в оцінці та виборі методологічних підходів до проектування та оптимізації складних інформаційних структурно-функціональних систем, розроблення та вдосконалення окремих алгоритмів, способів та процедур, що є складовими у процесі виявлення вторгнень.

Об'єкт дослідження – процеси забезпечення інформаційної безпеки в умовах впливів комп'ютерних вірусів.

Предметом дослідження є методи антивірусного захисту даних в ІКС.

У ході дослідження необхідно розглянути різні варіанти архітектури хмарних сховищ даних та визначити варіанти побудови хмарних антивірусних ресурсів, а також балансування навантаження.

1.6 Висновок до розділу 1

У даному розділі кваліфікаційної роботи був проведений аналіз основних загроз в ІКС, що безпосередньо впливають для стан її захищеності та стан захищеності користувача або країни в цілому. Тому застосування спеціальних заходів захисту є пріоритетною задачею в ІКС.

Був виконаний аналіз вимог безпеки в ІКС за допомогою різних технічних джерел та міжнародних стандартів безпеки, у ході якого визначено низку основних показників інформаційної безпеки, виділено критерії та показники оптимізації. Була представлена модель безпеки в інформаційній сфері, за якою можна проаналізувати вимоги щодо гарантування інформаційної безпеки підприємства. Зроблено висновок щодо важливості виділення показників антивірусного захисту даних.

З цією метою проведено аналіз вимог антивірусної безпеки в ІКС, а також методів та засобів захисту. Детально розглянута модель сучасних антивірусних систем, їх загальна структура, шлях розвитку, види архітектурних рішень та механізмів виконання поставленої задачі, оновлення технічних рішень з часом, недолі та переваги кожної. Для цього проаналізовано основні дослідження різних наукових праць, присвячених питанням математичного моделювання технології поширення комп'ютерних вірусів в інформаційних та ІКС. Наведено показники часу виявлення комп'ютерних вірусів. Тому було доведено необхідність у використанні сучасних методів та засобів захисту даних.

Проведені аналізи сучасних технологій антивірусного захисту даних, їх розгортання на безпосередньо підприємстві або за її межами та аналіз тенденцій

розвитку шкідливого ПЗ допомогли визначити перспективність та доцільність використання хмарних обчислювальних технологій у питаннях антивірусного захисту.

Отже, обґрунтовано науково-технічне завдання вдосконалення даного підходу антивірусного захисту та визначено шляхи їх вирішення у спеціальній частині кваліфікаційної роботи.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

У цьому розділі вдосконалено метод антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у антивірусні хмарні системи. Основними складовими методу є алгоритми формування безлічі маршрутів передачі метаданих, метод контролю ліній зв'язку ІКС, алгоритм безпечної маршрутизації на базовій безлічі шляхів передачі метаданих у програмний сервер.

Також у даному розділі наводяться результати порівняльних досліджень [26 - 28] та оцінки ефективності методу антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у хмарні антивірусні системи для забезпечення інформаційної безпеки. На основі результатів математичного та імітаційного моделювання обґрунтовується достовірність результатів математичного моделювання, пропонуються практичні рекомендації щодо використання вдосконаленого методу.

Отже, головна мета розділу – вдосконалення методу формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих в ХОС, його оцінка та надання практичних рекомендацій, щодо застосування методу.

2.1 Вдосконалення методу антивірусного захисту даних в ІКС

Тож вдосконалення методу та засобів антивірусного захисту даних і мінімізації наслідків кіберзлочинів, своєчасне виявлення і локалізація комп'ютерних вірусів є вкрай важливим і разом з тим складним завданням.

Відмінною особливістю алгоритмів формування безлічі маршрутів передачі метаданих є показники оптимізації та обмеження безпечної маршрутизації, що вводяться.

2.1.1 Алгоритм формування множин маршрутів передачі метаданих

Аналіз процесу функціонування ІКС, а також дослідження [26 - 28] процесів формування, передачі та обробки метаданих у хмарних антивірусних системах за дослідженнями авторів праць, дозволили визначити щільність розподілу ймовірностей часу передачі хешфайлу метаданих у хмарні антивірусні системи, а також обробки та доставки команд передачі управління, сформувати та математично формалізувати знання про зміни та характер поведінки основних імовірно-часових показників якості обслуговування в ІКС.

Для формування безлічі маршрутів потрібно виконання декількох основних процесів, що становлять такі алгоритми:

1. Алгоритм пошуку найкоротших шляхів між вузлами в ІКС;
2. Алгоритм формування базової множини маршрутів передачі метаданих;
3. Алгоритм безпечної маршрутизації на базовій безлічі шляхів передачі метаданих у програмний сервер.

2.1.1.1 Алгоритм пошуку найкоротших шляхів в ІКС

Тож для алгоритму пошуку найкоротших шляхів між вузлами були проведені дослідження, що показали розв'язання цієї задачі у площині вирішення загального завдання маршрутизації метаданих у хмарні антивірусні системи. Тому є необхідність вибору базового алгоритму пошуку найкоротших шляхів.

З аналізу відомих алгоритмів [28] пошуку найкоротших шляхів був обраний один з найоперативних алгоритмів, що задовольняв заданим вимогам (O(n2^n)) – алгоритм D'Esopo-Pape. Даний алгоритм рекомендується в результатах досліджень ряда авторів, а також підкріплені результатами експериментів, що проводились за допомогою імітаційної моделі. Інтерфейс прогрманого компоненту імітаційної моделі можна побачити на рисунку 2.1.

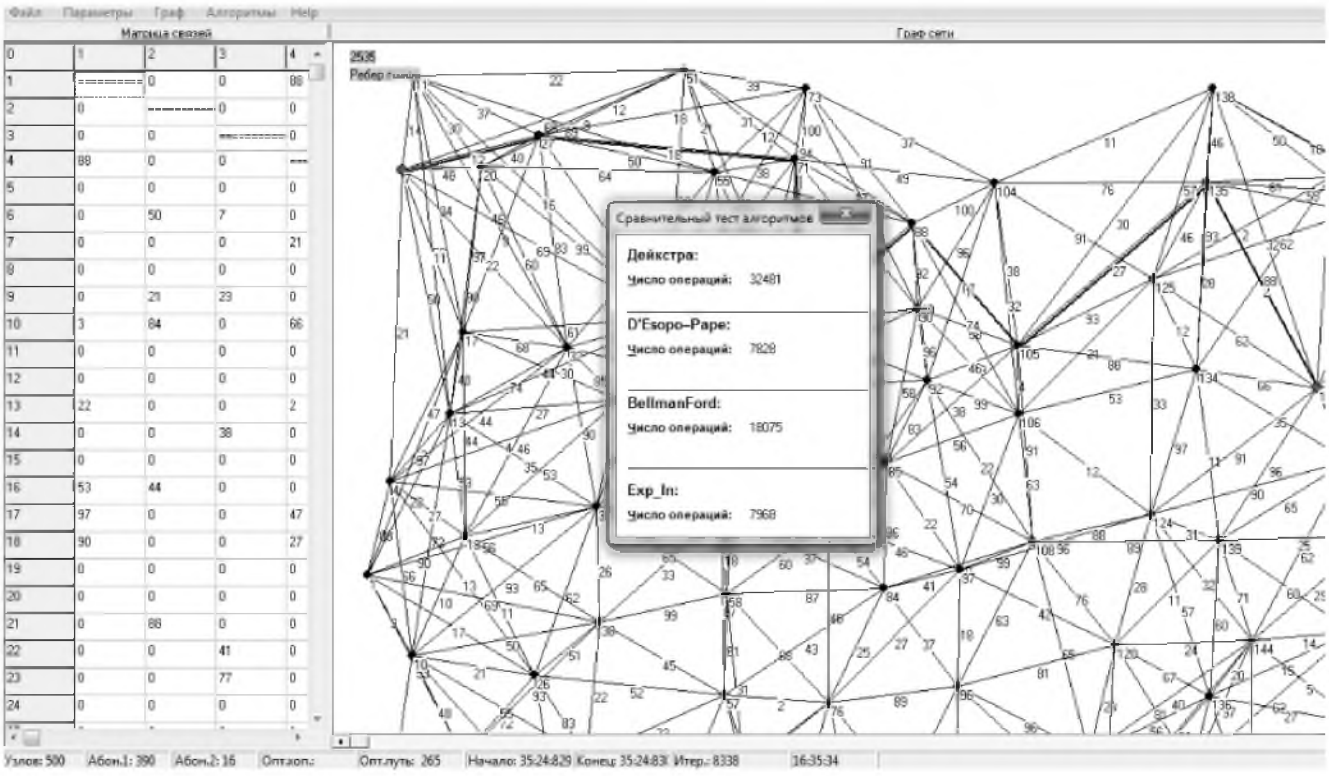

Рисунок 2.1 – Інтерфейс прогрманого компоненту імітаційної моделі

Також додається графік результатів досліджень відомих алгоритмів пошуку найкоротших шляхів на рисунку 2.2, графік залежності числа операцій порівняння кількості вершин графа.

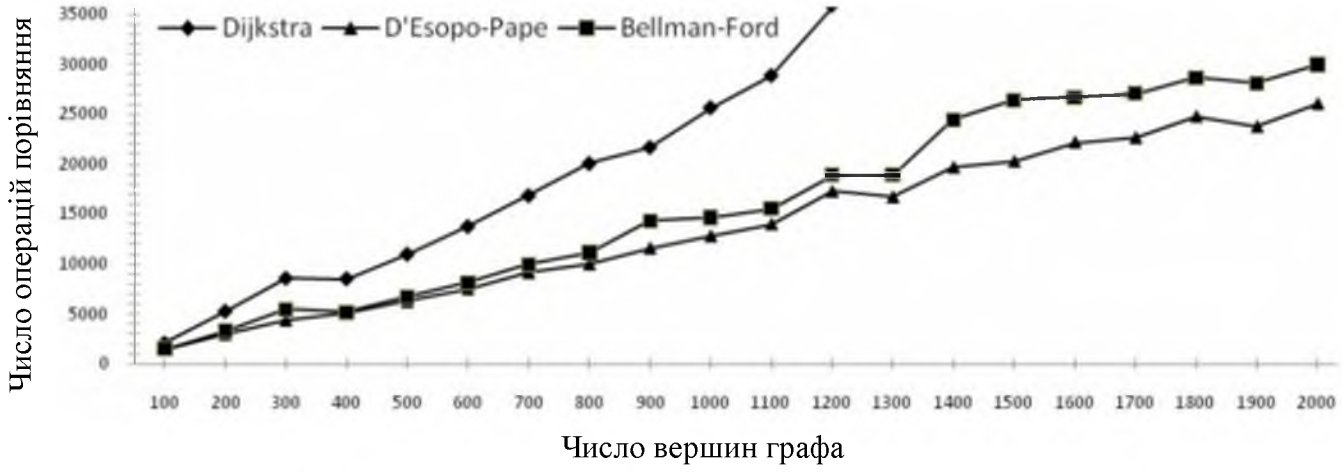

Рисунок 2.2 – Порівняльний графік відомих алгоритмів пошуку накоротших шляхів від числа вершин графу

Для підтвердження достовірності одержаних результатів були проведено розрахунки, що відповідають умовам моделювання:

– ступінь зв'язності мережі вибирався випадковим чином у рамках діапазону: від 5 до 10;

– кількість експериментів на кожному з етапів, що характеризується кількістю вузлів ТКС N =100 .

Більше того, деталі, що стосуються реалізації, а також архітектури структури для представлення даних, можуть суттєво впливати на продуктивність алгоритму.

Крім представлення співвідношення часу виконання задачі між алгоритмами, дослідження вказало на важливість і значущість відповідного вибору методу, призначеного для вирішення задачі, який був би найбільш ефективним.

Результати досліджень імітаційного моделювання підтверджують достовірність результатів аналіза алгоритмів пошуку найкоротших шляхів. Отже, таким чином, можна відзначити доцільність використання даного алгоритму, а саме D'Esopo-Pape, як базовий при покушу накоротших шляхів між вузлами в ІКС.

2.1.1.2 Алгоритм формування базової множини маршрутів передачі метаданих

Наступним кроком за встановленим планом дій буде розглядатися алгоритм формування базової множини маршрутів передачі метаданих, для знаходження множини маршрутів, виключаючи «петлі» (або зациклення алгоритму, що призводить до збільшення часу передачі інформаційних пакетів, а найчастіше і їхній втраті), представлено за структурною схемою (блок-схемою) на рисунку 2.3.

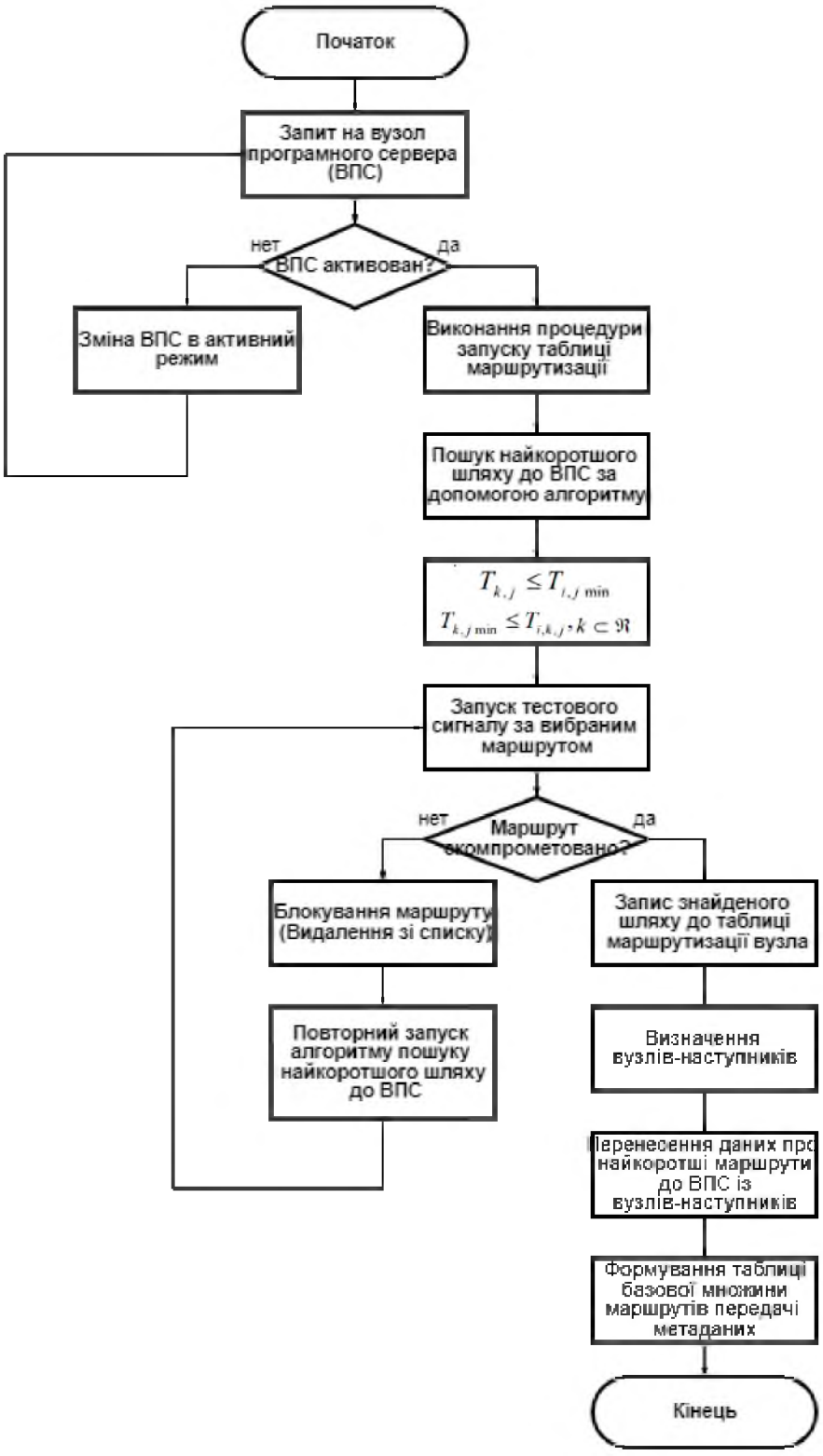

Рисунок 2.3 – Структурна схема алгоритму формування базової множини маршрутів передачі метаданих

Нехай програмний клієнт хмарної антивірусної системи інстальовано на деякому вузлі *i*, щодо якого існують множини:

$U = \{u_\alpha \mid \aleph(u_\alpha) \subset \aleph\}$ – рівнів ієрархії на дереві допустимих маршрутів;

$\aleph_{баз} = \bigcup_{u_\alpha = 1}^{|U|} \aleph(u_\alpha)$ – шуканих шляхів передачі метаданих;

$\aleph_{вб} \subset \aleph_{баз}$ – безліч маршрутів передачі метаданих, вибраних з множини $\aleph_{баз}$ для підвищення безпеки, де u_α – номер рівня ієрархії.

Тож на основі цих припущень та основних процесів разглядуємого алгоритму формування базової множини маршрутів передачі метаданих можна сформувати оптимальну задачу з збільшенням оперативності передачі метаданих у межах множини маршрутів $\aleph_{вб}$:

$$T_{mc}(\aleph_{вб}) \to min; \tag{2.1}$$

$$|U| = \{u_\alpha \mid \aleph(u_\alpha) \subset \aleph\}; \tag{2.2}$$

$$\aleph_{баз} = \bigcup_{u_\alpha = 1}^{|U|} \aleph(u_\alpha),\ |U| \geq 1,\ |U| < \max_{\eta_m \in \aleph} |\eta_m|; \tag{2.3}$$

$$\aleph_{вб} = \bigcup_{u_\alpha = 1}^{|U|} \aleph_{баз}(u_\alpha); \tag{2.4}$$

$$P_{без} \geq P_{без_{доп}}. \tag{2.5}$$

де $P_{без_{доп}}$ – допустима ймовірність безпечної передачі даних.

Але слід зазначити, що при вирішенні даної задачі пошуку найкоротших шляхів з використання даного алгоритму у більшості випадків є можливість зустрітися з проблемою «зациклювання» даних у знайдених шляхах, що

називається «петлями», і це призводить до збільшення часу, а іноді й втрати, передачі інформаційних пакетів.

Позбутися «петель» можна за допомогою додавання деяких обмежень, які представлені у вигляді вираження:

$$T_{k,j} \le T_{i,j\,\min}; \tag{2.6}$$

$$T_{k,j\,\min} \le T_{i,k,j},\ k \subset \Re, \tag{2.7}$$

де $T_{k,\,j\,min}$ – найкоротший час передачі інформаційних пакетів від вузла k до адресу j;

$T_{i,\,k,\,j}$ – час передачі інформаційних пакетів від вузла i до адресу j через вузол k;

Тож після того, як було сформовано базова $\aleph_{баз}$ множина маршрутів передачі метаданих стає необхідність проводити постійний моніторинг каналів зв'язку та адаптивно змінювати таблиці базової множини маршрутів у разі аномальних змін у показниках тестових сигналів. Отже, саме для вирішення цього завдання призначений алгоритм безпечної маршрутизації на базовій множині шляхів передачі метаданих у програмний сервер

2.1.1.3 Алгоритм безпечної маршрутизації на базовій безлічі шляхів передачі метаданих у програмний сервер

З проведених досліджень попередніх підрозділів з'ясовано, що виникає необхідність у знаходженні такої множини маршрутів, використання якої в умовах заданих обмежень, що накладаються, дозволили б забезпечити максимальну можливу інформаційну безпеку, а саме у моніторингу каналів зв'язку та виборі з всієї знайденої множини $\aleph_{баз}$ шляхів оптимальної сукупності $\aleph_{вб}$ маршрутів.

Основні вимоги до якості наданих послуг в ІКС задаються в параметричному вигляді, системою обмежень, тож їх можна привести до вигляду:

$$\{P_{иск} \le P_{иск_{доп}},\ Q_c \ge Q_{доп},\ T \le T_{доп}, P_{без} \ge P_{без_{доп}}\},$$

де $P_{иск_{доп}}$ – допустима ймовірність спотворення інформаційних пакетів у процесі передачі;

$Q_{доп}$ – допустима ймовірнусть прийому інформаційного покету за час T, не перевищуючи доступне;

$P_{без}$ – ймовірність безпечної передачі.

Також, слід зазначити, що в умовах підвищеної небезпеки при передачі та обробці метаданих у хмарних антивірусних системах, ймовірність $P_{без}$ безпечної передачі є одним з важливих показників, як слідство, завдання безпечнох маршрутизації даних трансформується в оптимізаційне завдання:

$$\{P_{без} \to max, \quad при \quad P_{иск} \le P_{иск_{доп}},\ T \le T_{доп},\ Q_c \ge Q_{доп}\}. \qquad (2.8)$$

Тому, в такому випадку, алгоритм безпечної маршрутизації на базовій множині шляхів передачі метаданих в програмний сервер можна розглядати як показано на рисунку 2.4.

Отже, головною особливістю розглянутого алгоритму є можливість постійного моніторингу та облік каналів зв'язку ІКС на маршрутах вузлів програмного сервера, що дають можливість виявляти можливості кібератак та несанкціонованого доступа до ІКС.

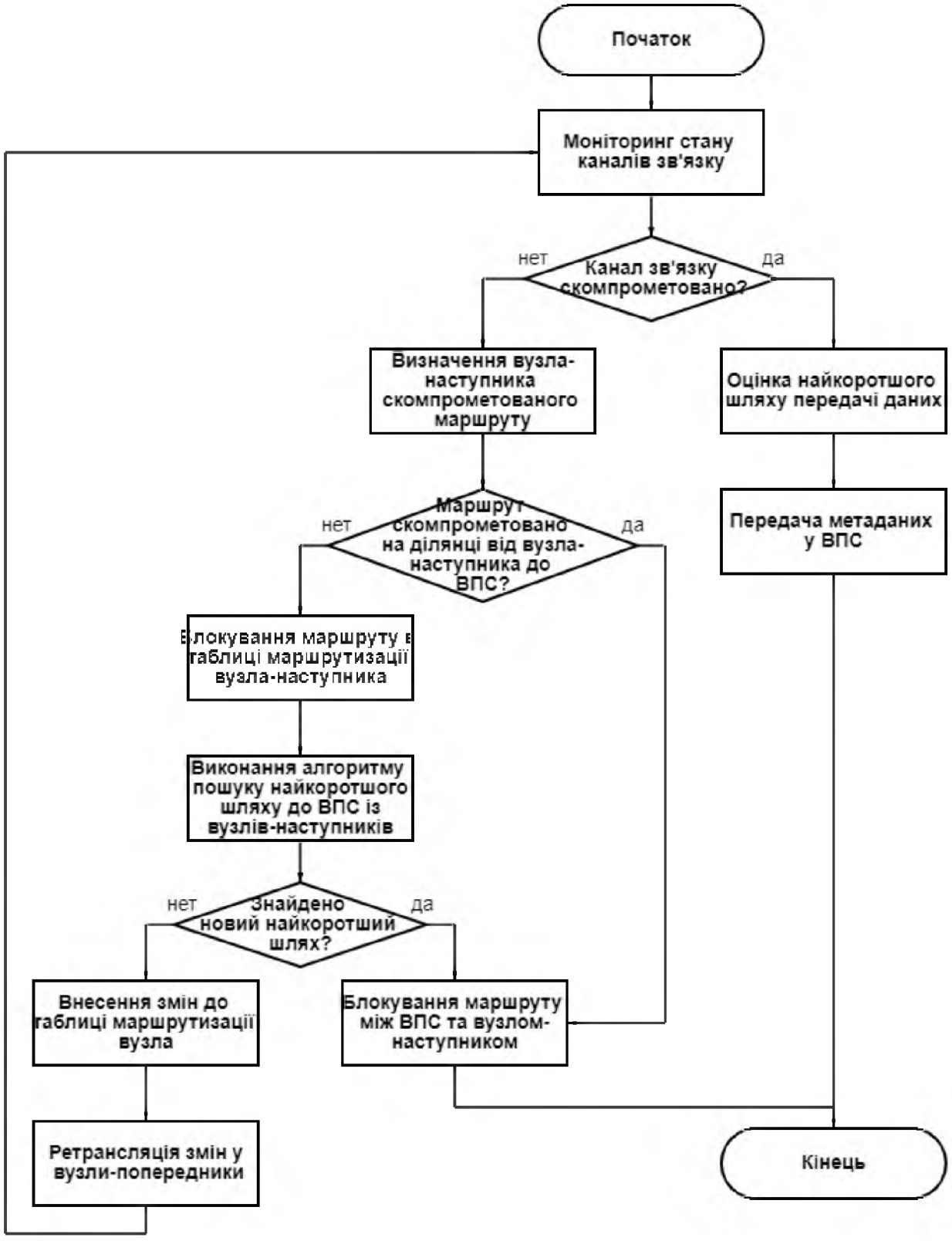

Рисунок 2.4 – Структурна схема алгоритму безпечної маршрутизації на базовій множині маршрутів передачі метаданих в програмний сервер

2.1.2 Метод контролю ліній зв'язку ІКС

У цьому підрозділі розглянута безпечна маршрутизація, що передбачає використання ліній зв’язку ІКС. Для того щоб маршрутизатор міг функціонувати, необхідно сформувати інформацію про стан з'єднань, що виходять з даного вузла. Кожному з'єднанню надається певний вектор параметрів, компоненти якого характеризують певну складову фізичної сполуки.

Слід зауважити, що одним із найважливіших параметрів, які необхідно враховувати при виборі подальшого шляху маршрутизації інформації, є тип каналу зв'язку, його пропускна здатність, швидкість передачі та функціональна безпека.

Для деяких каналів зв'язку характеристики, що використовуються для вибору маршрутів при передачі метаданих у антивірусні хмарні системи, наведені в табл. 2.1.

Таблиця 2.1 – Характеристики маршрутів при передачі метаданих

Пропускна здатність			Функціональна безпека	
Тип каналу	Швідкість передачі	Параметр пропускньої здатності	Тип кабелю	Параметр функціональної безпеки
Ethernet	10 Мбит/с	0,8	Коаксиальний кабель	
Ethernet	100 Мбит/с	0,9	«Товстий» коаксиальний кабель	0,31
Ethernet	1000 Мбит/с	0,95	«Тонкий» коаксиальний кабель	0,22

Продовження таблиці 2.1

Тип каналу	Швідкість передачі	Параметр пропускньої здатності	Тип кабелю	Параметр функціональної безпеки
Канал Т-1	1,544 Мбит/с	0,45	Телевізійний кабель	0,15
Канал Т-2	6,312 Мбит/с	0,61	Кручена пара	
Канал Т-3	44,736 Мбит/с	0,85	Екранований	0,6
Канал Т-4	274 Мбит/с	0,93	Неекранований	0,5
Канал 56	56 Гбит/с	0,33	Волоконно оптичний	
Канал Е-1	2,048 Тбит/с	0,55	Одномодовий	1,0
Канал Е-2	8,488 Гбит/с	0,65	Багатомодовий	0,8

Витік інформації може бути здійснено шляхом прямого приєднання до каналу зв'язку та зчитування її за допомогою технічних засобів. Внаслідок цього має бути можливість визначення спроб підключення до каналу.

Також в джерелах зазначено, що основна небезпека подібних зловмисних вторгнень припадає на неконтрольовані ділянки ІКС, тобто ділянки глобальних та регіональних мереж, в яких найчастіше використовуються канали типу Е-1 та Е-2.

Дослідження авторів [29 - 30] показівають, які є способи несанкціонованого доступу до волоконо-оптичної лінії зв'язку (ВОЛЗ), ці способи описані на рисунку 2.5:

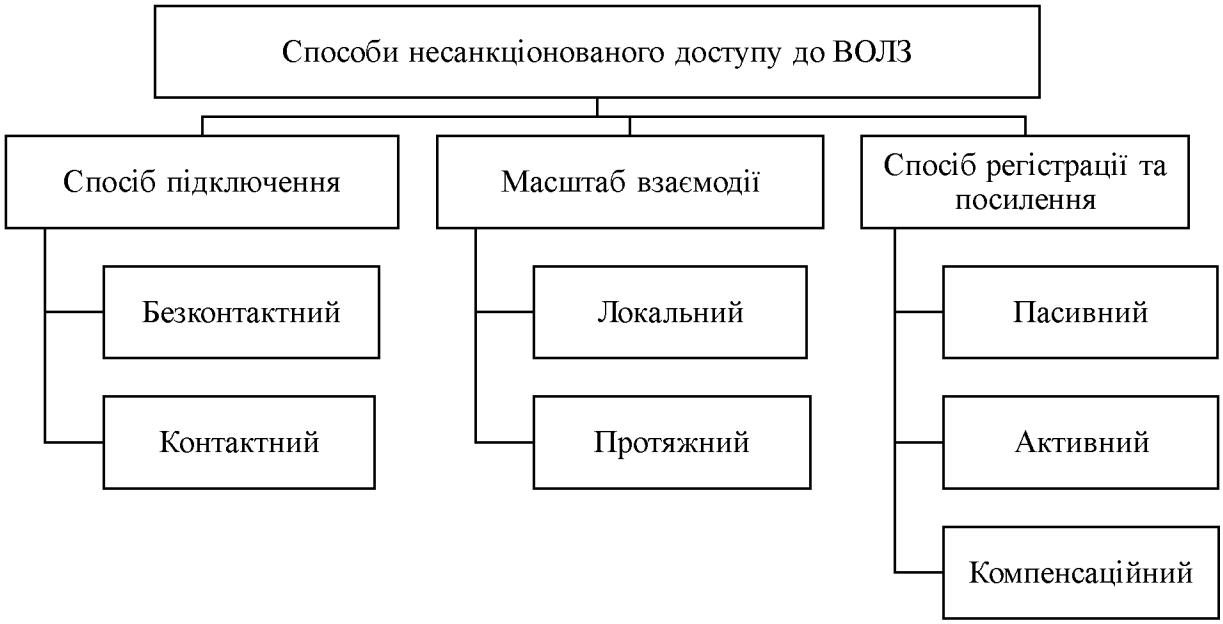

Рисунок 2.5 – Способи несанкціоновоного доступу до ВОЛЗ

Найпростішим способом незаконного підключення є контактне підключення, наприклад паралельне підключення телефону, досить поширене в побуті.

Безконтактне підключення до лінії зв'язку здійснюється двома шляхами:

1. За рахунок електромагнітних наведень на паралельно прокладені дроти;

2. За допомогою зосередженої індуктивності, що охоплює контрольовану лінію.

Найбільш небезпечними, з точки зору знімання метаданих, що передаються на програмні сервери надаються контактним методам несанкціонованого доступу. Таким чином, зловмисник має широкий спектр можливих впливів на

хмарну антивірусну систему в цілому, у зловмисника є можливість як знімати перехоплені метадані так і змінювати отриману інформацію. Також технічні пристрої контактного несанкціонованого доступу дозволяють здійснювати більш надійне знімання даних. Однак, слід зазначити, що контактне підключення вимагає тимчасового відключення ліній зв'язку, яке може послужити сигналізацією про наявність зловмисного вторгнення та перевірки системи в цілому.

Безконтактний спосіб під'єднання є біль непомітнішим для виявлення, адже у цьому способі для знімання сигналу використовується випромінювання, що виникає природним чином на з'єднувачах, пристроях введення та виведення оптичної потужності, найоптичнішому волокні.

Також при цьому можливо використання пасивних, активних та компенсаційних способів реєстрації даних:

1. Пасивні методи – засновані на реєстрації випромінювання з бічної поверхні волокна;

2. Активні методи – засновані на реєстрації випромінювання, що виводиться через бічну поверхню волокна за допомогою спеціальних технічних засобів;

3. Компенсаційні методи – базуються на реєстрації випромінювання, що виводиться через бічну поверхню за допомогою спеціальних технічних засобів, також з подальшим формуванням випромінювання та введення його у волокно, що дозволяє компенсувати втрати потужності при виведенні випромінювання.

На рисунку 2.6 зображено дослідження усіх можливих причин випромінювання та розсіювання у ВОЛЗ і, відповідно, атак несанкціонованого доступу.

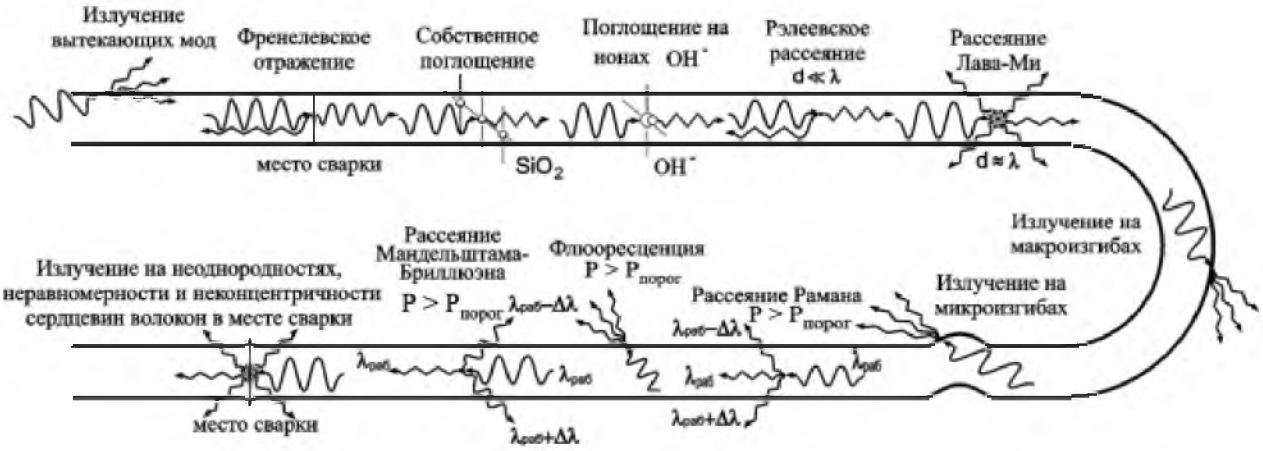

Рисунок 2.6 – Причини несанкціоновоного доступу до ВОЛЗ

Серед зображених причин несанкціонованого доступу до ВОЛЗ можна перерахувати такі методи: вигин волокна, зміна діаметра волокна (наприклад, шляхом тиску), мікровигини волокна, акустичний вплив на волокно, вплив хімічних реактивів.

Методи першого типу засновані на тому, що навіть у стаціонарному режимі в звичайних умовах невелика частина розсіяного випромінювання все ж таки проникає за межі волокна (випромінюється) і може бути каналом витоку інформації. Для несанкціонованого доступу до інформації необхідно використовувати місця посиленого бічного випромінювання, тобто слід знімати випромінювання в місцях згинів, а також у місцях зварних з'єднань і з'єднань волокна з підсилювачами. Однак, значна потужність випромінювання спостерігається лише в місцях роз'ємних з'єднань, тобто в комутаційних центрах, що ускладнює несанкціонований доступ.

Методи другого типу виводять зазвичай велику потужність, але при цьому відбувається зміна параметрів хвилі. Такими методами є, наприклад: механічний вигин волокна, підключення фотоприймача за допомогою відгалужувача, вдавлювання зондів в оболонку, безконтактне з'єднання волокна, шліфування та розчинення оболонки.

Тому основним методом виявлення цього способу несанкціонованого доступу є контроль за рівнем потужності на приймальній стороні. Якщо пристрій контролю виявляє її зниження, воно робить висновок про наявності несанкціонованого доступу до ВОЛЗ та вжити відповідних заходів. Тому аппаратура, яка розтошована на стороні сервера, крім своїх основних функцій повина включати в себе систему контроля та виявлення несанкціонованого доступу. В завдання цієї системи повинні входити: спостереження за станом ВОЛЗ, контроль сигналу та передача його в інтелектуальний асоціативний блок нейромережевих рішень

У роботах відомих авторів для розрахунку ймовірності хибного виявлення чи пропуску аномалій використовується таке вираження:

$$P_{ло} = \frac{1}{\sqrt{2\pi}\frac{\sigma_1}{\sqrt{N}}} \int_{-\infty}^{\gamma} e^{\frac{-(z-\lambda_1)^2}{2\sigma_1^2/N}} dz, \tag{2.9}$$

$$P_{проп} = \frac{1}{\sqrt{2\pi}\frac{\sigma_1^н}{\sqrt{N}}} \int_{-\infty}^{\gamma} e^{\frac{-(z-\lambda_1^н)^2}{2(\sigma_1^н)^2/N}} dz, \tag{2.10}$$

де $\lambda_1^н$ та $(\sigma_1^н)^2$ – математичне очікування та дисперсія випадкових величин y_i за наявності несанкціонованого доступу.

Розіб'ємо дані, що передаються на множину ділянок однакової тривалості N біт. При цьому досліджуємо величину y_i – параметр рівня сигналу в і момент часу. Відповідає нормальному закону розподілу:

$$P(y_i) = \frac{1}{\sqrt{2\pi\sigma_i}} e^{\frac{-(y-\lambda_i)^2}{2\sigma_i}}, \tag{2.11}$$

де λ_i, σ_i – математичне очікування та дисперсія випадкових величин y_i.

Суму величин y_i, що визначаються в аналізаторі ліній зв'язку для всіх y_i, відповідних позитивним імпульсам, позначимо як Z і порівняємо з порогом, за цим вираженням:

$$Z = \frac{1}{N}\sum_{j=1}^{N} y_j, \tag{2.12}$$

де N – інтервал аналіза.

Тож за результатами цих виражень порівнення в системі нейромережевих експертів буде прийнято рішення за наявність несанкціонованого доступу та, якщо атаки не було виявлено – процес повторюється (N).

Нехай x - число біт, переданих у ВОЛЗ після проведеної кібератаки, тоді загальна кількість «скомпрометованих» біт даних дорівнюватиме:

$$X_i = x_i + N \cdot T + T_{pa}, \tag{2.13}$$

де T_{pa} – час, за який розповсюдження даних про сигнал аномалій.

Отже, використання цього методу дозволить виявляти зміну характеристик ВОЛЗ у процесі функціонування ІКС та видавати необхідні сигнали аномалій (кібератак) у лініях зв'язку у систему нейромережевих експертів безпечної маршрутизації, а це, у свою чергу, дозволить знизити ймовірність маніпуляцій метаданими, що передаються в вузли програмного сервера.

2.1.3 Модель системи нейромережевих експертів безпечної маршрутизації

При вирішенні задач за допомогою нейромережевих методів, побудованих на застосування декількох нейронних мереж вхідні дані обробляються за допомогою множини нейромережевих експертів сукупності нейронних мереж різної архітектури з механізмом об'єднання рішень.

Щоб система системи нейромережевих експертів безпечної маршрутизації нормально функціонувала необхідно підготувати та систематизувати дані, за якими проводиться навчання його окремих нейромережевих компонентів. Для вирішення цього завдання частина цієї системи формування навчальної та тестової вибірки формує дані для навчання нейронної мережі, впорядковує та організує її з метою забезпечення можливості їх подальшої обробки за допомогою нейромережевих технологій.

Дана частина (блок системи), формування початкового стану маршрутів ІКС формує значення всієї системи перед початком її навчання.

Отже, дослідження авторів показали, що для вирішення цього завдання доцільно використовувати в якості алгоритма початкової установки параметрів – кооперативний імунний алгоритм із генерацією рішень на основі процедури генетичного пошуку з використанням нейронної мережі АРТ-1 (адаптивної резонансної теорії). Мережа навчається без вчителя і реалізує простий алгоритм кластеризації.

Повертаючись до системи нейромережевих експертів, доповнимо, що для нормального функціонування системи необхідно сформувати їх початкові стани, виражені попередньою установкою вагових коефіцієнтів нейронних мереж. Як було зазначено раніше для вирішення поставленого завдання доцільно використати імунний алгоритм оптимізації, побудований на основі принципів імунітету живих організмів.

Тож популяція антигенів виступає як область всіх можливих значень векторів ваги та порогів нейронів. Кожне антитіло кодує вектори вагових коефіцієнтів та пороги нейроні, як зображено на рисунку 2.7. В нейронну мережу послідовно підставляються параметри, закодовані у кожному з антитіл популяції. Обчислюється помилка навчання для кожного антитіла.

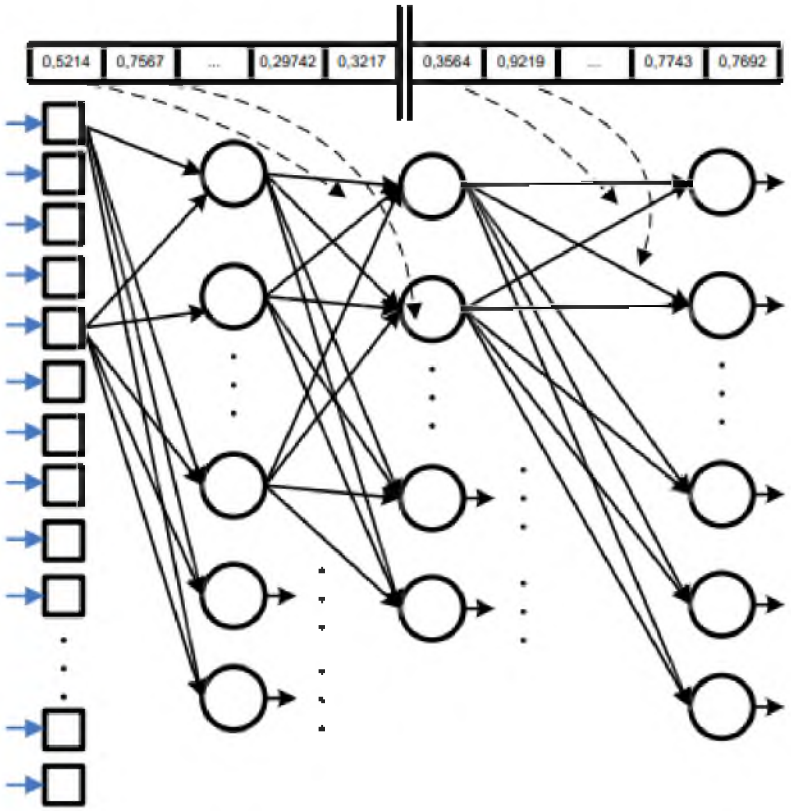

Рисунок 2.7 – Приклад можливого кодування при налаштуванні нейронної мережі

Також при обміні антитілами з популяцій видаляється частина антитіл, також це відбувається і після застосування оператора мутації. Мережа навчається без вчителя та реалізує простий алгоритм кластеризації. Відповідно до цього алгоритму перше антитіло вважається зразком першого кластеру. Наступне антитіло порівнюється із зразком першого кластеру. Антитіло належить першому кластеру, якщо відстань до зразка першого кластера менше за поріг. Інакше друге антитіло – зразок другого кластеру. Цей процес повторюється для всіх наступних антитіл.

Отже, в результаті, для кожного нейромережевого експерта створюється окремий комплекс популяцій антитіл, усередині кожної популяції проводиться розвиток антитіл, мутація та видалення.

2.2 Оцінка ефективності методу захисту хмарних даних

В даному підрозділі представлені результати порівняльних досліджень та оцінка ефективності методу антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у хмарних антивірусних системах. Також на основі отриманих даних додаються практичні рекомендації щодо вдосконаленого методу.

2.2.1 Результати порівняльних досліджень методу захисту в ІКС

На базі проведених досліджень та досліджень авторів [28] з математичного моделювання процесу передачі метаданих у хмарні антивірусні системи зможемо дослідити ефективність методу адаптивної маршрутизації в порівнянні з підходом одноколійної маршрутизації. У разі фіксованої маршрутизації від вузла джерела до вузла-адресата використовується єдиний маршрут для передачі всього трафіку, і завдання зводитися до вибору оптимального шляху з усіх можливих шляхів.

Тож для порівняння розробленого методу з методом одноколійної маршрутизації знайдемо відношення $T_{mc\ ом} / T_{mc\ мм}$ середнього часу доставки інформаційних пакетів в ІКС при використанні цих методів. Для цього використаємо рівність:

$$\frac{T_{mc\ ом}}{T_{mc\ мм}} = \frac{\sum_{i=1}^{n} 2p_i^{(k)} \frac{\left((\lambda p)^i \tau + i\right)}{\lambda p}}{\sum_{s=1}^{M} \left(\varphi_s \sum_{i=1}^{n} 2p_i^{(k)} \frac{\left((\lambda p)^i \tau + i\right)}{\lambda p} \right)}, \tag{2.14}$$

де M – кількість маршрутів;

φ_s – коефіцієнт розподілу потоку цифрових метаданих по s-ному маршруту.

При фіксованих значеннях середньої експлуатаційної пропускної спроможності каналів зв'язку, яка дорівнює 200 Мбіт/с та числа маршрутів передачі інформаційних пакетів в ІКС, яка дорівнюватиме M = 5, при використанні методів одноколійної маршрутизації від інтенсивності λ вхідних потоків інформації наведений графік залежності на рисунку 2.8.

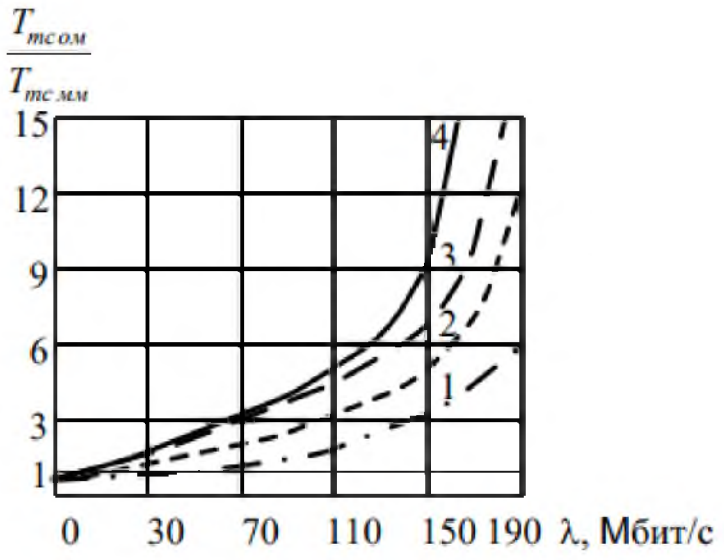

Рисунок 2.8 – Залежність відношення $T_{тс\,ом}$ / $T_{тс\,мм}$ від інтенсивності λ вхідних потоків інформації

За цим графіком, що ілюструє переваги методу одноколійної маршрутизації в порівнянні з методом багатошляхової маршрутизації при низькій λ = 15 Мбіт/с інтенсивності вхідного потоку інформації. Стає очевидним необхідність застосування методу антивірусної захисту даних у ІКС за рахунок безпечної маршрутизації метаданих у хмарні антивірусні системи за високого навантаження на ІКС.

При використанні методу багатошляхової маршрутизації від інтенсивності λ вхідного потоку даних з залежності відношення $T_{тс\,мп}$ / $T_{тс\,мм}$ середнього часу доставки інформаційних пакетів в ІКС з наступними параметрами:

1. При середній пропускній здатності $\rho_{пз} = 350$ Кбіт/с каналов связи для $m^{(m)} = 4$ на рисунку 2.9:

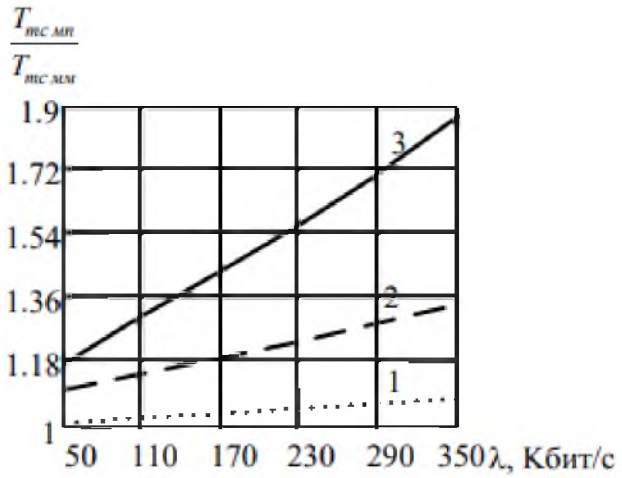

Рисунок 2.9 – Залежність відношення $T_{тс\ мп}$ / $T_{тс\ мм}$ від інтенсивності λ вхідних потоків інформації при $\rho_{пз} = 350$ Кбіт/с та $т^{(т)} = 4$

2. При середній пропускній здатності $\rho_{пз} = 350$ Кбіт/с каналов связи для $m^{(m)} = 3$ на рисунку 2.10:

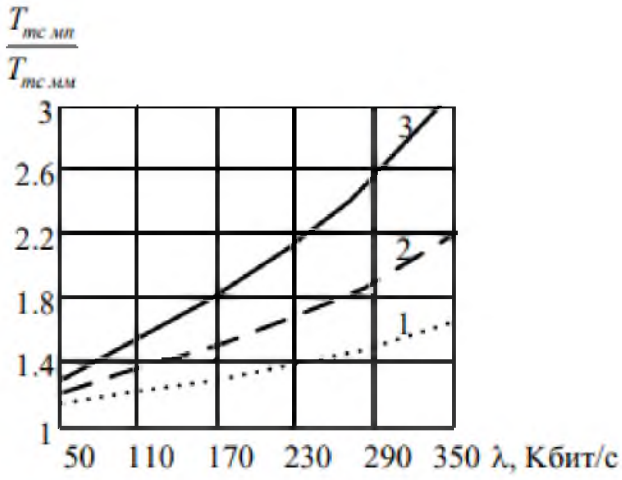

Рисунок 2.10 – Залежність відношення $T_{тс\ мп}$ / $T_{тс\ мм}$ від інтенсивності λ вхідних потоків інформації при $\rho_{пз} = 350$ Кбіт/с та $т^{(т)} = 3$

Отже, з графіків (рисунки 2.8-10) видно, що застосування антивірусного захисту даних у ІКС за рахунок багатошляхової маршрутизації метаданих у хмарні антивірусні системи скорочує час передачі інформаційних пакетів метаданих у 1,9-3 рази (при $m^{(m)} = 3$ та $m^{(m)} = 4$). Таким чином, проведений порівняльний аналіз дає відповідь, що застосування методу антивірусного захисту даних в ІКС за рахунок багатошляхової маршрутизації метаданих у хмарні антивірусні системи при передачі даних дозволить скоротити час передачі інформаційних пакетів до 15 разів.

Для обґрунтування достовірності отриманих результатів та оцінки ефективності антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у хмарні антивірусні системи були проведені дослідження авторів імітаційного моделювання. Як інструментарій імітаційного моделювання використано середовище символьної математики MathCAD 15 – система комп'ютерної алгебри з класу систем автоматизованого проєктування.

Для імітації зловмисних дій з використанням шкідливого програмного забезпечення використовувалися віруси на основі Svchost.exe. Svchost.exe у Windows 10, 8 та Windows 7 є основним процесом для завантаження служб операційної системи Windows, що зберігаються у динамічних бібліотеках DLL. Служби Windows, а особливо ті, за запуск яких відповідає svchost, є необхідними компонентами для повноцінної роботи операційної системи та завантажуються під час її запуску (не всі, але більшість із них). Зокрема, таким чином запускаються й використані віруси.

Проведені дослідження характерних «слідів», які залишають комп'ютерні віруси, слід зазначити звернення до WIN API функцій, зокрема функцій з бібліотеки kernel32.dll [34 - 35]. Також у вірусному ПЗ замість імен функцій використовуються хеш-значення імені функції, що ускладнює пошук алгоритму роботи програми у відладчику, автоматизовану перевірку наявності викликів цих

функцій у створюваній антивірусній програмі. Перелік цих функцій наведений у таблиці 2.2.

Таблиця 2.2 – Перелік WIN API функцій, що використовуються у ПЗ

Назва функції	Хеш-код	Опис та призначення функції
CloseHandle	0F867A91Eh	Дана функція закриває дескриптор відкритого об'єкта.
FindFirstFile	03165E506h	Функція FindFirstFile шукає каталог файлу або підкаталогу, назва якого відповідає вказаному імені файлу.
FindNextFile	0CA920AD8h	Функція FindNextFile продовжує пошук файлу з попереднього виклику функції FindFirstFile або FindFirstFileEx.
GetFileSize	0AAC2523Eh	Функція GetFileSize повідомляє про розмір файлу, розмір обмежується значенням подвійного слова.
CreateFile	0860B38BCh	Функція CreateFile створює або відкриває каталог, фізичний диск, буфер консолі, пристрій на магнітній стрічці, комунікаційний ресурс, поштовий слот або іменований канал. Функція повертає дескриптор, який може бути використаний для доступу до об'єкту.
GlobalAlloc	0CC17506Ch	Виділяє з глобальної множини пам'ять запитаного розміру.

Продовження таблиці 2.2

Назва функції	Хеш-код	Опис та призначення функції
ReadFile	029C4EF46h	Функція ReadFile читає дані з файлу, починаючи з позиції, позначеної вказівником файлу. Як операція читання буде закінчена, покажчик файлу переміщається на число дійсно прочитаних байтів, якщо дескриптор файлу не створено з атрибутом асинхронної операції. Якщо дескриптор файлу створюється для асинхронного введення висновку, програма повинна перемістити позицію покажчика файлу після операції читання.
SetFilePointer	07F3545C6h	Функція SetFilePointer переміщує вказівник позиції у відкритому файлі.
WriteFile	0F67B91BAh	Функція CreateFile пише дані у файл з місця, зазначеного маркером позиції в файл. Ця функція призначена і для синхронної та для асинхронної операції.
GlobalFree	03FE8FED4h	Звільняє розблокований блок глобальної пам'яті та робить недійсним його дескриптор.
VirtualProtect	015F8EF80h	Функція встановлює атрибути блоку пам'яті.
ExitProcess	0D66358ECh	Функція ExitProcess закінчує роботу процесу та всіх його потоків.

Продовження таблиці 2.2

Назва функції	Хеш-код	Опис та призначення функції
GetProcAddress	05D7574B6h	Функція GetProcAddress отримує адресу експортованої функції або змінної із заданою динамічно-підключеною бібліотеки (DLL).
LoadLibrary	071E40722h	Функція LoadLibrary відображає заданий модуль, що виконується в адресному просторі процесу, що викликає.
GetModuleFileName	059B44650h	Функція GetModuleFileName вказує повний шлях до файлу, що містить модуль, який входить до поточного процесу. Щоб визначити модулі, що використовуються в іншому процесі, використовують функцію GetModuleFileNameEx.
SetCurrentDirectory	00709DC94h	Встановлює поточний каталог для роботи з файлами.
FreeLibrary	0D64B001Eh	Функція FreeLibrary зменшує підсумкове кількість посилань на завантажені загальні бібліотеки (DLL) Коли підсумкове число посилань досягає нуля, модуль скасовує відображення в адресному просторі викликаючого процесу, а дескриптор стає більше не допустимо.

Продовження таблиці 2.2

Назва функції	Хеш-код	Опис та призначення функції
FindClose	0E65B28ACh	Функція Find Close закриває дескриптор пошуку файлу, відкритий функціями FindFirstFile та FindFirstFileEx.

З даного списку WIN API функций, що можуть бути використані в ПЗ зловмісника, слід виділити наступні: ReadFile, WriteFile, LoadLibrary, GetProcAddress.

Отже, можна виділити однією з найважливіших складових підсистеми захисту на основі хмарних антивірусних систем є підсистема безпечною маршрутизації тобто управління інформаційними потоками до хмарних телекомунікаційних ресурсах.

2.2.2 Результати моделювання безпечної маршрутизації в ХОС

На базі проведених досліджень проведено імітаційне моделювання передачі сигнатур в ІКС з наступними параметрами:

1. Використовуються аналізатори ліній зв'язку та інтелектуальні засоби прийняття рішень про компрометації маршрутів.
2. Можливість обслуговувати в одиницю часу таку кількість пакетів, яка відповідає кількості пакетів, що зберігаються в одному блоку пам'яті буфера в системі.
3. Довжина інформаційного пакету lp = 1024 біт.
4. Кількість експериментів N* = 100.

Тож на основі цих даних є результати імітаційного моделювання, що представлені на гістограмі часу передачі хеш-файлу метаданих у хмарні антивірусні системи до кількості реалізацій на рисунку 2.11.

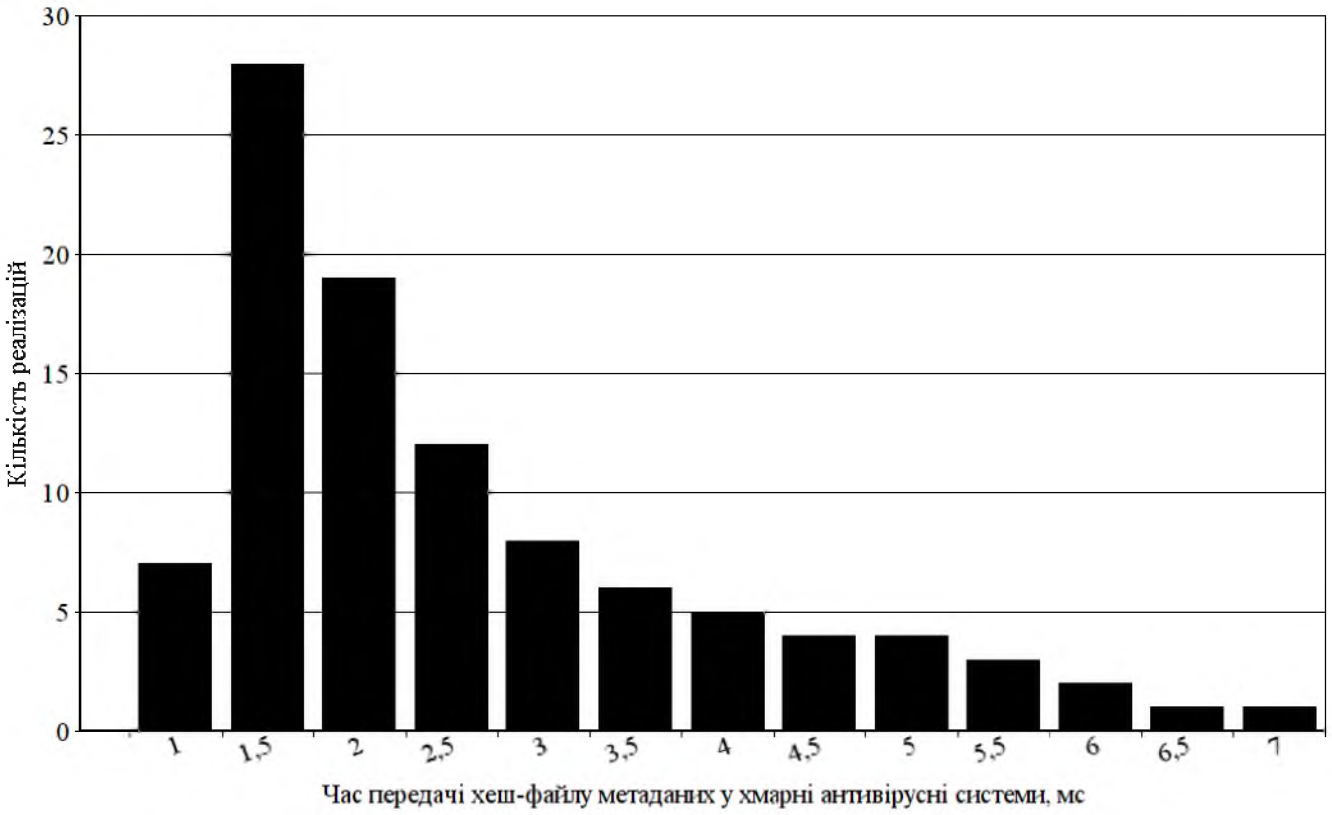

Рисунок 2.11 – Гістограми часу передачі хеш-файлу метаданих у хмарні антивірусні системи

Була проведена перевірка нормальному розподілі цієї випадкової величини з критерії згоди Пірсона x^2:

$$\chi^2 = N^* \sum_{i=1}^{k} (P_i^* - P_i)^2 / P_i , \qquad (2.15)$$

де k – число інтервалів статистичного ряду;

P_i^* и P_i – ймовірність влучення заданого показнику у *i-й* разряд.

Дана перевірка довела правдоподібність гіпотези, що величина часу передачі хеш-файлу метаданих у хмарні антивірусні системи розподілено за нормальним законом.

Також визначимо довірчу ймовірність того, що значення часу передачі хешфайлу метаданих в антивірусні хмарні системи «не відхилилося» від математичного очікування більше ніж на 1:

$$P\left(\left|\bar{t}_{пер}^{(i)} - t_{пер}^{(i)}\right| < 1\right) = 2\Phi\left(1 / \bar{t}_{пер}^{(i)}\right), \tag{2.16}$$

де Φ – функція Лапласа $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-t^2/2}\, dt$

Тож імітаційне моделювання показало, що довірча ймовірність того, що значення статистичної величини не відхилиться від математичного очікування більше ніж на 1 дорівнює $P = 0.95$

Результати порівняння представлені на рисунку 2.12 у вигляді графіка щільності розподілу ймовірностей часу передачі хешфайлу метаданих в хмарні антивірусні системи, а також обробки та доставки команд передачі управління, відповідних їм меж довірчого інтервалу.

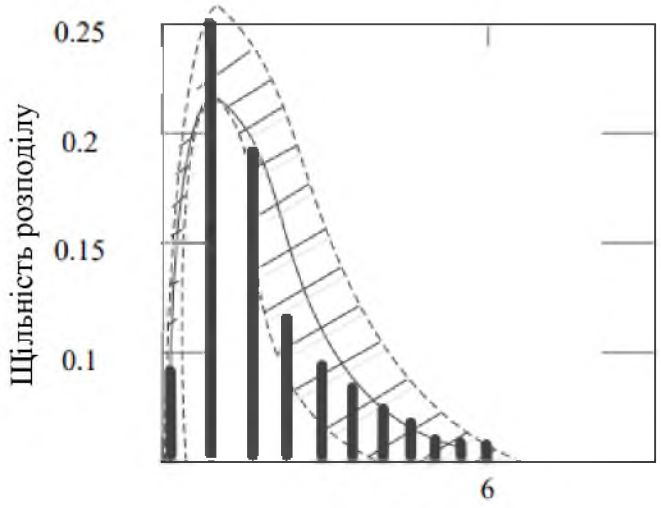

Рисунок 2.12 – Графік щільності росподілу

Отже, підтверджується достовірність математичної моделі технології хмарного антивірусного захисту ІКС та отриманого в результаті математичного моделювання аналітичного виразу.

2.3 Практичні рекомендації щодо застосування вдосконаленого методу

У даній роботі пропонується використання в інтелектуальних маршрутизаторах асоціативних блоків нейромережевих експертів та аналізаторів каналів зв'язку з урахуванням можливого зовнішнього впливу та компрометації маршрутів. Але джерела вказують, що інтелектуальні маршрутизатори повинні підтримувати різні алгоритми управління – CAR, WFQ, RRP, RSVP, DiffServ та інші. Також сучасні маршрутизатори повинні забезпечити максимальну швидкість обслуговування інформаційних пакетів та інших (нижчих) рівнів пріоритетності.

Хмарні антивірусні програми можуть бути встановлені на кількох серверах, конфігурованих для поділу робочої навантаження, як показано на рисунку 2.13, тип даної конфігурації – кластер з балансуванням навантаження.

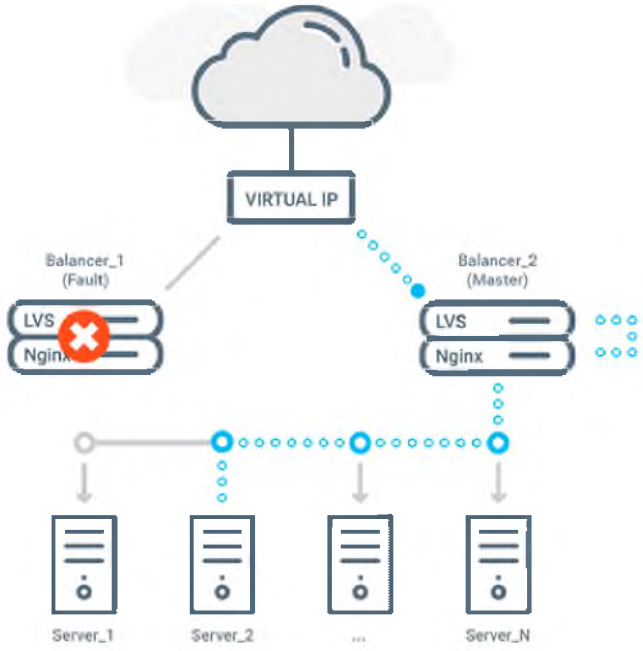

Рисунок 2.13 – Кластер з балансуванням навантаження

Джерела свідчать, що балансування навантаження дозволяє масштабувати продуктивність антивірусних серверних програм, через розподіл запитів клієнта між безліччю серверів.

Доводиться вдаватися до кластеризації: кілька серверів поєднуються в кластер; навантаження між ними розподіляється за допомогою комплексу спеціальних методів, які називаються балансуванням. Крім вирішення проблеми високих навантажень, кластеризація допомагає також забезпечити резервування серверів один на одного.

Ефективність кластеризації безпосередньо залежить від того, як розподіляється (балансується) навантаження між елементами кластеру. Балансування навантаження може здійснюватися за допомогою апаратних і програмних інструментів.

Вдосконалена технологія безпечної маршрутизації дозволяє виявляти скомпрометовані сервери та видаляти їх зі списку маршрутизації, щоб максимально скоротити наслідки збою. Також дослідження показали, що кластери з балансуванням навантаження забезпечують велику масштабованість та ефективність.

Слід зауважити, що при проектуванні балансування навантаження для хмарного антивірусної програми доцільно буде скористатися такими рекомендаціями:

1. При проектуванні хмарної антивірусної програми за можливості уникайте прив'язки до одного серверу, оскільки це може негативно зашкодити можливості масштабування програми. Прив'язка до сервера виникає, коли створюються умови, за яких усі запити одного клієнта мають оброблятися одним сервером. Зазвичай це відбувається при використанні локально оновлюваних кешів, зберігання стану сеансів у процесі або локальних сховищ стану сеансів. Якщо потрібно підтримувати прив'язку до одного сервера, конфігуруйте кластер

так, щоб він забезпечував маршрутизацію всіх запитів від певного користувача одного й того самого серверу.

2. Проектуйте для ХОС компоненти без збереження стану. Якщо потрібно зберігати стан користувачів, уникайте застосування у Веб-формі управління сеансами процесу, якщо не можете налаштувати прив'язку до сервера і гарантувати, що запити від одного користувача надсилатимуться на той самий сервер. Найкраще використовуйте зовнішній сервіс зберігання стану або сервер бази даних.

3. Використовуйте кластеризацію для скорочення негативних наслідків збоїв обладнання.

4. Якщо додаток (або ПЗ) висуває високі вимоги щодо вводу/виводу, виконуйте секціонування бази даних та розподіл її на множину серверів баз даних.

Сучасні рішення балансування навантаження залежать від розумних методів виділення ресурсів хмари та інших технологій, що становлять сучасне ІТ-середовище. Використання хмарного балансувальника навантаження не дозволить одному серверу програм стати єдиною точкою відмови, тим самим покращуючи загальну доступність програм, оперативність та надійність web-сервісу.

Отже, використання вдосконалених моделей та антивірусного захисту даних в ІКС в умовах модернізації мережевого телекомунікаційного обладнання дозволить підвищити рівень інформаційної безпеки.

2.4 Висновки до розділу 2

У даному розділі було вдосконалено метод антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у антивірусні хмарні системи. Основними складовими рішеннями методу є алгоритми формування безлічі

маршрутів передачі метаданих, метод контролю ліній зв'язку ІКС, моделі системи нейромережевих експертів безпечної маршрутизації.

Також були проведено розрахунки для підтвердження достовірності одержаних результатів та представлена структурна схема алгоритму формування базової множини маршрутів передачі метаданих. Наведені способи ймовірних атак несанкціонованого доступу до ВОЛЗ та рішення безпечної маршрутизації.

Були представлені результати порівняльних досліджень та оцінка ефективності методу антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у хмарних антивірусних системах. Також на основі отриманих даних додається практичні рекомендації щодо вдосконаленого методу.

У розділі проведено дослідження різних варіантів архітектур хмарних сховищ даних та запропоновані варіанти побудови хмарних антивірусних ресурсів, а також балансування навантаження.

Як практичні рекомендації запропоновані технічні нововведення та рішення, які дозволять підвищити ефективність інформаційного обміну у сучасній ІКС.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Вступ

Метою виконання економічного розділу [36] кваліфікаційного проекту є техніко-економічне обґрунтування доцільності запровадження вдосконаленого методу антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у антивірусні хмарні системи. Для цього будуть розраховані капітальні (фіксовані) та поточні (експлуатаційні) витрати на реалізацію рішень, буде проаналізована оцінка можливого збитку від загроз та ефект від впровадження системи інформаційної безпеки, розрахунок коефіцієнту повернення інвестицій та термін окупності капітальних інвестицій. Відштовхуючись від цих даних можна буде зробити висновок, щодо прибутковості або збитковості цих рішень запропонованих у кваліфікаційній роботі.

3.2 Визначення витрат на проектування та експлуатацію системи ІБ

3.2.1 Розрахунок капітальних (фіксованих) витрат

До фіксованих витрат, що повинні бути здійснені в рамках вдосконалення методу антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у антивірусні хмарні системи, необхідно включити:

1. Вартість створення документації проекту вдосконалення методу антивірусного захисту даних в ІКС;
2. Вартість апаратного та ліцензійного програмного забезпечення, необхідного для реалізації методу;
3. Вартість створення програмного забезпечення без урахування витрат на підтримку та обслуговування;
4. Витрати на впровадження методів інтеграції нового методу із середовищем, що вже функціонує.

Головна мета кваліфікаційного проекту запровадження та дослідження вдосконаленого методу антивірусного захисту, то для вибору засобів антивірусного захисту буде використовуватися абстрактна одиниця антивірусу з фіксованою первісною вартістю та модель розробки програмного забезпечення якої є open-source. Хмарне сховище та маршрутизатор надаються компанією постачальником антивірусної системи. Для первісного придбання цих активів плануються витрати, що наведені в таблиці 3.1.

Таблиця 3.1 — Витрати на первісне придбання активів

Продукт	Кількість	Вартість, грн.
Антивірус	1	15000
Хмарне сховище	1	–
Маршрутизатор	1	–

Щоб розрахувати загальні витрати вдосконалення методу антивірусного захисту даних в ІКС необхідно враховувати такі показники, як:

- трудомісткість розробки та опрацювання реалізованого методу;
- витрати при створенні програмного забезпечення.

Трудомісткість вдосконалення методу антивірусного захисту даних в ІКС можна розрахувати за формулою (3.1):

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д}, \text{ (годин)}, \quad (3.1)$$

де $t_{тз}$ – час складання технічного завдання на розробку програмних рішень;

$t_{в}$ – тривалість опрацювання технічного завдання;

$t_{а}$ – тривалість розробки проекту (алгоритму), за яким працюватиме метод;

$t_{пр}$ – тривалість процесу імплементації програмного рішення;

$t_{опр}$ – тривалість опрацювання вдосконаленого методу на ПК;

$t_д$ – час розробки експлуатаційної документації для даного програмного забезпечення.

Слід зазначити варіативність часу, за який можна виконати роботи та різні підходу до проектування, враховуючи різну кваліфікацію розробників. Тож буде використані середні показники кваліфікації та рівень досвіду спеціаліста до трьох років. Отже, умовну кількість операторів системи виявлення можна визначити за формулою (3.2):

$$Q = q \cdot c \cdot (1 + p), \text{ (штук)}, \tag{3.2}$$

де q – очікувана кількість операторів;

c – коефіцієнт складності програмного забезпечення;

p – коефіцієнт корекції програми у процесі опрацювання.

Очікувана кількість операторів програми складатиме:

$$q = 70 \text{ (штук)}.$$

Коефіцієнт складності програми c визначимо відносно складності програми типового завдання, що дорівнює:

$$c = 2{,}0.$$

Коефіцієнт корекції програми p збільшиться за рахунок внесення змін в алгоритм програми внаслідок роботи над технічним завданням, тож отримаємо значення p:

$$p = 0{,}09.$$

Тож, враховуючи усі наведені параметри, умовна кількість операторів програмного забезпечення, що розробляється, складатиме за формулою 3.2:

$$Q = 70 \cdot 2{,}0 \cdot (1 + 0{,}09) = 153,$$

Далі, беручи за увагу середню кваліфікацію спеціаліста, його досвід та специфіку роботи, то час реалізації технічного завдання на вдосконалення програмного методу буде:

$$t_{тз} = 24 \text{ (годин)}.$$

Тривалість вивчення технічного завдання, опрацювання літератури та кваліфікації програміста визначається за формулою (3.3):

$$t_в = \frac{Q \times B}{(75...85) \times k} \text{ (годин)}, \qquad (3.3)$$

де B – коефіцієнт збільшення тривалості роботи над розробкою через недостатнього опису завдання;

k – коефіцієнт, що залежить від стажу програміста.

$$t_в = \frac{153 \times 1{,}3}{(75) \times 1} = 2{,}7 \text{ (годин)}$$

Тривалість розробки блок-схеми алгоритму представлена формулою (3.4):

$$t_a = \frac{Q}{(20...25) \times k} \text{ (годин)}. \qquad (3.4)$$

$$t_a = \frac{153}{20} = 8 \text{ (годин)}.$$

Тривалість процесу імплементації вдосконаленого методу розраховано за такої ж формулою (3.4):

$$t_{пр} = \frac{153}{20} = 8 \text{ (годин)}.$$

Тривалість опрацювання вдосконаленого методу на ПК розраховується за формулою (3.5):

$$t_{опр} = \frac{1{,}5 \times Q}{(4 \ldots 5) \times k} \text{ (годин)}. \quad (3.5)$$

$$t_{опр} = \frac{1{,}5 \times 153}{4} = 58 \text{ (годин)}$$

Час розробки експлуатаційної документації для даного методу можна розрахувати за формулою (3.6):

$$t_{д} = \frac{Q}{(15 \ldots 20) \times k} + \frac{Q}{(15 \ldots 20)} \times 0{,}75 \text{ (годин)} \quad (3.6)$$

$$t_{д} = \frac{153}{15} + \frac{153}{15} \times 0{,}75 = 18 \text{ (годин)}$$

Отже, повертаючись до розрахунку трудомісткості вдосконаленого методу антивірусного захисту даних в ІКС за формулою (3.1):

$$t = 24 + 2{,}7 + 8 + 8 + 58 + 18 = 119 \text{ (годин)}$$

Далі для розрахунку загальних витрат на створення системи виявлення необхідно визначити необхідні витрати на заробітну плату виконавця роботи та витрати машинного часу, формула (3.7):

$$K_{рп} = З_{зп} + З_{мч}, \text{ (грн.)}, \quad (3.7)$$

де $З_{зп}$ – заробітна плата спеціаліста з інформаційної безпеки;

$З_{мч}$ – вартість витрат машинного часу, що необхідні для створення.

Для підрахунку заробітної плати спеціаліста будуть враховані основна та додаткова заробітна плата, а також відрахування на соціальні потреби (пенсійне страхування, соціальне страхування тощо), розраховується за формулою (3.8):

$$З_{зп} = t \cdot З_{пр}, \text{ (грн.)}, \quad (3.8)$$

де t – загальна тривалість розробки політики безпеки, годин;

$З_{пр}$ – середньогодинна заробітна плата спеціаліста з програмування з нарахуваннями, грн/годину. Проаналізувавши ринок послуг з програмного забезпечення середня заробітна плата розробника складає приблизно 450 (грн/год), отже отримаємо:

$$З_{зп} = 119 \cdot 450 = 53550 \text{ (грн.)},$$

А для того щоб визначити витрати машинного часу для налагодження програмно реалізованого методу використаємо формулу 3.9:

$$З_{мч} = t_{опр} \cdot С_{мч} + t_{д}, \text{ (грн.)}, \quad (3.9)$$

де $t_{опр}$ – час опрацювання реалізованого методу на ПК, у годинах;

$С_{мч}$ – вартість однієї години машинного часу ПК, грн/година;

$t_д$ – час розробки експлуатаційної документації для даного програмного забезпечення, у годинах.

Для визначення однієї години машинного часу ПК скористаємось формулою 3.10:

$$C_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p}, \text{ (грн.)}, \qquad (3.10)$$

де P – встановлена потужність ПК, кВт (складатиме 1.1 кВт);

$t_{нал}$ – кількість машин на яких вдосконалюється метод (становить одну машину);

C_e – тариф на електричну енергію, грн/кВт (на сьогодні складає 1,68);

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці (становить 0,8);

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення частки одиниці (становить 0,8);

F_p – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920).

Враховуючи зношення ПК за 1 рік його використання, залишкова вартість ПК на поточний рік складатиме:

$$Ф_{зал} = 18000 \text{ (грн.)}.$$

Наявності ліцензійного програмного забезпечення, витрати на нього вказані в таблиці 3.1, з урахуванням обладнання, що надається компанією постачальником:

$$К_{лпз} = 15000 \text{ (грн.)}.$$

Отже, вартість машинного часу для вдосконалення методу антивірусного захисту даних в ІКС на ПК буде становити:

$$С_{мч} = 0{,}65 \cdot 1 \cdot 1{,}68 + \frac{18000 \cdot 0{,}8}{8064} + \frac{15000 \cdot 0{,}8}{8064} = 5 \text{ (грн.)}.$$

Повертаючись до формули 3.9 – вартості машинного часу для налагодження програмно реалізованого методу складатиме:

$$З_{мч} = 40 \cdot 5 + 18 = 218 \text{ (грн.)}$$

Визначити остаточні капітальні витрати на проектування та впровадження методу виявлення атак можна за формулою (3.11):

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \text{ (грн.)}, \quad (3.11)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх спеціалістів, тис. грн.;

$К_{зпз}$ – вартість купівлі ліцензійного основного й додаткового програмного забезпечення, тис. грн.;

$К_{пз}$ – вартість створення основного програмного забезпечення, тис. грн.;

$К_{аз}$ – вартість купівлі апаратного забезпечення, тис. грн.;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн.;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Так як, ніякого апаратного забезпечення не розглядалося та не закуповується, то $К_{аз}$ та $К_н$ не буде враховуватися.

Одноразове підвищення кваліфікації технічного персоналу та співробітників, щодо вдосконаленого методу додається одноразова виплата у розмірі 8000 грн.

Отже, підсумовуючи усі розрахунки та використавши формулу 3.11, отримаємо повну вартість капітальних (фіксованих) витрат:

$$К = 40000 + 15000 + 8000 = 63000 \text{ (грн.)}.$$

3.2.2 Розрахунок поточних (експлуатаційних) витрат

До експлуатаційних витрат необхідно включити, що повинні бути здійснені в рамках вдосконалення методу антивірусного захисту даних в ІКС, необхідно включити:

1. Вартість систематичного відновлення системи;
2. Витрати на керування системою.

За методикою Gartner Group до поточних витрат будуть віднесені наступні:

1. Витрати на відновлення й модернізацію системи;
2. Витрати на керування системою в цілому;
3. Витрати, викликані активністю користувачів системи інформаційної безпеки.

Річні поточні витрати на функціонування системи інформаційної безпеки для даного підприємства визначаються за формулою 3.12:

$$С = С_в + С_к + С_{ак}, \text{ (грн.)}, \qquad (3.12)$$

де $С_в$ – вартість відновлення й модернізації системи;

$C_к$ – витрати на керування системою в цілому;

$C_{ак}$ – витрати, викликані активністю користувачів системи.

Для забезпечення користування ПЗ на рік визначаються витрати на подовження ліцензії продукту ($C_в$), що становить 3200 грн\рік.

Щоб порахувати витрати на керування системою інформаційної безпеки ($C_к$) використаємо формулу 3.13:

$$C_к = C_н + C_а + C_з + C_{єв} + C_{ел} + C_{тос}\text{ , грн.} \quad (3.13)$$

Де $C_н$ – витрати на навчання адміністративного персоналу, у грн.;

$C_а$ – витрати у фонд амортизаційних відрахувань, у грн.;

$C_з$ – річний фонд заробітної плати технічного персоналу, що складається з основної ($З_{осн}$) та додаткової ($З_д$) плати, у грн.;

$C_{єв}$ – єдиний внесок, що складає 22% від мінімальної заробітної плати, у грн.;

$C_{ел}$ – вартість електроенергії, у грн.;

$C_{тос}$ – витрати на технічне та організаційне адміністрування системи інформаційної безпеки, що складає 1-3% від обсягу капітальних вкладень, у грн..

Витрати на навчання адміністративного персоналу й кінцевих користувачів ($C_н$) становитиме 14000 грн.

Розрахувати річний фонд амортизації можна за наступною формулою (3.14):

$$C_а = \frac{\text{Кпз}}{2}, (\text{грн.}) \quad (3.14)$$

$$C_а = \frac{15000}{2} = 7500\ (\text{грн.})$$

Річний фонд заробітної плати програмісту та технічному персонажу, що буде обслуговувати систему інформаційної безпеки наведений у формулі (3.15):

$$C_з = З_{осн} + З_д, \text{ (грн.)}, \quad (3.15)$$

$$C_з = 216000 + 216000 \cdot 0{,}1 = 237600 \text{ (грн.)}$$

Також розрахуємо ставку ЄСВ, що на 2021 рік для всіх категорій платників становить 22%, тому даний відсоток розраховується від суми основної та додаткової заробітної плати, а отже, становитиме 3960 грн.

Вартість електроенергії, що споживається апаратурою ($C_{ел}$) визначається за формулою 3.16:

$$C_{ел} = P \cdot F_р \cdot Ц_е, \text{ (грн.)}, \quad (3.16)$$

де P – встановлена потужність апаратури інформаційної безпеки;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки;

$Ц_е$ – тариф на електроенергію.

Так як тариф на електроенергію 1.68 грн/кВт на годину, та встановлена потужність апаратури дорівнює 0.65, маємо:

$$C_{ел} = 0.65 \cdot 8064 \cdot 1.68 = 8806 \text{ (грн.)}.$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($C_{тос}$) визначається від вартості капітальних (K) витрат (1-3%), тому:

$$C_{тос} = 63000 \cdot 0.03 = 1890 \text{ (грн.)}.$$

Тож, витрати на керування системою інформаційної безпеки ($C_к$) становлять за формулою 3.13:

$$C_к = 14000 + 7500 + 237600 + 3960 + 8806 + 1890 = 273756 \text{ (грн.)}.$$

Отже, повертаючись до річних поточних витрат на функціонування системи інформаційної безпеки, будуть складати:

$$C = 3200 + 273756 = 276956 \text{ (грн.)}.$$

3.3 Оцінка можливого збитку від атаки

3.3.1 Оцінка величини збитку

Для розрахунку вартості збитку, що понесе компанія, при реалізації атаки, необхідно враховувати наступні дані:

1. $t_п$ – час простою вузла корпоративної мережі, у годинах;
2. $t_в$ – час, необхідний для відновлення системи, у годинах;
3. $t_{ві}$ – час відновлення інформації, у годинах;
4. $З_0$ – заробітна платня обслуговуючого персоналу;
5. $З_с$ – заробітна платня співробітників атакованого вузла;
6. $Ч_0$ – чисельність обслуговуючого персоналу;
7. $Ч_с$ – чисельність співробітників атакованого вузла;
8. $О$ – обсяг продажів атакованого вузла, у грн.;
9. $П_{зч}$ – вартість доопрацювання, модифікації програмного забезпечення чи апаратного устаткування;
10. $І$ – число атакованих вузлів;
11. N – середнє число атак на рік.

Втрати від простою атакованого вузла можна визначити за формулою (3.17):

$$U = П_П + П_В + V, \text{ (грн.)}, \quad (3.17)$$

де $П_п$ – оплачувані витрати робочого часу та простої співробітників активного вузла, грн.;

$П_в$ – вартість відновлення працездатності вузла (переустановлення системи, заміна конфігурації та ін.), грн.;

V – втрати від зниження обсягу продажів за час простою активного вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегменту корпоративної мережі є втрата їх заробітної плати (оплата непродуктивної праці) за час простою, що знаходиться за формулою (3.18):

$$П_п = \frac{\sum З_с}{F} \cdot t_п \text{ , (грн.)}, \quad (3.18)$$

де $З_с$ – розмір заробітної плати працівника;

F – місячний фонд робочого часу;

$t_п$ – час простою корпоративної мережі внаслідок атаки.

$$П_п = \frac{216000}{160} \cdot 6 = 8100 \text{ (грн.)}.$$

Щоб відновити працездатність вузла або сегмента корпоративної мережі треба кілька складових за формулою (3.19):

$$П_в = П_{ві} + П_{пв} + П_{зч} \text{ , грн.}, \quad (3.19)$$

де $П_{ві}$ – витрати на повторне введення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла корпоративної мережі, грн.;

Пзч – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації ($П_{ви}$) треба розраховувати виходячи з розміру заробітної плати співробітників ($З_с$), що будуть цим займатися з урахуванням необхідного для цього часу ($t_{ві}$), за формулою (3.20):

$$П_{ві} = \frac{З_с}{F} \cdot t_{ві}\ , (грн.), \quad (3.20)$$

$$П_{ві} = \frac{216000}{160} \cdot 4 = 5400\ (грн.).$$

Далі визначимо витрати на відновлення вузла корпоративної мережі, визначається за часом відновлення після атаки ($t_в$) і розміром заробітної плати обслуговуючого персоналу ($З_о$), за формулою (3.21):

$$П_{пв} = \frac{З_о}{F} \cdot t_в, (грн.), \quad (3.21)$$

$$П_{пв} = \frac{216000}{160} \cdot 7 = 9450\ (грн.).$$

Отже, вартість відновлення системи становить:

$$П_в = 5400 + 9450 = 14850\ (грн.).$$

Для розрахунку втрат від зниження обсягу продажів під час простою використовується формула (3.22):

$$V = \frac{О}{F_г} \cdot (t_п + t_в + t_{ві})\ , грн., \quad (3.22)$$

де $О$ – обсяг продажів атакованого вузла корпоративної мережі, грн/рік;

$F_Г$ – річний фонд часу роботи організації.

Так як у дипломній роботі не розглядається конкретний об'єкт, компанія або підприємство, то для розрахування втрат буде розглядатися маркетингова компанія ТОВ «Машина» (*V*), що вже виступала об'єктом дослідження у дипломній роботі:

$$V = \frac{2400000}{2259} \cdot (8 + 12 + 10) = 31872 \text{ (грн.)}.$$

Повертаючись до формули 3.17, маємо упущену вигоду від простою атакованого вузла:

$$U = 8100 + 14850 + 31872 = 54822 \text{ (грн.)}.$$

Показник загального збитку від реалізації атаки становить (3.23):

$$B = \sum_i \sum_n U \text{ , (грн.)}. \quad (3.23)$$

де I – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число атак на рік.

$$B = 3 \cdot 8 \cdot 54822 = 1315728 \text{ (грн.)}.$$

3.3.2 Загальний ефект від впровадження системи ІБ

Загальний ефект від впровадження системи виявлення атак розраховується за формулою (3.24):

$$E = B \cdot R - C, \text{ (грн.)}. \quad (3.24)$$

де R – очікувана ймовірність атаки на вузол, у частках одиниці;

С – щорічні експлуатаційні витрати.

Отже, загальний ефект від впровадження системи інформаційної безпеки становить:

$$E = 1315728 \cdot 0{,}4 - 273756 = 252535 \text{ (грн.)}.$$

3.4 Визначення та аналіз показників економічної ефективності системи ІБ

Для визначення оцінки економічної ефективності системи інформаційної безпеки здійснюються такі основні аналізи як:

1) Коефіцієнт повернення інвестицій ROSI;
2) Термін окупності капітальних інвестицій T_o.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Знайдем за формулою 3.25:

$$ROSI = \frac{\text{Е}}{\text{К}}, \text{ частки одиниці,} \qquad (3.25)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, тис. грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

$$ROSI = \frac{252535}{63000} = 4{,}01$$

Реалізація проекту ввижається економічно доцільним, якщо значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції, за формулою (3.26):

$$ROSI > (N_{деп} - N_{інф}) / 100, \quad (3.26)$$

де $N_{деп}$ – річна депозитна ставка;

$N_{інф}$ – річний рівень інфляції.

Маємо, що для обраної компанії ТОВ «Машина» реалізація проекту є економічно доцільним за даної умови:

$$4{,}01 > (18 - 8) / 100 = 4{,}01 > 0{,}1.$$

Термін окупності капітальних інвестицій T_o показує за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки, знайдемо за формулою (3.27):

$$T_o = \frac{К}{Е} = \frac{1}{ROSI}, \text{ (років)}, \quad (3.27)$$

$$T_o = \frac{63000}{252535} = \frac{1}{4{,}01} = 0{,}25 \text{ (років)}.$$

3.5 Висновок розділу 3

Тож, дослідження економічного розділу дипломного проекту є техніко-економічне обґрунтування доцільності запровадження вдосконаленого методу антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у антивірусні хмарні системи.

В даному розділі були розраховані капітальні (фіксовані) витрати, що становлять 63000 грн. та поточні (експлуатаційні) витрати, що становлять 273756 грн. на заходи інформаційної безпеки. Для кращого порівняння й розуміння ефективності даного методу розраховано за даними дослідження підприємства ТОВ «Машина» дипломної роботи, була оцінена величина збитків – 1315728 грн., та, відповідно, ефект від впровадження системи безпеки компанії – 252535 грн. Був проведений розрахунок коефіцієнту повернення інвестицій (ROSI), що становить для компанії – 4,01, і термін окупності капітальних інвестицій – 0,25 або 1\4 року.

Отже, згідно з результатами економічного розділу, можна зробити висновок, що проект є економічно доцільним та вигідним для реалізації на підприємстві ТОВ «Машина».

ВИСНОВКИ

У цій кваліфікаційній роботі було досліджено та вдосконалено метод антивірусного захисту даних в ІКС з використанням сучасних хмарних обчислювальних систем, задля забезпечення інформаційної безпеки від негативного та руйнівного впливу комп'ютерних вірусів. В ході виконання поставленої мети були здійснені наступні кроки:

1. Проведений аналіз загроз, що впливають на стан захисту даних в ІКС, вимоги до інформаційної безпеки та антивірусного захисту, були розглянуті засоби та методи забезпечення заданих вимог, обґрунтовуваний вибор напрямку дослідження та сформована задача вдосконалення методу антивірусного захисту даних з використанням хмарних обчислювальних систем.

2. Досліджено та описано вдосконалення методу антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у антивірусні хмарні системи. Основними складовими методу якого є алгоритми формування безлічі маршрутів передачі метаданих, метод контролю ліній зв'язку ІКС, моделі системи нейромережевих експертів безпечної маршрутизації.

3. Також виконано техніко-економічне обґрунтування доцільності запровадження вдосконаленого методу антивірусного захисту даних в ІКС за рахунок безпечної маршрутизації метаданих у антивірусні хмарні системи. Для підрахунку економічної доцільності було разглянуто підприємство ТОВ «Машина».

Отже, проведена робота з вдосконаленням методу відповідає поставленим вимогам та завданню для підвищення надійності, захищеності даних, та своєчасної локалізації комп'ютерних вірусів та інших дій зловмисників у інформаційно-комунікаційному просторі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Смірнов С. А. "Метод антивірусного захисту даних з використанням хмарних обчислювальних технологій" [Електронний ресурс] // Редакція від 2017 // Режим доступу до ресурсу: http://www.dut.edu.ua/uploads/p_1539_83709095.pdf

2. Закон України "Про інформацію" [Електронний ресурс] // Редакція від 21.12.2019. – 1992. // Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.

3. Закон України "Про захист персональних даних" [Електронний ресурс] // Редакція від 20.03.2020. – 2010. // Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.

4. Закон України "Про захист інформації в інформаційно телекомунікаційних системах" [Електронний ресурс] // Редакція від 19.04.2014. – 1994. // Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-вр.

5. Інформаційно-комунікаційні технології [Електронний ресурс] // Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Інформаційно-комунікаційні_технології.

6. «Информационные системы:оценка рисков» Захаров О. І. [Текст] // Редакція від 2005 №6.

7. Вітлінський, В. В. «Ризикологія в економіці та підприємництві» [Текст] // В. В. Вітлінський, Г. І. Великоіваненко. – К.: КНЕУ, 2004. – 480 с.

8. Завгородний, В. И. «Системный анализ информационных рисков» [Текст] // В. И. Завгородний // Вестник Финансовой академии. № 4, 2008. – С. 102–109.

9. Зегжда, П. Д. «Теория и практика обеспечения информационной безопасности» [Текст] // П. Д. Зегжда. – М.: Яхтсмен, 1996. – 192 с.

10. Клименюк, М. М. «Управління ризиками в економіці: Навч. посіб. для студ. вищ. навч. закл.» [Текст] // М. М. Клименюк, І. А. Брижань; Акад. муніцип. упр. – К., 2000. – 253 с.

11. Ортинський, В. Л. «Економічна безпека підприємств, організацій та установ» [Електронний ресурс] // В. Л. Ортинський // Модель побудови системи інформаційної безпеки. – Режим доступу до ресурсу: http://westudents.com.ua/glavy/16530-model-pobudovi-sistemi-nformatsyno-bezpeki.html

12. "Аналіз принципів побудови моделей інформаційної безпеки в корпоративних інформаційних системах" [Електронний ресурс] // Редакція від 2015 №8 // Режим доступу до ресурсу: http://www.economy.nayka.com.ua/?op=1&z=4257.

13. Мельников В.В. «Защита информации в компьютерных системах» [Текст] // В.В. Мельников. – М.: Финансы и статистика. Электроинформ, 1997. – 367 с.

14. Романец Ю.В. «Защита информации в компьютерных системах и сетях» [Текст] // Ю.В Романец., П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

15. Новіков О. М., Грайворонський М. В. «Безпека інформаційно-комунікаційних систем» [Електронний ресурс] // Модель побудови системи інформаційної безпеки. – Режим доступу до ресурсу: http://is.ipt.kpi.ua/wp-content/uploads/sites/4/2015/03/Graivorovskyi_Novikov.pdf

16. Левин В.К., Гайкович В.Ю., Дорошкевич П.В. и др. Информационная безопасность компьютерных сетей. [Текст] // Технологии электронных коммуникаций. – М. 1993. т.5.–128 с.

17. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах [Текст] // 2005. – 147 с.

18. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. [Текст] // Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.

19. Семенов С.Г. Методика математического моделирования защищенной ИТС [Текст] // Вісник Національного технічного університету «Харківський політехнічний інститут». – Х.:НТУ «ХПІ». – 2012. – №62 (968). – С 173-181.

20. Семенов С.Г. Защита данных в компьютеризированных управляющих системах [Текст] // С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко. – LAP Lambert Academic Publishing GmbH , 2014. – 236 с.

21. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей [Текст] // А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.

22. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко [Текст] // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління», 2011.

23. Касперский Е. Компьютерное зловредство [Текст] // Е. Касперский. – СПб.: Питер, 2007. – 208 с.

24. Касперски К. Техника сетевых атак. [Електронний ресурс]. // Режим доступу до ресурсу: http://rghost.ru/download/43730077/8e48b6263ce45c7dc2a65a7453383dc33b22486d/Крис%20Касперски%20-%20Техника%20сетевых%20атак.pdf

25. Касперски К. Техника и философия хакерских атак [Текст] // К. Касперски. 2004 – 272 с.

26. Котенко И В. Аналитические модели распространения сетевых червей [Текст] // И.В. Котечко, В.В. Воронцов / Труды СПИИРАН - СПб.: Наука, 2007. № 4.

27. Rohloff K Stochastic Behavior of Random Constant Scanning Worms /K. Rohloff, T. Basar [Текст] // Computer Communications and Networks, 2005.

ICCCN 2005. Proceedings 14th Internationa Conference on 17-19 Oct. 2005.— P. 339-344.

28. Сравнительный анализ моделей распространения компьютерных вирусов в автоматизированных системах [Електронний ресурс] // Национальный технический университет «ХПИ», Харьков, 2018. // Режим доступу до ресурсу: https://www.researchgate.net/publication/344726820_COMPARATIVE_ANALYSIS_OF_MODELS_OF_DISTRIBUTION_OF_COMPUTER_VIRUSES_IS_IN_THE_AUTOMATED_TECHNOLOGICAL_PROCESS_CONTROL_SYSTEMS

29. Яковлєв А. В. Волоконно-оптичні системи передачі конфіденційної інформації. [Текст] // Електрозв'язок, №10, С 11-13. 99

30. Манько А. А., Каток В.Б., Задорожній М.Д. «Захист інформації на волоконно-оптичних лініях зв'язку від несанкціонованого доступу.» [Текст] // Ювелійна науково-технічна конференція «Правове, нормативне та Метрологічне забезпечення системи захисту інформації в Україні» Україна, Київ, 2001.№2.

31. Гришачев В.В., Кабашкин В.Н., Фролов А.Д. «Физические принципы формирования каналов утечки информации в волоконно-оптических линиях связи.» [Текст] // "Информационное противодействие ургозам терроризма" №3, 2005 г. – С 75-76.

32. Гришачев В.В., Кабашкин В.Н., Фролов А.Д. «Анализ каналов утечки информации в волоконно-оптических линиях связи: нарушение полного внутреннего отражения.» [Текст] // "Информационное противодействие ургозам терроризма" №4, 2005 г.

33. Каток В.Б., Манько А. А., «Захист інформації в оптичних лінійних трактах методом спектрального розподілу.» [Текст] // Ювелійна науково-технічна конференція «Правове, нормативне та Метрологічне забезпечення системи захисту інформації в Україні» Україна, Київ, 1998.

34. Довідник з функцій Windows [Електронний ресурс] // Процедури та функції – Режим доступу до ресурсу: http://platonov-andrei.narod.ru/Delphi/FuncAPI/index.htm

35. Windows API Index [Электронный ресурс]. – Режим доступа к ресурсу: https://msdn.microsoft.com/enus/library/windows/desktop/ff818516 (v=vs.85).aspx

36. Пілова Д. П. Методичні вказівки до виконання економічної частини дипломного проекту для студентів спеціальності 125 Кібербезпека [Текст] // Д. П. Пілова. – 2019. – С.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	20	
6	А4	2 Розділ	32	
7	А4	3 Розділ	18	
8	А4	Висновки	1	
9	А4	Перелік посилань	5	
10	А4	Додаток А. Відомість матеріалів кваліфікаційної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгуки керівників розділів	1	
13	А4	Додаток Г. ВІДГУК	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

16 Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи