Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система виявлення атак з використанням Honeypot»

Виконав: студент 2 курсу, групи 1БС-20 м
спеціальності 125 Кібербезпека
_____ Жакун Г.А.

Керівник: к.т.н., старший викладач каф. ЗІ
_____ Лукічов В.В.
« ___ » _____ 2021 р.

Опонент:
_____
« ___ » _____ 2021 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Лужецький В. А.
«____» _____ 2021 р.

Вінниця ВНТУ – 2021 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформацій
Рівень вищої оствіти ІІ (магістерський)
Галузь знань – 12 інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д.т.н., проф.
_____ В.А. Лужецький
«___» _____ 2021 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Жакуну Геннадію Андрійовичу

1. Тема роботи: «Система виявлення атак з використанням Honeypot»
керівник роботи: Лукічов Віталій Володимирович, к.т.н., старший викладач каф. ЗІ,
затверджені наказом ректора ВНТУ від 24 вересня 2021 року №277.
2. Строк подання студентом роботи 20 грудня 2021 р.
3. Вихідні дані до роботи:
   - Метод авторизацій;
   - Можливість перехвату аткак;
   - спосіб реалізації – програмний модуль.
4. Зміст текстової частини: Вступ. 1. Аналіз інформаціїних джерел. 2. Створення та розробка алгоритмів таметодів. 3. Тестування системи виявлення атак. 4. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Огляд Honeypot по областям застосування (плакат, А4). Схема роботи СВВ (плакат, А4). Схема роботи СЗВ (плакат, А4). Блок-схема виявлення атака з використанням Honeypot (плакат, А4). Блок-схема вводу даних та розподілення запит входу (плакат, А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанти	Підпис, дата	
		завдання видав	виконання прийняв
1	Лукічов В.В., к.т.н., старш. викл. каф. ЗІ		
2	Лукічов В.В., к.т.н., старш. викл. каф. ЗІ		
3	Лукічов В.В., к.т.н., старш. викл. каф. ЗІ		
4	Лукічов В.В., к.т.н., старш. викл. каф. ЗІ		
5	Лесько О.Й., к.е.н., професор каф. ЕПВМ		

7. Дата видачі завдання 9 вересня 2021 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	01.09.2021 – 04.09.2021	
2	Розробка технічного завдання	05.09.2021 – 15.09.2021	
3	Аналіз інформаційних джерел за напрямком магістерської кваліфікаційної роботи	16.09.2021 – 22.09.2021	
4	Розробка рішень	23.09.2021 – 04.10.2021	
5	Практична реалізація, моделювання, експериментування, результати	05.10.2021 – 24.10.2021	
6	Розробка розділу економічного обґрунтування доцільності розробки	25.10.2021 – 17.11.2021	
7	Аналіз виконання ТЗ, висновки	18.11.2021 – 24.11.2021	
8	Оформлення пояснювальної записки	25.11.2021 – 30.11.2021	
9	Попередній захист та доопрацювання МКР	03.12.2021	
10	Представлення МКР до захисту	20.12.2021	
11	Захист МКР	21.12.2021	

Студент _____ Г.А. Жакун

Керівник роботи _____ В.В. Лукічов

АНОТАЦІЯ

УДК 004.056

Жакун Г.А. Система виявлення атак з використанням Honeypot. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2021. 114 с.

На укр. мові. Бібліогр.: 16 назв; рис.: 47; табл.: 9.

Магістерська кваліфікаційна робота присвячена розробці системи виявлення атак з використанням Honeypot. Підготовлено аналіз Honeypot та техніко-економічне обґрунтування доцільності досліджень. У роботі здійснено аналіз існуючих методів та представлено покращення систем виявлення атак серед аналогів. Розроблено метод та схему роботи системи. Реалізовано програмний засіб, який дозволив протестувати запропонований метод.

Ілюстративна частина складається з 6 плакатів з демонстрацією результатів моделювання і проведених досліджень.

В економічному розділі оцінено витрати на розробку.

Ключові слова: Honeypot, система виявлення атак.

ABSTRACT

Zhakun G. Honeypot attack detection system. Master's thesis in the specialty 125 – Cybersecurity. Vinnytsia: VNTU, 2021. – 114 p.

In Ukrainian language. Bibliographer: 16 titles; fig.: 47; tabl.: 9.

The master's qualification work is devoted to the development of the method and means of the attack detection system and Honeypot. The Honeypot analysis and the feasibility study of the expediency of the research have been prepared. The method and scheme of system operation are developed. A software tool has been developed that allows testing the proposed method.

The graphic part consists of 6 posters demonstrating the results of modeling and research.

The economic section estimates the development costs.

Keywords: Honeypot, attack detection system.

ЗМІСТ

ВСТУП

На даний час доволі часто може бути проблема авторизації та виявлення атак. Для цього використовують стандартні системи виявлення атак та стандартний захист від різних спроб підбора даних. Але більшість таких заходів спрямовані тільки на окремі групи атак, прикладом може бути Firewall або пасивні сисстеми виявлення атак. Тому **актуальною** задачею є розробка спеціального методу та системи, які дадуть змогу відслідкувати атаки та дослідитити різні види атак.

Система виявлення атак з використанням Honeypot дозволить покращити захист внутрішньої мережі та зовнішньої сережі також це дає можливість дослідити різні види атак.

Honeypot раніше досліджувались такими вченими: A. Menezes, Pvan Oorschot, S. Vanstone, Spitzner, L, Закер К. [5, 2, 9]

Об’єктом дослідження є процес захисту інформації шляхом використання Honeypot.

Предметом дослідження є системи виявлення атак та дослідження можливих атак з використанням Honeypot.

Метою магістерської кваліфікаційної роботи є покращити захист сисстеми вияленння атак з використання Honeypot.

Для досягнення мети необхідно:

- проаналізувати відомі методи, які використовуються у системах Honeypot;
- проаналізувати системи Honeypot, що представлені на ринку;
- розробити власний метод для Honeypot;
- розробити програмний засіб для роботи системи Honeypot.

Наукова новизна полягає в тому, що удосконалено систему виявлення аткак Brute-force , що засобами Honeypot, на відміну від існуючих приладів, уможливлює надійний захист персональних акаунтів користувачів.

Апробація результатів магістерської кваліфікаційної роботи. Результати магістерської роботи доповідалися на таких конференціях:

- Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 62)" / Збірник тез доповідей: випуск 62 (м. Тернопіль, 12 жовтня 2021 р.). [15];
- Молодь в науці: дослідження, проблеми, перспективи (МН-2022). Вінницький національний технічний університет.

Публікації магістерської кваліфікаційної роботи опубліковано двоє тез у збірниках матеріалів конференції [15, 16].

1 АНАЛІЗ ІНФОРМАЦІЇНИХ ДЖЕРЕЛ

1.1 Методи та властивості Honeypot

Honeypot – це комп‘ютерна система, яка створена для того, щоб заманювати кіберзлочинців, а також виявляти, відхиляти або вивчати спроби отримати несанкціонований доступ до інформаційних систем. Еволюцію Honeypots можна побачити не озброєним оком, поглянувши на те, як ці системи використовуються разом із IDS для запобігання, виявлення та реагування на атаки. Дійсно, honeypots все частіше знаходить своє місце поряд з мережевими і хост-системами захисту від вторгнень. Honeypots можуть запобігти атакам кількома способами.

Перше – сповільнення або припинення автоматичних атак, таких як хробаки або авторучки [1]. Це атаки, які випадково сканують всю мережу, яка шукає вразливі системи. (Honeypots використовують різноманітні трюки TCP, щоб помістити зловмисника в "холдинг"). Другий шлях – запобігти людським атакам. Тут honeypots прагнуть зіткнутися з нападником, змушуючи його приділяти увагу діяльності, яка не завдає ні шкоди, ні втрати, надаючи організації час відповісти і блокувати атаку.

Існують два основних типи реалізацій: адаптовані і реальні.

Адаптовані здатні моделюють взаємодію від імені певного сервісу, наприклад, прийняти з'єднання на tcp-порт 22, прийняти від атакуючого ім'я користувача і пароль і так далі, при цьому фіксуючи всі дії атакуючого. Дана атака показана на рисунку 1.1.

Реальні honeypot, засновані на застосуванні реальних ОС і реальних сервісів, трохи складніше в застосуванні. Фактично вони являють собою спеціально спроектовані мережеві сегменти, підключені до мереж загального користування. Мережевий трафік між honeypot і зовнішнім світом контролюється і фіксується, щоб повністю зберегти всі дії атакуючих, при цьому

не допустивши шкоди для власної інфраструктури. Типовими прикладами є honeyd і honeynet [2].

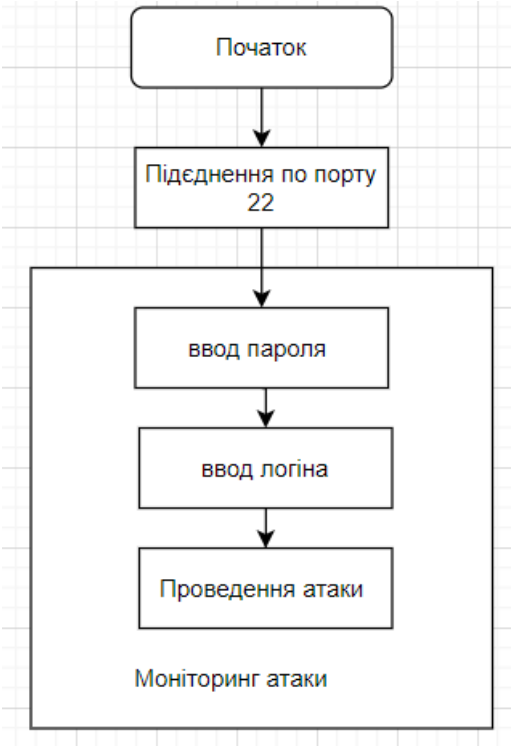


Рисунок 1.1 – Схема алгоритму роботи адаптивного Honeypot.

Honey дозволяє користувачам налаштовувати кілька віртуальних Honeypots з різними характеристиками і послугами на одній машині.

Honeyd – це мережа, розміщена за реверсивним мереженим екраном, що фіксує усі вхідні і вихідні дані. Реверсивний файрвол обмежує об‘єм шкідливого трафіку, що може покинути Honeynet-мережу. Ці дані зберігаються, фіксуються і контролюються. У середовищі Honeynet може бути розміщена будь-яка система, включаючи такі системи, які уже функціонують у виробничій мережі, яку покликана захищати Honeynet.

Honeynet – це мережа, призначена бути атакованою і скомпрометованою для отримання відомостей про наявні та потенційні вразливості і загрози в мережі. Сьогодні існує три основні архітектури Honeynet-мереж: I-ого покоління (Gen I Honeynets); II-ого покоління (Gen II Honeynets) та III-ого покоління (Gen III Honeynets). Gen I Honeynets. Honeynet-мережі I-ого покоління обмежені в

можливостях контролю та приборкування зловмисників, проте вони демонструють достатню ефективність у виявленні автоматизованих атак і атак початківців.

Передусім Gen I Honeynets фокусуються на атаках відповідно можливостей. Такі мережі-приманки достатньо легко ідентифікуються.

Архітектура Honeynet-мереж I-ого покоління досить проста – ізольована мережа розміщується за пристроєм контролю доступу до мережі, найчастіше таким служить мережевий екран (рисунок 1.2, а). Мета такого розміщення – забезпечити неможливість атаки не honeypot-систем. Часто поряд з Honeynet-мережею знаходиться виробнича ІКС для адміністрування і накопичення зафіксованих даних. Також, можливим є розміщення інших контролюючих пристроїв (наприклад, маршрутизатора) для додаткового контролю [2]. Фіксація активності шляхом комбінації можливостей файрволу, IDS-сенсорів і системних логів забезпечує перехоплення інформації на таких чотирьох рівнях: активність в мережі, системна активність, активність програм та активність користувача.

Gen II Honeynets. Технологія Gen II була розроблена в 2002 р. і направлена на усунення недоліків попередньої. Honeynet-мережі II-ого покоління простіші в розгортанні і складніші у виявленні [3]. Як описувалося вище, технологія Gen I виконувала контроль даних за допомогою мережевого екрану, що обмежував кількість можливих вихідних підключень. Незважаючи на свою відносну ефективність таке рішення є недостатньо гнучким і забезпечує легке «зняття зліпку».

Honeynet-мережі II-ого покоління вирішують цю проблему шляхом модифікації загальної архітектури (рисунок. 1.2, б). Перша основна розбіжність – використання єдиного Honeynet-сенсора, що об‘єднує функціонал файрвола та IDS. Друга основна відмінність – сама реалізація Honeynet-сенсора, що представляє собою пристрій другого рівня OSI (схожий на міст). Така реалізація значно ускладнює виявлення, так як відсутня маршрутизація пакетів, зменшення TTL і MAC-адреси пристроїв [4]. За рахунок описаних принципів Honeynet-

мережа II-ого покоління може бути частиною основної виробничої мережі, а не ізольованою як в технології Gen I (рис. 1.2).

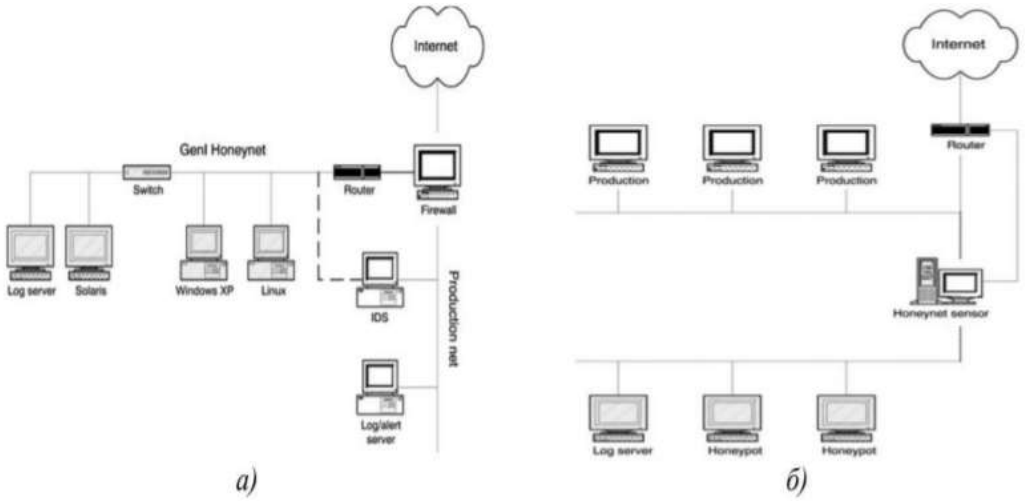


Рисунок 1.2 – Типи Honeynet мереж.

Технологія Gen III реалізує подальше удосконалення і розширення можливостей контролю і аналізу даних. Модель аналізу даних базується на таки абстракціях: хости, процеси, мережеві потоки і файли (рис. 1.3). Такий підхід реалізується на основі використання системи Honeywall, розроблений фахівцями проекту Honeynet Project. Для контролю підключень і даних застосовується підхід IP Performance Measerment Working Group, що полягає в моніторингу потоків.

У випадку використання Honeywall для цього застосовується система Argus [5]. Іншим удосконаленням є використання засобу пасивного зняття зліпку системи (passive fingerprinting), що ініціює TCP-підключення. Для об‘єднання цих двох типів даних (активність в ІКС і процесів на хості) навколо суцільної картини концепції потоків мережі використовують додаткову зв‘язуючу ланку. Для цього застосовують систему Sebek, що проводить моніторинг активності в мережі з перспективи хоста [6]. У роботі виконано окремий вид моделювання Honeynet Gen III у спецальному віртуальному середовищі UML, а праця містить різні варіани віртуалізації повно інтерактивних та різних приманок .

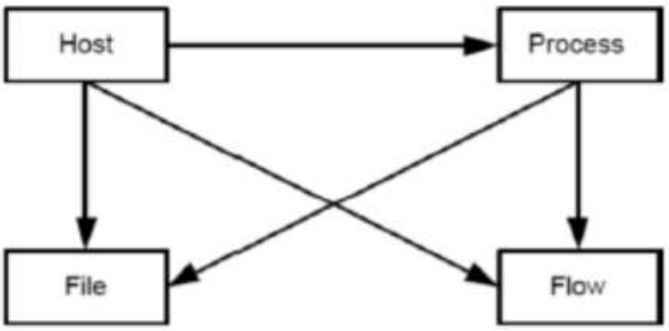


Рисунок 1.3 – Модель взаємозв’язків даних у системі Gen 3.

Honeypots захоплюють лише активність, спрямовану проти них, і буде пропускати напад на інші системи. З цієї причини фахівці з безпеки не рекомендують ці системи, щоб замінити існуючі технології безпеки. Замість цього, вони бачать honeypots як додаткову технологію захисту від вторгнення.
Планування розгортання приманок HoneyPots

По-перше, планування розгортання даної системи має підходити під цілі і особливості організації. Вам слід визначити, які дані в компанії особливо цінні? Які системи містять важливі активи? Як зловмисник може отримати до них доступ?

Все це допоможе визначити, які типи приманок потрібно використовувати конкретно для вашої інфраструктури. Крім іншого, розгортання приманок HoneyPot має враховувати і географічний фактор.

HoneyPots бувають різні - від простих змодельованих систем до систем, що працюють на операційних системах або навіть у апаратному та віртуальному режимі.

Як говорилося раніше, HoneyPots призначені для трансляції вразливостей, щоб залучити зловмисників. Наприклад, може використовуватися служба з уразливістю, застаріла або неліцензійна операційна система, мережеві ресурси з підозрілими назвами [7].

Особливість ресурсів HoneyPot в тому, що всі вони - помилкові і спрямовані виключно на піймання хакера. Вони налаштовані на відстеження

зловмисників в системі без їх відома. Це забезпечує компаніям раннє попередження та дозволяє досліджувати методи кіберзлочинців (рис. 1.4).

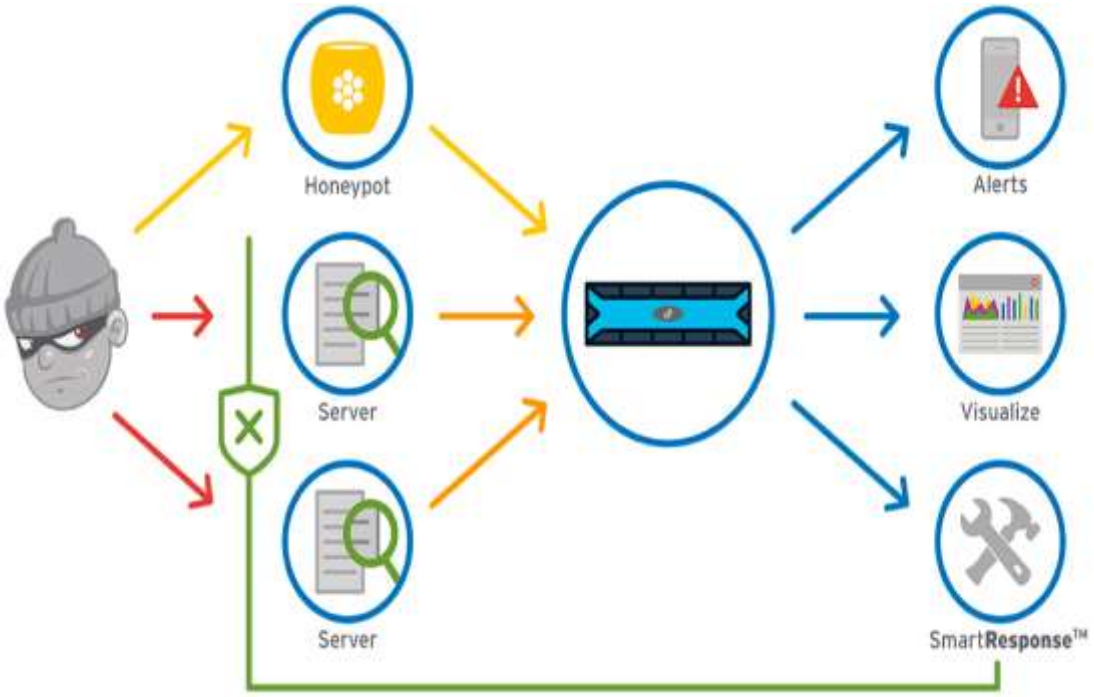


Рисунок 1.4 – Приклад роботи приманки Honeypot.

В даний час абсолютно універсального рішення, яке використовує концепцію Honeypot, не існує. Якщо розглядати її як імітаційну модель реального обчислювального процесу, то до будь-якого програмно-апаратного рішення на базі цієї концепції може бути застосовано обмеження Тьюринга. Останнє вимагає застосування субоптимальних (раціональних) підходів до реалізації Honeypot-рішень в контексті більш конкретного завдання [7]. Так з'явилися рішення на базі Honeypot, які поділяються за об'єктами, категоріям і області застосування в мережі показані на рисунку 1.5.

Таблиця відображає типові технологічні Honeypot-рішення, складена на основі аналізу їх функціональних можливостей і результатів тестування, описаних в літературі з урахуванням специфіки завдань, і відповідно, імітованих об'єктів. Функціональні можливості Honeypot-продуктів можуть розширюватися, області застосування перетинатися.

Fake Honeypot	Honeypot	Server	✗	✓
Honeyentries	Table, data set	Database	✓	✗
MTD	Topo., net. interf., memory, arch.	Versatile	✓	✓
Honeyword	Password	Authentica-tion	✓	✗
Honeyaccount	User account	Authentica-tion	✓	✗
Honeyfile	(Cloud-)File	File system	✓	✓
Honeypatch	Vulnerability	Server	✓	✓
–	Memory	Server	✓	✗
–	Metadata	File	✓	✗
HoneyURL	URL	File	✗	✓
Honeymail	E-Mail adress	File	✗	✓
Honeypeople	Social network profile	File	✗	✗
Honeyport	Network port	Server	✗	✓
Decep. web server	Error codes, Robot.txt	Server	✗	✓
OS interf.	System call	Server	✓	✗

Рисунок 1.5 – Огляд Honeypot по областям застосування

В міру ускладнення мереж і обчислювальних систем, збільшення числа можливих загроз, ускладнилися завдання і для Honeypot. Їх розробка стала циклічним процесом, так як вимагала постійного вдосконалення для все більш ефективного залучення зловмисників, які використовуються ними інструментів і шкідливих програм.

Шкідливі програми, захоплені на Honeypot, аналізуються ретроспективно з метою подальшої переробки приманки. З цієї точки зору внесок Honeypot в безпеку вважається реактивним, якщо імітація реального об'єкта проста і передбачає тільки реєстрацію дій, т. е. виявлення не надто кваліфікованого порушника. Прості Honeypot імітують поведінку реальних систем, проте навіть побіжний погляд, наприклад, на процес і результати сканування, дозволяє більш кваліфікованому порушнику побачити, що мета має аномальне кількість відкритих портів зі службою віддаленого управління (рис. 1.6).

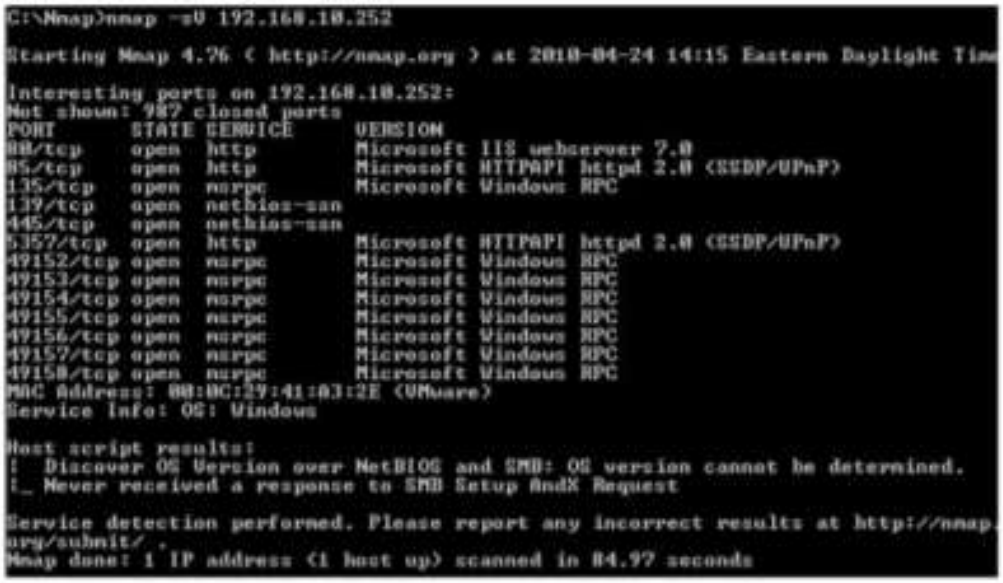


Рисунок 1.6 – Приклад розкритого Honeypot з допомогою nmap

Наступним етапом розвитку Honeypot стала більш реальна імітація на основі шаблонів реакції реальних систем. Але з початком використання в мережах Honeypot і розвитку рішень на базі цієї концепції, зловмисниками стали розроблятися і застосовуватися інструментальні засоби.

Honeypot-рішення, як і технології «обманки» в цілому, в значній мірі ґрунтуються на людської психології, тому єдиним способом протистояти їх виявлення є розвиток Honeypot шляхом ускладнення поведінки, використання гнучких масштабованих конфігурацій, які можуть бути побудовані на основі функціоналу та інструментів з відкритим кодом.

Кошти Honeypot мають кілька недоліків. Саме через ці недоліки Honeypot не замінюють жодних механізмів безпеки; вони тільки працюють та розширюють повну архітектуру безпеки.

Головними проблемами засобів Honeypot:

- обмежена область бачення;
- можливість розкриття Honeypot;
- ризик злому Honeypot та атаки вузлів сторонніх організацій.

Простий рахунок Honeypot: рахунок Honeypot у фінансовій установі – це рахунок, який виглядає точно так само, як справжній рахунок, за винятком,

звичайно, реальних грошей там немає. У будь-якому іншому відношенні його неможливо відрізнити від реального рахунку. Він має всі атрибути, які мав би справжній рахунок: ім’я, адреса, обліковий запис електронної пошти, інформація про бенефіціарів, історія рахунку, баланс, авуари тощо.

Під час входу в будь-який обліковий запис користувач зазвичай очікує, що зможе:

- змінити інформацію облікового запису (наприклад, ім'я, адресу, бенефіціарів тощо)
- купуйте або продавайте інструменти (наприклад, переводіть гроші з чеків на заощадження, купуйте або продавайте акції тощо).
- надсилайте гроші на раніше використовувані рахунки (наприклад, комунальні послуги, іпотека)
- надіслати гроші новому одержувачу

Зловмисник, який входить на рахунок honeypot, матиме доступ до всього спектру послуг, за винятком, звичайно, того, що банк фактично нікому не передаватиме гроші. Однак він буде робити вигляд, що він це зробив. Лише зловмисники потраплять в медовий горщик, а мета облікового запису - створити ілюзію реальності. Таким чином, банк зробить все можливе, щоб увічнити ілюзію, окрім того, щоб розлучитися з грошима.

Генерація рахунків Honeypot: для захисту від зловмисників, банку можуть знадобитися тисячі або навіть мільйони рахунків Honeypot. Тому важливо мати можливість створювати такі облікові записи за бажанням. Це насправді просто. Наше рішення полягає в тому, щоб скопіювати атрибути з пулу реальних рахунків, але ввести вигадані атрибути для імені, адреси, бенефіціарів тощо. Це гарантує, що honeypot містить дійсну історію рахунку та деталі транзакцій. Наприклад, зловмисник побачить реальну інформацію про оплату рахунків в Інтернеті разом із сумами та датами, але для вигаданого користувача.

Облікові записи створюються на вимогу під час першого входу, але інформація облікового запису зберігається через послідовні логіни.

1.2 Аналоги Honeypot

Технологія обману - це практика захисту кібербезпеки, яка має на меті обдурити зловмисників, розповсюдивши колекцію пасток і приманок по всій інфраструктурі системи, щоб імітувати справжні активи. Якщо зловмисник викликає приманку, то сервер реєструватиме та контролюватиме вектори атаки, які використовуються протягом усього часу залучення.

Базовий принцип, покладений в основу honeypots - це створення пасток для хакерів. На такому ж принципі були розроблені та покращені найперші рішення Deception. Але на даний час, сучасні DDP значно перевершують Honeypot, як за своїм функціоналом, так і по ефективності. Deception платформи включають в себе: пастки (англ., Decoys, traps), приманки (англ., Lures), додатки, дані, бази даних, Active Directory. Сучасні DDP можуть забезпечити широкі можливості для виявлення загроз, аналізу атак і автоматизації дій у відповідь [8].

Таким чином, Deception представляють собою техніки імітації IT-інфраструктури підприємства і введення в оману хакерів. У підсумку, такі платформи дозволяють зупиняти атаки до нанесення значного збитку активам компанії. Ханіпоти, звичайно ж, не мають такого широкого функціоналу і такого рівня автоматизації, тому їх застосування вимагає більшої кваліфікації від співробітників департаментів ІБ (рис. 1.7).

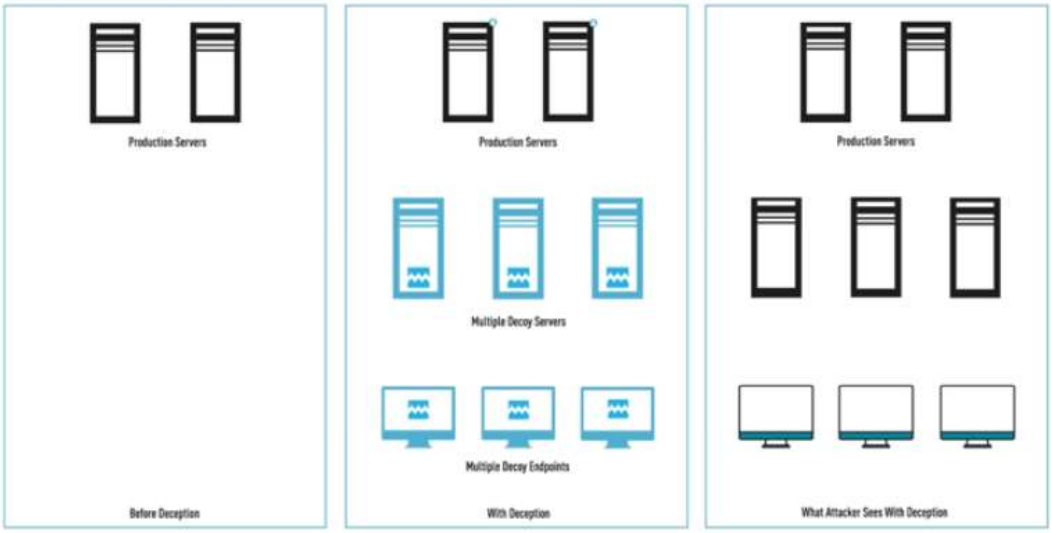


Рисунок 1.7 – Принцип роботи Distributed Deception Platform

Зловмисник може виявити помилкові бази даних з «конфіденційними документами», підроблені облікові дані нібито «привілейованих користувачів» - все це помилкові цілі, вони можуть зацікавити порушників, тим самим забираючи їх увагу від справжніх інформаційних активів компанії (рис. 1.8).

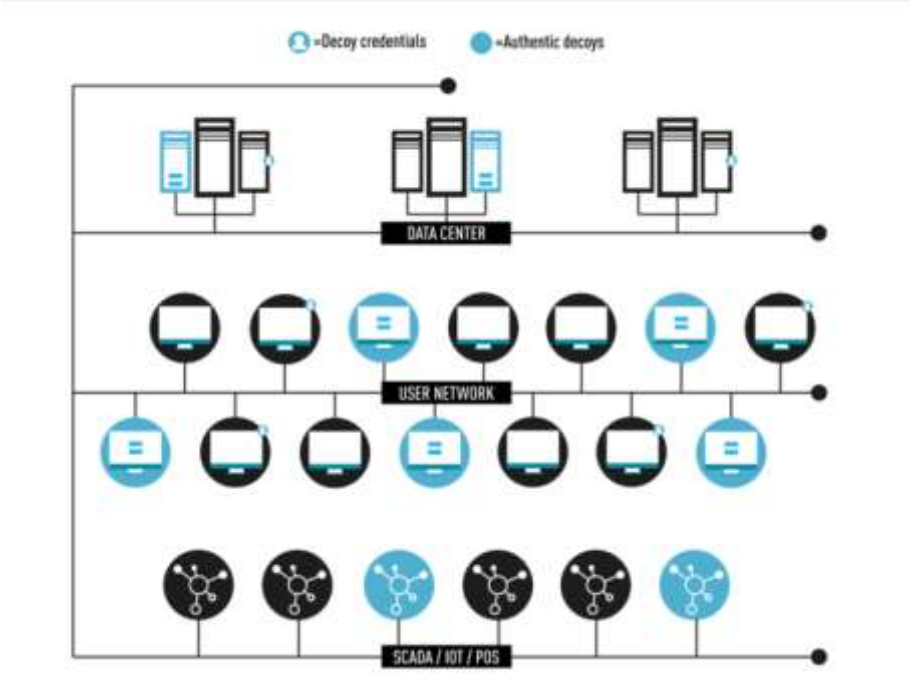


Рисунок 1.8 – Технологія імітація IT-інфракстури та дезінформацій зловмисників

DDP – це новинка на ринку продуктів ІБ, цим рішенням лише кілька років і поки що їх може дозволити собі лише корпоративний сектор. Але малий і середній бізнес скоро також зможе скористатися Deception, орендуючи DDP у спеціалізованих провайдерів, як послугу. Такий варіант навіть зручніше, тому що немає потреби у власних висококваліфікованих кадрах [8].

1.3 Системи моніторингу види та аналоги

Поняття моніторингу. На сьогодні поняття моніторинг (буквально означає відслідковування), використовуване як метод наукового дослідження, знаходить усе більш широке застосування (рис. 1.9).

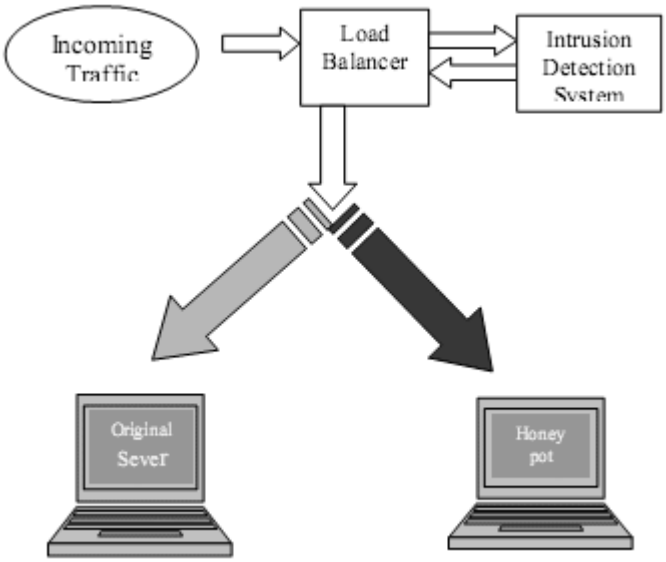


Рисунок 1.9 – Приклад роботи з використанням Honeypot і системи моніторингу

Багато функціональна по своїй сутності й змісту роль моніторингу породила ряд його визначень: комплекс спостережень і досліджень, станом деяких об'єктів з метою комплексної оцінки і підвищення ефективності функціонування [9].

Моніторинг прийнято розглядати в двох значеннях — теоретичному і практичному.

У теоретичному плані моніторинг — своєрідна філософія, концепція управління. Тут можна говорити про вихідні цілі, принципи моніторингу, особливості організаційних структур. Сюди варто віднести й моніторингові дослідження. Це сфера теоретичної діяльності, здійснювана ученими, спеціалістами, відповідними відділами, лабораторіями та ін.

У практичному значенні моніторинг — одна з зовнішніх функцій управління, різновид управлінської діяльності, що має свої цілі і задачі. Вона здійснюється багатьма суб'єктами і спрямована на множину об'єктів, тобто містить у собі розробку пропозицій щодо розвитку об'єкта в потрібному напрямку і висновки щодо ефективності заходів для управління об'єктом. Подібна діяльність здійснюється широко і цілеспрямовано, складається на практиці у своєрідний комплекс моніторингу, тобто складну специфічну систему управління, яку можна вивчати з різноманітних позицій: соціально-економічних, економічних, соціальних, соціально-демографічних, етнічних.

Сфери застосування моніторингу. Сфера використання моніторингу за останнє десятиліття надзвичайно розширилися. Вперше моніторинг був використаний у ґрунтознавстві, потім в екології й інших суміжних науках. В даний час він вивчається і використовується також у технічних, соціальних науках, в різноманітних сферах практичної діяльності. Є підстави стверджувати, що залишилося мало галузей діяльності, де тим чи іншим чином не використовувався б моніторинг [10].

Основні сфери, що виявляють інтерес до моніторингу, як засобу наукового дослідження – це екологія, біологія, соціологія, педагогіка, економіка, психологія, теорія управління. Основна сфера практичного застосування моніторингу – це управління, а точніше інформаційне обслуговування управління в різноманітних галузях діяльності.

У ряді сфер науково-практичної діяльності створюють можливість моніторингу тільки освоюється, як на теоретичному і практичному рівні.

Види та типи моніторингу користувача за використанням комп’ютера.

Контроль подій:

- натиснення клавіш на клавіатурі;
- натиснення клавіш миші;
- Logon та Logoff користувача;
- ім'я поточного користувача.

Скріншоти екрану:

- десктоп (desktop capturing);
- активне вікно (active windows capturing);
- розрізання скріншоту і склеювання в пам'яті;
- скріншот навколо місця кліків клавіш миші.

Email:

- вихідна пошта;
- вхідна пошта;
- двосторонній контроль пошти.

Час і дата:

- завантаження системи і ім'я поточного користувача;
- прикладних програм, що запускаються;
- перемикання між завданнями.

Тексти, що набирають:

- графічні вікна;
- консольні вікна.

Активність:

- файлова;
- системного реєстру.

Черга завдань:

- принтер.

Перехват певних файлів:

- по назві;
- по розширенню;
- по ключовому слову.

Віддалене адміністрування.

Відео інформація.

Аудіо інформація.

Тільки метод застосування моніторингових програмних продуктів дозволяє побачити грань між керування безпекою і порушенням безпеки.

Несанкціоноване застосування — встановлення моніторингових програмних продуктів відбувається без відома власника (адміністратора безпеки) автоматизованої системи або без відома власника конкретного персонального комп'ютера. Несанкціоновано вживані моніторингові програмні продукти називаються шпигунськими програмними продуктами. Несанкціоноване застосування, як правило, пов'язане з незаконною діяльністю (illegal activity) [11].

Як правило, несанкціоновано встановлені шпигунські програмні продукти мають можливість конфігурації і отримання «скомплектованого» виконуваного файлу, який при інсталяції не виводить ніяких повідомлень і не створює вікон на екрані; такі продукти також мають вбудовані засоби доставки і дистанційного встановлення з конфігуровано модуля на комп'ютер користувача, тобто процес інсталяції не потребує безпосереднього фізичного доступу до комп'ютера користувача і часто не вимагає наявності прав адміністратора системи;

Санкціоноване застосування — встановлення моніторингових програмних продуктів відбувається з відома власника (адміністратора безпеки) автоматизованої системи або з відома власника конкретного персонального комп'ютера. Моніторингові програмні продукти, що вживаються санкціоновано зазвичай вимагають або фізичного доступу до комп'ютера користувача, або

обов'язкової наявності прав адміністратора системи для конфігурації і інсталяції цих програм;

Відомі моніторингові програмні продукти. До даної категорії відносяться моніторингові програмні продукти, сигнатура яких (на будь-якій підставі) включена до сигнатурних баз основних відомих фірм-виробників анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів.

Невідомі моніторингові програмні продукти. До даної категорії відносяться моніторингові програмні продукти, сигнатура яких не включена до сигнатурних баз основних відомих фірм-виробників анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів і, ймовірно, ніколи не буде в них включена з різних причин, а саме:

– моніторингові програмні продукти (модулі), що розробляються під егідою різних урядових організацій;

– шпигунські програмні продукти, які розроблені в обмеженій кількості (часто тільки в одній або декількох копіях) для вирішення конкретного завдання, пов'язаного з викраданням критичної інформації з комп'ютера користувача (наприклад, програмні продукти, що вживаються зловмисниками-професіоналами).

Дані програмні продукти можуть бути трохи видозміненими відкритими початковими кодами моніторингових програмних продуктів, що взяті з мережі Інтернет та скомпільовані самим зловмисником, що дозволяє змінити сигнатуру моніторингового програмного продукту;

– комерційні моніторингові програмні продукти, які дуже рідко вносяться до сигнатурних баз відомих фірм-виробників анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів. Це призводить до того, що публікація зловмисниками в мережі Інтернет повнофункціональної версії даного комерційного моніторингового програмного продукту може перетворити останній на шпигунський програмний продукт, який не виявляється

анти-шпигунськими програмними продуктами і/або антивірусними програмними продуктами;

– шпигунські програмні продукти, що включаються до складу програм-вірусів. До моменту внесення сигнатурних даних до вірусної бази ці шпигунські програмні продукти є невідомими.

До базового захисту ІТС підприємства можна віднести: 1. Firewall (укр. міжмережевий екран) – це програма або обладнання, яке перешкоджає зловмисникам і деяким типам шкідливих програм отримувати доступ до комп'ютера по мережі або через Інтернет [12]. Для цього Firewall перевіряє дані, що надходять з Інтернету або по мережі, і блокує їх або дозволяє передачу на комп'ютер (рис. 1.10).

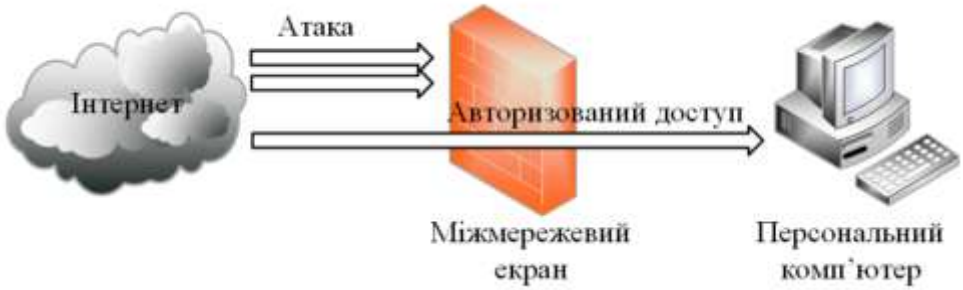


Рисунок 1.10 – Схема роботи Firewall.

VPN (англ. Virtual Private Network, укр. віртуальна приватна мережа). Віртуальна приватна мережа представляє собою підключення типу «точка-точка» (логічне з'єднання), яка працює поверх приватної або публічної мережі [13]. VPN-підключення типу «мережа-мережа» (логічне з'єднання) дозволяють організаціям встановлювати маршрутизовані підключення між окремими офісами (або між іншими організаціями) по публічній мережі, при цьому забезпечуючи захищеність зв'язку (рис. 1.11).

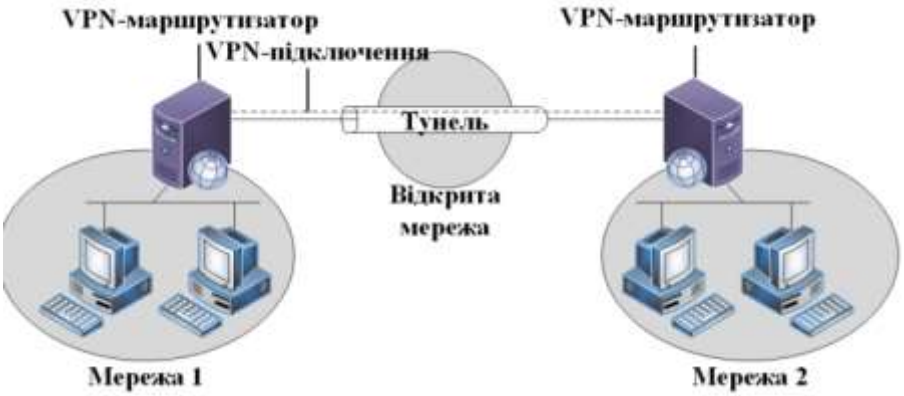


Рисунок 1.11 – Схема роботи VPN.

3.IDS/IPS (англ. Intrusion Detection System /Intrusion Prevention System, укр. Система виявлення вторгнення (СВВ)/Система запобігання вторгнення (СЗВ)). СВВ – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему (мережу), або несанкціонованого управління такою системою. СЗВ – програмна або апаратна система забезпечення безпеки, яка активно блокує вторгнення у разі їх виявлення. Архітектура СВВ (рис. 1.12) і СЗВ (рис. 1.13).

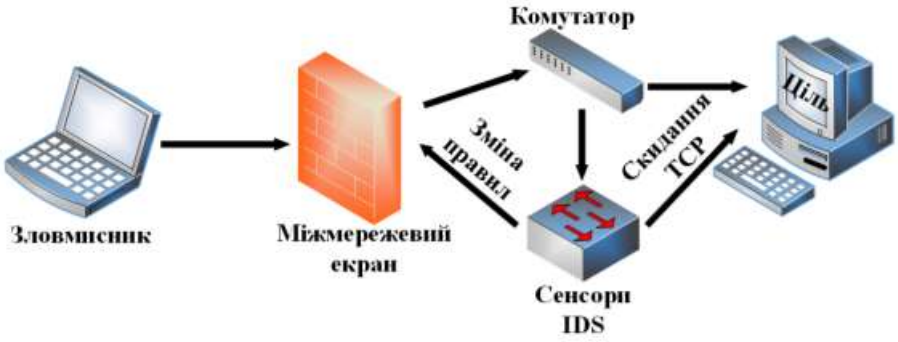


Рисунок 1.12 – Схема роботи СВВ.

Рисунок 1.13 – Схема роботи СЗВ.

4. Антивірусний захист – програмне забезпечення, яке здатне знаходити, «лікувати», блокувати, а також повністю видаляти віруси з системи. Антивірусний захист здатний моментально попереджати про те, що на тій чи іншій веб-сторінці є вірус і ваша система може бути пошкодженою. Це дуже зручно, так як сама програма в цей же час прийме всі необхідні заходи. На даний момент існують багато різних програм антивірусного захисту, які відрізняються за: ціною, швидкістю роботи, якістю антивірусних баз та іншими параметрами. 5. Білі списки – перелік певних програм та служб, які може використовувати користувач. Контролює білі списки – адміністратор. Білі списки можна створити, як за допомогою вбудованих засобів операційної системи, так і за допомогою стороннього програмного забезпечення. 6. Фільтрація спаму – процедура, яка перевіряє вхідну кореспонденцію (E-mail) за встановленими налаштуваннями фільтрів і забезпечую виявлення небажаної розсилки, яка може містити в собі: рекламні пропозиції, «листи щастя», комп'ютерні віруси або опинитися спробою фішингу. До основних способів фільтрації спаму відносяться: · Спеціалізовані постачальники сервісів фільтрації спаму; · Програмне забезпечення для фільтрації спаму на власних поштових серверах. 7. Підтримка програмного забезпечення (ПЗ) в актуальному стані. Своєчасне оновлення ПЗ це є усуненням вразливостей виявлених у програмному продукті. Підтримка системи, ПЗ в актуальному розробником стані – означає роботу в більш безпечному середовищі. В більшості систем передбачений механізм повного автоматичного оновлення. 8. Фізична та технічна безпека корпоративної мережі. Маючи фізичний доступ до мережевого пристрою зловмисник, в більшості випадків,

легко отримає несанкціонований доступ до мережі підприємства. Забезпечення фізичної та технічної безпеки корпоративної мережі унеможливлює фізичний доступ до її складових [13]. Необхідно звернути увагу на те, що утримувати захист корпоративної мережі на високому рівні досить важко. Ви повинні бути впевнені, що компанія не залежить всього лише від одного-двох рубежів захисту. Завжди прагніть стежити за актуальною інформацією і свіжими рішеннями на ринку інформаційної безпеки.

Системи виявлення вторгнень (СВВ) все частіше стають необхідним доповненням інфраструктури мережевої безпеки. СВВ служать механізмами моніторингу та спостереження підозрілої активності [14]. Вони можуть виявити атакуючих, які змогли обійти Firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить подальші кроки щодо запобігання атаки. Технології виявлення вторгнень не роблять систему абсолютно безпечною. Як правило, СВВ мають наступну структуру (рис. 1.14).

Рисунок 1.14 – Структура СВВ

Сенсорна підсистема – відповідає за збір інформації, пов’язану з безпекою мережі. У сховищі, зберігається інформація, що надходить від сенсорів й аналізатору.

Аналізатор – виявляє підозрілий трафік і атаки, ґрунтуючись на даних від сенсорів.

Консоль управління, дозволяє конфігурувати СВВ [14].

За характером відповідної реакції:

пасивні – системи виявлення, в яких після виявлення та розпізнавання підозрілого трафіку, СВВ тільки повідомляє користувача або адміністратора про загрозу; ·

активні – системи запобігання, що протистоять вторгненням, шляхом скидання з'єднання або зміна правил Firewall з метою блокування підозрілого трафіку; гібридні, що здійснюють виявлення та протистоять вторгненням в автоматичному режимі.

На основі проаналізованих інформаційних джерел про сучасні систем виявлення вторгнень є необхідно позбутися недоліків з допомогою покращення існуючих методів.

Дане порівняння дозволяє виділити недоліки існуючих методі та систем побудованих на цих методах і на основі недоліках покращенти існуючі системи виялення вторгнень і розгядаються різні види моніторингу.

2 СТВОРЕННЯ ТА РОЗРОБКА АЛГОРИТМІВ ТА МЕТОДІВ

2.1 Розробка загальної схеми роботи

Для початку розроблено загальну схему роботи програми. Яка включає в себе окремі компоненти системи. Блок схема показана на рисунку 2.1.

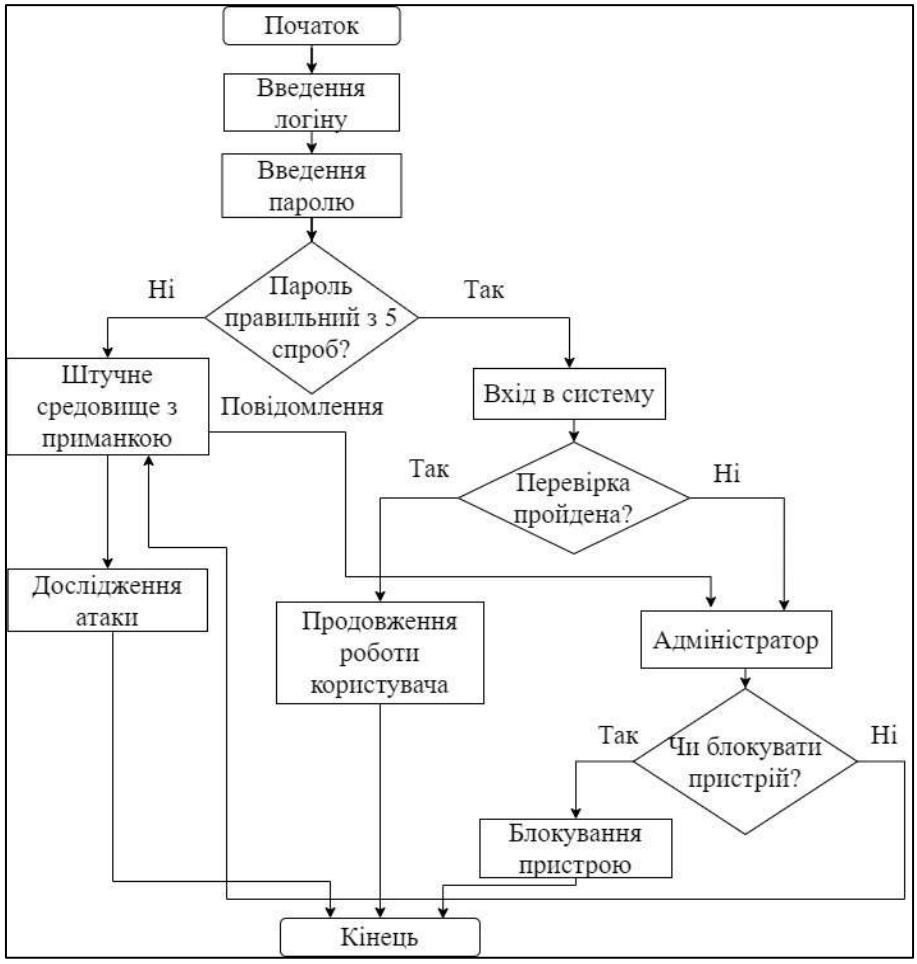


Рисунок 2.1 – Блок-схема виявлення атака з використанням Honeypot.

Дана схема складається з 3 основних частин такі як введення даних, аналіз, повідомлення. Було продумані сценарії можливих події такі як проникнення в прямою атакою, проникнення в внутрішню мережу та захід користувача.

Метод виявлення атак з використанням Honeypot

1. Ведення логіну та паролю
2. Перевірка на правильність ведення паролю

3. Якщо було більше 5 спроб невірних вводу то перехід у штучне середовище

4. Якщо пароль вірний перехід внутрішньо середовище.

5. Перевірка користувача на предмет незафіксованих дії.

6. Якщо були виконанні незафіксовані дії буде відправлено повідомлення адміністратору.

7. Якщо адміністратор на протязі 3 хвилин не прийме рішення автоматично блокується комп’ютер.

Даний метод можливість оперативно виявити зловмисника, а також дає змогу запобігти втраті даних.

2.2 Розробка входу в систему та розподілення

Першим кроком було вибрано створення розподілення між користувачами та зловмисниками для цього було вирішено створити окрему базу даних а також метод входу в систему.

Авторизація — керування рівнями та засобами доступу до певного захищеного ресурсу, як у фізичному розумінні (доступ до кімнати готелю за карткою), так і в галузі цифрових технологій (наприклад, автоматизована система контролю доступу) та ресурсів системи залежно від ідентифікатора і пароля користувача або надання певних повноважень (особі, програмі) на виконання деяких дій у системі обробки даних.

Для входу в систему буде розроблено алгоритм входу та розподілення. Для початку буде необхідно ввести дані користувача логін та пароль (рис. 2.2).

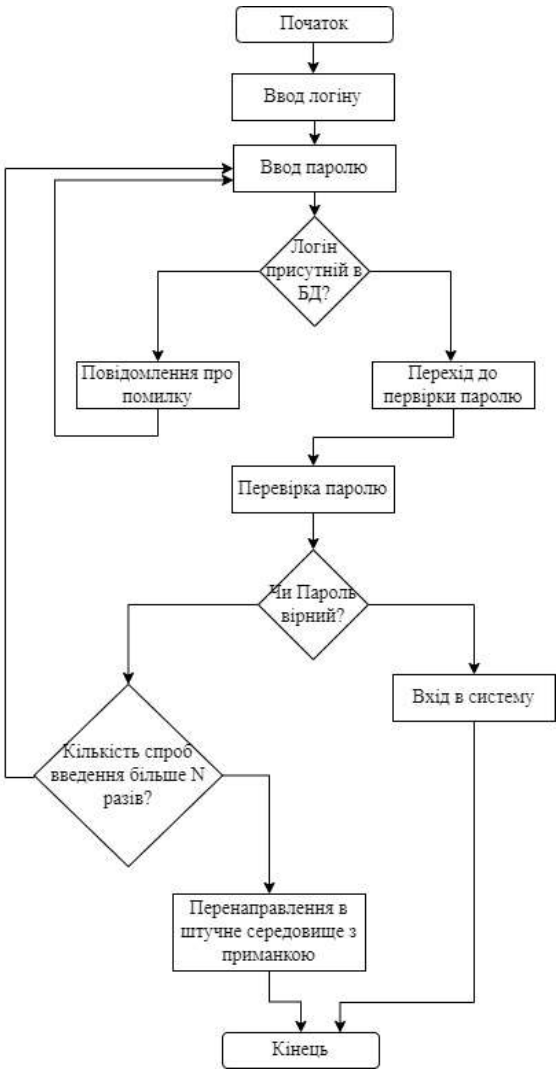


Рисунок 2.2 – Блок-схема вводу даних та розподілення запит входу.

Для зберігання даних користувачів буде використовуватися база даних SQl Server. Microsoft SQL Server - система управління реляційними базами даних (СУРБД), розроблена корпорацією Microsoft. Основну мову запитів, що використовується - Transact-SQL, створений спільно Microsoft і Sybase. Transact-SQL є реалізацією стандарту ANSI/ISO із структурованої мови запитів (SQL) з розширеннями. Використовується до роботи з базами даних розміром від персональних до великих баз даних масштабу підприємства; конкурує з іншими система управління базами даних у цьому сегменті ринку.

2.3 Розробка повідомлення адміністратору

Наступним кроком є створення повідомлень адміністратору. Даний частина системи буде відповідати за комунікацію між користувачами та адміністратору і повідомляти про порушення або вхід в штучне середовище (рис. 2.3).

Рисунок 2.3 – Блок схема повідомлень з штучного середовища

Спочатку почнеться формування даних яке буде включати IP-адрес зловмисника, пристрій, по можливості дані про ip-адрес. В формуванні повідомлення буде які дії виконав зловмисник. Після відправки повідомлення буде продовжуватися запис в журнал дії зловмисника.

Для внутрішніх мережі буде використовуватися інший алгоритм повідомлень (рис. 2.4).

Рисунок 2.4 – Блок схема повідомлень внутрішній мережі

Під несанкціонованими діями користувача є використання несанкціонованого ПО, відкривання портів, спроби отримання прав адміністратора. Наступний крок це активація файлу який не має бути відкритим бо має певні обмеження або скритий налаштуваннями. При записі буде використовуватися журнал подій. Після відправки повідомлення адміністратору якщо користувач буде продовжувати то почнеться нове формування повідомлення.

Більшість комп’ютерних мереж – це різноманітна колекція комп’ютерів і комп’ютерних систем, особливо в академічних та професійних умовах. Часто існує широкий спектр операційних систем для робочих станцій і серверів, і кожна з них має різні мережеві порти, відкриті для виконання своїх індивідуальних завдань. Багато мереж також повинні задовольняти потребу окремих людей брати свою роботу додому або підключатися віддалено із зовнішнього середовища. Потім вони підключаються до мережі, коли прийдуть на роботу наступного дня. Ці дії змінюють структуру мережі, оскільки підключені пристрої розвиваються та змінюються з часом, деякі передбачувано,

а інші менше. Ефективна та автентична емуляція цих змін вимагає, щоб система honeynet динамічно (за допомогою використання в реальному часі або періодичного виконання оновлення).

2.4 Розробка алгоритму робити штучного середовища

Наступним кроком буде мінімальна розробка штучного середовища для дослідження атак. Для цього спочатку буде збір інформацій а після повідомлення адміністратору про вхід в середовище (рис. 2.5).

Рисунок 2.5 –Блок схема роботи штучного середовища

Моніторинг зловмисника буде проводитися в мережі та в середовищі. Для знаходження слабостей захисту буде скопійовано частина захист. Також буде проводитися постійний запис дії.

Honeypot доволі часто можуть виявити як на сервері так і на персональному комп’ютері після чого зловмисник вже не підключається до такого порту або машини і спрямовує атаки на інші частини системи захисту. Для прикладу було вибрано статичні Honeypots які зазвичай відкривають

послуги сервера та чекають на атаку зловмисник відправляє певні повідомлення та по отриманим даним розуміє що це Honeypots.

Honeypots, незалежно від того, чи є вони високою чи низькою взаємодією, дозволяють адміністраторам виявляти аномалії, які інакше могли б залишитися непоміченими. Оскільки honeypots не мають виробничої цінності, будь-яка взаємодія всередині машини може бути або скануванням перед атакою, або потенційною атакою. Це дозволяє системному адміністратору націлювати й аналізувати журнали, створені системою honeypot, без необхідності визначати, який трафік є підозрілим, а який законним, як це було б під час аналізу журналів із виробничих систем.

На рисунку 2.6 показано роботу штучного середовища для системи виявлення атак для моніторингу є можливість використання різних програм які присутні на ринку. В додаткові функцій можна віднести:

- додавання вірусного ПЗ;
- штучних файлів;
- штучний захист;
- скопійований захист;
- моніторинг трафіку;
- створення під системи honeypot.

Ряд даних функцій дасть можливість додатково вийти на зловмисника також функцій моделювання захисту дасть можливість знайти слабкості а бо помилки нульового дня.

Рисунок 2.6 – Блок-схема роботи штучного середовища.

Також є можливість розшити можливості Honeypot якщо створити зв’язок між Honeypot та внутрішньою системою підприємства та дати можливість розкрити даний зв’язок зовні що спровокує зловмисників шукати слабкості в Honeypot для можливості зламу, що в свою чергу дасть можливість дослідити методи та атаки зловмисників.

2.5 Розробка блокування пристрою

Даний компонент системи буде відповідати за відключення зловмисника від пристрою а також забезпечити не отримання важливої інформацій зловмисником. Для було запропоновано пару методів:

1. Блокування особистого запису.
2. Блокування робочого столу.

3. Блокування контролерів мишки та клавіатури.

Також для цього була можливість використати додаткові програми такі як Program Blocker, AskAdmin, AppLocker але дані програми мають функціонал тільки блокування окремих додатків (рис. 2.7).

Рисунок 2.7 – Блок схема блокування пристрою

Після виходу усіх облікового запису буде тільки адміністратора можливість зайти в пристрій та вносити зміни. Також це може дати можливість викрити зловмисника на робочому місці користувача.

2.6 Розробка компонентів Honeypot

Першим Honeypot це файли які будуть скриті системою або в спеціальні папці. Коли даний файл буде розкрито або відкрито це буде сигналом администратору що даний користувач був зламаний. На рисунку 2.8 показана робота даного файлу.

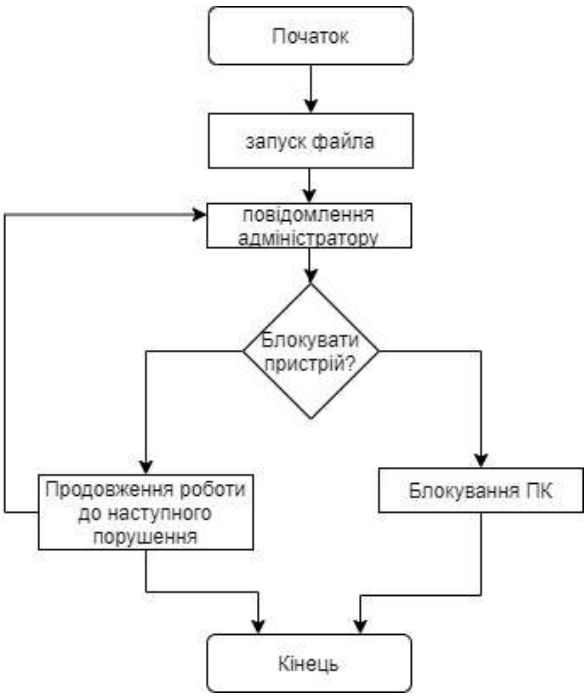


Рисунок 2.8 – Блок схема роботи файла

Наступний файл буде знаходитися в штучному середовищі для зловмисника та створений для можливості вийти на зловмисника. Для цього буде використовується IP-логер. На ринку показаний принцип роботи даного файлу (рис. 2.9).

Рисунок 2.9 – Блок-схема роботи файлу з Honeypot

IP Logger – зручний сервіс скорочення посилань для збору статистики про відвідуваність вашого блогу, форуму чи сайту. За допомогою наших сервісів Ви

можете дізнатися вашу IP адресу, визначити геолокацію IP адреси, а також визначити точне розташування будь-якого пристрою. Найпростіший у використанні сервіс IP Logger надає найбільш розширену інформацію щодо кожного переходу. Вам доступно кілька способів збору докладної аналітики: короткі посилання, невидимий піксель, унікальний сервіс геологгер.

Найбільший недолік Honeypot – вузька область бачення. Honeypot здійснюють моніторинг діяльності, яка спрямована проти них. Якщо дії атакуючого направлені на різні підсистеми мережі, то Honeypot не виявлятиме цю діяльність, якщо вона не спрямована безпосередньо на Honeypot. Якщо зловмисник ідентифікував Honeypot, він може спробувати обійти його і проникнути в організацію. Таким чином, дуже обмежена область бачення Honeypot може виключити події, що трапляються поза цією областю.

Даний метод дозволяє зменшити недоліки існуючих методів та систем побудованих на цих методах. Для перевірки роботи методу перейдемо до створення програмного засобу систему виявлення вторгнень з допомогою Honeypot.

3 ТЕСТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ АТАК

3.1 Обґрунтування вибору засобів для реалізації

Програмні засоби даного спрямування можуть написані будь якою об’єктно орієнтованою мовою: C++, Java, C#, Pyton, Delfi. Для реалізацій даної магістерської роботи було вибрано роботи мову C# оскільки вона має такі переваги, як:

- портативність;
- особливі типи даних;
- наявність шаблонів;
- безпечність
- об’єктно орієнтованість.

C# – це об'єктно-орієнтована мова програмування з безпечною системою типізації на платформі .NET. Розроблена такими людьми як: Андерсом Гейлсбергом, Скотом Вілтамутом та Пітером Гольде під компанією Microsoft Research (при фірмі Microsoft).

Синтаксис C# близький до C++ і Java. Мова має строгу статичну типізацію, підтримує поліморфізм, перевантаження операторів, вказівники на функції-члени класів, атрибути, події, властивості, винятки, коментарі у форматі XML. Перейнявши багато що від своїх попередників – мов C++, Delphi, Модула і Smalltalk – C#, спираючись на практику їхнього використання, виключає деякі моделі, що зарекомендували себе як проблематичні при розробці програмних систем, наприклад множинне спадкування класів (на відміну від C++).

Портативність. C# розроблялась як мова програмування прикладного рівня для CLR і тому вона залежить, перш за все, від можливостей самої CLR. Це стосується, перш за все, системи типів C#. Присутність або відсутність тих або інших виразних особливостей мови диктується тим, чи може конкретна мовна особливість бути трансльована у відповідні конструкції CLR. Так, з розвитком CLR від версії 1.1 до 2.0 значно збагатився і сам C#; подібної взаємодії слід

чекати і надалі. (Проте ця закономірність буде порушена з виходом C# 3.0, що є розширеннями мови, що не спираються на розширення платформи .NET.) CLR надає C#, як і всім іншим .NET-орієнтованим мовам, багато можливостей, яких позбавлені «класичні» мови програмування. Наприклад, збірка сміття не реалізована в самому C#, а проводиться CLR для програм, написаних на C# точно так, як і це робиться для програм на VB.NET, J# тощо.

C# підтримує строго типізовані неявні оголошення змінних з ключовим словом var і неявно типізовані масиви з ключовим словом new , за яким слідує ініціалізатор колекції.

C# безпечніший в порівнянні з C++. Єдиними неявними перетвореннями за замовчуванням є ті, які вважаються безпечними, наприклад, розширення цілих чисел. Це застосовується під час компіляції, під час JIT і, в деяких випадках, під час виконання. Не відбувається неявних перетворень між булевими і цілими числами, а також між членами перерахування і цілими числами (крім літерала 0, який може бути неявно перетворений в будь-який нумерований тип). Будь-яке призначене для користувача перетворення повинно бути явно позначене як явне або неявне, на відміну від конструкторів копіювання C++ і операторів перетворення, які за умовчанням є неявними.

C# має явну підтримку коваріантної та контраваріантності в родових типах, на відміну від C++, яка має певний рівень підтримки контраваріантності просто через семантику типів, що повертаються, на віртуальні методи.

Динамічний тип dynamic допускає прив'язку методу під час виконання, що дозволяє використовувати JavaScript-подібні виклики методів і склад часу виконання.

C# надає властивості як синтаксичного цикл для загального шаблону, в якому пара методів, accessor (getter) і mutator (setter) інкапсулює операції по одному атрибуту класу. Не потрібно писати надлишкові сигнатури методів для реалізацій гетеро / сетера і до цієї властивості можна отримати доступ, використовуючи синтаксис атрибутів, а не більш докладні виклики методів.

3.2 Розробка засобу та головний функцій

Для початку було розроблено основне вікно входу в програму для цього було створено окремі поля входу такі як Login та Password. Що показано на рисунку 3.1.

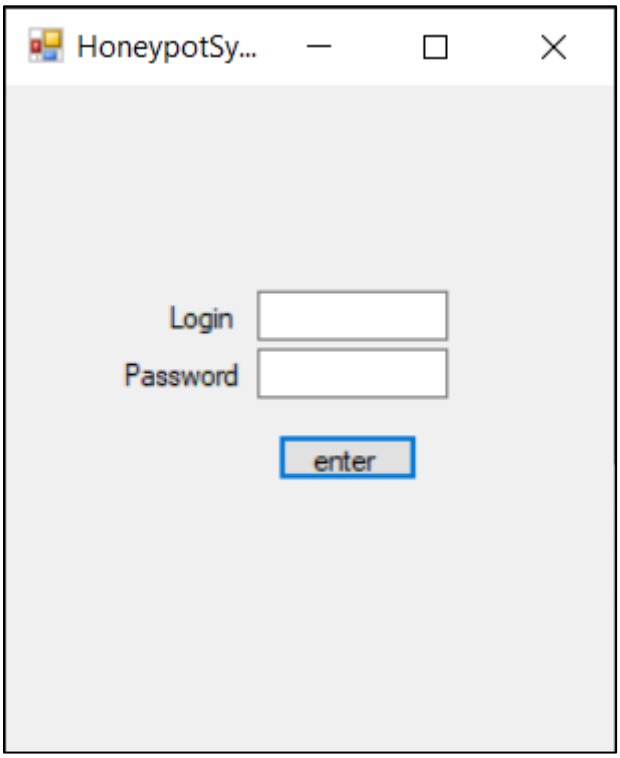


Рисунок 3.1 –Головний інтерфейс

Після чого було додано окремі таблиці для користувачів та стандарних паролів які будуть використовуватися для перенаправлення зловмисників (рис. 3.2).

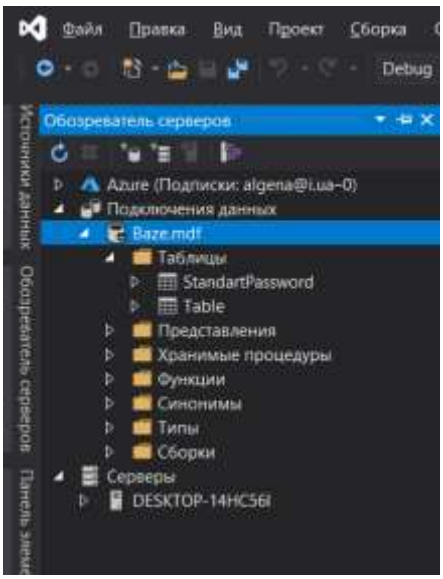


Рисунок 3.2 – База даних

Для цього було використано SQL базу даних, тому що дана база є практичною, а також гнучкою для використання запитів (рис. 3.3).

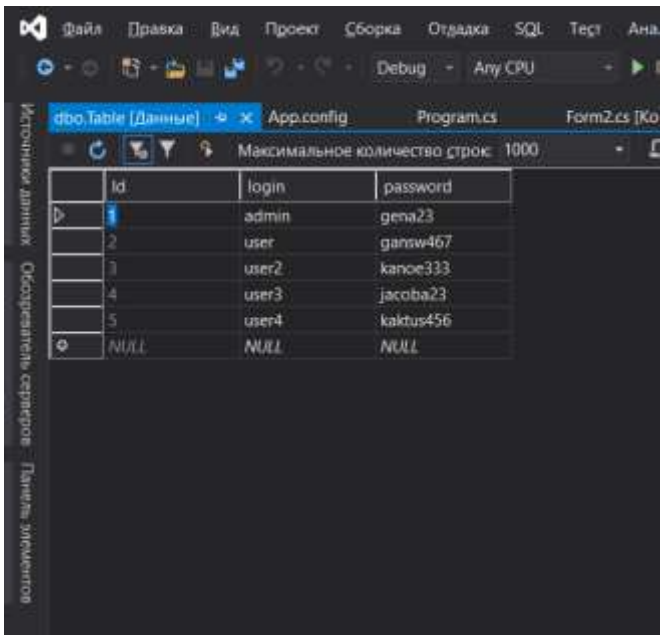


Рисунок 3.3 – Дані таблиці користувачів

Далі було заповнено таблицю користувачів а після створено окрема таблиця для стандарних паролів. При вводі яких виводиться повідомлення (рис. 3.4).

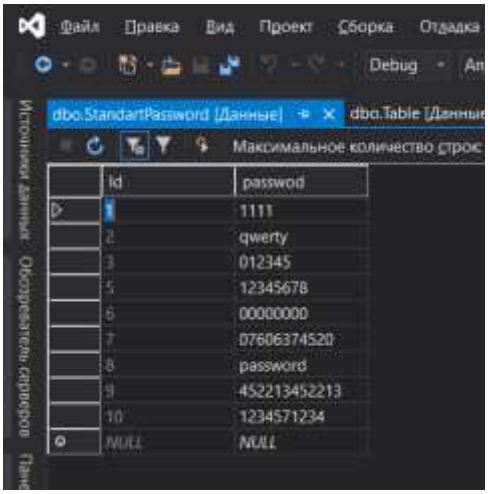


Рисунок 3.4 –Дані з стандартними паролями

Для цього було використано локальну мережі яка було створено при використаня протоколу TCP.

Далі було створено інтерфейс адміністратора. Для роботи програми та обратного зв’язку з користувачем (рис. 3.5).

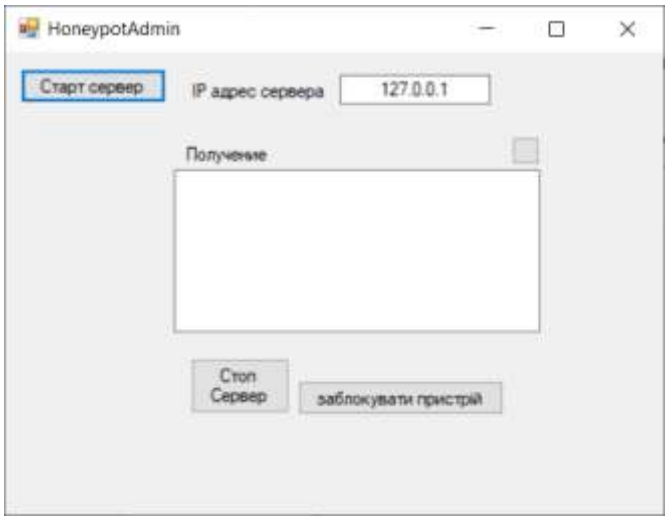


Рисунок 3.5 – Інтерфейс адміністратора.

Даний інтерфейс використовувався для приймання повідомлень від користувача.

Наступним кроком було розроблено вхід з правильним паролем та з стандарним при не правильному паролі не має входу до локальной мережі.

Та розролена перевірка код який показаний нижче.

```
 string loginuser = textBoxLogin.Text;
            string legpassword = textBoxPass.Text;
            SqlDataAdapter adapter = new SqlDataAdapter();
            DataTable table12 = new DataTable();
            SqlCommand command = new SqlCommand("SELECT * FROM
Table WHERE login=@uL AND password=@up", sqlConnection);
            command.Parameters.Add("@ul",
SqlDbType.NVarChar).Value = loginuser;
            command.Parameters.Add("@up", SqlDbType.NChar).Value =
legpassword;
            adapter.SelectCommand = command;
            adapter.Fill(table12);
            if (table12.Rows.Count > 0)
            {
                MessageBox.Show("log right");
            }
            else
            {
                meddaga = "Brute-forse";
                    Thread t = new Thread(_tcpmodule.SendData);
                    t.Start();           }
```

Після перевірки було розроблено та додано компоненти локальної мережі на основі TCP з’єднання. Було додано кнопка блокування пристрою, яка вимикала пристрій користувача. Вигляд форми від адміністратора показано на рисунку 3.6.

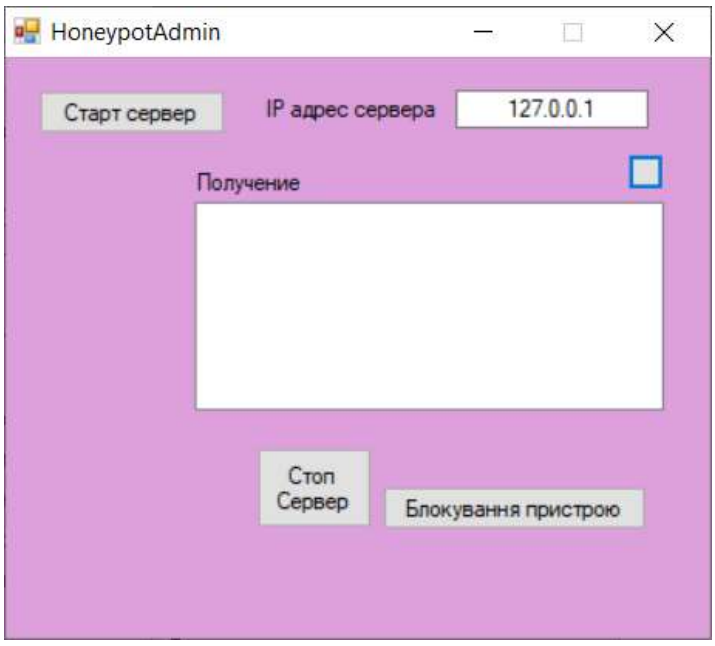


Рисунок 3.6 – Інтерфейс адміністратора в активному стані.

Наступним кроком було налаштовані повідомлення про авторизацію або використання стандартних паролей. Для цього необхідно підключення до серверу адміністора в майбутньому даний метод можна буде застосовувати на серверах. Активне вікно користувача показано на рисунку 3.7.

Рисунок 3.7 – Інтерфейс користувача в активному стані.

Наступним було розроблено кнопка блокуання користувача яка при натискані вимикала пристрій код показний нижче.

```
ManagementBaseObject mboShutdown = null;
                ManagementClass mcWin32 = new
ManagementClass("Win32_OperatingSystem");
                mcWin32.Get();
                mcWin32.Scope.Options.EnablePrivileges = true;
                ManagementBaseObject mboShutdownParams =
 mcWin32.GetMethodParameters("Win32Shutdown");
                mboShutdownParams["Flags"] = "1";
                foreach (ManagementObject manObj in
mcWin32.GetInstances())
{
                    mboShutdown =
manObj.InvokeMethod("Win32Shutdown",
mboShutdownParams, null);
                }
```

При п’яти неправильних введень або використання стандарних паролів іде повідомення Адміністратору (рис. 3.8).

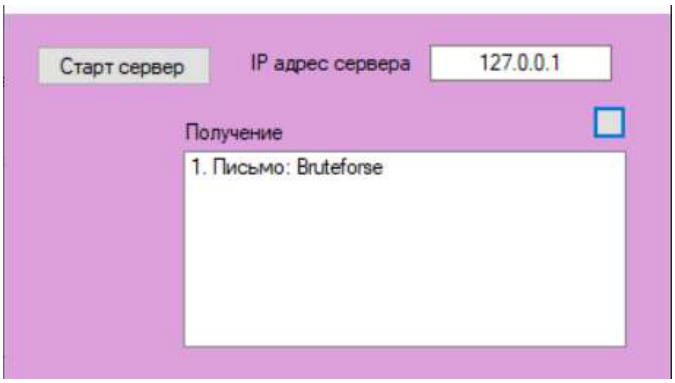


Рисунок 3.8 – Повідомлення про проведення атаки.

Для того щоб повідомлення не закривали весь listbox було вирішено створити окрему кнопку яка буде очишювати даний listbox.

3.3Тестування систмстеми виялення атак.

Для проведення тестування буде використовуватися Radmin VPN дана програма емулює локальну мережу яка необхідна для роботи програми(рис. 3.9).

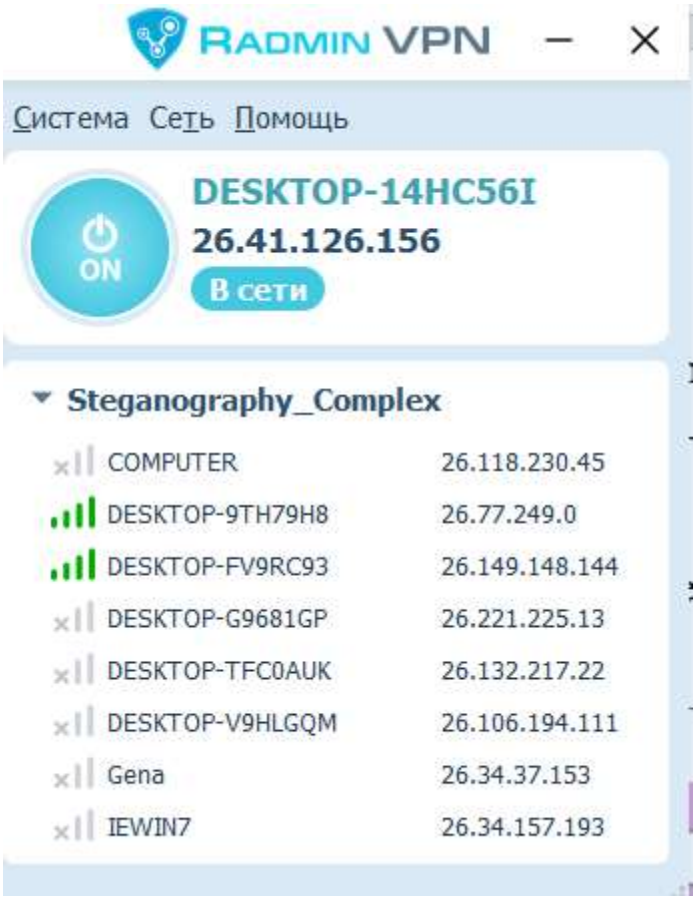


Рисунок 3.8 – Вигляд програми емуляці локальной мережі.

Першим кроком буде запуск HoneypotAdmin для запуску сервера і можливості підключення клієнта(рис. 3.9). Також при використані даного засобу необхідно вимкнути брандмауер на двох пристоях.

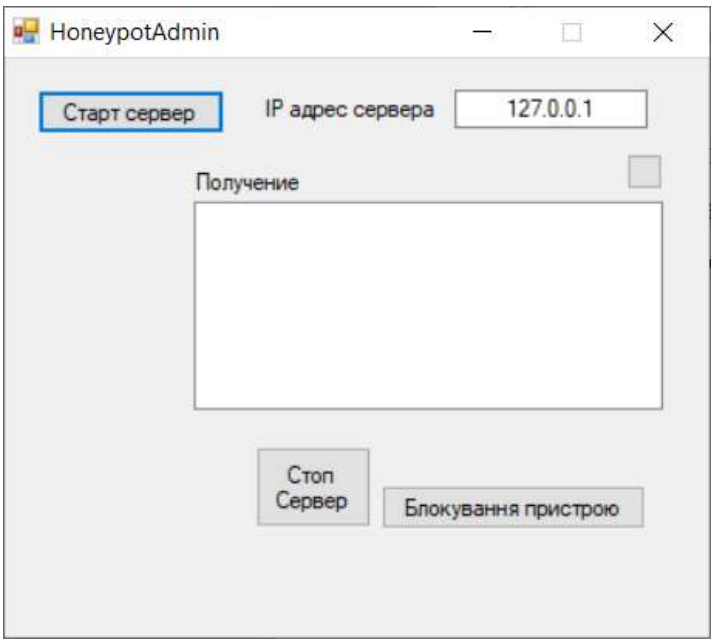


Рисунок 3.9 – Вигдяд інтерфейсу адміністратора.

Наступним кроком буде запис в “IP адрес сервера” адресу 26.41.126.156 яка буде відповідати за локальну мережу. Після чого необхідно запустити сервер для чого необхідно натиснути кнопку “Старт сервер” на рисунку 3.10.

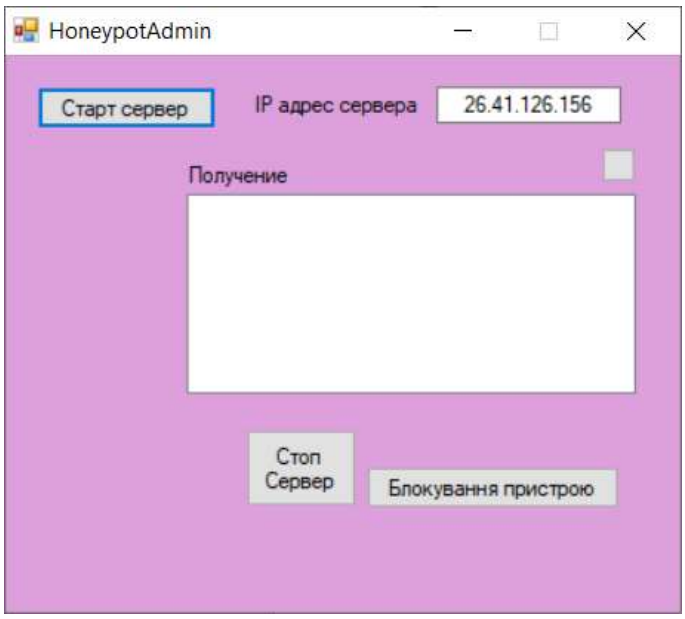


Рисунок 3.10 – Вигдяд інтерфейсу адміністратора після запуску сервера.

Після чого необхідно запусти HoneypotSystem для підключення до HoneypotAdmin і проходження авторизації (рис. 3.11).

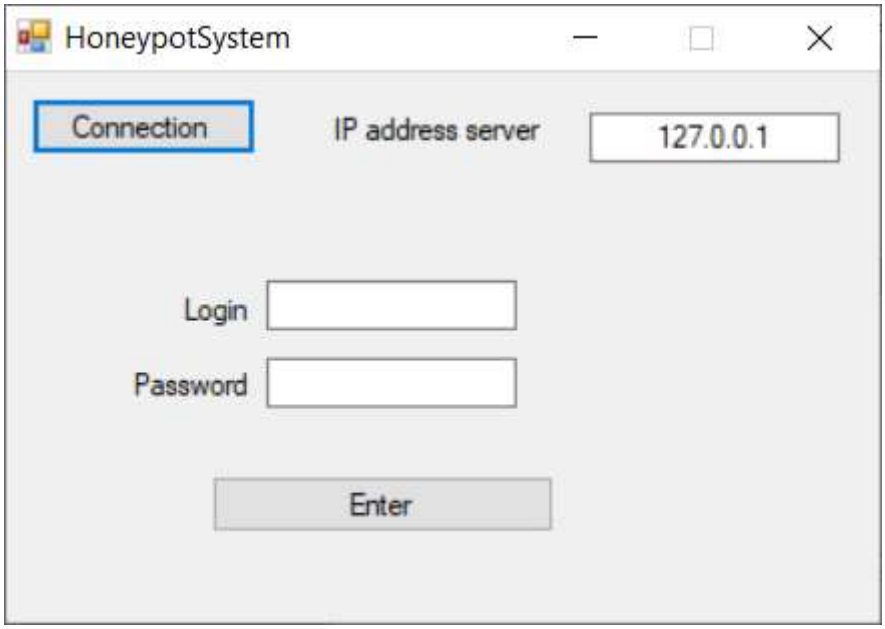


Рисунок 3.11 – Вигдяд інтерфейсу користуача.

Далі необхідно продублювати “IP address server” з HoneypotAdmin або з додатку RadminVPN. Після чого натиснути кнопку “Connection”(рис. 3.12).

Рисунок 3.11 – Вигдяд інтерфейсу користуача після під’єднення до сервера.

Далі в залежності від введених даних будуть різні операцій. Для початку буде продемонстровано перший випадок з атакою на зовнішню систему яяк показано на рисунку 3.12.

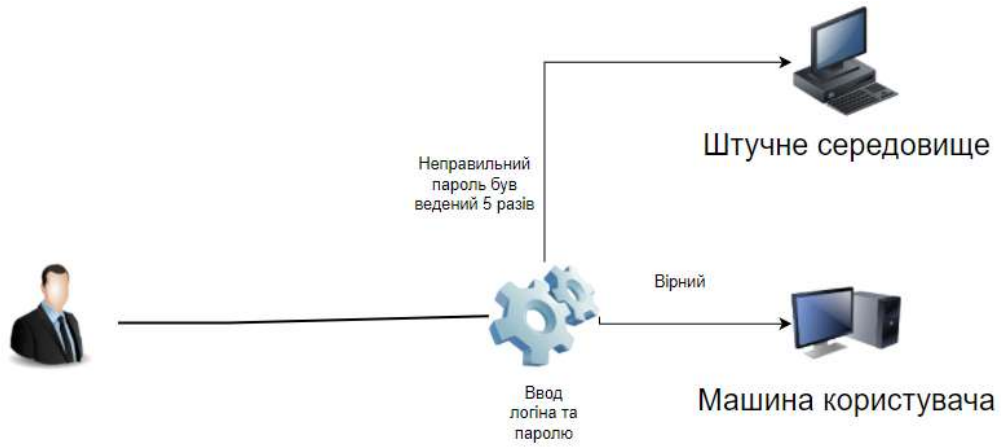


Рисунок 3.12 - Принцип робити з зловмисником.

Для початку будуть ведені стандартні паролі для user1. Та продемонстрована реакція на сервері. Для демонстрацій різних паролів дані поля не будуть скриті точками що продемонстровано на рисунках 3.13 – 3.14.

Рисунок 3.13 - Дані з стандартм паролем.

Рисунок 3.14 - Дані з стандартм паролем для іншого користувача.

Після вводу стандарних паролів дане повідомлення надіїшло адміністратору. Про атаку грубой сили яка було виконана на користувача(рис. 3.15).

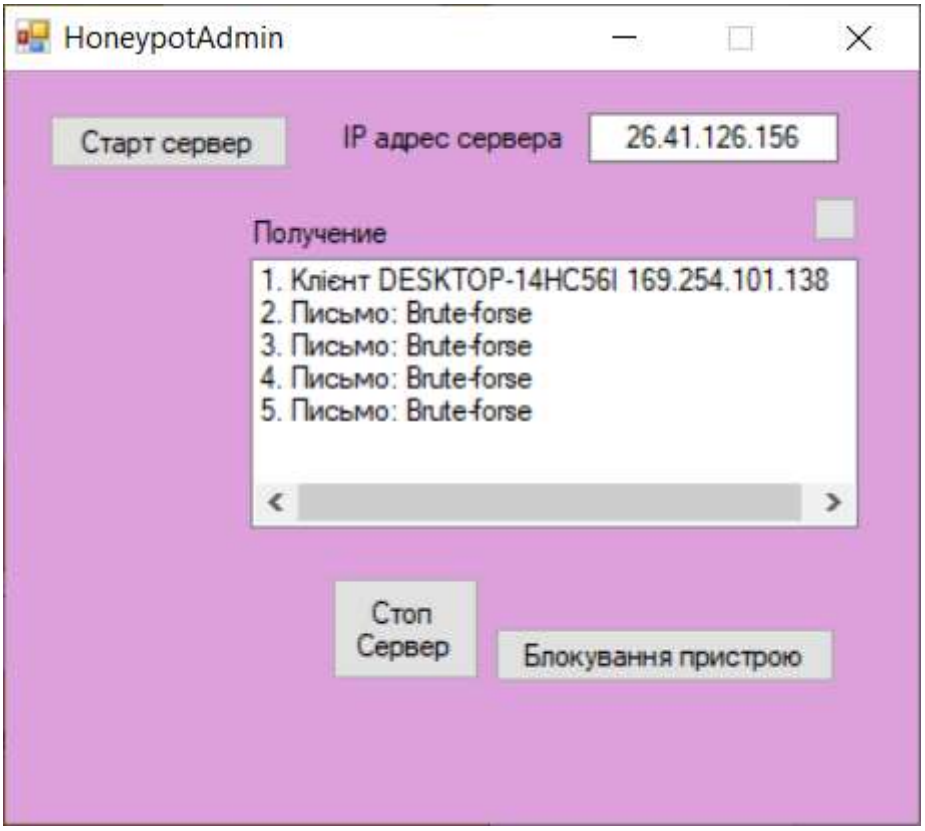


Рисунок 3.15 - Повідомлення про атаки.

Далі відкрилася папка Artificial environment як демонстрація штучного середовища (рис. 3.16).

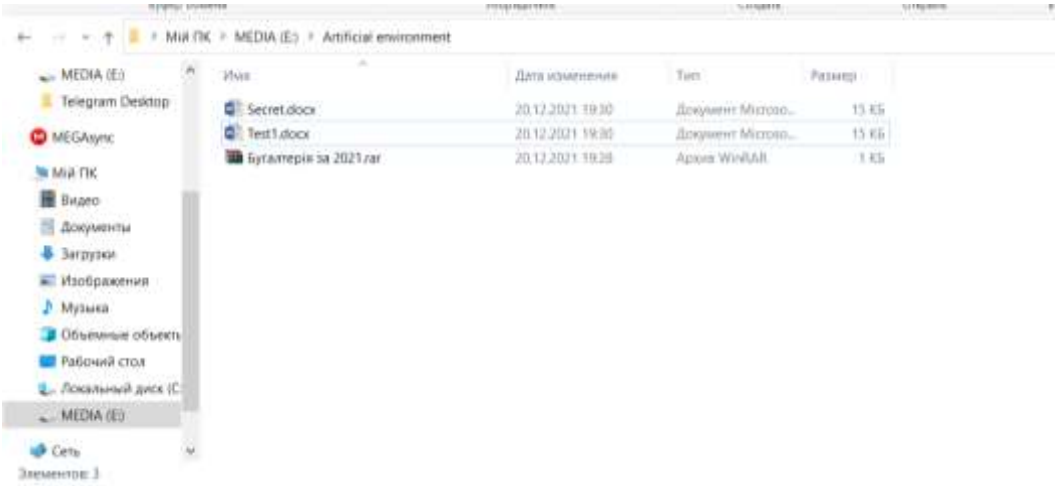


Рисунок 3.16 - Дані з стандартм паролем для іншого користувача.

Наступним при вводі неправильного пароля декілька разів буде також буде повідосмлення(рис. 3.17).

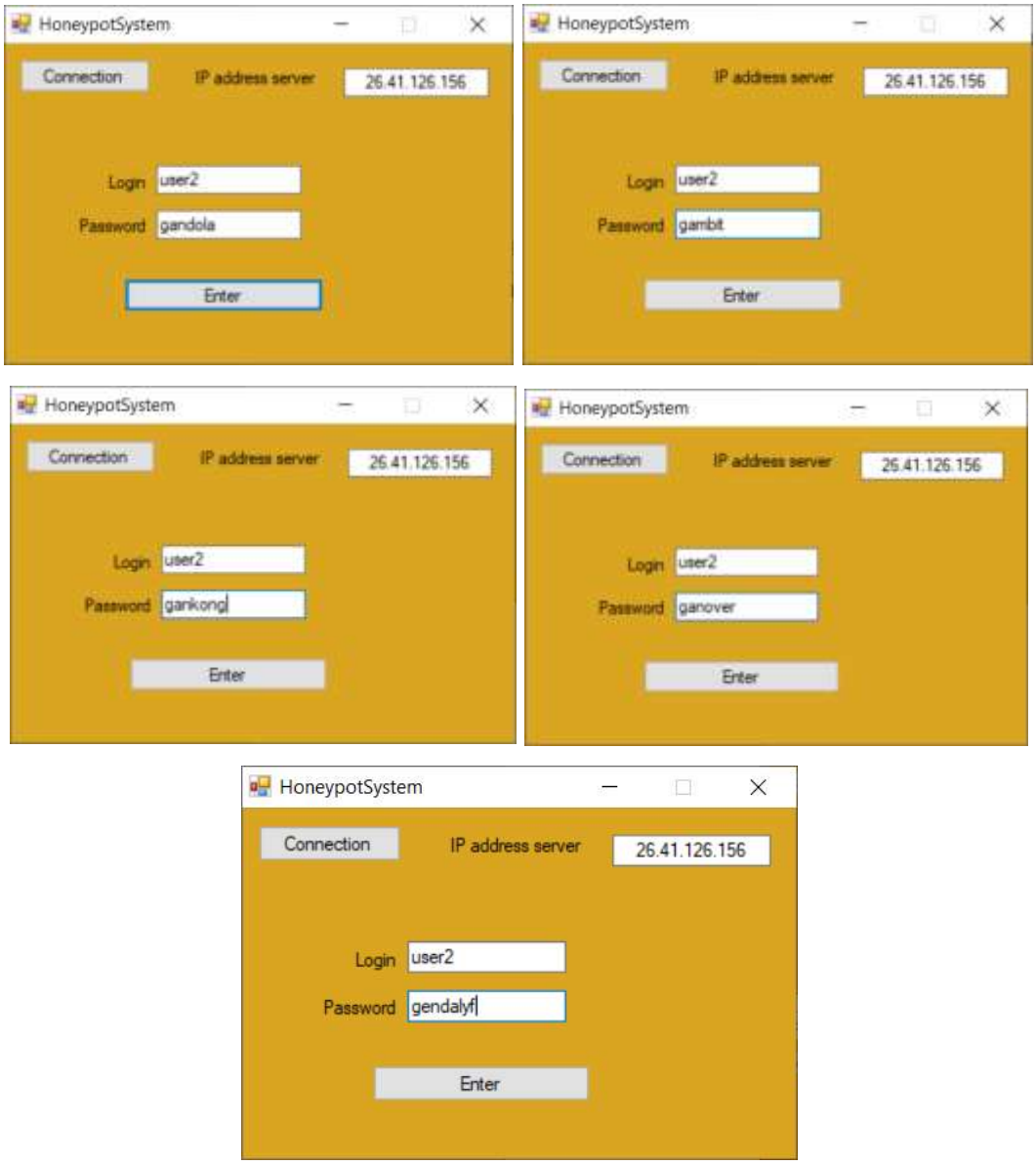


Рисунок 3.17 - Ввод декілька неправильних паролів.

Після чого їде повідомлення адміністратору про перехід даного користувача в штучне середовище(рис. 3.18).

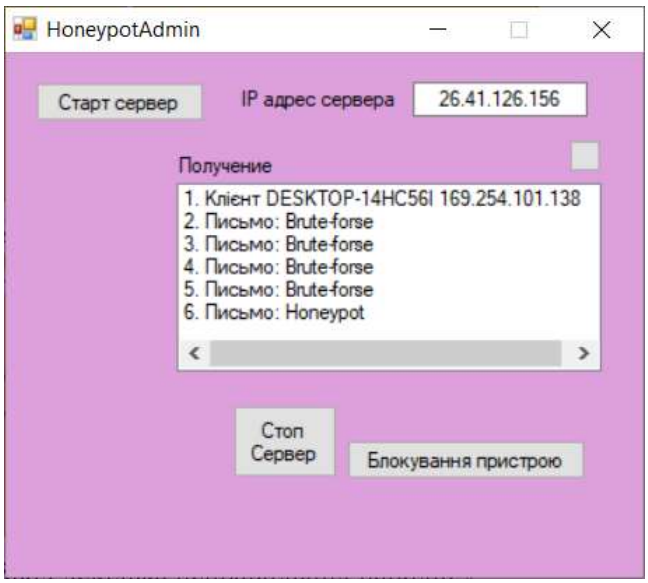


Рисунок 3.18 - Дані з стандартм паролем для іншого користувача.

Для прикладу були введені дані користувача в внутрішнії мережі що був записаний в базі даних (рис. 3.19).

Рисунок 3.19 - Дані користувача.

Після успішно вводу даних користувачів з’явиться повідомлення про успішну авторизацію (рис. 3.20).

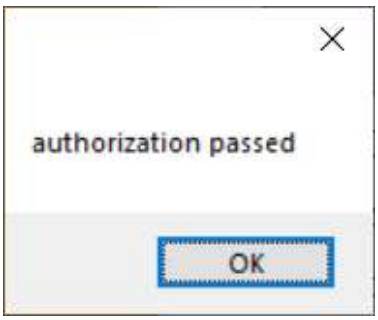


Рисунок 3.20 - Повідомлення про успішну авторизіцію.

Наступним кроком є перевірка в внутрішній мережі як для виялення можливого злому. Дана захист показний на рисунку 3.21.

Рисунок 3.21 - Принцип роботи з зловмисником в внутрішній мережі

Коли зловмисник відкриє певний каталог і зміне або відкриє файл буде відправлено повідомлення (рис. 3.22).

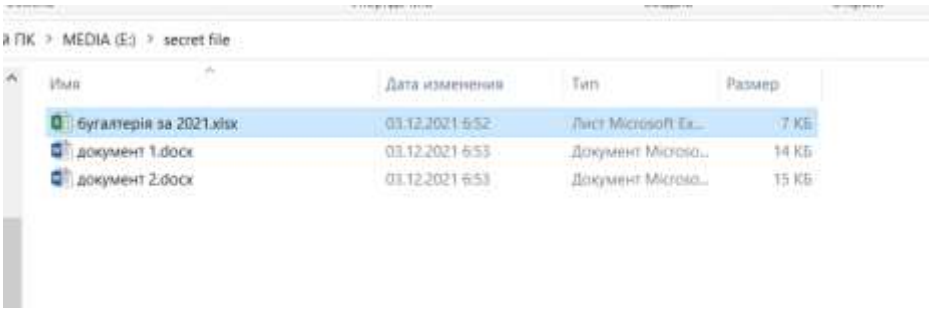


Рисунок 3.22 – Відкритий каталог та файла

Після чого буде відправлене повідомлення HoneypotAdmin та дасть можливість заблокувати користувача та вимкнути користувача (рис. 3.23).

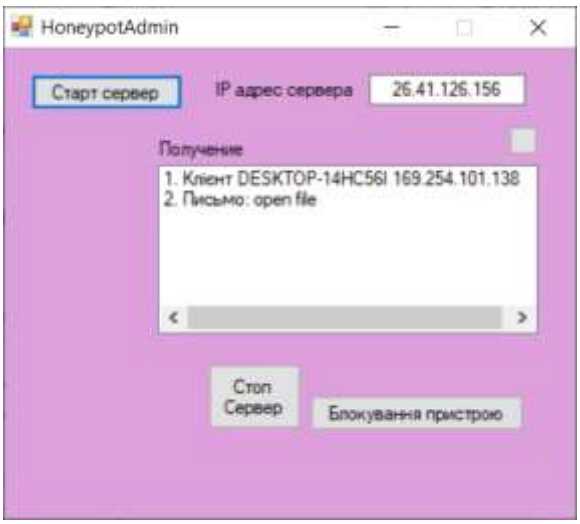


Рисунок 3.23 – Повідомлення про відкриття файлу

Даний метод дає можливість виявити зловмисника в внутрішній мережі. В даному розділі було обгрунтовано вибір мови програмування та показана розробка засобу також було продемонстровано роботу методу системи виявлення атак з допомогою Honeypot.

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Оцінювання комерції продукту та його новизни на ринку

В умовах жорсткої конкуренції як на міжнародних, так і на вітчизняних ринках здатність промислових підприємств функціонувати та розвиватись залежить від їхньої спроможності створювати й впроваджувати нові або значно вдосконалені традиційні товари. Найчастіше з новим товаром пов’язують результат творчого пошуку, який суттєво поліпшує розв’язання певної вже відомої проблеми споживача або розв’язує проблему, що раніше взагалі не поставала. Одночасно, для визначення можливості отримання перспективних прибутків, потрібно сформулювати найважливі-шу з погляду майбутнього покупця споживчу цінність інноваційного продукту, тобто встановити рівень новизни споживчих властивостей; радикальності задумів; новацій у дослідженнях, розробленні, техніці і технології виготовлення; суттєвості змін у ринковому просуванні та обслуговуванні.

В цьому руслі інноваційна діяльність у сфері створення товарних пропозицій є основою подальшого стратегічного вектора розвитку ринкових можливостей промислових підприємств, що ґрунтується на засадах концепції інноваційного маркетингу. Проте вітчизняні промислові підприємства, які мають достатньо високий науково-технічний, виробничо-технологічний та кадровий потенціал, мають значну кількість унікальних сучасних технологій, продовжують розвиватись, пропонуючи на ринку морально, а й нерідко і фізично застарілу продукцію, що містить езначний рівень ринкової новизни. Саме від рівня новизни залежить позитивне сприйняття продукції на ринку цільовими споживачами. Виводячи на ринок новинку виробник вважає, що тієї новизни, якою наділений новий товар є достатньо для того, щоб він був сприйнятий споживачем як новий. Але це не завжди так, в силу того, що споживач і виробник неоднозначно визначать її рівень новизни.

Споживча новизна – здатність нового чи традиційного товару задовольняти або зовсім нову потребу, або значно ефективніше задовольняти вже існуючу.

Товарна новизна – часткова чи принципова зміна споживчих (або функціональних, економічних тощо) властивостей продукції.

Виробнича новизна – товар, що вперше виготовляється даним підприємством без огляду на його якісні відмінності, та ступінь новизни для ринку та споживача.

Прогресивна новизна – будь-які прогресивні зміни, що відрізняють виріб від його аналогів і прототипів. Ці зміни можуть стосуватися сировини, матеріалів, конструкції, технології тощо.

Ринкова новизна – товари, які існують на інших ринках, але є новими для даного ринку.

Маркетингова новизна – створення унікальних ринкових умов реалізації товару, методів ціноутворення, комунікацій, маркетингових стратегій.

Екологічна новизна – нові екологічні характеристики товару, що призводять до зниження інтегрального екодеструктивного впливу на навколишнє середовище при одночасному підвищенні економічної ефективності у сферах їхнього виробництва та споживання.

Соціальна новизна – нові соціальні характеристики товару, що приводять до отримання певного соціального та економічного ефекту, одержуваного суспільством від виробництва та споживання інноваційного товару.

Необхідно зазначити, що перелічені вище види, в сукупності становлять сукупну новизну товару або інтегральну новизну. Саме визначення рівня і ступеня інтегральної новизни товару є найбільш актуальним, оскільки її рівень визначає ступінь однакового позитивного сприйняття новизни товару як виробником, так і споживачем, а отже і ринком в цілому, а це, у свою чергу, є гарантією того, що новинка знайде своє місце на ринку, користуватиметься попитом у споживачів і забезпечить відшкодування витрат, зазнаних товаровиробником під час розроблення та виробництва інноваційного продукту.

Виходячи з отриманих даних, розрахувати значення новизни розробки за кожним чинником, згідно з формулою;

Розрахувати інтегральний показник новизни розробки у відповідності до формули 4.1 та зробити висновки відносно новизни за кожним чинником та інтегральним показником, виходячи рекомендацій наведених в таблицях 4.1 та 4.2.

Таблиця 4.1 – Відносна новизна

Види та чинники	**Експерти та виставлені бали**					Розрахунки		
	E1	**E2**	**E3**	**E4**	**E5**			
1	**2**							
Споживча новизна						**25**	**I=**	
1. Зміна поведінкових звичок споживача	2	1	3	3	3	2,4	11,2	0,448
2. Ступінь задоволення потреб і запитів	2	0	1	5	4	2,4		
3. Спосіб задоволення потреби	1	4	3	4	5	3,4		
4. Формування нової потреби	1	1	2	2	0	1,2		
5. Формування нового споживача	0	4	1	0	4	1,8		
Товарна новизна						**30**	**I=**	
1. Параметричні зміни показників продукції								
1.1. Якісні	0	2	5	0	2	1,8	7,2	0,24
1.2. Технічні	1	2	2	2	0	1,4		
1.3. Економічні	5	-1	1	1	3	1,8		
1.4. Сервісні	0	4	-1	2	2	1,4		
2. Якість продукції щодо відношення до конкурентів	1	4	0	-1	0	0,8		
3. Функціональні зміни	2	5	1	1	1	2		
Виробнича новизна						**25**	**I=**	
1. Рівень унікальності товару для підприємства	0	5	1	5	5	3,2	11,8	0,472
2. Рівень унікальності для галузі	2	2	0	5	0	1,8		
3. Рівень унікальності товару для країни	1	0	3	5	0	1,8		
4. Зміна конструктивного виконання	4	1	4	2	-1	2		
5. Рівень застосування інновацій	1	5	5	-1	5	3		
Прогресивна новизна						**25**	**I=**	
1. Зміна технології виготовлення	1	2	5	2	-1	1,8	7,6	0,304

Продовження таблиці 4.1

2. Рівень застосування нових компонентів і матеріалів	4	1	0	2	2	1,8		
3. Зміна технологічного принципу дії виробу	-1	1	0	2	1	0,6		
4. Зміна конструктивного виконання	1	-1	1	2	1	0,8		
5. Рівень застосування інновацій	3	0	4	2	4	2,6		
Ринкова новизна						**20**	**I=**	
1. Новий виріб на новому ринку	5	0	1	3	0	1,8	8,6	0,43
2. Новий виріб на відомому ринку	3	2	1	2	-1	1,4		
3. Модернізований виріб	5	3	4	5	4	4,2		
4. Нова модель	3	0	3	-1	1	1,2		
Екологічна новизна						**20**	**I=**	
1. Рівень екологічної чистоти технології виробництва	0	0	-1	2	1	0,4	3,8	0,19
2. Рівень впровадження мало- та безвідходних технологій	1	-1	3	0	4	1,4		
3. Рівень екологічно небезпечних режимів експлуатації продукції	1	1	2	-1	2	1		
4. Рівень забруднення навколишнього середовища	-1	4	-1	0	3	1		
Соціальна новизна						**20**	**I=**	
1. Використання нового товару приводить до покращення стану здоров’я нації	5	2	1	5	3	3,2	5,6	0,28
2. Використання нового товару приводить до зростання доходів населення	-1	0	2	4	0	1		
3. Виробництво нового товару приводить до збільшення (зменшення) кількості робочих місць на підприємстві	3	2	2	-1	1	1,4		
4. Виробництво нового товару приводить до підвищення кваліфікації персоналу	1	0	0	2	1	0,8		
Маркетингова новизна						**20**	**I=**	
1. Нові методи маркетингових досліджень	0	5	5	3	5	3,6	10	0,5
2. Вживання нових стратегій сегментації ринку	3	4	4	0	0	2,2		
3. Вибір нової маркетингової стратегії обхвату і розвитку цільового сегмента	0	4	0	1	3	1,6		
4. Побудова нових каналів збуту	2	1	5	2	3	2,6		

Таблиця 4.2 – Вагомість видів новизни

Експерти	Вагомість видів новизни (W)							
	Спожив	Товар	Виробнича	Прогресивна	Ризкова	Екологічна	Соціальна	Маркетинова
Е1	0,223	0,241	0,029	0,181	0,115	0,03	0,024	0,157
Е2	0,274	0,204	0,031	0,164	0,101	0,031	0,044	0,151
Е3	0,215	0,248	0,021	0,154	0,079	0,048	0,041	0,194
Е4	0,245	0,208	0,033	0,174	0,101	0,041	0,031	0,167
Е5	0,255	0,233	0,024	0,181	0,107	0,031	0,05	0,129
Середня оцінка	0,2424	0,2268	0,0276	0,1708	0,1006	0,0362	0,038	0,1596

Значення і-го виду новизни пропонується розраховувати за формулою:

$$\mathrm{I_i} = \frac{\mathrm{Б_{iотр}}}{\mathrm{Б_i}MAX}, \tag{4.1}$$

де $\mathrm{Б_{іспоживче}}$ – отримана кількість балів за шкалою оцінок чинників, що визначають і-й вид новизни.

$\mathrm{Б_{спожив.}}MAX = 25$ -(максимальна к-сть балів, що може бути отримана за і-м видом новизни за чинником споживчий.

Загальний рівень інтегральної новизни розраховується шляхом перемноження отриманого значення і-го виду новизни на її вагомість, за формулою

$$N_{\mathrm{інт}} = \sum_i^n W_{\mathrm{i}} * \mathrm{I_i}, \tag{4.2}$$

де $N_{\mathrm{інт}}$ –рівень інтегральної новизни;

W_{i}- вагомість (питома вага) і-го виду новизни;

n- загальна кількість видів новизни.

$N_{\mathrm{інт}} = (0{,}2424 * 0{,}448) + (0{,}2268 * 0{,}24) + (0{,}0276 * 0{,}472) + (0{,}1708 * 0{,}304) + (0{,}1006 * 0{,}43) + (0{,}0362 * 0{,}19) + (0{,}038 * 0{,}28) + (0{,}1596 * 0{,}5) =$0,368554.

Наступним кроком є сегментування товару.

У системі ринкових відносин напрямки розвитку виробництва і торгівлі визначає споживач, який купує товари і тим самим показує виробнику, що потрібно виробляти і продавати. Тому, щоб ефективно діяти, виробникам

необхідно визначити потреби та попит і задовольнити їх. Потреби діляться на дві групи: потреби суспільства і потреби особисті.

Потреби суспільства – це потреби виробничі, у державному управлінні, у забезпеченні конституційних прав, гарантій, охорони навколишнього середовища, оборони та ін.

Особисті потреби – це потреби, які виникають і розвиваються у процесі життєдіяльності людини.

Потреби і попит відрізняються по своїй суті. Потреба може бути явною і прихованою. Дуже важливим для виробника є не тільки прогнозувати існуючі потреби, але і виявляти й формувати попит на приховані потреби. Орієнтація на споживача потребує правильного розуміння його потреб і розуміння можливих перспективних змін в способах їхнього задоволення. Потреби промислового виробництва направлені на забезпечення потреб виробництва в устаткуванні, сировині, основних та допоміжних матеріалах, комплектуючих виробах, паливі, енергії та ін., а також направлені на надання послуг різноманітного характеру.

Попит – це бажання з урахуванням наявної купівельної спроможності, тобто забезпечена грошима потреба в товарах (послугах), які реалізуються на ринку.

З погляду маркетингового управління розрізняють два основних типи ринків: споживчий і промисловий. Поділ базується на основі подальшого використання придбаних товарів та послуг.

Споживчий ринок – це ринок, на якому придбання товарів і послуг відбувається для особистого або сімейного користування.

Промисловий ринок – це ринок, на якому придбання товарів і послуг відбувається для подальшого використання в процесі виробництва, для перепродажу чи здачі в оренду. Охоплює таких учасників, як виробники, посередники, державні заклади й установи та недержавні, некомерційні організації і заклади.

Промисловий ринок має такі особливості попиту:

вторинність попиту – попит на промисловому ринку зумовлюється попитом на споживчому ринку. Збільшення попиту на споживчому ринку на 10

відсотків може привести до збільшення попиту на промисловому ринку в 5 разів і більше;

- нееластичність попиту – незначні коливання цін не призводять до змін попиту на промислові товари;
- перехресна еластичність попиту – попит на один товар залежить від ціни на інші товари, передусім на товари-субститути;
- нестійкість попиту – зумовлюється технологічними змінами та коливаннями попиту на споживчому ринку;
- пов’язаність попиту – попит на один тип товару приводить до попиту на пов’язані з ним товари.

Аналіз попиту на нову продукцію – один з найважливіших напрямів діяльності підприємств-розробників. Основою конкурентного успіху підприємства-інноватора є його спроможність виявити реально існуючі чи потенційні потреби та попит споживачів щодо інновацій (або ж сформувати їх) і задовольнити їх ефективнішим, ніж конкуренти, способом. Специфіка полягає у тому, що розробка інновацій у багатьох випадках пов’язана зі створенням товарів, аналогів яких раніше просто не існувало:

- потреби й попит споживачів, для задоволення яких призначені нові товари, раніше задовольнялися зовсім іншим способом;
- потреб, для задоволення яких призначено нові товари, яких раніше просто не існувало.
- Для аналізу попиту на інновації використовують такі специфічні методи, як:
- прогнозування майбутніх потреб і попиту споживачів, змін мотивації їхньої поведінки;
- ситуаційне й імітаційне моделювання поведінки споживачів у сьогоденні й майбутньому;
- аналіз тенденцій розвитку науково-технічного прогресу, тенденцій зміни технологічної, економічної, соціальної, політичної, культурної, правової, екологічної й інших складових середовища господарювання.

З метою максимального задоволення потреб споживачів, а також раціоналізації витрат підприємства-розробника проводять сегментування ринку.

Сегментування ринку:

- це виокремлення певної кількості покупців, що мають аналогічну реакцію на комплекс маркетингових засобів підприємства, тобто однаково сприймають параметри промислового товару, його ціну, місце збуту та маркетингові комунікації;
- це формування груп споживачів за певними ознаками.

Сегмент – це об’єднана, заздалегідь виявлена кількість споріднених покупців за певними ознаками.

Цілі сегментування:

пошук та виокремлення на ринку тих покупців, чий платоспроможний попит підприємство може забезпечити в поточний і довгостроковий термін;

виключення тих покупців, чий попит краще можуть забезпечити конкуренти;

концентрація зусиль тільки на тих покупцях, чиї потреби підприємство може забезпечити краще інших.

Сегментування ринку здійснюється шляхом макро та мікро- сегментування на таблиці 4.3.

Таблиця 4.3 – Сегментування товару

Потреби	Технології								
	традиціїні			Модернізовані			Нові		
	Споживачі								
	жінки	чоловіки	діти	жінки	чоловіки	діти	жінки	чоловіки	діти
Задоволення потреб у послугах									
Задовольнити потреби у непродовольчих товарах									
Задовольнити потреби у продовольчих товарах									

Таблиця 4.4 – Макросегментація продукту

Критерій	Значимість критерію	Бали залежно від характеристики сегмента		
		1	2	3
Тенденція розвитку сегмента	3	Сегмент зменшується	Сегмент сталий	Сегмент збільшується
Конкуретна привабливсть продукта	1	Значна привабливість сегмента для конкурентів	Помірна привабливість сегмента для конкурентів	Слабка привабливість сегмента для конкурентів
Сталість потреб покупців	2	Потреби значно змінюються під впливом різноманітних факторів	Потреби покупців змінюються незначно під впоивом різноманітних факторів	Потреби покупців відносно постійні
Ступінь мінливості потреб і запитів покупців відносно товарів номенклатури підприємства	3	Переваги і смаки покупців значно змінюються під впливом різноманітних факторів	Переваги і смаки покупців змінюються незначно під впливом різноманітних факторів	Переваги і смаки покупців відносно постійні
Ступінь чутливості покупців до зміни рівня цін на товари	1	Покупці дуже чутливі до змін рівня цін на товари	Покупці чутливі незначно до зміна рівня цін на товари	Покупці не чутливі до зміни рівня цін на товари
Ступінь чутливості покупців до стимулювання збуту	3	Покупці не чутливі до стимулювання збуту	Покупці незначно чутливі до стимулювання збуту	Покупці дуже чутливі до стимулювання збуту
Разом	13	13<X<33		

Остаточний вибір цільового ринку здійснюється на основі побудови карти обґрунтування вибору цільового ринку підприємства.

Метод стандартного розподілу ймовірностей (PERT від program evaluation and review) предсталено на рисунку 4.1.

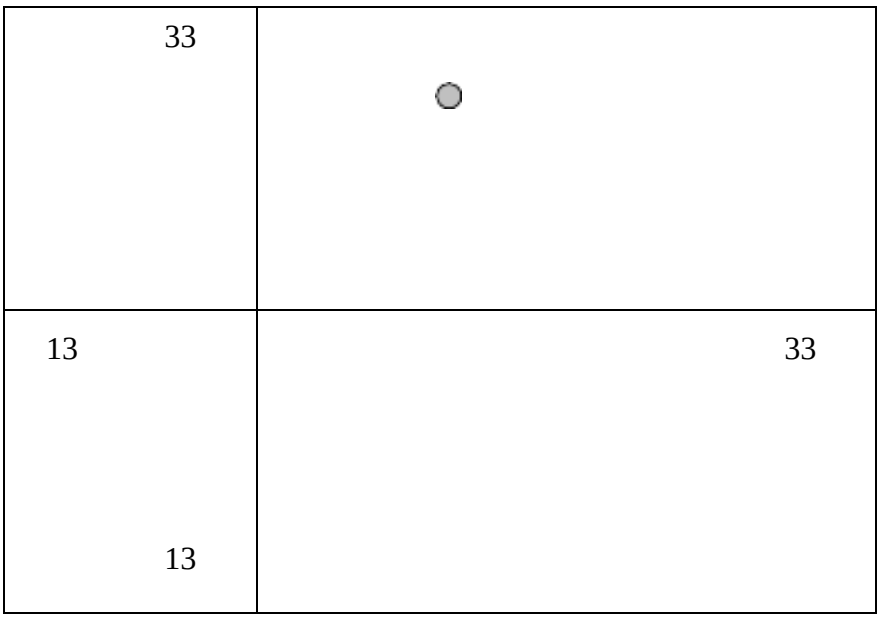


Рисунок 4.1 – Стандартний розподіл ймовірностей

Згідно з цим методом, перш за все, експертним шляхом визначається значення трьох або двох видів прогнозу збуту: оптимістичного, песимістичного та найбільш імовірного (можливого). Далі розраховується очікуване (реалістичне) значення прогнозу збуту (РП) за формулами:

при трьох видах прогнозу збуту:

$$РП = \frac{ПП + 4 \cdot МП + ОП}{6}, \qquad (4.3)$$

де ПП – песимістичний (мінімальний) прогноз збуту продукції;

МП – найбільш імовірний (можливий) прогноз збуту продукції;

ОП – оптимістичний (максимальний) прогноз збуту продукції.

Основними ознаками наукового ефекту науково-дослідної роботи є новизна роботи, рівень її теоретичного опрацювання, перспективність, рівень розповсюдження результатів, можливість реалізації. Науковий ефект НДР можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Значення показників ступеня новизни і рівня теоретичного опрацю- вання науково-дослідної роботи в балах наведені в табл. 4.5 та 4.6.

Таблиця 4.5 – Показники ступеня новизни науково-дослідної роботи

Ступінь новизни	Характеристика ступеня новизни	Значення показника ступеня новизни, бали
1	2	3
Принципово нова	Робота якісно нова за постановкою задачі і грунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отримані принципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод	60…100
Нова	Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів	40…60
Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв’язок (або знайдено новий зв’язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об’єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональна модифікація (з ознаками новизни)	10…40
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим	2…10
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам	1…2

Таблиця 4.6 – Показники рівня теоретичного опрацювання науково-дослідної роботи

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали
Відкриття закону, розробка теорії	80…100
Глибоке опрацювання проблеми: багатоаспектний аналіз зв'яз- ків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	60…80
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	20…60
Елементарний аналіз зв'язків між фактами та наявною гіпоте- зою, класифікація, практичні рекомендації для окремого випадку тощо	6…20
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	1…5

Показник, який характеризує науковий ефект, визначається за формулою:

$$E_{нау} = 0{,}6 \cdot k_{нов} + 0{,}4 \cdot k_{теор}, \qquad (4.4)$$

де $k_{нов}, k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, бали;

0,6 та 0,4 – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

Визначення характеристики показника $E_{нау}$ проводиться на основі висновків експертів виходячи з граничних значень.

$$E_{\text{нау}} = 0{,}6 * 55 + 0{,}4 * 60 = 57$$

Таблиця 4.7 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Всноновши що дана робота має середній рівень научной новизни.

Наступним кроком буде визначення якості іноваційного проекту.

Сучасна ринкова економіка висуває принципово нові вимоги до якості продукції. Це пов'язано з тим, що будь-яке підприємство може «вижити» та забезпечити стабільне положення на ринку товарів тільки в тому випадку, коли його продукція є конкурентоспроможною.

Сьогодні вважається, що якість продукції є найефективнішим засобом задоволення вимог споживачів і одночасно з цим – зниження витрат виробництва.

Міжнародний стандарт ІСО 8402 «Якість. Словник» визначає якість продукції як сукупність її властивостей, які обумовлюють здатність продукції задовольняти певні потреби споживачів відповідно до свого призначення.

Властивість продукції – це об'єктивна її особливість, яка виявляється при створенні, експлуатації (використанні) або споживанні цієї продукції. Продукція однієї назви, але різного призначення, може мати різні властивості.

Кількісне оцінювання властивостей продукції здійснюється за допомогою показників якості.

4.2 Пронозування витрат на науково-дослідні та конструкторсько-технологічної роботи.

Витрати на основну заробітну плату дослідників ($З_о$) розраховують у відповідності до посадових окладів працівників, за формулою:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} * t}{T_p} \quad (4.5)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, $T_p=21…23$ дні. Проведені розрахунки бажано звести до таблиці.

Таблиця 4.8 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	1200	126	60	2250
Розробник	600	78	60	1110
Всього				3360

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і пре- дмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за прямим призначенням згідно з нормами їх витрачання, а також витрачені придбані напівфабрикати, що підля- гають монтажу або виготовленню й додатковій обробці в даній організації, чи дослідні зразки, що виготовляються виробниками за документацією нау- кової організації.

Витрати на комплектуючі вироби *($К_в$)*, які використовують при дослі- дженні нового технічного рішення, розраховуються, згідно з їхньою номен- клатурою, за формулою:

$$К_в = \sum Н_j \cdot Ц_j \cdot К_j \; j=1 \qquad (4.6)$$

де $Н_j$ – кількість комплектуючих *j*-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих *j*-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 ... 1,15*).

Проведені розрахунки бажано звести до таблиці 4.9.

Таблиця 4.9 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Комп’ютер	2	10000	20000
Сервер	1	9668	9668
Всього			11 668

Дані комплектуючі можуть мати слабкі характеристики тому ціна занижена.

4.3 Прогнозування комерціних ефектів від реазізації результату розробки

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження резуль- татів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку. Саме зростання чистого прибутку за- безпечить потенційному інвестору надходження додаткових коштів, дозво- лить покращити фінансові результати його діяльності, підвищить конкурентоспроможність та може позитивно вплинути на ухвалення рі- шення щодо комерціалізації цієї розробки.

Для того, щоб розрахувати можливе зростання чистого прибутку у потенційного інвестора від можливого впровадження науково-технічної розро- бки необхідно:

а) вказати, з якого часу можуть бути впроваджені результати науково-технічної розробки;

б) зазначити, протягом скількох років після впровадження цієї науково-технічної розробки очікуються основні позитивні результати для потен- ційного інвестора (наприклад, протягом 4-х років після її впрова- дження);

в) кількісно оцінити величину існуючого та майбутнього попиту на цю або аналогічні чи подібні науково-технічні розробки та назвати основ- них суб’єктів (зацікавлених осіб) цього попиту;

г) визначити ціну реалізації на ринку науково-технічних розробок з аналогічними чи подібними функціями.

При розрахунку економічної ефективності слід обов’язково враховувати зміну вартості грошей у часі, оскільки від вкладення інвестицій до отри- мання прибутку минає чимало часу.

При оцінюванні ефективності інноваційних проектів передбачається розрахунок таких важливих показників:

– абсолютного економічного ефекту (чистого дисконтованого доходу);

– внутрішньої економічної дохідності (внутрішньої норми дохідності);

– терміну окупності (дисконтованого терміну окупності).

Аналізуючи напрямки проведення науково-технічних розробок, розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором можна об’єднати, враховуючи визначені ситуації з відповідними умовами.

Розробка чи суттєве вдосконалення машини (механізму, приладу, пристрою) для використання кінцевими споживачами.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

ΔN – збільшення кількості споживачів пристрою, у періоди часу, що аналізуються, від покращення його певних характеристик;

N – кількість споживачів які використовували аналогічний пристрій у році довпровадження результатів нової науково-технічної розробки;

$Ц_б$ – вартістьпристрою (машини, механізму) у році до впровадження результатів розро-бки;

$\pm\Delta Ц_о$ – зміна вартості пристрою (зростання чи зниження) від впровадження результатів науково-технічної розробки у періоди часу, що аналізуються.

Розробка для комерційної реалізації нової чи модернізованої технології виготовлення (відновлення, надання послуг тощо) продукції, яка призначена кінцевому споживачеві.

В цьому випадку основу майбутнього економічного ефекту будуть формувати такі показники:

ΔN – прогнозоване зростання кількості реалізованоїпродукції завдяки використанню нової чи модернізованої технології, завдяки покращенню їх певних характеристик у році що аналізується;

N – кількість споживачів які використовували аналогічний продукт у році довпровадження результатів нової науково-технічної розробки;

$Ц_б$ – ціна продукції у році до впровадження результатів розробки (нової чи модернізованої технології);

$\pm\Delta Ц_о$ – зміна ціни реалізації продукції (зростання чи зниження) від впровадження результатів науково-технічної розробки у періоди часу, що аналізуються. Причому зміна ціни враховує можливе підви- щення якості продукції та зміну собівартості:

$$\pm\Delta Ц_о = Ц_б \cdot (k-1) - (\pm\Delta S),$$

де k – коефіцієнт зміни якості продукції, що випускається за новою чи модернізованою технологією виготовлення (відновлення);

$\pm\Delta S$ – зміна собівартості виготовлення продукції (зростання чи зниження) від впровадження результатів науково-технічної розробки у періоди часу, що аналізуються.

Для всіх наведених випадків можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховується за формулою:

де $\pm\Delta Ц_о$ – зміна основного якісного показника від впровадження результатів науково-технічної розробки у році що аналізується. Зазвичай, таким показником може бути зміна ціни реалізації одиниці нової розробки у році що аналізується (відносно року до впровадження цієї розробки); $\pm\Delta Ц_о$ може мати як додатне, так і від'ємне значення (від'ємне – при зниженні ціни відносно року до впровадження цієї розробки, додатне – при зростанні ціни);

N – основний кількісний показник, який визначає величину попиту на аналогічні чи подібні розробки у році до впровадження результатів нової науково-технічної розробки;

$Ц_о$ – основний якісний показник, який визначає ціну реалізації нової науково-технічної розробки у році що аналізується,

$$Ц_о = Ц_б \pm \Delta Ц_о;$$

$Ц_б$ – основний якісний показник, який визначає ціну реалізації існуючої (базової) науково-технічної розробки у році до впровадження результатів;

ΔN – зміна основного кількісного показника від впровадження результатів науково-технічної розробки у році що аналізується. Зазвичай таким показником може бути зростання попиту на науково-технічну розробку у році що аналізується (відносно року до впровадження цієї розробки);

λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2021 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0{,}8333$; ρ – коефіцієнт, який враховує рентабельність інноваційного продукту (послуги).

Рекомендується приймати $\rho = 0{,}2...0{,}5$;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2021 році $\vartheta = 18\%$;

Далі розраховують приведену вартість збільшення всіх чистих прибутків ПП, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t} \quad (4.7)$$

де $\Delta П_i$ - збільшення чистого прибутку у кожному з років, протягом якихвиявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau = 0{,}05...0{,}15$;

t – період часу (в роках) від моменту початку впровадження науково- технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

Далі розраховують величину початкових інвестицій PV , які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки.

Для цього можна використати формулу:

$$PV = k_{інв} \cdot ЗВ, \qquad (4.8)$$

4.4 Розрахунок ефективності та окупності інвестиції

Досить часто в магістерських кваліфікаційних роботах трапляється ситуація, коли проектувальник (замовник) певної науково-технічної розробки використовує її тільки на своєму підприємстві (чи в організації) і не виводить її на ринок. У цьому випадку позитивним результатом від впровадження цієї науково-технічної розробки може бути покращення певних економічних та фінансових показників діяльності підприємства. Це може бути, наприклад, зменшення собівартості продукції, що виготовляється на підприємстві, підвищення якості продукції або якості послуг, що надаються підприємством своїм клієнтам, економія певних видів ресурсів, скорочення часу виконання тих чи інших операцій, скорочення втрат від випуску бракованої продукції, скорочення травматизму на підприємстві тощо.

Але в будь-якому випадку всі ці покращення в кінцевому результаті підвищують конкурентоспроможність підприємства, збільшують частку споживачів його продукції, розширюють кордони ринку, що його займає підприємство тощо, а це, своєю чергою, приводить до зростання чистого прибутку, що його може отримати підприємство, яке розробляє та впрова- джує нову науково-технічну продукцію.

Для того, щоб розрахувати можливе зростання чистого прибутку від впровадження розробником нової науково-технічної продукції на своєму підприємстві (організації) необхідно:

а) вказати, з якого часу можуть бути впроваджені результати науково-технічної розробки;

б) зазначити, протягом скількох років після впровадження цієї науково-технічної розробки очікуються основні позитивні результати для потен- ційного інвестора (наприклад, протягом 4-х років після її впрова- дження);

в) кількісно оцінити, які саме економічні та фінансові показники діяльності підприємства і на скільки будуть покращені в результаті впрова- дження науково-технічної розробки;

г) визначити обсяг продукції, яка виготовлялася на підприємстві і яка буде виготовлятися після впровадження науково-технічної розробки.

При розрахунку економічної ефективності слід обов’язково враховувати зміну вартості грошей у часі, оскільки від вкладення коштів у розробку до отримання прибутку минає чимало часу.

При оцінюванні ефективності таких проектів передбачається розраху- нок окремих важливих показників:

– абсолютного економічного ефекту (чистого дисконтованого доходу);внутрішньої економічної дохідності (внутрішньої норми дохідності);

– терміну окупності (дисконтованого терміну окупності).

Аналізуючи напрямки проведення науково-технічних розробок, розрахунок економічної ефективності науково-технічної розробки при її використанні розробником для власних потреб, можна об’єднати на основі відповідних ситуацій і умов.

Ситуації та умови:

Розробка та впровадження автоматизованої системи управління (електронного документообігу, управління логістикою, управління складсь- кою системою, управління перевезеннями тощо) для конкретного підприєм- ства (організації)

В даному випадку майбутній економічний ефект та ефективність будеформуватися на основі використання таких показників:

$$П_я = \frac{ΔЧП * ЗП * 12}{N} \quad (4.9)$$

$\Delta ЧП$ – економія чисельності працівників виконання виробничої чи управлінської функції яких було автоматизовано у році що аналізується, осіб;

N – кількість функцій, які виконуються вручну у році до впровадження результатів нової науково-технічної розробки, шт;

ΔN_i – прогнозоване зростання кількості виробничих чи інформаційно-технічних управлінських функцій, виконання яких автоматизується, у році що аналізується (відносно року до впровадження даної розробки), шт.

Для всіх наведених випадків можливе збільшення чистого прибутку у потенційного інвестора Пі для кожного із років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховується за формулою:

$$\Delta П_i = (\pm \Delta Ц_o * N + Ц_o * \Delta N)_i * \lambda * p * (1 - \frac{\vartheta}{100}) \quad (4.10)$$

де $\pm \Delta Ц_o$ – зміна основного якісного показника від впровадження результатів науково-технічної розробки у році що аналізується. Зазвичай, таким показником може бути зміна ціни реалізації одиниці нової розробки у році що аналізується (відносно року до впровадження цієї розробки); $\pm \Delta Ц_o$ може мати як додатне, так і від'ємне значення (від'ємне – при зниженні ціни від- носно року до впровадження цієї розробки, додатне – при зростанні ціни);

N – основний кількісний показник, який визначає величину попиту на аналогічні чи подібні розробки у році до впровадження результатів нової науково-технічної розробки;

$Ц_o$ – основний якісний показник, який визначає ціну реалізації нової науково технічної розробки у році що аналізується,

$Ц_o = Ц_б \pm \Delta Ц_o$; $Ц_б$ – основний якісний показник, який визначає ціну реалізації існуючої (базової) науково-технічної розробки у році до впровадження результатів;

ΔN – зміна основного кількісного показника від впровадження резуль-

татів науково-технічної розробки у році що аналізується. Зазвичай таким по- казником може бути зростання попиту на науково-технічну розробку у році що аналізується (відносно року до впровадження цієї розробки);

λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2021 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту (послуги). Рекомендується приймати $\rho = 0,2...0,5$;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2021 році $\vartheta = 18\%$;

$$\Delta П_i = (1200 * 20 + 120 * 28)_i * 0,8333 * 0,2 * \left(1 - \frac{0,18}{100}\right) = 4552$$

Далі розраховують приведену вартість збільшення всіх чистих прибут- ків *ПП*, що їх може отримати потенційний інвестор від можливого впрова- дження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t} \quad (4.11)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом якихвиявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних ре-зультатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau = 0,05...0,15$;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додат- кових чистих прибутків у цьому році.

$$ПП = \sum_{i=1}^{5} \frac{4552}{(1+0,10)^4} = 15545 \text{ грн.}$$

Далі розраховують величину початкових інвестицій PV, які потенцій- ний інвестор має вкласти для впровадження і комерціалізації науково-тех- нічної розробки. Для цього можна використати формулу:

$$PV = k_{\text{інв}} * \text{ЗВ}, \quad (4.12)$$

де $k_{інв}$ коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}$ *=2...5,* але може бути і більшим;

ЗВ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

$$PV = 2 * 3500 = 7000$$

Тоді абсолютний економічний ефект $E_{абс}$ або чистий приведений дохід*(NPV, Net Present Value)* для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$\text{Е}_{\text{абс}} = \text{ПП} - PV, \quad (4.13)$$

де *ПП* – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, грн;

PV – теперішня вартість початкових інвестицій, грн.

$$\text{Е}_{\text{абс}} = 15545 - 7000 = 8545$$

Якщо величина $E_{абс}$буде мати велике додатне значення, то це може свідчити про потенційну зацікавленість інвесторів у впровадженні та комерціа- лізації цієї науково-технічної розробки. Але для остаточного прийняття рішення про впровадження науково-технічної розробки та виведення її на ринок (тобто її комерціалізації) цього недостатньо.

Для остаточного прийняття рішення з цього питання необхідно розраху- вати внутрішню економічну дохідність $E_в$, або показник внутрішньої норми дохідності *(IRR, Internal Rate of Return)* вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну

внутрішню економічну дохідність, нижче якої інвестиції в будь-яку нау- ково-технічну розробку вкладати буде економічно недоцільно.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки, розраховується за формулою:

$$\mathrm{E_в} = \sqrt[\text{Тж}]{1 + \frac{\mathrm{E_{абс}}}{PV}} - 1, \qquad (4.14)$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, грн;

PV – теперішня вартість початкових інвестицій, грн;

$T_{ж}$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впро- вадження, роки.

$$\mathrm{E_в} = \sqrt[5]{1 + \frac{8545}{7000}} - 1 = 1.041$$

Далі визначають бар'єрну ставку дисконтування $\tau_{мін}$, тобто мінімальну внутрішню економічну дохідність інвестицій, нижче якої кошти у впрова- дження науково-технічної розробки та її комерціалізацію вкладатися не бу- дуть. Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$ визначається за формулою:

$$\tau_{\text{мін}} = d + f, \qquad (4.15)$$

де d – середньозважена ставка за депозитними операціями в комерцій- них банках; в 2020 році в Україні $d = 0{,}9...0{,}12$;

f – показник, що характеризує ризикованість вкладення інвестицій; за- звичай величина $f = 0{,}05...0{,}5$, але може бути і значно вищою.

$$\tau_{\text{мін}} = 0{,}11 + 0{,}2 = 0{,}31$$

Якщо величина $E_в > \tau_{мін}$ то потенційний інвестор може бути зацікавлений у фінансуванні впровадження науково-технічної розробки та виведенні її на ринок, тобто в її комерціалізації.

Далі розраховуємо період окупності інвестицій $T_{ок}$ (*DPP*, *DiscountedPayback Period*) які можуть бути вкладені потенційним інвестором у впро- вадження та комерціалізацію науково-технічної розробки:

$$T_{ОК} = \frac{1}{E_{в}}, \quad (4.16)$$

де $E_{в}$ – внутрішня економічна дохідність вкладених інвестицій.

$$T_{ОК} = \frac{1}{1.041} = 0.96$$

Якщо $T_{ок} <$ 3-х років, то це свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

В даному розділі було показана новизна даного проетку а також його окупність протягом певного періоду часу.

ВИСНОВКИ

Розглянуто основні поняття системи Honeypot та системи виявлення атак. Проаналізовано основні методи адаптовані та реальні і розгялнуті види Honeyd та Honeynet. Також було показані аналоги Honeypot та проаналізовані системи виялвлення аткак. Поставлено завдання на розробку системи виялення атак з використанням Honeypot, базуючись на проаналізованих джерелах.

В другому розділі були створені методи та алгоритми для роботи сисстеми виялення атак. Також були розроблені різні методи для різних частин роботи системи.

В дані роботі було покращено систеим виявлення атак та було створений метод який використовує Honeypot. Даний метод дозволяв зменшити недоліки існуючих методів та систем побудованих на цих методах.

В третьому розділі було обгрунтовано вибір мови програмування та показана розробка засобу також було продемонстровано роботу методу системи виявлення атак з допомогою Honeypot. Також було розроблено та протестований засіб який використовує метод системи виявдення аткак з використання Honeypot. Після тестування розробленого програмного засобу помилок у роботі не виявлено.

В економічному розділу було проаналізовано та прораховано отримання прибутку в 8545 грн та визначено термін окупності 1 рік.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мережні хробаки. Режим доступу: https://studfiles.net/preview/5206321/page:10/;
2. Spitzner, L. (2002), Honeypots: Tracking Hackers, 1st edition, Addison-Wesley, Boston, MA
3. Know Your Enemy: Learning about Security Threats / Honeynet Project. — NY.: Addison-Wesley Professional, 2004. — 800 с.
4. Deal R. Router Firewall Security / R. Deal. — SF. : Cisco Press, 2004. — p. 912.
5. A. Menezes, Pvan Oorschot, S. Vanstone. Handbook of Applied Cryptography
6. Argus and Infiniband URL: (ARGUS – Auditing Network Activity) // QoSient — Режим доступу: http://www.qosient.com/argus;
7. Balas E. Honeynet data analysis: A technique for correlating sebek and network data / E. Balas // Workshop on Information Assurance and Security US Military Academy, West Point, NY. — IEEE, 2004.
8. Honeypot vs Deception на прикладі Xello Режим доступу: URL: https://habr.com/ru/company/tssolution/blog/522374/
9. Закер К. Комп'ютерні мережі. Модернізація і пошук несправностей // СПб. : БХВ - Петербург, 2001. - 1008 с.
10. Програмні продукти для комп'ютерного моніторингу — принципи роботи, основні особливості та приклади використання Режим доступу: URL: https://www.keylogger.org/keylogger.html
11. Масштабованість HONEYPOT-рішення для забезпечення безпеки в корпоративних мережах URL: https://cyberleninka.ru/article/n/masshtabiruemoe-honeypot-reshenie-dlya-obespecheniya-bezopasnosti-v-korporativnyh-setyah
12. Scarfone Karen. Guide to Intrusion Detection and Prevention Systems (IDPS) — 2007. — 127 p
13. Mattord Verma. Principles of Information Security — 2008. — 300 p.

14. Jackson Kathleen. A Phased Approach to Network Intrusion Detection — 1991. – – 30 p

15. Жакун Г.А. Система виявлення атак з використанням honeypot. Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 62)" / Збірник тез доповідей: випуск 62 (м. Тернопіль, 12 жовтня 2021 р.). с. 24-26. URL: http://www.konferenciaonline.org.ua/ua/article/id-252/
16. Жакун Г.А. Штучне середовище системи виявлення атак з використанням honeypot. Молодь в науці: дослідження, проблеми, перспективи (МН-2022). Вінницький національний технічний університетhttps режим доступу: //conferences.vntu.edu.ua/index.php/mn/mn2022/paper/view/14078

Додатки

Додаток А

Технічне завдання

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Затверджую
д. т. н., проф.
_____ В. А. Лужецький
«____» _____ 2021 р.

ТЕХНІЧНЕ ЗАВДАННЯ
на виконання магістерської кваліфікційної роботи

на тему: «Система виявлення атак з використанням Honeypot.»
08-20.МКР.004.00.000 ТЗ

Керівник магістерської кваліфікаційної роботи
к.т.н., ст. викл. каф. ЗІ
_____ В. В. Лукічов

Розробив студент групи 1БС-20м
_____ Г. А. Жакун

Вінниця 2021

1 Підстави для проведення робіт

Робота проводиться на підставі наказу ректора ВНТУ від 24 вересня 2021 року № 277.

Дата початку роботи 01.09.21 р.

Дата закінчення роботи 20.11.21 р.

2 Мета та призначення МКР

Мета – магістерської кваліфікаційної роботи є покращити захист сисстеми виялення атак з використання Honeypot.

Об’єктом дослідження є процес захисту інформації шляхом використання Honeypot.

Предметом дослідження є системи виявлення атак та дослідження можливих атак з використанням Honeypot.

Актуальність теми. На даний час доволі часто може бути проблема авторизації та виявлення атак. Для цього використовують стандартні системи виявлення атак та стандартний захист від різних спроб підбора даних. Але більшість таких заходів спрямовані тільки на окремі групи атак, прикладом може бути Firewall або пасивні сисстеми виявлення атак. Тому актуальною задачею є розробка спеціального методу та системи, які дадуть змогу відслідкувати атаки та дослідитити різні види атак.

3 Вихідні дані для проведення МКР

МКР проводиться вперше і вихідними даними для проведення МКР є:

3.1 Deal R. Router Firewall Security / R. Deal. — SF. : Cisco Press, 2004. — p. 912

3.2 A. Menezes, Pvan Oorschot, S. Vanstone. Handbook of Applied Cryptography

3.3 Програмні продукти для комп'ютерного моніторингу — принципи роботи, основні особливості та приклади використання Режим доступу: URL: https://www.keylogger.org/keylogger.html

3.4 Масштабованість HONEYPOT-рішення для забезпечення безпеки в корпоративних мережах Режим доступу: URL: https://cyberleninka.ru/article/n/masshtabiruemoe-honeypot-reshenie-dlya-obespecheniya-bezopasnosti-v-korporativnyh-setyah

3.5 Закер К. Комп'ютерні мережі. Модернізація і пошук несправностей // СПб. : БХВ - Петербург, 2001. - 1008 с.

4 Виконавці МКР

Студент групи 1 БС-20 м Жакун Геннадій Андрійович

5 Вимоги до виконання МКР

Для покращення системи виявдення атак за рахунок виявлення різних атак удосконаленими методами Honeypot необхідно розв’язати такі задачі:

- науково-досліджене обґрунтування необхідності дослідження та розробки нового методу системи виявлення атак;
- аналіз наукової літератури щодо існуючих методів та засобів сисмем виявлення атак та Honeypot з метою виявлення потенційних вразливосте сисстем виявлення атак nj Honeypot;
- удосконалення методу системи виявлення атак;
- розробка алгоритмівфункцій роботи системи;
- розробка програмного засобу згідно розроблених алгоритмів функціонування для демонтсрацій роботи;

6 Вимоги до супровідної документації

Графічна і текстова документація повинна відповідати діючим стандартам України – ДСТУ 3008:2015.

7 Етапи МКР

Робота з теми виконується у 8 етапів.

Зміст етапу	Початок - закінчення	Очікувані результати	Звітна документація
Аналіз завдання. Вступ	01.09.2021 – 04.09.2021	Вступ	Чернетка вступу
Розробка технічного завдання	05.09.2021 – 15.09.2021	Технічне завдання	Проект технічного завдання
Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	16.09.2021 – 22.09.2021	Аналіз існуючих аналогів. Вибір напрямку дослідження Аналіз відомих методів. Постановка завдання	Чернетка першого розділу
Покращення методів системи виявлення аткак	23.09.2021 – 04.10.2021	Поеращення системи виялення аткак з використанням Honeypot.	Чернетка другого розділу
Експериментальні дослідження	05.10.2021 – 14.11.2021	Програмний засіб, який реалізує розроблювані методи	Чернетка третього розділу
Розробка економічного розділу	15.11.2021 – 24.11.2021	Економічні показники дослідження	Чернетка з економічного розділу
Оформлення пояснювальної записки	25.11.2021 – 30.11.2021	Пояснювальна записка	Пояснювальна записка

8 Очікувані результати та порядок реалізації МКР

Передбачається розробка нових покращено існуючих методів які спрямовані на захист від атак. Заплановане створення програмного засобу, демонтсрує роботу методу.

9 Матеріали які подаються після закінчення МКР

По завершенню роботи подається пояснювальна записка та ілюстративна частина.

10 Порядок приймання МКР та її етапів

Апробація на науково-технічних конференціях та семінарах. Результати роботи будуть розглядатися на засіданні ДЕК із захисту магістерських кваліфікаційних робіт.
Попередній захист та доопрацювання МКР – 3-4 грудня 2021 р.
Представлення МКР до захисту – 20 грудня 2021 р.
Захист МКР – 21.12.21.

11 Вимоги до розроблення документації

Документація буде виконуватись за допомогою комп’ютерного набору у відповідності вимог ДСТУ 3008:2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання».

12 Вимоги щодо технічного захисту інформації з обмеженим доступом

У зв’язку з тим, що дана робота не містить інформації, що потребує захисту у відповідності до законів України, заходи з її технічного захисту не передбачаються.

Додаток Б

Текс програми.

Код класа Tcpmodule

```
namespace TcpSendFiles
{

    class ReceiveEventArgs : EventArgs
    {
        private SendInfo _sendinfo;

        public ReceiveEventArgs(SendInfo sendinfo)
        {
            _sendinfo = sendinfo;
        }

        public SendInfo sendInfo
        {
            get { return _sendinfo; }
        }

    }



    class TcpModule
    {


        public delegate void AcceptEventHandler(object sender);
        public event AcceptEventHandler Accept;


        public delegate void ConnectedEventHandler(object sender,
string result);
        public event ConnectedEventHandler Connected;
```

```
        public   delegate   void   DisconnectedEventHandler(object
sender, string result);
        public event DisconnectedEventHandler Disconnected;

        public  delegate  void  ReceiveEventHandler(object  sender,
ReceiveEventArgs e);
        public event ReceiveEventHandler Receive;




        public Form1 Parent;


        private TcpListener _tcpListener;

        private TcpClientData _tcpClient;


        public enum Mode { indeterminately, Server, Client};

        public Mode modeNetwork;



        #region Интерфейсная часть TCP модуля


        public void StartServer()
        {
            if (modeNetwork == Mode.indeterminately)
            {
                try
                {
                    _tcpListener  =  new  TcpListener(IPAddress.Any,
15000);
                    _tcpListener.Start();

_tcpListener.BeginAcceptTcpClient(AcceptCallback, _tcpListener);
                    modeNetwork = Mode.Server;
```

```
                Parent.ChangeBackColor(Color.Plum);
            }
            catch (Exception e)
            {
                _tcpListener = null;
                Parent.ShowReceiveMessage(e.Message);
            }
        }
        else
        {
            SoundError();
        }
    }



    public void StopServer()
    {
        if (modeNetwork == Mode.Server)
        {
            modeNetwork = Mode.indeterminately;
            _tcpListener.Stop();
            _tcpListener = null;


            DeleteClient(_tcpClient);



Parent.ChangeBackColor(Color.FromKnownColor(KnownColor.Control));
        }
    }



    public void ConnectClient(string ipserver)
    {
        if (modeNetwork == Mode.indeterminately)
        {
            _tcpClient = new TcpClientData();
```

```
_tcpClient.tcpClient.BeginConnect(IPAddress.Parse(ipserver), 15000,
new AsyncCallback(ConnectCallback), _tcpClient);

                modeNetwork = Mode.Client;
            }
            else
            {
                SoundError();
            }
        }



        public void DisconnectClient()
        {
            if (modeNetwork == Mode.Client)
            {
                modeNetwork = Mode.indeterminately;
                DeleteClient(_tcpClient);

Parent.ChangeBackColor(Color.FromKnownColor(KnownColor.Control));
            }
        }



        private void DeleteClient(TcpClientData mtc)
        {
            if (mtc != null && mtc.tcpClient.Connected == true)
            {
                mtc.tcpClient.GetStream().Close();
                mtc.tcpClient.Close();
            }
        }



        private byte[] GetHeader(int length)
        {
            string header = length.ToString();
            if (header.Length < 9)
```

```
            {
                string zeros = null;
                for (int i = 0; i < (9 - header.Length); i++)
                {
                    zeros += "0";
                }
                header = zeros + header;
            }

            byte[] byteheader = Encoding.Default.GetBytes(header);


            return byteheader;
        }



        public string SendFileName = null;
        public void SendData()
        {


            SendInfo si = new SendInfo();
            si.message = Parent.meddaga;



            if   (String.IsNullOrEmpty(si.message)   ==   true   &&
String.IsNullOrEmpty(SendFileName) == true) return;

            if (SendFileName != null)
            {
                FileInfo fi = new FileInfo(SendFileName);
                if (fi.Exists == true)
                {
                    si.filesize = (int)fi.Length;
                    si.filename = fi.Name;
                }
                fi = null;
            }

            BinaryFormatter bf = new BinaryFormatter();
```

```
            MemoryStream ms = new MemoryStream();
            bf.Serialize(ms, si);
            ms.Position = 0;
            byte[] infobuffer = new byte[ms.Length];
            int r = ms.Read(infobuffer, 0, infobuffer.Length);
            ms.Close();

            byte[] header = GetHeader(infobuffer.Length);
            byte[]    total    =    new    byte[header.Length    +
infobuffer.Length + si.filesize];

            Buffer.BlockCopy(header, 0, total, 0, header.Length);
            Buffer.BlockCopy(infobuffer,  0,  total,  header.Length,
infobuffer.Length);


            if (si.filesize > 0)
            {
                FileStream   fs   =   new   FileStream(SendFileName,
FileMode.Open, FileAccess.Read);
                fs.Read(total,  header.Length  +  infobuffer.Length,
si.filesize);
                fs.Close();
                fs = null;
            }


            NetworkStream ns = _tcpClient.tcpClient.GetStream();

            ns.Write(total, 0, total.Length);


            header = null;
            infobuffer = null;
            total = null;
            SendFileName = null;

            GC.Collect();
            GC.WaitForPendingFinalizers();

            Parent.ShowReceiveMessage("Данные                    успешно
отправлены!");
```

```
        }


        public void CloseSocket()
        {
            StopServer();
            DisconnectClient();
        }


        private void SoundError()
        {
            Console.Beep(3000, 30);
            Console.Beep(1000, 30);
        }

        #endregion


        #region Асинхронные методы сетевой работы TCP модуля



        public void AcceptCallback(IAsyncResult ar)
        {
            if (modeNetwork == Mode.indeterminately) return;

            TcpListener listener = (TcpListener)ar.AsyncState;
            try
            {
                _tcpClient = new TcpClientData();
                _tcpClient.tcpClient                                    =
listener.EndAcceptTcpClient(ar);



                NetworkStream                ns                 =
_tcpClient.tcpClient.GetStream();
                _tcpClient.buffer = new byte[global.LENGTHHEADER];
```

```
                ns.BeginRead(_tcpClient.buffer,                    0,
_tcpClient.buffer.Length,     new     AsyncCallback(ReadCallback),
_tcpClient);



                listener.BeginAcceptTcpClient(AcceptCallback,
listener);


                if (Accept != null)
                {
                    Accept.BeginInvoke(this, null, null);
                }
            }
            catch
            {

                SoundError();
            }
        }



        public void ConnectCallback(IAsyncResult ar)
        {
            string result = "Подключение успешно!";
            try
            {

                TcpClientData              myTcpClient              =
(TcpClientData)ar.AsyncState;
                NetworkStream                  ns                   =
myTcpClient.tcpClient.GetStream();
                myTcpClient.tcpClient.EndConnect(ar);


                myTcpClient.buffer = new byte[global.LENGTHHEADER];
                ns.BeginRead(myTcpClient.buffer,                   0,
myTcpClient.buffer.Length,     new     AsyncCallback(ReadCallback),
myTcpClient);
                Parent.ChangeBackColor(Color.Goldenrod);
```

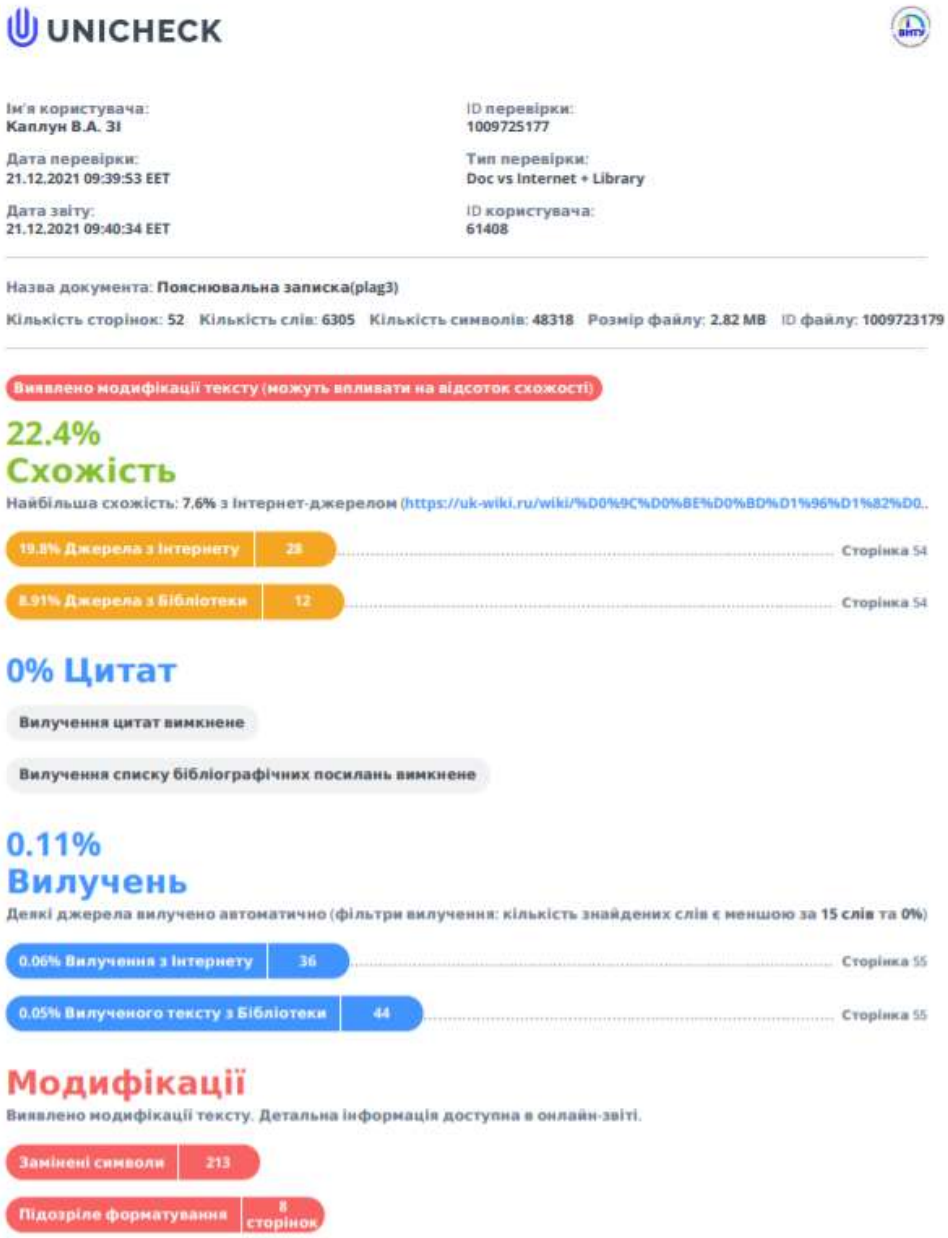
```
            }
            catch (Exception e)
            {

                DisconnectClient();
                result = "Подключение провалено!";
                SoundError();
            }


            if (Connected != null)
                Connected.BeginInvoke(this, result, null, null);
        }




        public void ReadCallback(IAsyncResult ar)
        {
            if (modeNetwork == Mode.indeterminately) return;

            TcpClientData               myTcpClient                =
(TcpClientData)ar.AsyncState;

            try
            {
                NetworkStream                  ns                  =
myTcpClient.tcpClient.GetStream();

                int r = ns.EndRead(ar);

                if (r > 0)
                {

                    string                  header                 =
Encoding.Default.GetString(myTcpClient.buffer);
                    int leninfo = int.Parse(header);


                    MemoryStream ms = new MemoryStream(leninfo);
                    byte[] temp = new byte[leninfo];
```

```
                    r = ns.Read(temp, 0, temp.Length);
                    ms.Write(temp, 0, r);
                    BinaryFormatter bf = new BinaryFormatter();
                    ms.Position = 0;
                    SendInfo sc = (SendInfo)bf.Deserialize(ms);
                    ms.Close();
                    if (sc.filesize > 0)
                    {

                        FileStream fs = new FileStream(sc.filename,
FileMode.Create,     FileAccess.ReadWrite,     FileShare.ReadWrite,
sc.filesize);
                        do
                        {
                            temp = new byte[global.MAXBUFFER];
                            r = ns.Read(temp, 0, temp.Length);

                            fs.Write(temp, 0, r);

                            if (fs.Length == sc.filesize)
                            {
                                fs.Close();
                                fs = null;
                                break;
                            }
                        }
                        while (r > 0);
                        temp = null;
                        GC.Collect();
                        GC.WaitForPendingFinalizers();
                    }


                    if (Receive != null)
                        Receive(this, new ReceiveEventArgs(sc));

                    myTcpClient.buffer            =            new
byte[global.LENGTHHEADER];
                    ns.BeginRead(myTcpClient.buffer,            0,
myTcpClient.buffer.Length,     new     AsyncCallback(ReadCallback),
myTcpClient);
```

```
                }
                else
                {
                    DeleteClient(myTcpClient);

                    if (Disconnected != null)
                        Disconnected.BeginInvoke(this, "користувач
відключився!", null, null);
                }
            }
            catch (Exception e)
            {
                DeleteClient(myTcpClient);
              if (Disconnected != null)
                    Disconnected.BeginInvoke(this, "Клієнт втратив
зв'язок", null, null);
                SoundError();
            }
        }
        #endregion
    }




    class TcpClientData
    {
        public TcpClient tcpClient = new TcpClient();

        public byte[] buffer = null;

        public TcpClientData()
        {
            tcpClient.ReceiveBufferSize = global.MAXBUFFER;
        }

    [Serializable]
    class SendInfo
    {
        public string message;
        public string filename;
        public int filesize;    }}
```

Додаток В

Протокол перевірки на наявність плагіату



UNICHECK

Ім'я користувача:
Каплун В.А. ЗІ

ID перевірки:
1009725177

Дата перевірки:
21.12.2021 09:39:53 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
21.12.2021 09:40:34 EET

ID користувача:
61408

Назва документа: Пояснювальна записка(plag3)

Кількість сторінок: 52 Кількість слів: 6305 Кількість символів: 48318 Розмір файлу: 2.82 MB ID файлу: 1009723179

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

22.4%
Схожість

Найбільша схожість: 7.6% з Інтернет-джерелом (https://uk-wiki.ru/wiki/%D0%9C%D0%BE%D0%BD%D1%96%D1%82%D0..

19.8% Джерела з Інтернету 28 Сторінка 54

8.91% Джерела з Бібліотеки 12 Сторінка 54

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0.11%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 15 слів та 0%)

0.06% Вилучення з Інтернету 36 Сторінка 55

0.05% Вилученого тексту з Бібліотеки 44 Сторінка 55

Модифікації

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

Замінені символи 213

Підозріле форматування 8 сторінок

ІЛЮСТРАТИВНА ЧАСТИНА

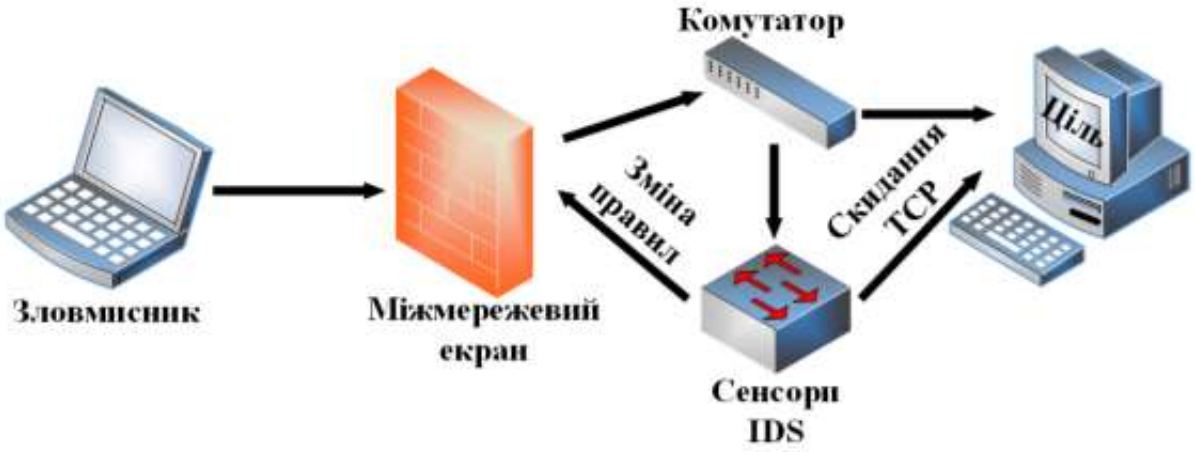
СИСТЕМА ВИЯВЛЕННЯ АТАК З ВИКОРИСТАННЯМ HONEYPOT.

Огляд Honeypot по областям застосування

Fake Honeypot	Honeypot	Server	✗	✓
Honeyentries	Table, data set	Database	✓	✗
MTD	Topo., net. interf., memory, arch.	Versatile	✓	✓
Honeyword	Password	Authentica-tion	✓	✗
Honeyaccount	User account	Authentica-tion	✓	✗
Honeyfile	(Cloud-)File	File system	✓	✓
Honeypatch	Vulnerability	Server	✓	✓
–	Memory	Server	✓	✗
–	Metadata	File	✓	✗
HoneyURL	URL	File	✗	✓
Honeymail	E-Mail adress	File	✗	✓
Honeypeople	Social network profile	File	✗	✗
Honeyport	Network port	Server	✗	✓
Decep. web server	Error codes, Robot.txt	Server	✗	✓
OS interf.	System call	Server	✓	✗

					08-20.МКР.004.00.000 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Жакун Г. А.			Система виявлення атак з використанням Honeypot.	Літ.	Арк. 1 / Аркушів 1
Перевір.		Лукічов В. В.					
Рецензент		Азарова А. О.				ВНТУ гр. 1БС-20м	
Н. Контр.		Лукічов В. В.					
Затверд.		Лужецький В. А.					

Схема роботи СВВ

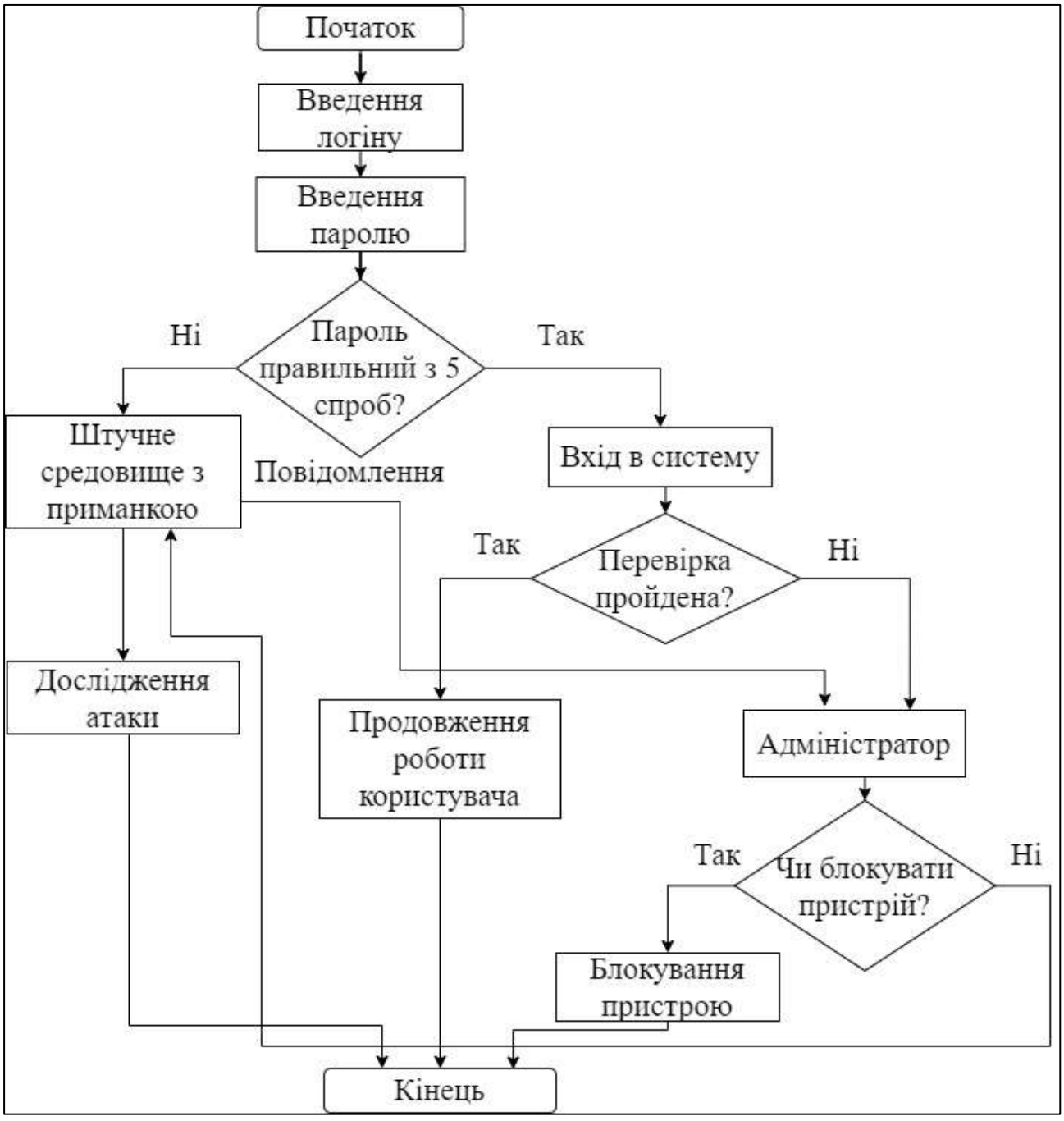


					08-20.МКР.004.00.000 І42			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Жакун Г. А.			Система виявлення атак з використанням Honeypot.	Літ.	Арк.	Аркушів
Перевір.		Лукічов В. В.					1	1
Рецензент		Азарова А. О.				ВНТУ гр. 1БС-20м		
Н. Контр.		Лукічов В. В.						
Затверд.		Лужецький В. А.						

Схема роботи СЗВ

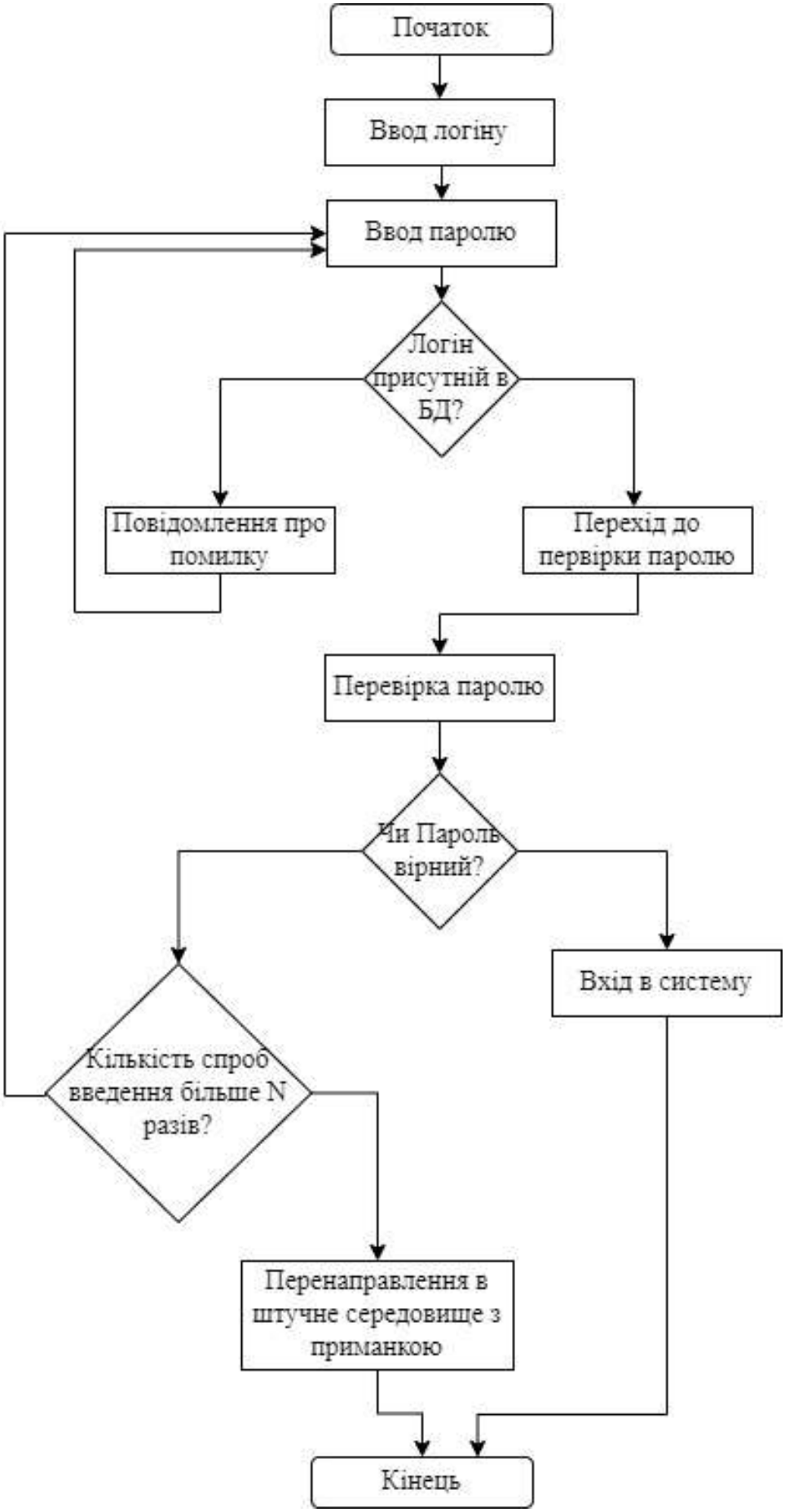
					08-20.МКР.004.00.000 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Жакун Г. А.			Система виявлення атак з використанням Honeypot.	Літ.	Арк. 1 / Аркушів 1
Перевір.		Лукічов В. В.					
Рецензент		Азарова А. О.				ВНТУ гр. 1БС-20м	
Н. Контр.		Лукічов В. В.					
Затверд.		Лужецький В. А.					

Блок-схема виявлення атака з використанням Honeypot



					08-20.МКР.004.00.000 І44		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Жакун Г. А.			Система виявлення атак з використанням Honeypot.	Літ.	Арк. 1 / Аркушів 1
Перевір.		Лукічов В. В.					
Рецензент		Азарова А. О.				ВНТУ гр. 1БС-20м	
Н. Контр.		Лукічов В. В.					
Затверд.		Лужецький В. А.					

Блок-схема вводу даних та розподілення запит входу



					08-20.МКР.004.00.000 145			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Жакун Г. А.			Система виявлення атак з використанням Honeypot.	Літ.	Арк.	Аркушів
Перевір.		Лукічов В. В.					1	1
Рецензент		Азарова А. О.				ВНТУ гр. 1БС-20м		
Н. Контр.		Лукічов В. В.						
Затверд.		Лужецький В. А.						