Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інформаційних радіотехнологій і технічного захисту інформації

Кафедра Радіотехнологій інформаційно-комунікаційних систем

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (мігістерський)

Дослідження діяльності хакерів щодо побудови системи кібербезпеки
(тема)

Виконав:
студент _2_ курсу, групи АПСм-22-1
Клочко С.Р.
(прізвище, ініціали)

Спеціальність 126 Інформаційні системи та технології
(код і повна назва спеціальності)
Тип програми освітньо-професійна

Освітня програма
Архітектурне проектування інформаційних систем
(повна назва освітньої програми)

Керівник професор Кузьомін О.Я..
(посада, прізвище, ініціали)

Допускається до захисту

В.о.зав. кафедри _____ Зарудний О. А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет_ Інформаційних радіотехнологій і технічного захисту інформації _

Кафедра Радіотехнологій інформаційно-комунікаційних систем

Рівень вищої освіти другий (магістерський)

Спеціальність 126 Інформаційні системи та технології

Тип програми освітньо-професійна

Освітня програма Архітектурне проєктування інформаційних систем

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«____» 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Клочко Сергію Романовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження діяльності хакерів щодо побудови системи кібербезпеки

затверджена наказом університету від 3 жовтня 2023 р. № 1295Ст_

2. Термін подання студентом роботи до екзаменаційної комісії 24 січня 2024 р.

3. Вихідні дані до роботи
_Провести аналіз діяльності хакерів, методи їх роботи, провести аналіз_існуючих методів протидії, їх переваги та недоліки,_визначити технології моделювання діяльності хакерів та можливості застосування моделей щодо побудови системи кібербезпеки,

4. Перелік питань, що потрібно опрацювати в роботі Вступ
_1. Сучасні виклики до кібербезпеки та методи боротьби з хакерами
_2._Огляд існуючих методів моделювання кіберзагроз та дослідження відомих прикладів шкідливого програмного забезпечення
3. Опис програмного забезпечення для моделювання діяльності хакерів
4. Моделювання діяльності хакерів з використання мережі Петрі
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____

Слайди у форматі Power Point(назва роботи, вступ, необхідний функціонал, проекту-вання веб додатку, технології реалізації, висновки)

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантівзгідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Основна частина	професор Кузьомін О.Я.		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів	Примітка
1	Ознайомлення із завданням.Уточнення тз	07.10.2023	Виконано
2	Підбір літератури за темою роботи	10.10.2023 – 15.10.2023	Виконано
3	Дослідження сучасних методів боротьби з	20.10.2023 – 29.10.2023	Виконано
	кіберзагрозами та актуальність такої розробки		
4	Дослідженя відомих вірусів та методів їх роботи	29.10.2023 – 09.11.2023	Виконано
5	Ознайомлення з програмним забезпеченням	12.10.2023 – 20.11.2022	Виконано
	PTRSIM та Петрі-об'єктивного моделювання		
6	Моделювання діяльності хакерів з використаням	21.11.2023 – 27.12.2023	Виконано
	Мережі Петрі		
7	Створення презентації, підготовка до захисту	28.12.2023 – 24.01.2024	Виконано

Дата видачі завдання 6_ жовтня 2023р.

Студент _____
(підпис)

Керівник роботи _____ професор Кузьомін О.Я.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 71с., 34 рис., 4 табл. , 15 джерел, 2 додатка.

КІБЕРЗЛОЧИННІСТЬ, ХАКЕРИ, ПРОТИДІЯ

Актуальність теми: з кожним роком зростає вплив та інтегрованість інформаційних технології на життя як звичайних людей так і великих компаній, а разом з цим зростає і рівень злочинності в кіберпросторі. Лише за 2022 в Україні звичайні громадяни зазнали збитків на один мільярд гривень в результаті діяльності хакерів, окрім цього кіберзлочинність може використовується у вигляді хакерських атак на державні підприємства, що в черговий раз підкреслює важливість розуміння можливостей хакерів та методів протидії.

Мета та завдання дипломної роботи: дослідження методів роботи хакерів, існуючих видів атак та методик протидії, серед яких основну увагу буде приділено моделюванню їх діяльності.

THE ABSTRACT

Explanatory note: 71 p., 34 fig, 4 tables, 15 sources, 2 app.

CYBERCRIME, HACKERS, COUNTERMEASURES

The relevance of the topic: every year the influence and integration of information technology on the lives of both ordinary people and large companies increases, and along with this, the level of crime in cyberspace also increases. Only in 2022 in Ukraine, ordinary citizens suffered losses of one billion hryvnias as a result of the activities of hackers, in addition, cybercrime can be used in the form of hacker attacks on state-owned enterprises, which once again emphasizes the importance of understanding the capabilities of hackers and methods of attack.

The aim and objectives of the thesis: study of hackers' work methods, existing types of attacks and countermeasures, among which the main attention will be paid to the modeling of their activities.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАК ТА СКОРОЧЕНЬ

SIEM – Security Information and Event Management;

SDL – Security Development Lifecycle;

IDS – Intrusion Detection Systems;

VPN – Virtual Private Network.

UML – Unified Modeling Language

ІС – Інформаційна Система

ВСТУП

В сучасному світі повідомлення про кіберзлочини вже стали не вважаються чимось незвичним, навпаки, щомісяця можна зустріти дійсно гучні новини про черговий акт крадіжки в мережі інтернет. Із зростаючим рівнем діджиталізації росте і кількість злочинів в інтернет-просторі. Зазвичай діяльність хакерів пов’язана із незаконним збагаченням за рахунок інших людей чи установ, це можуть бути як звичайні обчищення вашого банківського рахунку за рахунок соціальної інженерії, вірусних розсилок чи інших шкідливих застосунків. Варто зазначити що більшість з таких зловмисників не становлять реальної загрози фірмам чи установам з мінімальним рівнем захисту, інша ж справа коли мова заходить про організовані хакерські угрупування, основною ціллю яких є полювання на дані з серверів великих компаній чи навіть державних установ. За останні кілька років ми бачили багато прикладів організованих атак на державні установи тієї чи іншої країни які прямо було проспонсовані та зроблені на замовлення уряду зацікавленної в таких діях країни. Такі події підводять нас до висновку що важливість захисту інформації в наш час є надважливою.

Жертвами шкідливого впливу у мережі інтернет, серед пристроїв, зараз, за статистикою, може налічувати кожен четвертий пристрій, котрий може бути ураженим, чи навпаки, вже відновлений після інфікування. Під шкідливим впливом розуміють наявність стороннього програмного забезпечення, котре має певну дію на стан приладу або створює нові процеси у операційній системі приладу.

Одним методів протидії хакерським діям є процес моделювання їх діяльності у визначеній системі, це може дозволити виявити слабкі місця в системі захисту інформації, а також звертає увагу на непримітні можливості для шкідливого впливу на інформаційну систему. В дипломній роботі будуть використані моделі створені завдяки Петрі-об’єктивному моделюванню.

Петрі-об'єктне моделювання є технологією імітаційного моделювання систем, що ґрунтується на стохастичних мережах Петрі та надає можливість створювати моделі складних систем з конструктивних елементів. На відміну від інших відомих технологій імітаційного моделювання, Петрі-об'єктна технологія ґрунтується на формалізованому описі динаміки системи мережею Петрі, що дозволяє досягти найбільш абстрактного і водночас найбільш детального опису процесів функціонування системи.

1 ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ БОРОТЬБИ З КІБЕРЗАГРОЗАМИ

1.1 Кібербезпека в сучасності

Кібербезпека – це захист підключених до Інтернету пристроїв і служб від зловмисних атак хакерів, спамерів і кіберзлочинців. Ця практика використовується компаніями для захисту від фішингових схем, атак програм-вимагачів, крадіжки особистих даних, витоку даних і фінансових втрат.

Озирніться навколо сучасного світу, і ви побачите, що повсякденне життя більше, ніж будь-коли раніше, залежить від технологій. Переваги цієї тенденції варіюються від майже миттєвого доступу до інформації в Інтернеті до сучасних зручностей, які забезпечують технологія автоматизації розумного дому та такі концепції, як Інтернет речей.

З огляду на стільки хорошого, що приносить технологія, важко повірити, що за кожним пристроєм і платформою ховаються потенційні загрози. Проте, незважаючи на райдужне сприйняття суспільством сучасних досягнень, загрози кібербезпеці, які представляють сучасні технології, є реальною небезпекою.

Постійне зростання кіберзлочинності підкреслює недоліки пристроїв і послуг, від яких ми звикли залежати. Це занепокоєння змушує нас запитати, що таке кібербезпека, чому вона важлива та що про неї варто дізнатися.

Організації стають більш обізнаними з інформацією та пов'язаними технологіями практично в кожній функції, особливо в роботі над інноваціями та здобутті конкурентної переваги. Корпоративні інформаційні та технологічні сервіси вразливі перед різними загрозами безпеки в сучасному інформаційному середовищі, включаючи витік конфіденційних даних та тривалі порушення у доступі до електронної пошти та Інтернету, всі ці чинники значно впливають на безперервність бізнесу. Організація повинна впроваджувати стратегію інформаційної безпеки, встановлюючи всесвітню

систему, яка дозволяє розробляти, інституціоналізувати, оцінювати та вдосконалювати програму інформаційної безпеки для вирішення цих загроз безпеки. Зокрема, стратегія інформаційної безпеки повинна підтримувати загальні стратегічні плани організації, і її зміст повинен бути відстежуваний до цих джерел вищого рівня. Навіть якщо більшість організацій використовують "базові" заходи безпеки, кількість випадків безпеки зростає.

Згідно з дослідженням, понад 60% підприємств використовують технічні контрзаходи із забезпечення інформаційної безпеки, такі як антивірусне програмне забезпечення, брандмауери, антишпигунське програмне забезпечення, віртуальні приватні мережі (VPN), вразливості/управління виправленнями, шифрування даних у транзиті та системи виявлення вторгнень. Зазначається, що організації постійно стають об'єктом цілеспрямованих атак. Ці ж самі дослідження показують, що загрози безпеки зростають через збільшення внутрішніх та зовнішніх загроз. Як результат, управління безпекою стає більш викликаючим завданням. Підприємства повинні використовувати стратегії для спрямування своїх зусиль у сфері безпеки та раціонального використання обмежених ресурсів у цьому середовищі. Однак одна система може бути недостатньою [1]. Автори аргументують, що для забезпечення ефективності заходів безпеки та дотримання політик безпеки, підприємства повинні використовувати кілька стратегій інформаційної безпеки. Більшість літератури фокусується на операційних аспектах інформаційної безпеки, зокрема на засобах безпеки та їх впровадженні для "попередження" кібератак на підприємства. Однак, окрім запобігання, в літературі було запропоновано кілька стратегій безпеки, таких як виявлення, стримування та обман. Проте, досліджень у сфері, які б визначали, які стратегії безпеки використовують організації для вирішення різних загроз безпеки та як вони впроваджуються, було проведено невдостатньо. Менеджери з безпеки в основному ігнорували ризики безпеки підприємств. Загалом плани впроваджувалися ад-гок, а не як частина систематичного та запланованого підходу до управління ризиками.

Для боротьби з кіберзлочинцями спеціалісти використовують широкий спектр моделей та підходів які розвивають та оновлюються намагаючись не відставати від можливих загроз які представлені в таблиці 1.1.

Таблиця 1.1 – Моделі та підходи для протидії кіберзлочинцям

Назва моделей та підходів	Опис
Attack Taxonomies and Frameworks:	MITRE ATT&CK: фреймворк з базою знань і моделей поведінки кіберзлочинця та різні фази життєвого циклу атки Kill Chain Model: допомогає визначити етапи кібератаки і захиститися від неї
Behavioral and Anomaly Detection:	Intrusion Detection Systems (IDS): відстеження мережового трафіка і системних журналів User and Entity Behavior Analytics (UEBA): використання машинного навчання для виявлення незвичної поведінки в структурі організації
Machine Learning-Based Approaches:	Supervised Learning: класифікування даних на звичайні та шкідливі за допомогою моделей машинног онавчання Unsupervised Learning: використання моделей навчання без нагляду для виявлення аномалій Deep Learning: застосування нейромереж для виявлення зловмисного програмного забезпечення та спроб вторгнення
Threat Intelligence Models:	STIX/TAXII: стандарти для обміну інформації про загрози між організаціями Threat Intelligence Feeds: підписка на канали які надають інформацію про загрози кібербезпеці
HoneyPots and Deception Technologies:	Розгортання приманок для зловмисників з метою їх подальшого вивчення
SIEM (Security Information and Event Management):	Системи SIEM збирають і аналізують пов’язані з безпекою дані з різних джерел, щоб виявити інциденти та загрози безпеці.
Zero Trust Security Model:	Модель нульової довіри передбачає існування загроз як ззовні так і всередині моделі, та наголошує на обмеженні доступу до різних рівнів системи та постіних перевірках

Продовження таблиці 1.1

Назва моделей та підходів	Опис
Cyber Threat Hunting:	Мисливці за загрозами активно шукають ознаки зловмисної діяльності в мережі та системах організації.
Incident Response Models:	Дотримування структурних моделей реагування на інциденти кіберзагроз для більш ефективного реагування
Vulnerability Management Models:	Впровадження процесів керування загрозами такі як CVE
Adaptive Security Architecture:	Розробляйте адаптивні архітектури безпеки, які можуть динамічно коригувати заходи безпеки на основі нових загроз і ризиків.
Quantitative Risk Assessment Models:	Використання моделей таких як FAIR для кількісної оцінки ризиків безпеки
Cyber Threat Intelligence Sharing Platforms:	Використання онлайн-платформ як ISACдля обміну інформацією та співпраці між організаціями
Blockchain for Security:	Дослідження можливостівикористання технології блокчейн для підвищення безпеки в таких сферах як: керування ідентифікацією та захист ланцюгів поставок
AI and Machine Learning for Threat Detection:	Впровадження моделей штучного інтелекту для виявлення загроз, розпізнавання шаблонів і аналізу даних безпеки в реальному часі
Cloud Security Models:	Впровадження спеціальних модеейі безпеки та інфраструктури для захисту даних і робочих процесів у хмарних середовищах.
Security Development Lifecycle (SDL):	Інтегруйте безпеку в процес розробки програмного забезпечення, використовуючи такі моделі, як SDL Microsoft, щоб запобігти вразливостям у програмах.
Regulatory Compliance Frameworks:	Дотримування нормативних атків та стандартів кібербезпеки що стосуються галузі розробки, такі як GDPR, HIPAA або стандартів NIST.

1.2 Проблематика кібератак

Проблематика кібератак стає все більш актуальною в сучасному цифровому світі, де комп'ютери та інтернет відіграють важливу роль у нашому житті. Ось деякі аспекти проблематики кібератак:

1) Кібербезпека: Кібератаки загрожують безпеці інформаційних систем, комп'ютерів, мереж та даних. Хакери можуть здійснювати атаки для отримання конфіденційної інформації, фінансової вигоди або просто зруйнувати важливі дані.

Кібербезпека є важливою складовою сучасного світу, де практично всі аспекти життя пов'язані з комп'ютерами та Інтернетом. Кібератаки можуть призвести до серйозних наслідків, таких як втрати фінансових активів, порушення конфіденційності особистих даних, втрата довіри споживачів до компаній і організацій, а також можуть створити загрозу національній безпеці[2]. Хакери, що ведуть атаки, можуть бути індивідуальними злочинцями, групами, державними агентствами або терористичними організаціями, і їх цілі можуть бути різноманітні - від здобуття великих сум грошей до викривлення політичних процесів або тероризування національних установ. Однією з основних проблем кібератак є їх постійна еволюція: хакери постійно шукають нові способи вторгнення в системи, що вимагає постійного вдосконалення заходів безпеки та удосконалення засобів виявлення та реагування на загрози. Необхідність забезпечення високого рівня кібербезпеки вимагає спільних зусиль від урядових організацій, приватного сектору та індивідуальних користувачів, щоб створити надійне і стійке цифрове середовище для всіх.

2) Кібершпигунство: Держави та конкуруючі компанії можуть використовувати кібератаки для збору конфіденційної інформації один від одного. Це являє собою спеціально спроектовані кібератаки з метою здобуття важливої інформації або впливу на рішення та процеси в інших країнах.

Основні аспекти кібершпигунства включають:

-кібершпигунство державами: держави можуть використовувати кібершпигунство для отримання секретної військової, політичної чи економічної інформації із зарубіжних країн. Ця інформація може бути використана для розвідки, формування політики та планування військових або політичних дій.

-кібершпигунство Конкуруючими Організаціями: Компанії і організації можуть вести кібершпигунство для отримання конфіденційної інформації про конкурентів. Це може включати в себе плани розвитку, нові технології чи договори з клієнтами.

-індустріальне кібершпигунство: країни можуть використовувати кібершпигунство для отримання технічної або індустріальної інформації, яка може бути використана для розвитку власної економіки або підвищення конкурентоспроможності на світовому ринку.

-кібершпигунство для політичних цілей: кібершпигунство може бути використане для впливу на політичні процеси в інших країнах, включаючи втручання у виборчі кампанії, розповсюдження пропаганди чи збільшення соціальних розділень.

-кібершпигунство злочинцями: кіберзлочинці можуть використовувати кібершпигунство для отримання особистої інформації про окремих осіб або компаній з метою вимагання викупу або вчинення ідентичності крадіжок.

У зв'язку зі зростанням кількості кіберзагроз, багато країн та організацій вдосконалюють свої заходи кібербезпеки для захисту від кібершпигунства, використовуючи різноманітні технічні, правові та організаційні заходи.

3) Кібертероризм: Групи терористів можуть використовувати кібератаки та інформаційні технології для здійснення терористичних актів або тиску на держави, організації чи індивідуальних осіб[3]. Кібертероризм може мати різноманітні форми та мети, і його ціль може бути політичною, економічною або суспільною.

Основні аспекти кібертероризму включають:

-державний кібертероризм: деякі держави можуть використовувати кібертероризм для впливу на політичні процеси в інших країнах, включаючи спроби втручання у виборчі кампанії, поширення пропаганди або атаки на критичну інфраструктуру.

-терористичні групи: терористичні організації можуть використовувати кібертероризм для тиску на владу, шантажування чи завдає загрози

громадській безпеці. Це може включати в себе атаки на важливі мережі, державні установи або критичні інфраструктурні об'єкти.

-ідентичністю крадіжки та розповсюдження пропаганди: Кібертерористи можуть використовувати ідентичність крадіжки для здійснення атак в інтернеті або поширення фальшивих повідомлень з метою створення паніки або заплутування громадськості.

-фінансові атаки: терористичні групи можуть здійснювати фінансові атаки на банки, фінансові установи або компанії з метою викликання економічних труднощів або втрат для економіки.

-кібервійна: в сучасному світі конфлікти можуть розгортатися не тільки на полі бою, але й у кіберпросторі. Кібервійна охоплює кібератаки, спрямовані на військові об'єкти, комунікації та інші важливі аспекти військових операцій.

-боротьба з кібертероризмом вимагає співпраці між державами, міжнародними організаціями та приватними компаніями для розробки імунітету до кіберзагроз і підвищення свідомості щодо кібербезпеки.

4) Соціальна інженерія: Хакери можуть використовувати соціальну інженерію, щоб отримати доступ до конфіденційних даних. Це може включати в себе фішинг, відправку шкідливих вірусів через електронну пошту або маніпулювання людьми для отримання доступу до систем.

Хакери використовують соціальну інженерію в різних ситуаціях, включаючи:

-фішинг: це відомий метод, коли хакери намагаються виглядати як довірена особа чи організація, щоб отримати від користувачів конфіденційні дані, такі як паролі, кредитні картки тощо. Вони можуть надсилати електронні листи або повідомлення, що видаватимуться офіційними, і просити користувачів вказати свої особисті дані або перейти за посиланням на фішинговий веб-сайт.

-відволікаючі тактики: хакери можуть відволікати увагу людей і використовувати цю відволікаючу інформацію для втручання в комп'ютерні системи або мережі.

-імітація авторитетних осіб або організацій: хакери можуть виглядати як вищий керівник компанії або технічна підтримка, щоб переконати користувачів надати доступ до конфіденційної інформації чи виконати певні дії.

-використання соціальних мереж: хакери можуть здійснювати дослідження про особистість через соціальні мережі, використовуючи зібрану інформацію для маніпулювання жертвами.

-психологічні впливи: хакери можуть використовувати психологічні впливи, такі як страх, смуток або радість, щоб спонукати жертв виконати певні дії, наприклад, відправити гроші або надати доступ до системи.

-соціальна інженерія інші людей: хакери можуть використовувати соціальну інженерію для впливу на інших людей, щоб ті отримали доступ до систем або надали інформацію.

-для захисту від соціальної інженерії, важливо бути обережним і ніколи не надавати конфіденційну інформацію або доступ до системи особам, які не можуть перевірити свою автентичність. Це також може включати навчання персоналу та користувачів визнавати підозрілі ситуації та звільняти з пам'яті особисті інформаційні дані, які можуть бути використані проти них.

5) Інтернет-приватність: Кібератаки можуть порушувати приватність користувачів Інтернету, зокрема, коли особисті дані стають доступними для несанкціонованих осіб. Ці атаки можуть призвести до витоку особистої інформації, фінансових втрат, крадіжки ідентичності, а також інших негативних наслідків.

Ось деякі типові кібератаки на інтернет-приватність:

-фішинг: атаки фішингу цілють на користувачів, намагаючись виглядати як довірені особи або організації, щоб зловити особисту інформацію. Це може включати в себе відправку підроблених електронних листів, текстових повідомлень або створення підроблених веб-сайтів, які виглядають як офіційні.

-кража кукі-файлів: зловмисники можуть вкрасти кукіси, які зберігаються в браузері користувача, щоб отримати доступ до особистих

даних, таких як паролі, сесійні ключі та інші інформаційні фрагменти.

-додатки шкідливого ПЗ: кіберзлочинці можуть створювати програми-шкідливі додатки, які можуть використовувати незахищені або вразливі платформи для здійснення атак на інтернет-приватність користувачів.

-Wi-Fi інтерцепція: атаки на відкритих або недостатньо захищених Wi-Fi мережах можуть дозволити зловмисникам перехоплювати трафік, включаючи конфіденційну інформацію, яка надсилається через мережу.

-кібершпигунство через програми-шпигуни: додатки та розширення, які виглядають безпечно, можуть збирати особисті дані користувачів та передавати їх третім особам без їхнього дозволу.

-розкриття IP-адреси: зловмисники можуть намагатися дізнатися реальну IP-адресу користувача для відстеження їхнього місцезнаходження та ідентифікації.

Для захисту від цих атак, користувачам слід використовувати надійне програмне забезпечення антивірусів та брандмауерів, уникати відкритих Wi-Fi мереж та вчасно оновлювати всі програми та операційні системи. Також важливо бути обережними щодо подібних атак і не надавати особисту інформацію на сумнівних веб-сайтах чи через електронні повідомлення.

6) Економічні збитки: Кібератаки можуть спричинити великі економічні збитки, включаючи втрати фінансових даних, зупинення бізнес-процесів та репутаційні втрати для компаній і організацій.

7) Загроза критичній інфраструктурі: Кібератаки можуть бути спрямовані на критичні інфраструктурні об'єкти, такі як електростанції, транспортні системи чи медичні установи, що може призвести до серйозних наслідків для суспільства.

Ось деякі загрози, які існують для критичної інфраструктури від кібератак:

-відключення енергопостачання: кібератаки можуть призвести до відключення електроенергії в масштабі регіону чи навіть країни, що призведе до припинення роботи важливих установок і підприємств, а також може

спричинити невідновні збитки.

-відключення комунікаційних мереж: атаки на комунікаційні інфраструктури можуть призвести до втрати зв'язку між важливими установами і службами, що може ускладнити реагування на екстрені ситуації та вплинути на координацію допомоги.

-кібератаки на фінансові установи: атаки на банки та фінансові установи можуть призвести до крадіжки грошей, фінансових даних клієнтів та загрозити стабільності фінансової системи.

-кібератаки на транспортні системи: кібератаки можуть призвести до втрати контролю над транспортними системами, такими як авіація, залізничний транспорт або автомобільні мережі, що може призвести до аварій і навіть загибелі людей.

-кібератаки на водопостачання та системи очищення води: атаки на системи водопостачання можуть забезпечити доступ до водних мереж для зловмисників, що може призвести до інтоксикації та поширення захворювань.

-кібератаки на медичні установи: кібератаки можуть вплинути на роботу медичних систем, лікарень і аптек, може заблокувати доступ до медичної інформації або навіть ускладнити проведення лікування.

-індустріальні шпигунства та саботаж: кібератаки можуть спрямовуватися на промислові об'єкти, заводи і виробництва з метою крадіжки комерційних секретів або завдання шкоди виробничим процесам.

Запобігання кібератакам на критичну інфраструктуру вимагає вдосконалення кібербезпеки, використання передових технологій захисту, навчання персоналу безпеки і впровадження ефективних стратегій реагування на інциденти[4]. Крім того, співпраця між владними органами, приватним сектором і міжнародними організаціями також є надзвичайно важливою для виявлення, протидії і відновлення від кібератак.

Ці аспекти підкреслюють важливість розвитку ефективних заходів кібербезпеки для захисту інформації та забезпечення стабільності в цифровому світі.

1.3 Фінансові збитки

Де кіберзлочинність неперевершено лідирує, це у її здатності зробити сотні мільйонів людей жертвами. Імовірно, близько двох третин людей онлайн - понад два мільярди осіб - мали свою особисту інформацію вкрадену чи скомпрометовану. Одне дослідження виявило, що 64% американців стали жертвами шахрайських операцій або втрати особистої інформації. Кіберзлочинність знаходиться на першій сторінці новин, оскільки вона стосується кожного.

Кіберзлочинність також виграє за співвідношенням ризику та вигоди. Це злочин із низьким ризиком, який надає величезні вигоди. Розумний кіберзлочинець може заробити сотні тисяч, навіть мільйони доларів і практично не має шансів бути затриманим чи ув'язненим.

Коли ми говоримо про великих кіберзлочинців, від Target до SWIFT до Equifax, жодного із винуватців досі не притягали до відповідальності. Законодавчі органи можуть бути агресивними та вправними в переслідуванні кіберзлочинців, але багато з них діють поза їхнім контролем. Це одна з причин, чому вартість кіберзлочинності продовжує зростати[5]. У 2014 році Центр зовнішньої та міжнародної стратегії (CSIS) оцінив, що кіберзлочинність коштує світову економіку майже 500 мільярдів доларів, або близько 0,7% глобального доходу. Це більше, ніж дохід усіх країн, крім кількох невеличких, що робить кіберзлочинність дуже прибутковою справою. Наші поточні оцінки свідчать, що кіберзлочинність зараз може коштувати світову економіку майже 600 мільярдів доларів, або 0,8% глобального ВВП. Причини цього зростання наступні:

-швидке впровадження нових технологій кіберзлочинцями

-збільшена кількість нових користувачів в Інтернеті (які часто є з країн з низьким рівнем доходу та слабким кіберзахистом)

-збільшена легкість в скоюванні кіберзлочину, завдяки росту кіберзлочинства-як-сервісу.

-зростаюча кількість "центрів" кіберзлочинності, до яких зараз відносяться Бразилія, Індія, Північна Корея та В'єтнам.

-зростаюча фінансова вдосконаленість серед перших кіберзлочинців, яка, серед іншого, полегшує монетизацію.

Монетизація вкрадених даних, яка завжди була проблемою для кіберзлочинців, здається, стала менш складною через вдосконалення чорних ринків кіберзлочинства та використання цифрових валют. Номери крадених кредитних карток та особисто ідентифікована інформація (PII) пропонуються для продажу великими партіями на темному веб-сайті за допомогою складної системи транзакцій, які включають посередників і інших посередників на чорних ринках. Фінансову втрату переводять на власні банківські рахунки злочинців через серію переказів, призначених для маскування та ускладнення слідування. Інтелектуальна власність використовується або продається отримувачами. Використання цифрових валют полегшує та ускладнює відстеження викупу від розшифровування вірусів, що вимагають викупу. Збільшена легкість монетизації - ще одна причина зростання кіберзлочинності.

Кіберзлочинство працює на великому масштабі. Кількість зловмисної діяльності в Інтернеті дивує. Один із провайдерів основних Інтернет-послуг повідомляє, що він бачить 80 мільярдів зловмисних сканувань щодня, результат автоматизованих зусиль кіберзлочинців ідентифікувати вразливі цілі. Багато дослідників ведуть облік кількості нових шкідливих програм, що вивільнюються, з оцінками від 300 000 до мільйона вірусів та інших шкідливих програм, створених щодня. Більшість з них - це автоматизовані сценарії, які пересукають веб для пошуку вразливих пристроїв та мереж.

Фішинг залишається найпопулярнішим та найлегшим способом скоїти кіберзлочин, із Групою з боротьби з фішингом (APWG), яка зафіксувала понад 1,2 мільйона атак у 2016 році, багато з яких були пов'язані із розкраданням даних.

Ця кількість може бути недооцінена, оскільки Федеральне бюро розслідувань США (FBI) оцінило, що щодня в 2016 році було 4 000 атак із вимаганням викупу. Організація Privacy Rights Clearing House оцінює, що у

2016 році через порушення безпеки було втрачено 4,8 мільярда записів, з яких близько 60% були втрачені через хакерські атаки.

Таблиця 1.2 – Оцінена щоденна активність кіберзлочинців

Кіберзлочинності	Оцінена щоденна активність
Зловмисні сканування	80 мільярдів
Новий шкідливий програмний засіб	300,000
Фішинг	33,000
Рансомвар	4,000
Записи, втрачені через взлом	780,000

Нові технології роблять людей і компанії більш ефективними та продуктивними, і до них відносяться й кіберзлочинці. Кіберзлочинці швидко адаптуються до нових технологій. Писання шкідливих програм є автоматизованим, з тисячами нових екземплярів, які генеруються щодня. TOR, безкоштовний програмний продукт, який забезпечує анонімну та неслідовану активність в Інтернеті, став вибраною платформою для кіберзлочинців, які віддають перевагу "Темному вебу". З розвитком Інтернет-активності на мобільних платформах, за нею слідує й кіберзлочинність. Деякі кіберзлочинці навіть використовують інструменти штучного інтелекту для пошуку цілей. Урешті, біткоїн та інші цифрові валюти є об'єктами крадіжок, а також засобами оплати та грошових переказів для кіберзлочинців[6]. Північна Корея, наприклад, робила з взлому південнокорейських біткоїн-обмінників - ще до того, як біткоїн був заборонений - справжнє мистецтво. Інші біткоїн-обмінники інших країн також можуть бути вражені, і зростання вартості цифрових валют робить їх бажаними цілями. Поєднуючи анонімнізуючі служби та анонімнізовані цифрові валюти із вже вдосконаленими чорними ринками кіберзлочинності - вдосконаленими за організацією, спеціалізацією та атакуючими інструментами, які вони надають, часто спеціально розробленими для ухилення від мережевих захистів - ми вирішуємо одну з основних проблем, з якою кіберзлочинці стикалися у минулому: як зробити прибуток з інформації, яку вони вкрали. Сполучення анонімнізуючих служб, таких як мережа "Tor", цифрових валют та темного вебу, створює паралельний світ, який надає кіберзлочинцям як арсенал, так і притулок.

2 ОГЛЯД МЕТОДІВ МОДЕЛЮВАННЯ КІБЕРЗАГРОЗ

2.1 Класифікація кіберзагроз

Першим етапом класифікацією кіберзагроз є розділення атак на два підтипи, а точніше на типи взаємодії на технології інтернет речей: фізичні атаки, на рівні взаємодії з самим приладом і його оснащенням, і атаки на рівні інформаційному, за допомогою програмного забезпечення.

Порушення роботи пристроїв інтернет речей фізичним втручанням зазвичай виконуються створенням нестандартних умов для самого приладу. Під такими умовами розуміють порушення роботу приладу методами взаємодії технологіями генерації радіочастотних хвиль(Bluetooth, RFID, NFC) або звичайною підміною ідентифікаторів для зчитування(QR).

Класифікацію атак можна здійснювати конкретизуючи ознаки за якою виконуються кібератаки. Виділимо такі ознаки: характер взаємодії, цілі взаємодії, умова початку здійснення атаки, наявність зворотного зв’язку з об’єктом атаки, розташування відносно об’єкту атаки.

За характером взаємодії розрізняють кіберзагрози на пасивні та активні. При виконанні активних, порушник виконує активні дії, які пов’язані зі зміною потоків даних. При пасивних атаках шкідливий програмний код розміщується, наприклад, у просторі інтернету, і порушник сподівається, що жертва самостійно через неуважність (атаки методом фішингу) виконає запуск шкідливого коду.

За цілями взаємодії розрізняють загрози, які спрямовані на порушення конфіденційності, цілісності або працездатності інформації.

За умовою початку здійснення вирізняють атаки за запитом від жертви, безумовну атаку та атаку з урахуванням умов. Атаку за запитом від жертви можна вважати продовженням пасивної атаки. Після переходу на шкідливий ресурс відбувається «добровільний» запуск шкідливого програмного коду. Безумовною є атака без дослідження систем захисту жертви. Атака з

урахуванням умов виконується на основі визначення коефіцієнту успішності проведення атаки.

За наявністю зворотного зв’язку з об’єктом атаки можна поділити на атаки зі зворотнім зв’язком та однонаправлені атаки.

Одним із основних факторів атаки є місце розташування суб’єкту атаки, тому розрізняють зовнішню та внутрішню атаки[7]. При внутрішній атаці порушник може знаходитися одразу в системі, наприклад, як співробітник компанії, або мати доступ до внутрішньої мережі від самого початку. При зовнішній, - порушнику потрібно спочатку оминути зовнішній захист. Класифікацію зображено на рисунку 2.1.

Рисунок 2.1 - Класифікація кіберзагроз

Атаки можна розділити на вісім класів за уразливими місцями операційної системи:

-соціальна інженерія - атака, яка направлена на введення жертви в оману;

-запозичення прав - атака, яка має на меті захоплення прав авторизованих користувачів;

-використання - використання вразливостей програмного забезпечення чи операційної системи;

-відносна довіра - використання довіри до мереж чи сайтів;

-атаки управлінням даними - троянські програми, віруси, хробаки;

-інфраструктурна вразливість - використання особливостей стандартів, специфікацій;

-відмова в обслуговуванні - атака, яка направлена на перешкоджання використанню системи;

-чародійство - невідома атака, яка ще не зафіксована або не розшифрована. На рисунку 2.2 представлено класифікацію атак в залежності від вразливості.

Рисунок 2.2 - Класи атак за уразливими місцями

Характер кіберзагроз, у більшості випадків, можна визначити за класом атаки та її спрямованістю. Часто одна атака може бути відволіканням уваги від іншої атаки. Найбільш розповсюдженими атаками в мережі інтернет, а також найбільш простими та, водночас, найбільш ефективними серед усіх методів зараження пристроїв є атаки розповсюдження стороннього програмного забезпечення, які використовують, наприклад, для майнінгу криптовалюти, створення ботнета, інформаційного збирання (особистих та банківських даних, в тому числі, паролів)

2.2 Методи розповсюдження кіберзагроз

Для описання методів кіберзагроз спочатку потрібно описати те як прилади з’єднуються між собой у мережі. Для цієї цілі опишемо принцип з’єднання приладів математичною теорією графів, тому що усі мережі, безпосередньо, побудовані на технології вузлів і ребер що буде зображено на рисунку 2.3.

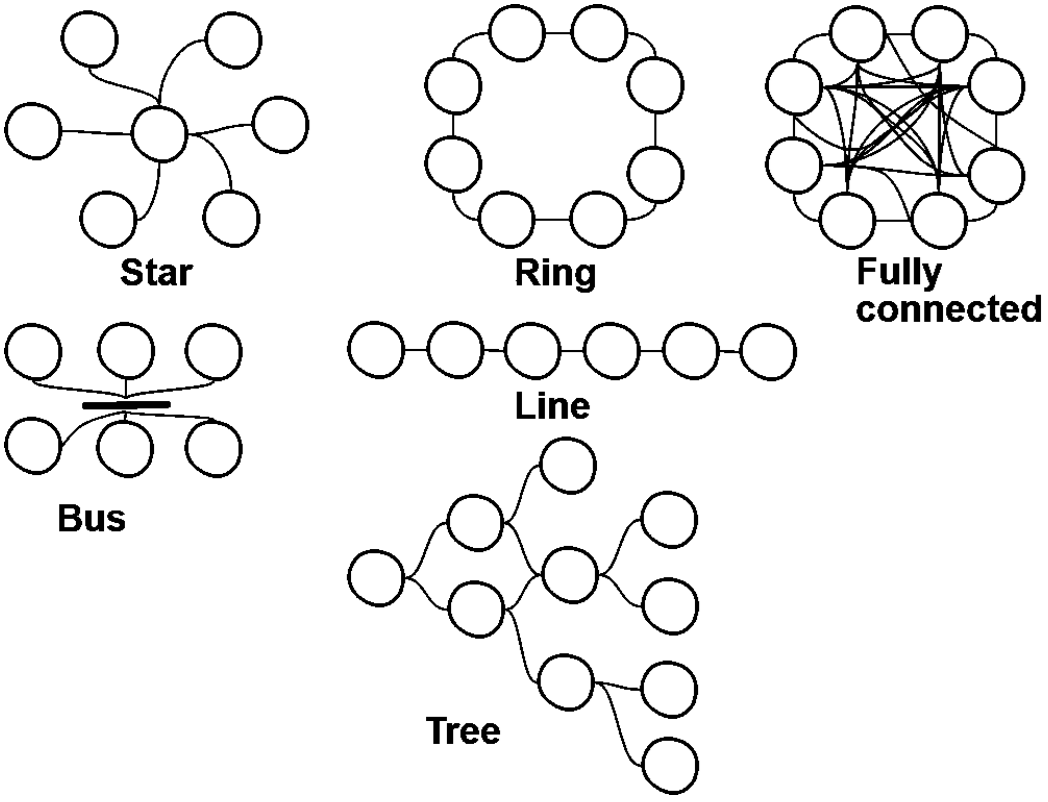

Рисунок 2.3 - Типи з’єднаних мереж пристроїв

Базові типології з’єднання мережевих пристроїв:

– шина;
– зірка;
– кільце.

Похідні типології з’єднання мережевих пристроїв:

– подвійне кільце;
– решітка;
– дерево;
– fat tree;
– сніжинка;
– повнозв’язний граф.

Всі типи з’єднання мереж розповсюджуються як на локальні так і глобальні мережи. За технологією підключення мереж і відповідно розповсюдження атак на апаратному рівні поділяються на:

– WiMax, WiFI;
– LAN, WAN, VPN, Ethernet, оптичні кабелі, вита пара, тощо;
– Телефоні лінії ADSL, Dial-up;
– Телевізійні кабеля Docsis;
– Мобільне і супутникове з’єднання.

2.3 Визначення основних етапів кіберзагроз

Планування і реалізація кібератаки складається з кількох етапів. На етапі збору інформації, який зображено на рисунку 2.4, здійснюється втручання в мережу методами шкідливого коду або використанням навичок, які мають вузький профіль (використання певних мов програмування, вразливих місць специфікацій і стандартів).

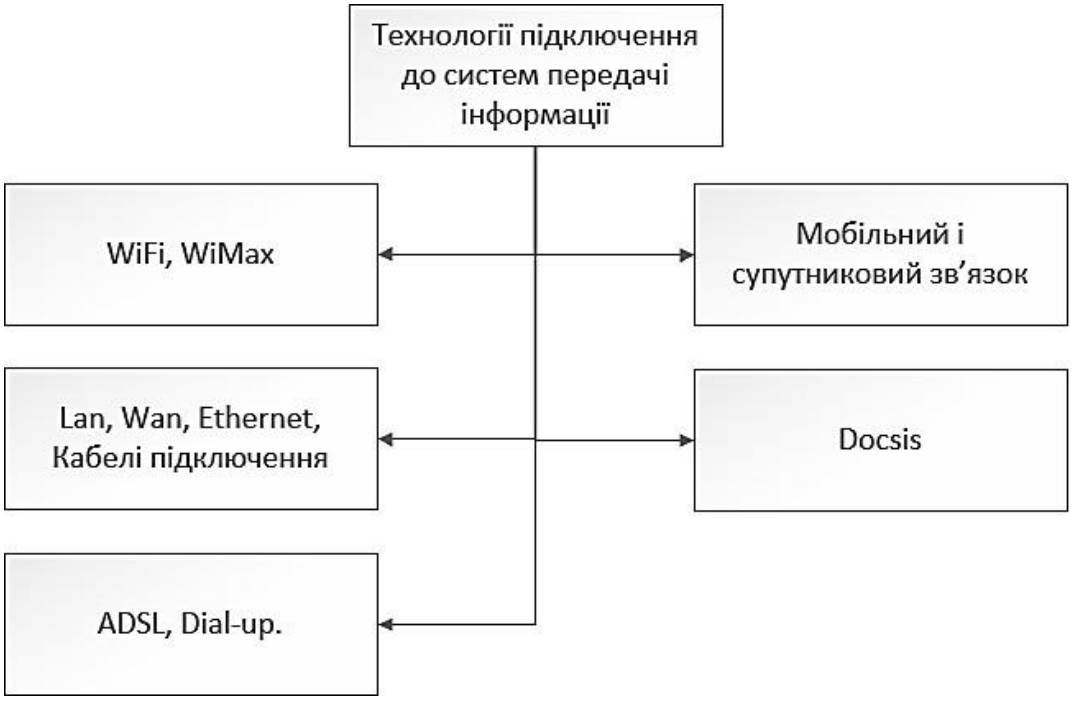

Рисунок 2.4 - Технології підключення мереж і розповсюдження вірусів на апаратному рівні

На наступному етапі відбувається інфікування пристрою, який є ціллю кібератаки [8]. Після вдалого враження пристрою відбувається етап маніпуляції з даними, що відображено на рисунку 2.5, та виконання функцій розповсюдження атаки що проілюстровано на рисунку 2.6.

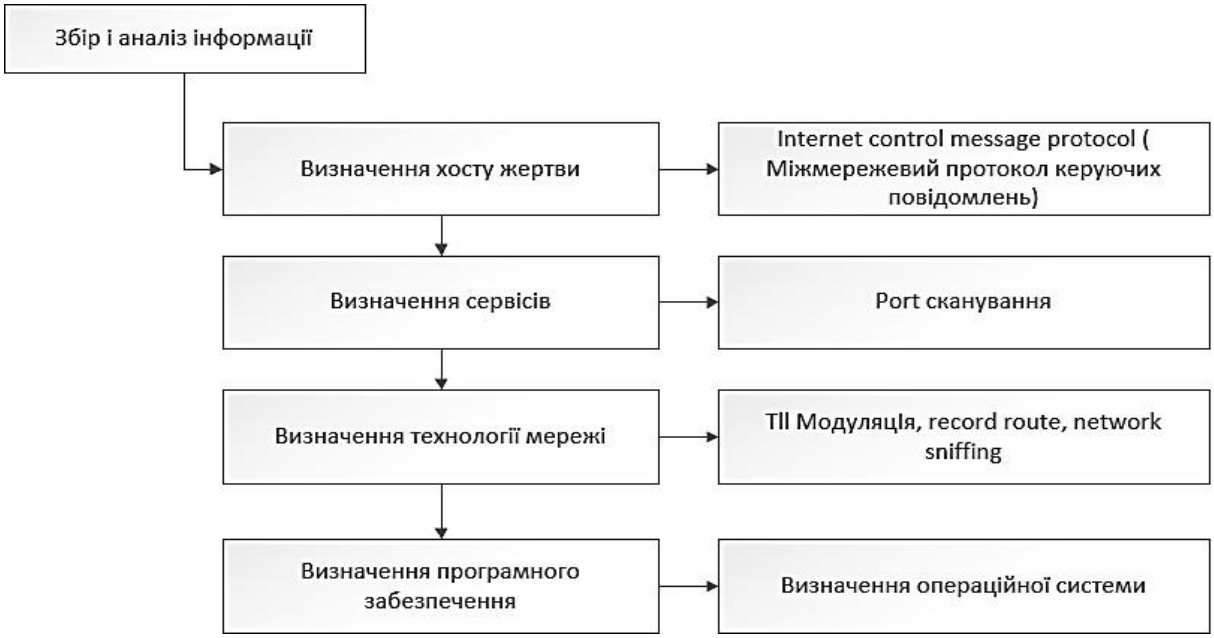

Рисунок 2.5 - Етап розвідки. Збір і аналіз інформації

Рисунок 2.6 - Етап розповсюдження атаки

На рисунку 2.7 зображено поетапний процес інфікування комп'ютера користувача вірусом.

2.4 Дослідження існуючих видів кіберзагроз

Для розгляду кіберзагроз і кібератак були обрані найактивніші і найрозповсюдженіші ботнети, котрі становлять чи становили найбільшу небезпеку для Інтернет речей.

Кожен досліджений вірус має змогу реалізовувати ddos атаку, так як являється сукупністю уражених пристроїв, котрі мають змогу з'єднуватись з мережею інтернет, має свій «ip» і «mac» адресу і має змогу виконувати запити у мережі.

Представлення деяких ботнетів і інтернет хробаків для розгляду і аналізу на таблиці 2.1.

Таблиця 2.1 - Досліджуємі віруси

Кібератака	Метод впливу
Storm	Трояньский вірус, мережевий хробак, спамбот
SpyEye	Банківський троянський вірус
Satori	Мережевий хробак

Продовження таблиці 2.1

Кібератака	Метод впливу
Carberp	Банківський троянський вірус
Sality	Троянський вірус
Bredolab	Трояньский вірус, спамбот
Zeus	Банківський троянський вірус
Mirai	Мережевий хробак
Conficker	Мережевий хробак
TDL	Троянський вірус
Reaper	Мережевий хробак
Rustock	Спамбот

Рисунок 2.7 - Етап інфікування пристрою чи мережі

Вірус **Storm**, також відомий як Storm Worm чи Ecard malware, був однією з найвизначніших кіберзагроз у 2007 році. Його унікальність полягала в ефективному поєднанні соціального інженерінгу та технічної складності. Атака розпочиналася через електронну пошту, де використовувалися провокативні заголовки та текст для залучення уваги. Вкладення в електронних листах містили шкідливий код, який при відкритті запускав процес інфікування. Особливістю Storm була його здатність швидко адаптуватися та міняти свій код (поліморфізм), ускладнюючи виявлення антивірусними програмами.

Принциповою частиною вірусу було створення потужного ботнету, що складався з тисяч комп'ютерів, інфікованих Storm. Цей ботнет можна було використовувати для розсилки спаму, проведення DDoS-атак, а також для інших злочинних дій повний перелік яких проілюстровано на рисунку 2.8.

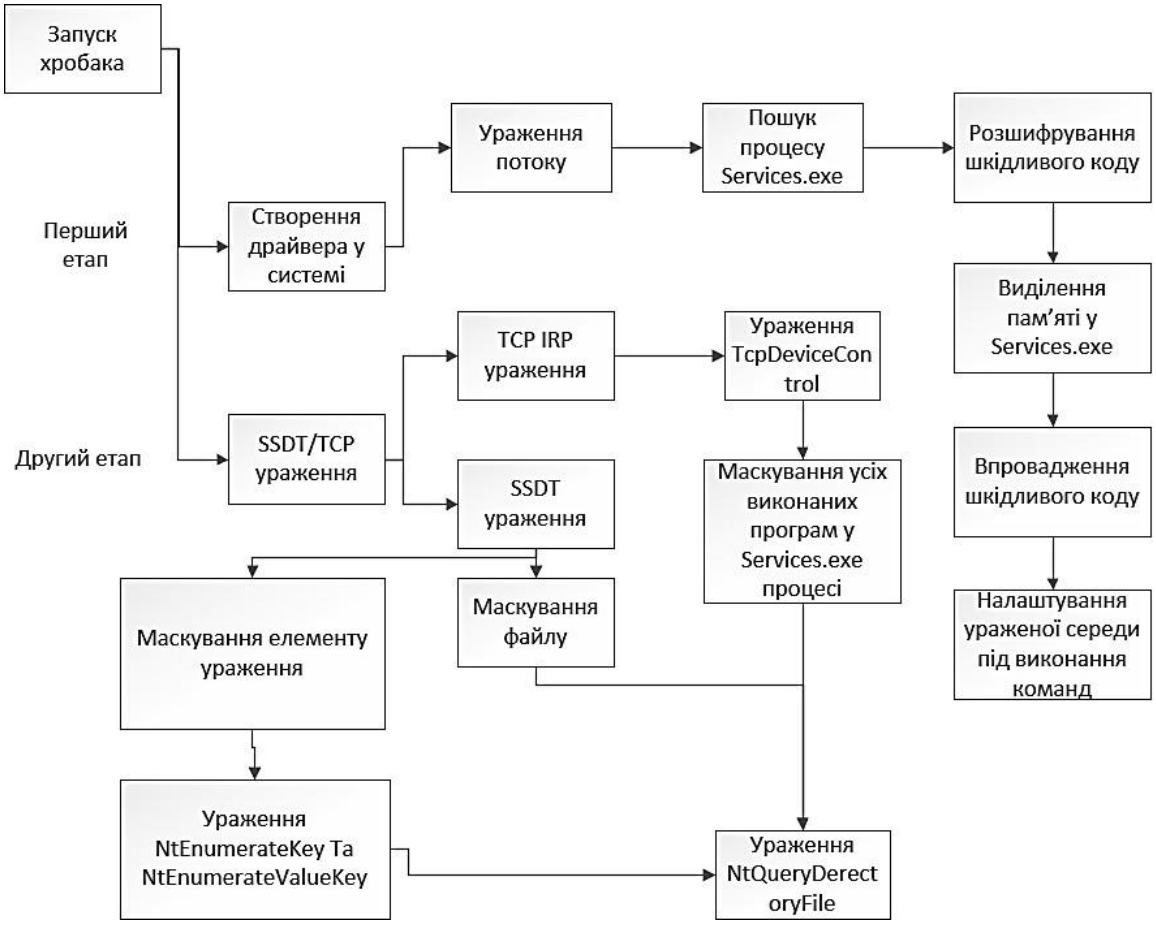

Рисунок 2.8 - Принцип дії вірусу Storm

Його поширення зумовлювалося не лише технічною спритністю, але й соціальною інтелектуальністю, оскільки зловмисники активно використовували актуальні події та соціокультурні контексти для маскування атак та залучення нових жертв. Внаслідок цього Storm Worm став важкою викликаємою загрозою для кібербезпеки та викликав значний інтерес з боку фахівців з інформаційної безпеки.

Вірус **Mirai** представляє собою особливий тип шкідливого програмного забезпечення, яке визначається своєю спроможністю здійснювати атаки за допомогою ботнету скомпрометованих пристроїв Інтернету речей (IoT). Він вперше з'явився восени 2016 року та надав загрозу для пристроїв, таких як веб-камери, маршрутизатори та інші з'єднані пристрої, які мали недостатню захист від несанкціонованого доступу.

Принцип дії Mirai полягає в тому, що він сканує Інтернет у пошуках пристроїв із залишеними фабричними налаштуваннями або з вразливими паролями. Після того, як вірус виявляє слабкість у безпеці пристрою, він намагається заволодіти ним, встановлюючи зловмисний код. Коли пристрій стає частиною ботнету Mirai, він може використовуватися для здійснення розподілених атак з відмовою в обслуговуванні (DDoS).

Mirai відзначився своєю унікальністю, оскільки він використовував свою ботмережу для великих атак, зокрема, напади на інтернет-постачальників та інші інтернет-сервіси. Його автори спрямовувались на підкорення пристроїв IoT, використовуючи їх масовий об'єм для скоординованих атак. Наслідком цього стало величезне завантаження на інфраструктуру та значні втрати для бізнесів та постраждалих організацій. У відповідь на поширення Mirai, багато виробників IoT почали вдосконалювати заходи безпеки та вимагати від користувачів змінювати фабричні паролі для своїх пристроїв.

За наявністю статистики, найбільша кількість уражених пристроїв із парою логін-пароль у таблиці 2.2.

Таблиця 2.2 - Пари доступу до адміністративної панелі(логін – пароль)

Логін	**Пароль**
admin	admin
root	xc3511
root	vizxv
root	juantech
root	default
admin	admin1234
root	password
root	root
root	xmhdipc
admin	smcadmin

Satori — це шкідливий програмний код, який спеціалізується на атаках на мережеві пристрої та обладнання, зокрема, на маршрутизатори та інтернет-протоколи з технологією блокчейн. Принцип дії Satori відрізняється високою рівнем спритності та складності, спрямованим на отримання контролю над великою кількістю пристроїв для здійснення різноманітних злочинних дій.

Вірус використовує ряд експлойтів та вразливостей для вторгнення в мережеве обладнання, включаючи уразливості, такі як недоліки в захисті паролів та слабкі місця в безпеці[9]. Одним із основних методів розповсюдження є використання ботнету для автоматизованого сканування Інтернету та пошуку залишених пристроїв з експлойтованими вразливостями.

Satori здобув популярність завдяки великому обсягу атак на пристрої з підтримкою протоколів блокчейнів, зокрема Ethereum. Вірус використовувався для великої кількості атак на різноманітні об'єкти, включаючи розподілені служби, що використовують технології блокчейн. Наслідком цього було значне завантаження мереж та підсилення існуючих проблем безпеки в цих системах. Зловмисники, які стоять за Satori, використовують атаки для видалення конкурентів, викрадання криптовалюти та вчинення інших злочинних дій.

Для захисту від вірусу Satori та подібних загроз, рекомендується виробництво патчів для вразливих пристроїв, зміна стандартних паролів,

використання мережевих фаєрволів та систем виявлення вторгнень, а також ретельне моніторингове ведення мережі для виявлення надзвичайної активності.

Вірус **Reaper**, також відомий як IoTroop або IoT_reaper, є шкідливим програмним кодом, спрямованим на масове скомпрометування та використання пристроїв Інтернету речей (IoT) для створення ботнету. Він вперше був виявлений у жовтні 2017 року і представляє серйозну загрозу для безпеки підключених пристроїв. Принцип дії Reaper визначається його здатністю ефективно використовувати вразливості в пристроях IoT для розширення свого ботнету та виконання різноманітних атак.

Основний принцип дії Reaper полягає в автоматичному скануванні Інтернету для пошуку підключених пристроїв, які мають відомі вразливості. Ці вразливості можуть включати залишені фабричні налаштування, слабкі паролі чи інші недоліки в захисті. Після знаходження пристрою зі слабкістю безпеки, Reaper намагається використати цю вразливість для встановлення свого власного коду на пристрій, роблячи його частиною ботнету. Принцип дії вірусу описаний на рисунку 2.8.

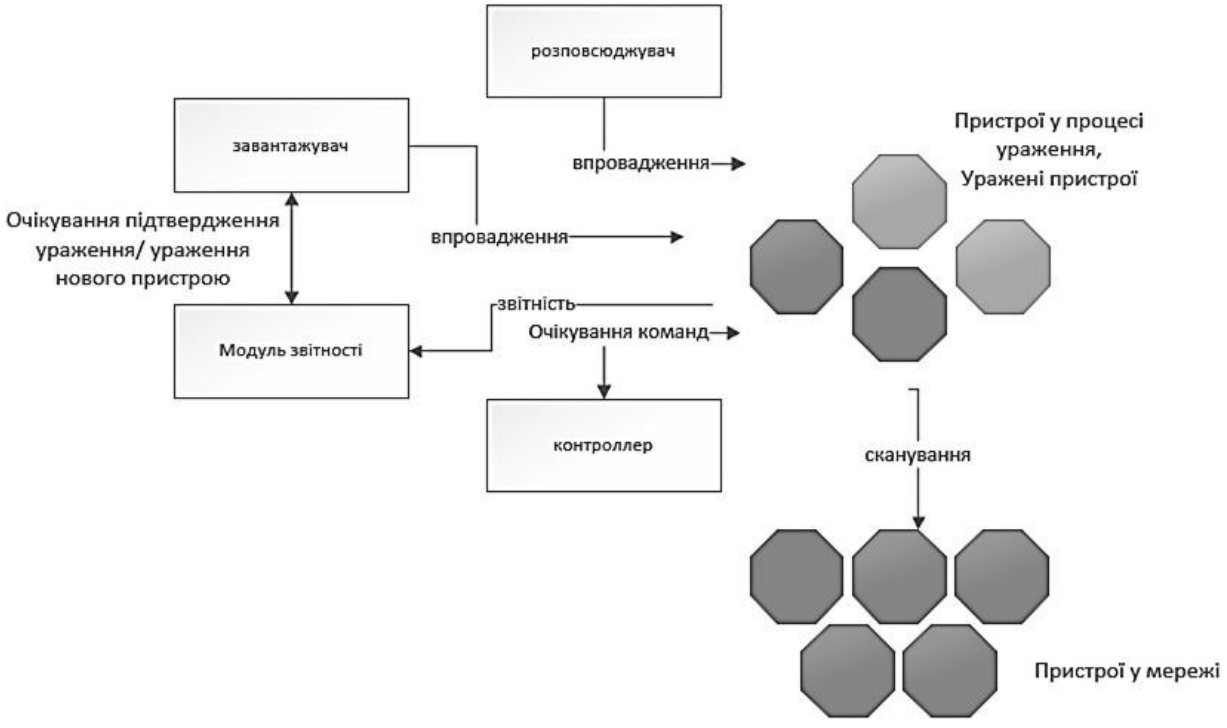

Рисунок 2.8 - Принцип дії хробака Reaper

Основними фактами щодо Reaper є його здатність до автоматичного розширення та оновлення ботнету, а також використання багатьох технік для уникнення виявлення та вирішення. Він може використовувати методи, подібні до тих, що використовуються адміністраторами для управління та контролю за компрометованими пристроями, зробивши важчим виявлення та виведення його з експлуатованих мереж. Reaper є прикладом еволюції загроз для IoT, що вимагає вдосконалених заходів безпеки, оновлень програмного забезпечення та усвідомленості користувачів щодо безпеки підключених пристроїв.

Rustock є розповсюджувачем спаму через електронну пошту, використовуючи складні технічні методи для створення ботнету та ефективного обходу антивірусних заходів. Вірус інфікує комп'ютери, перетворюючи їх на зомбі-комп'ютери, під контролем зловмисників, які використовують їх для масового розсилання спаму з метою поширення реклами чи шкідливого коду.

Одним із визначальних аспектів Rustock є його здатність до постійної модифікації свого коду та сигнатур, використовуючи методи поліморфізму. Це робить вірус важкозасікавим для антивірусних програм, ускладнюючи їх завчасне виявлення та блокування. Така технічна спритність та здатність адаптуватися до нових заходів безпеки роблять Rustock надзвичайно витонченим та небезпечним інструментом для кіберзлочинців у сфері кіберзагроз.

Carberp - це шкідливий програмний код, який визначається як великою фінансовою загрозою, спрямованою на крадіжку фінансових даних та конфіденційної інформації. Вірус вперше з'явився в 2010 році та швидко став одним із провідних банківських троянів. Принцип дії Carberp базується на розповсюдженні через електронну пошту, вразливостях у браузерах та використанні атак "Man-in-the-Browser" для перехоплення та зловживання фінансовою інформацією користувачів.

Основні факти про Carberp включають його архітектуру, яка здатна на віддалене керування та оновлення вірусу через серверні команди. Він виявляє особливий інтерес до банківських даних, використовуючи модуль перехоплення клавіатури та "вбудовані" веб-браузери для моніторингу та крадіжки фінансової інформації під час онлайн-операцій. Крім того, Carberp демонструє здатність обходу антивірусних заходів шляхом постійного оновлення свого коду та використання користувацьких комп'ютерів як частини ботнету для масштабних фінансових атак. Його складна технічна структура та висока надійність зробили його серйозною загрозою для фінансового сектору та інших користувачів.

Принцип дії вірусу описаний на рисунку 2.9.

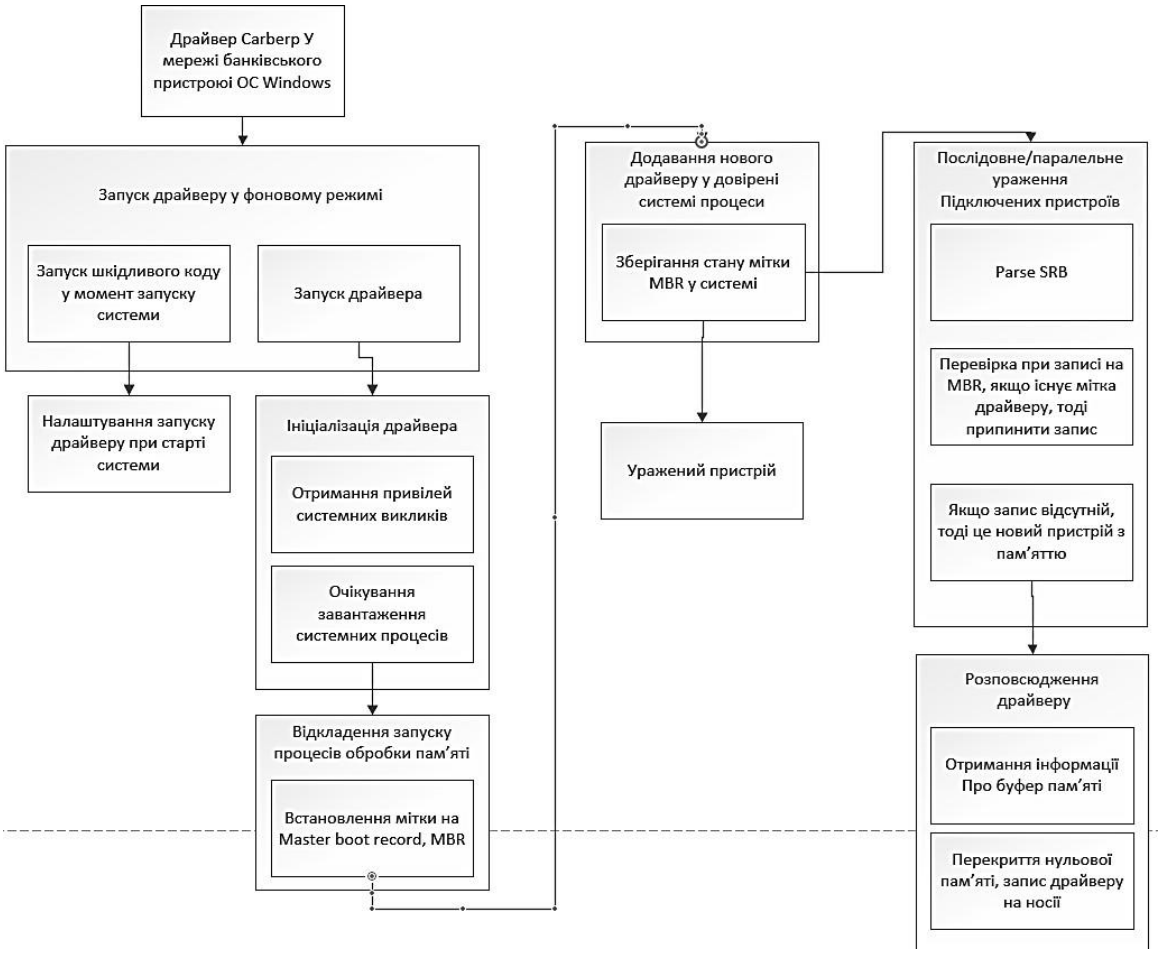

Рисунок 2.9 - Принцип дії банківського хробака Carberp

Sality - це поліморфний вірус, який вперше був виявлений у 2003 році і є одним із визначальних представників вірусів-паразитів. Вірус Sality відзначається високою рівнем складності та розповсюджується шляхом інфікування виконуваних файлів та вкрай складного захоплення системних процесів. Його принцип дії базується на техніках самозахисту та поліморфізму, що дозволяє йому постійно змінювати свій код, унікально приховуючи себе від сигнатур антивірусних програм.

Основною характеристикою Sality є його здатність до маніпулювання та контролю за виконанням файлових операцій, зокрема, він може замінювати виконувані файли на інфіковані копії. Цей вірус активно поширюється через інфіковані USB-накопичувачі, мережі і інші зовнішні носії. Крім того, Sality спрямований на вторгнення в області інформаційної безпеки, викрадання конфіденційних даних, а також може служити платформою для інших злочинних дій, включаючи розповсюдження інших вірусів чи здійснення атак на мережеву інфраструктуру. У світі кібербезпеки Sality є однією з найбільш найстійких та небезпечних загроз, що вимагає ретельних заходів для виявлення та ефективного лікування інфікованих систем.

Bredolab - це вірус, який визначається своєю спроможністю поширювати шкідливе програмне забезпечення шляхом відправки спаму та інфікування користувацьких комп'ютерів через електронну пошту. Принцип дії Bredolab базується на соціальному інженерінгу та використанні соціальних елементів для заманювання користувачів до відкриття забраклєтованих вкладень або переходу за шкідливими посиланнями в електронних повідомленнях. Після інфікування системи, Bredolab може встановлювати додаткове шкідливе програмне забезпечення, створювати ботнет, а також використовувати комп'ютер для надсилання спаму та здійснення інших злочинних дій в мережі.

Bredolab надавав зловмисникам віддалений доступ та контроль над інфікованими комп'ютерами, використовуючи їх для виконання різноманітних завдань, таких як розсилка спаму, крадіжка особистої інформації, атаки з

відмовою в обслуговуванні та інші злочинні акції. Bredolab відзначався своєю здатністю швидко адаптуватися до нових методів обхіду захисту та ефективно обходити антивірусні заходи, використовуючи техніки поліморфізму та шифрування свого коду. Завдяки своїм хитромудрим та навіть передовим методам поширення та функціоналу, Bredolab вважається однією з помітних загроз в сфері кібербезпеки.

Zeus, також відомий як Zbot, представляє собою складний банківський троян, розроблений для крадіжки фінансової інформації та конфіденційних даних користувачів. Основний принцип його дії полягає в інфікуванні комп'ютерів через спамові електронні листи, експлойти веб-браузерів або вразливості в системах. Після інфікування, Zeus створює зв'язок із віддаленим сервером, що дозволяє зловмисникам віддалено керувати інфікованими системами та використовувати їх для викрадання фінансової інформації під час онлайн-транзакцій. Відомий своєю майстерністю в уникненні виявлення та здатністю адаптуватися до нових заходів безпеки, Zeus залишається однією з найсерйозніших і довговічних загроз у сфері кіберзлочинності.

TDL, або ботнет TDL, є складною і надзвичайно стійкою загрозою, яка вперше з'явилася в 2008 році. Принцип його дії ґрунтується на використанні технік rootkit, завдяки чому вірус здатен невидимо вбивати себе в ядро операційної системи, ускладнюючи виявлення та лікування. TDL зазвичай розповсюджується через експлойти та соціальний інженерінг, використовуючи вразливості у веб-браузерах та інших програмах для інфікування комп'ютерів. Однією з основних особливостей TDL є його здатність до самозахисту, регулярного оновлення та перехоплення даних користувачів, що робить його інструментом вибору для виконання різноманітних кіберзлочинних завдань, включаючи відправку спаму, крадіжку особистих даних та встановлення інших шкідливих програм.

Функціонал дії вірусу описаний на рисунку 2.10

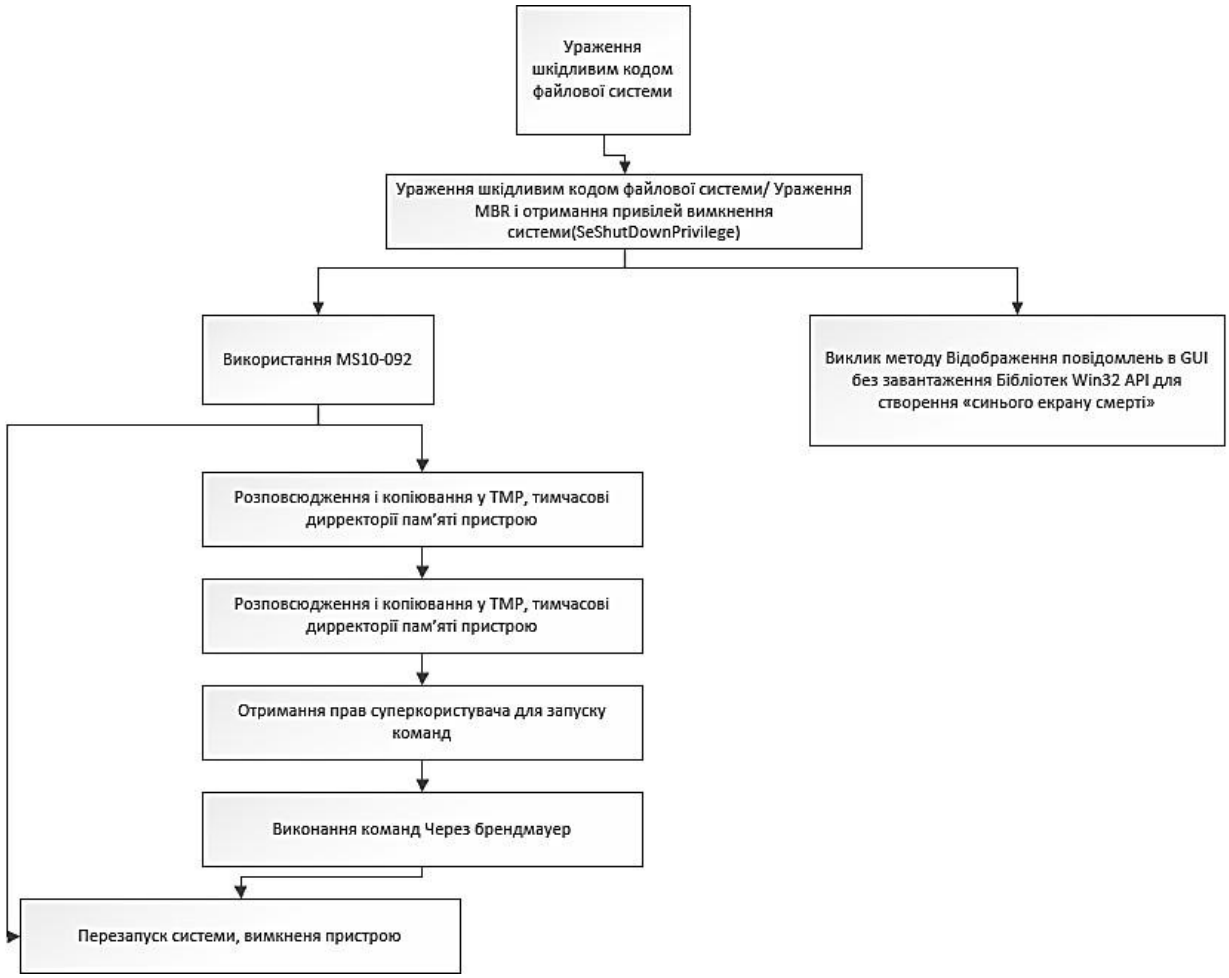

Рисунок 2.10 - Принцип функціонування TDL

Conficker, також відомий як Downadup, є вірусом, який визначається своєю складністю та ефективністю в поширенні та уникненні виявлення. Його принцип дії ґрунтується на використанні різних методів зараження, включаючи експлойти в операційних системах Windows та вразливості в мережевих протоколах. Conficker також використовує алгоритми генерації доменних імен для збору інструкцій від зловмисників та оновлення свого коду.

Основні факти щодо Conficker включають його здатність створювати ботнети, що дозволяють зловмисникам використовувати інфіковані комп'ютери для різних злочинних цілей, включаючи розсилку спаму, крадіжку конфіденційної інформації та використання в атаках з відмовою в обслуговуванні. Вірус також визначається своєю здатністю шифрувати свій власний код, ускладнюючи аналіз та виявлення. Conficker залишається однією

з найвпливовіших загроз в сфері кібербезпеки завдяки своїм технічним особливостям та надзвичайній стійкості.

Функціонал вірусу описаний на рисунку 2.11.

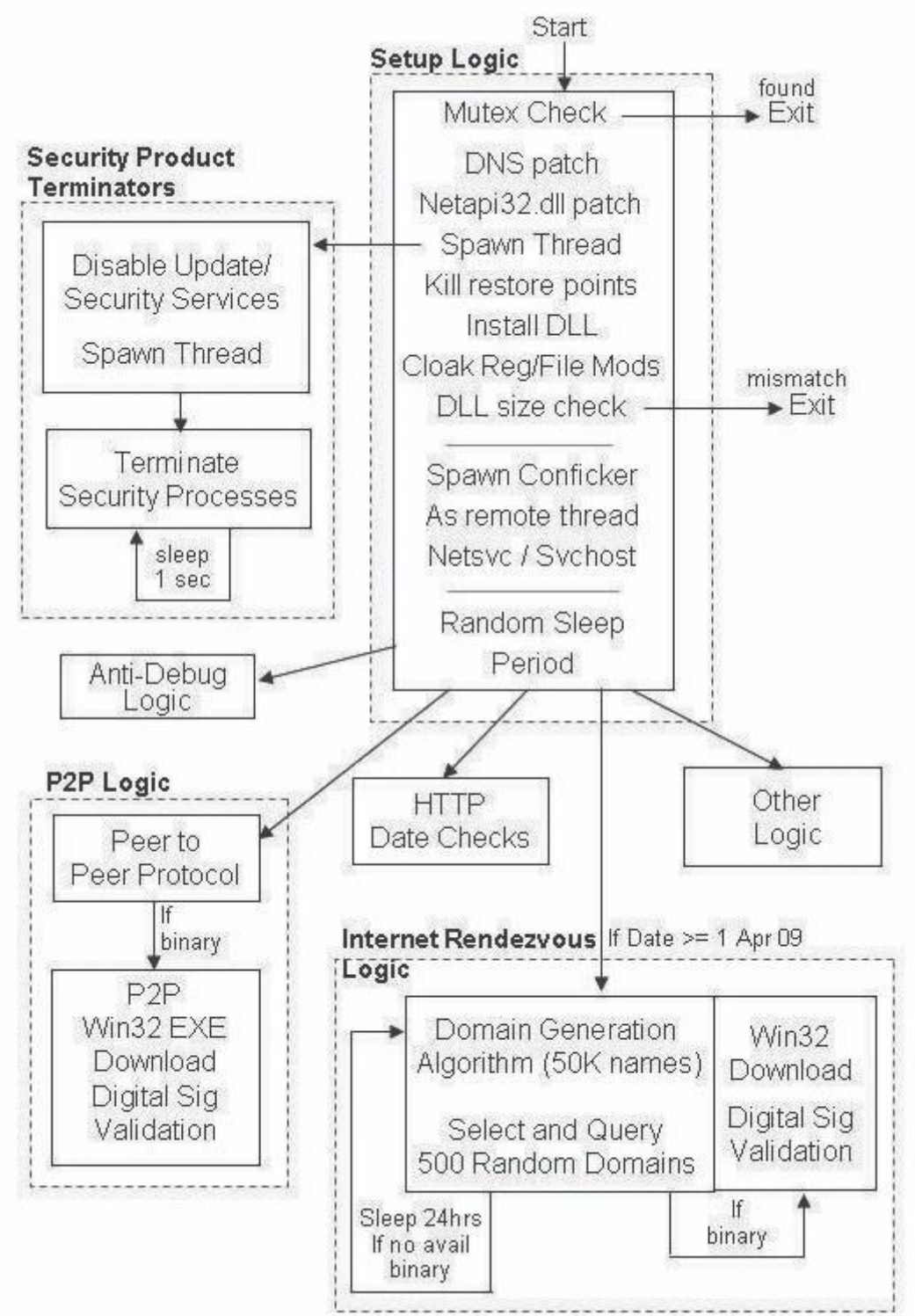

Рисунок 2.11 - Принцип роботи вірусу Conficker у операційній системі

SpyEye представляє собою складний банківський троян та шкідливу програму для крадіжки фінансових даних, яка вперше з'явилася на кіберсцені в 2009 році. Принцип дії SpyEye базується на створенні задніх дверей у комп'ютерах користувачів через експлойти та соціальний інженерінг, щоб надати зловмисникам віддалений доступ та контроль. Вірус володіє рядом додаткових функцій, включаючи вивчення інтернет-поведінки користувача, перехоплення клавішниці для отримання логін-інформації та інших конфіденційних даних, а також впровадження технік "webinjects" для модифікації веб-сторінок для обходу аутентифікації та виходу на облікові записи банківських систем. Зловмисники використовують SpyEye для створення ботнетів, виконання атак на електронні банківські системи та викрадання фінансової інформації, роблячи його серйозною загрозою для безпеки онлайн-банкінгу та електронної комерції.

Сам вірус складається з декількох модулів зображених на рисунку 2.12, котрі відповідають за встановлення і керування вірусом, маскування і викрадення інформації.

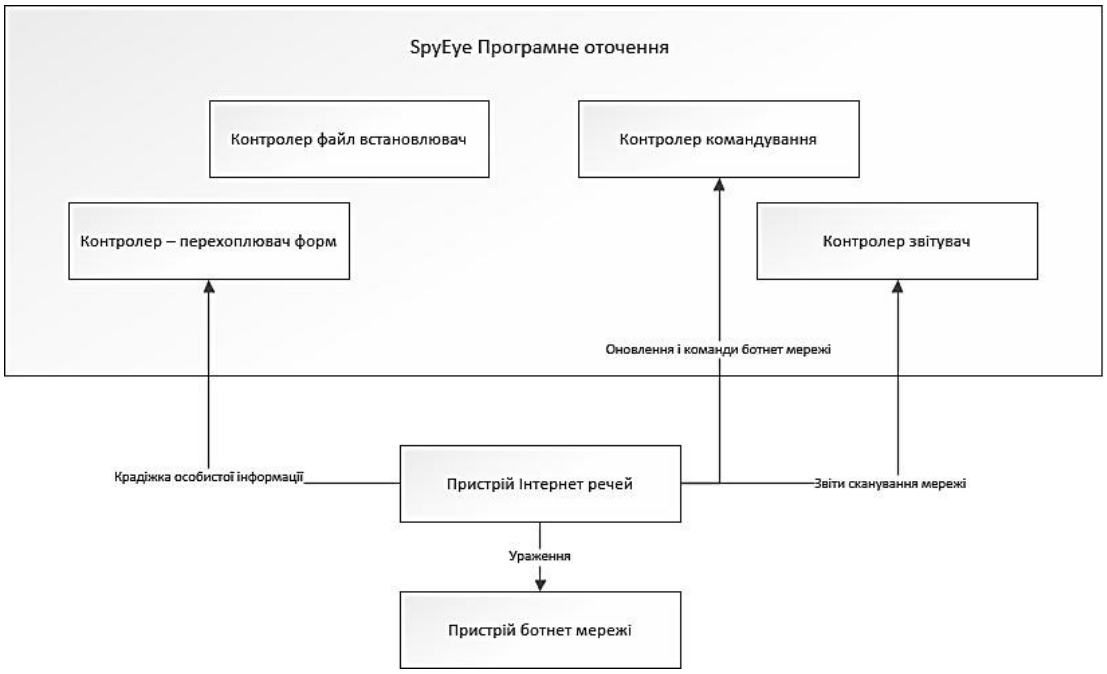

Рисунок 2.12 - Опис функціонування SpyEye

Вірус SpyEye використовує так звані "контролери файлів" або "файли встановлення" для забезпечення свого розгортання та управління інфікованими системами. Зазвичай це виконується шляхом непомітного впровадження вірусу в систему користувача за допомогою соціального інженерінгу або використання експлойтів та вразливостей у програмному забезпеченні.

Після інфікування, SpyEye розміщує свій виконуваний файл або компонент в системному каталозі чи іншому місці, яке забезпечує йому постійний доступ та виконання. Цей контролер файлу служить основою для іншого компоненту, який може бути завантажений та виконаний при необхідності, дозволяючи вірусу взаємодіяти з інфікованою системою та виконувати різноманітні завдання за дистанційними інструкціями зловмисників. Здійснюючи такий контроль, вірус може періодично оновлювати свій код, уникати виявлення антивірусними програмами та взагалі зберігати свій шкідливий функціонал.

У випадку вірусу SpyEye, контролер командування або панель керування представляє собою централізований веб-інтерфейс, який забезпечує зловмисникам віддалений доступ та управління інфікованими системами. Ця панель керування є інструментом для зловмисників, який дозволяє їм керувати функціоналом вірусу та взаємодіяти з інфікованими комп'ютерами.

За допомогою панелі керування SpyEye, зловмисники можуть відправляти команди до інфікованих систем, такі як перехоплення банківської інформації, збір конфіденційних даних, створення ботнетів та виконання інших злочинних завдань[10]. Панель також може містити інструменти для аналізу збору даних, статистики поширення вірусу, а також можливості для зміни та оновлення самого вірусу для уникнення виявлення антивірусними програмами.

Використання цієї панелі керування дозволяє зловмисникам забезпечити однорідне та централізоване управління великою кількістю інфікованих комп'ютерів, що робить SpyEye потужним інструментом для

кіберзлочинців, здатним до широкого спектру злочинних дій в онлайн-середовищі.

Вірус виконує втручання у команди у FlashXP, Total Comander(TC), CuteFTP, FileZilla, WinSCP, FTP Commander, WsFTP, Adobe Flash Player, Mozilla Firefox та інші клієнти з'єднання, встановлених програм на комп'ютері і викрадає дані логінів, паролей, кукі-файлів.

Керуючий сервер вірусу написаний на мові PHP і також використовує програмне забезпечення PHP Bug Scaner для пошуку уразливих місць, скриптів і бази з можливістю атаки SQL ін'єкцією.

Контролер перехоплювача форм SpyEye - це компонент вірусу, який відповідає за перехоплення та викрадання конфіденційних даних користувачів, зокрема, інформації про банківські реквізити та інші особисті дані. Цей функціонал найчастіше використовується для атак на банківські дані та онлайн-платіжні системи. На рисунку 2.13 зображено перехоплення клавіатури користувача.

Рисунок 2.13 - Перехвачений скріншот з клавіатури користувача

Контролер перехоплювача форм в SpyEye інтегрується в браузер користувача, найчастіше шляхом впровадження спеціального модуля (плагіну) у браузер. Цей модуль взаємодіє з веб-сторінками, які відображаються на екрані користувача, і вибірково перехоплює введені дані, такі як логіни, паролі та банківські реквізити.

Зловмисники можуть використовувати ці перехоплені дані для здійснення фінансових атак, зламування акаунтів, викрадання грошей та ідентифікаційної інформації. Цей аспект функціоналу SpyEye робить його особливо небезпечним для користувачів та організацій, оскільки вірус спроможний шахрайським чином отримувати доступ до конфіденційних фінансових ресурсів.

Викрадені облікові дані відображаються в керуючій панелі цієї форми з оновленнями у реальному часі. Існує багато різних модулів у вигляді php файлів, які призначені для викрадення інформації з форм чи їх редагування що буде зображено на рисунку 2.14.

```
require_once 'mod_dbase.php';
require_once 'mod_crypt.php';

$id = $_POST['id'];
if (!@$id) exit();
$dbase = db_open();
if (!$dbase) exit;

  $num_card      = $_POST['num'];
  $card_sec_code = $_POST['csc'];
  $exp_date      = $_POST['exp_date'];
  $name          = $_POST['name'];
  $surname       = $_POST['surname'];
  $address       = $_POST['address'];
  $city          = $_POST['city'];
  $state         = $_POST['state'];
  $country       = $_POST['country'];
  $post_code     = $_POST['post_code'];
  $tel           = $_POST['phone'];
  $email         = $_POST['email'];

    if ($card_sec_code == '')$card_sec_code = 0;
    if ($id_email == '')$id_email = 0;
    if ($id_country == '') $id_country = 0;
    $num_card = base64_encode(encode($num_card, $card_sec_code));
      $sql = "UPDATE cards "
       . "  SET num = '$num_card', csc = '$card_sec_code', exp_date =
           '$exp_date', name = '$name', surname = '$surname', address =
            '$address', city = '$city', state = '$state', post_code =
            '$post_code', phone_num = '$tel', fk_email = $id_email,
fk_country = $id_country"
        . " WHERE id_card = $id"
        . " LIMIT 1";
  $res = mysqli_query($dbase,  $sql);
```

Рисунок 2.14 - Скрипт модифікації персональних даних на веб сторінці

Функціональність яка включені у звичайний form Grabber без модифікацій:

– Модуль зчитування введеної інформації з клавіатури;

– Модуль котрий читає дані з сайтів банків чи банківських форм оплати методом перехоплення «http» запитів;

– Модуль котрий слідкує за історією відвідувань сайтів на ураженій машині, також веде облік уражених сайтів в мережі загалом;

– Модуль функціоналу створення скріншотів у момент заповнення даних карт;

– Додатковий модуль «Boa grabber», при активності клієнта Bank of America це окремий модуль котрий призначений саме для перехоплення оплат з використанням функціоналу BOA. Також наявність додаткових модулей з перехоплення POP3 і FTP клієнт серверних протоколів;

– Однією з налаштувань функції вірусу, на котру потрібно звернути увагу, це те, що при зборі інформації на зараженому комп'ютері, він не надсилає інформацію одразу як тільки її перехопив, вірус намагається отримати даних мінімум об'ємом п'ять байтів, після чого він буде намагатися надіслати перехоплену інформацію до адміністративної панелі. На рисунку 2.15 зображено звіт перехопленої інформації з сайту оплати.

На рисунку 2.16 буде зображено процес перехоплення http запитів. Інтерфейс програми користувача зображено на рисунку 2.17, він має налаштування і команди, які можна направити на уражені прилади у мережі. Останній інтерфейс об'єднує у собі функціонал вірусу Zeus, так як код вірусу був переданий розробникам SpyEye. Функціонал додатку керування вірусом пропонує очистити прилади жертв від вірусу Zeus, налаштувати автооновлення, слідкування за запитами у мережі, налаштування скріншотів робочого стола.

Рисунок 2.15 - Звіт перехопленої інформації з сайту оплати

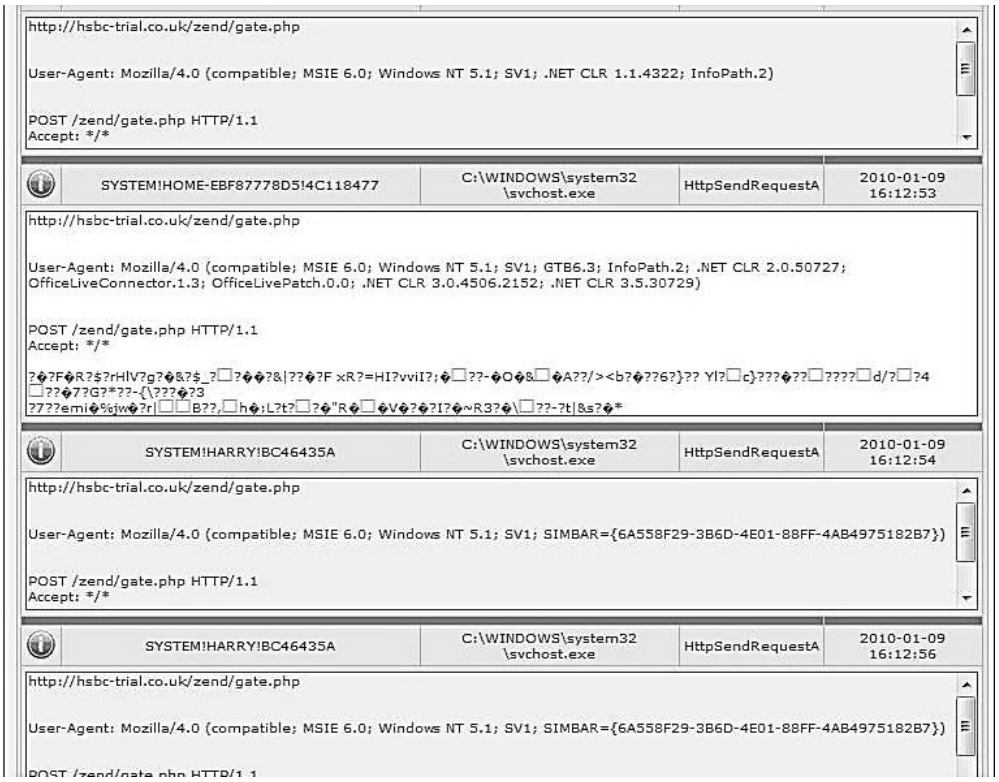

Рисунок 2.16 - Перехоплення http запитів

Рисунок 2.17 - Панель управління вірусом SpyEye

Опис характеристик приладів які уразливі для цього типу вірусу є:

– Windows XP/7/8,10;
– Windows Server 2003/2008/R2;
– Перехоплення процесів WinAPi, втручання у режим користувача і створення багатьох потокових процесів паралельно із звичайними процесами користувача.

На прикладі впровадження шкідливого скрипту при виявленні вразливостей додатком PHP Bug Scanner, зловмисними через WEB браузер можуть зібрати дані з полів форми автозаповнення.

Встановлення вірусу у системі.

Архів з вірусом встановлюється на комп'ютері через спам лист, через оновлення з ураженого комп'ютеру у локальній мережі або через завантаження файлів з піратських або уражених сайтів. Архів має файл

config.bin і зашифровану папку з самим вірусом. Файл config.bin має 32-бітний ключ у верхньому регістрі. Має розмір 13005 байтів і складається з модулів-налаштувань для встановлення вірусу у системі, що відображено на рисунку 2.18.

Після розпакування вірус видаляє встановлюючий файл-архів, за посиланням **«%SystemDrive%\cleansweep.exe**».

```
+0000h [1000] ActionUrl (e.g.,
"http://localhost/spyeye/main/bt_version_checker.php")
    +03E8h [1000] ActionUrl2 (e.g.,
"http://localhost/spyeye/main/bt_version_checker.php")
    +07D0h [1000] LatestExeUrl (e.g.,
"http://localhost/spyeye/main/bt_getexe.php")
    +0BB8h [1000] KnockHdrs (e.g.,
"http://localhost/spyeye/main/bt_knock_hdrs.php")
    +0FA0h [1000] RightTimeUrl (e.g.,
"http://localhost/spyeye/main/datetime.php")
    +1388h [1000] IncHistoryUrl (e.g.,
"http://localhost/spyeye/main/bin/page0.html")
    +1770h [1000] CurrentUaUrl (e.g.,
"http://localhost/spyeye/main/bin/ua.html")
    +1B58h [1000] ClickBnkUrl (e.g.,
"http://localhost/spyeye/main/bt_plg_clkbnk_ct.php")
    +1F40h [1000] KvipUrl (e.g.,
"http://localhost/spyeye/main/bt_plg_kvip.php")
    +2328h [1000] CheckUrl (e.g., "http://www.microsoft.com")
    +2710h [1000] FormgrabberHostUrl (e.g., "localhost")
    +2AF8h [1000] FormgrabberPathUrl (e.g.,
"http://localhost/spyeye/formgrabber/websitechk.php")
    +2EE0h [1000] FormgrabberPath2Url (e.g.,
"http://localhost/spyeye/formgrabber/websitechk.php")
    +32C8h DWORD connector interval in milliseconds (e.g.,
300,000)
    +32CCh BYTE kill Zeus flag
```

Рисунок 2.18 - Архів модулей файлу конфігурації

Далі бот перевіряє результат запущеної системної функції «GetModuleFileNameA» на значення «Null», якщо запит повертає необхідне місцеположення для ініціалізації шкідливого коду, тоді вірус намагається виконати наступні дії на ураженому пристрої:

– Створення каталогу «SystemDrive%\cleansweep.exe» або «SystemRoot\cleansweep.exe»;

– Імітація поведінки файлу «ntdll.dll» для приховання підозрілої поведінки вірусу;

– Завантаження останньої версії пакетів оновлення у файл «cleansweepupd.exe» через виклики InternetOpenA («Microsoft Internet Explorer»), InternetOpenUrlA (INTERNET_FLAG_NO_CACHE_WRITE), InternetQueryDataAvailable и InternetReadFile.

Якщо оновлення пакетів вірусу було успішним, відбувається виклик іншого мютекса боту «CreateMutexA ("__CLEANSWEEP_UNINSTALL__")», ця команда робить виклик функції cleansweepupd.exe. Якщо вірус виконується зі свого спеціального каталогу, він намагається спочатку зробити впровадження себе у деякі процеси «explorer.exe», а далі у всі можливі системні процеси комп'ютера.

У момент спроб впровадження себе у системні процеси, вірус намагається викликати системну команду «CreateToolhelp32Snapshot, (TH32CS_SNAPPROCESS), Process32First і Process32Next », за описом ці функції дають змогу отримати список виконуємих процесів, а також модулей і потоків які використовують ці процеси у момент запиту функції. Ця інформація слугує для впровадження до виконуємих процесів додаткового процесу вірусу[11]. Щоб впровадити до системного процесу виконання шкідливих дій використовується системна функція «CreateRemoteThread», який створює потік, котрий виконується у віртуальному адресному просторі іншого процесу.

Після встановлення вірусу він створює запис у реєстрі системи, що дозволяє виконуватись шкідливому коду постійно при запуску системи: «HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"cleansweep.exe" = "%SystemDrive%\cleansweep.exe\cleansweep.exe"». Після цього вірус виконує запуск самого себе у процесах програм файлових менеджерів, щоб мати змогу перехопити мережевий трафік, зчитувати інформацію і додавати додаткові пакети для обходу антивірсних додатків. Коли в системі виконується сканування на наявність вірусів, SpyEye має варіанти захисту.

3 МОДЕЛЮВАННЯ ДІЯЛЬНОСТІ

3.1 Програмне забезпечення для моделювання

Для моделювання можливої діяльності хакерів за описаними вище процесами буде використане програмне забезпечення для Windows, PTRSIM (Сітки Петрі – українська назва). Програма постачається у вигляді .exe файлу та файла конфігурації [12]. Функція моделювання може використовуватись без встановлення на комп’ютері.

Автор програми Бойко О.В.

Версія використаної програми 1.02.

Програма має простий та дружній до користувача інтерфейс.Містить увесь необхідний функціонал для побудування стохастичних мереж з Петрі-об’єктивним підходом, налаштування і пояснення будуть представленні на зображеннях 3.1 та 3.2.

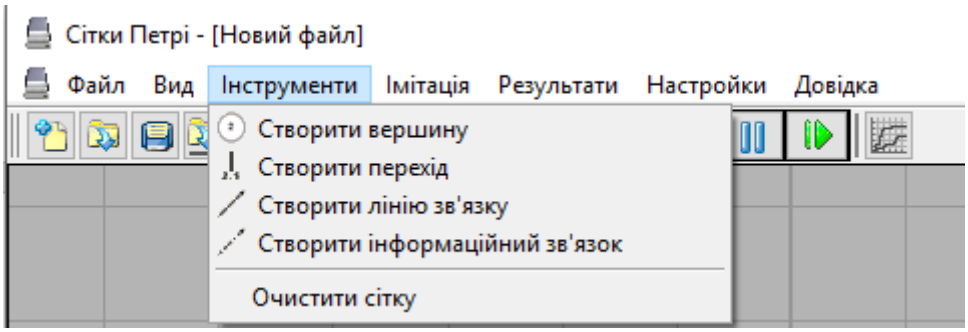

Рисунок 3.1 - Інтерфейс інструментів програми Сітки Петрі

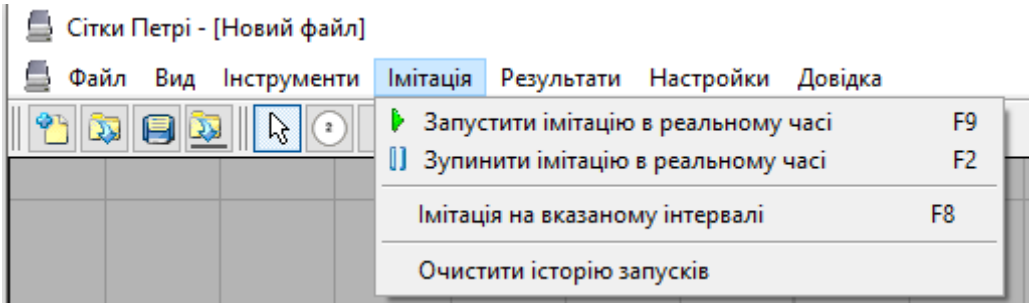

Рисунок 3.2 - Інтерфейс інструментів програми сітки Петрі

На рисунку 3.3 буде представлена додаткова панель для детального налаштування вхідних параметрів переходів і ліній зв’язків.

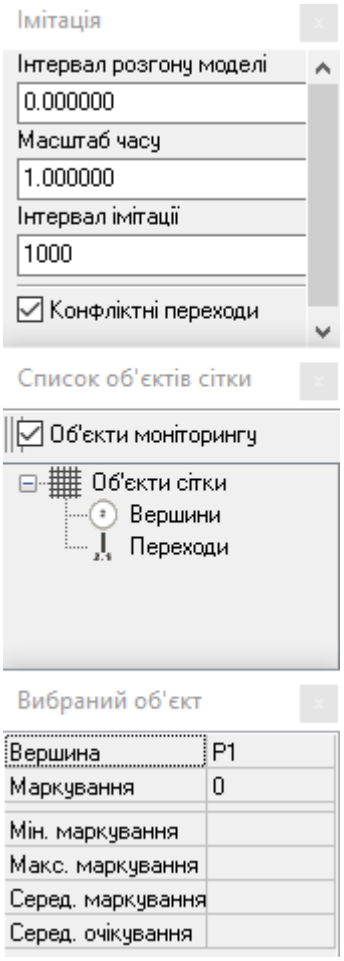

Рисунок 3.3 - Налаштування вхідних параметрів

Функціонування програми при побудові сценарію стохастичною мережею Петрі зображено на рисунку 3.4.

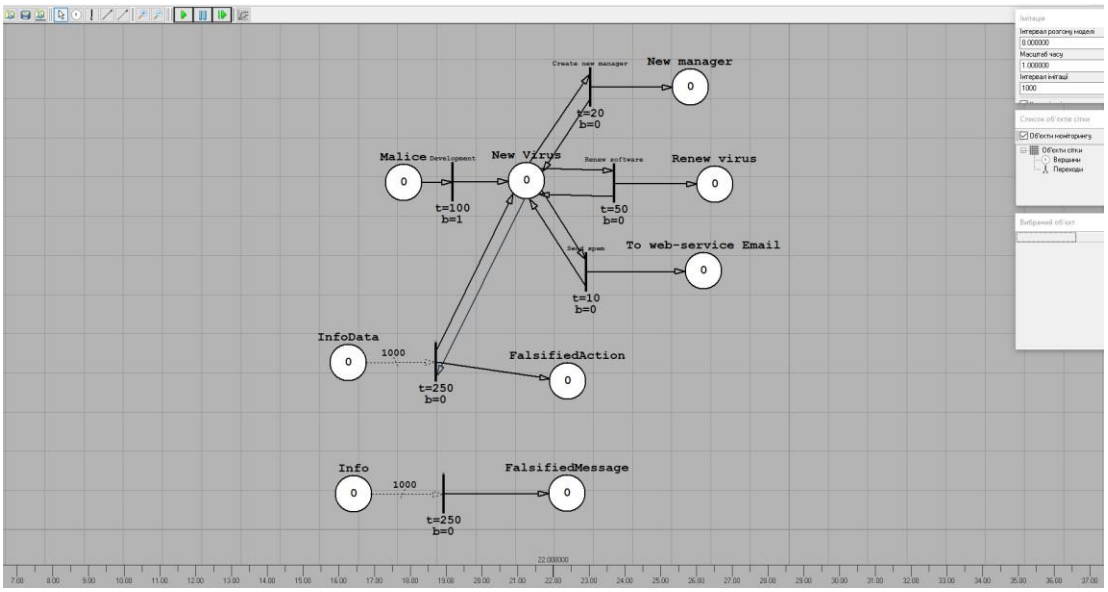

Рисунок 3.4 - Моделювання сценарію кібератаки методами побудови стохастичної мережі Петрі

Після моделювання за отриманою інформацією станів, програма дозволяє скласти графік для аналізу, представлено на рисунках 3.5 та 3.6.

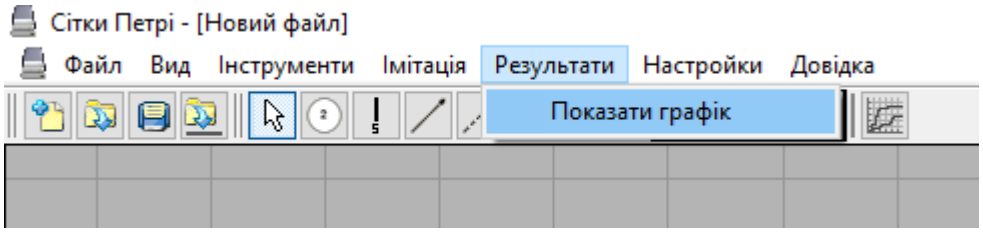

Рисунок 3.5 - Складання графіку

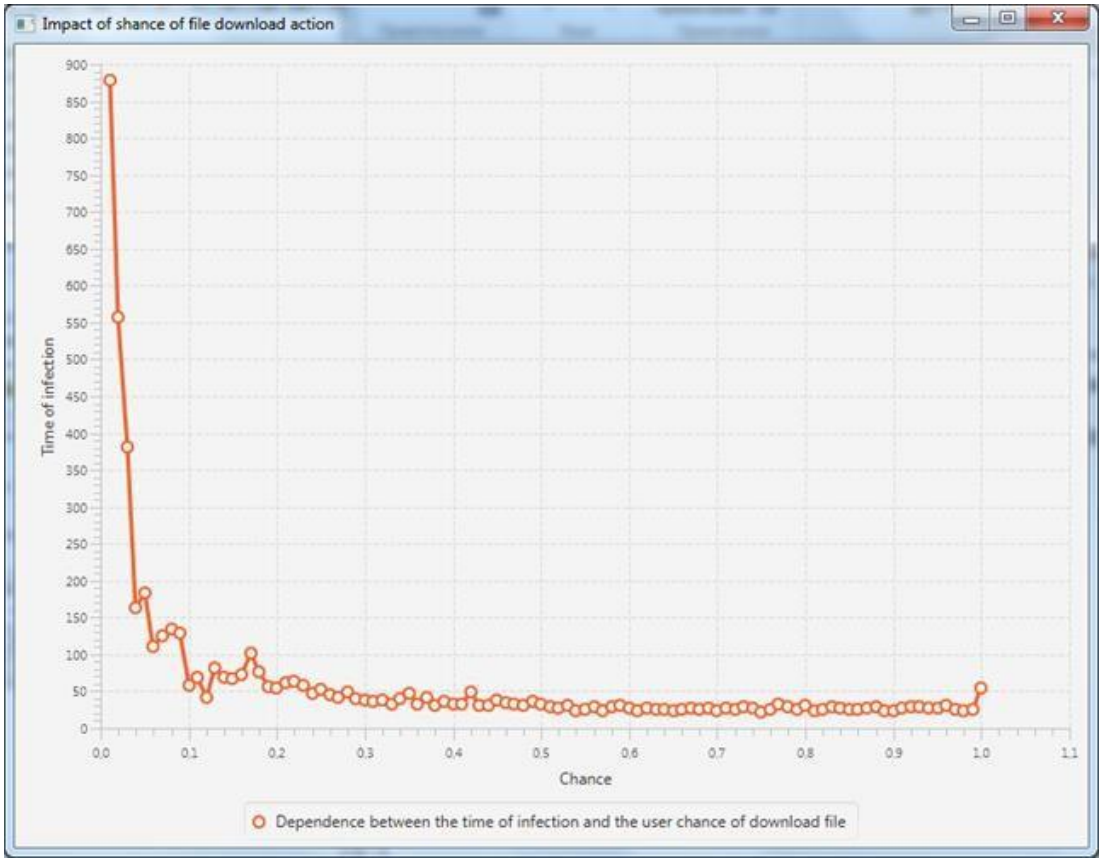

Рисунок 3.6 - Складений графік для аналізування результатів

3.2 Використання алгоритму Мережі Петрі для моделювання сценарію кіберзагрози вірусом SpyEye

Існує багато сценаріїв моделювання кіберзагроз з вірусом SpyEye, в першому варіанті користувач вже будучи вже інфікованним або ні заходить на сайт та виконує на ньому дії (завантаження файлу). Сам сайт може бути як інфікованим так і ні. Якщо сайт був інфікованим то при зберіганні файлу пристрій буде інфіковуватись вірусом. Інфікований пристрій буде відправляти на сайт інформацію про вразливосі.

По результатам стохастичного моделювання визначають наявні характеристики моделі інформаційної системи які знаходять під кібератакою:

– поточна завантаженність ресурсів ІС;

– середній час потрібний на обробку запитів користувача;

– середній час, за який відбувається часткову інфікування або пошкодження ресурсів ІС для даної інтенсивності кібератак;

– середній час, за який відбувається повне інфікування або пошкодження ресурсів ІС;

– відсоток запитів користувача які не були оброблені внаслідок пошкодження системи.

Набори необхідних вразливостей, як і набори ушкоджень, будуть змінюватись в залежності від типу застосовуваної хакерської програми. Подію «ушкодження» ресурсу ІС можна деталізувати з урахуванням степені ушкодження (часткового або повнго) і процессу відновлення цього ресурсу[13]. П Після завершення процесу відновлення ресурс може перейти в працездатний стан або ж атака виявиться успішною, а інформаційна система стане зламаною.

Умовні позначення:

Вірус – засіб кібератаки або кібезагрози.

Хакер – людина котра розробляє і використовує вірус.

Покупець вірусу – людина яка купила вірус або його частковий функціонал.

Інфікування – результат впливу кібератаки на ІС хакером або покупцем вірусу що використовують вірус.

Спам – надсилання великої кількості повідомлень на пошту чи у соціальні мережі з вкладанням вірусу.

Користувач – людина яка керує пристроєм чи взаємодіє з комп'ютерними пристроями (комп'ютери, сайти, сервери, Інтернет речі). На зображенні 3.7 буде схематично представлено процес ушкодження обчислювального ресурсу системи під час атаки.

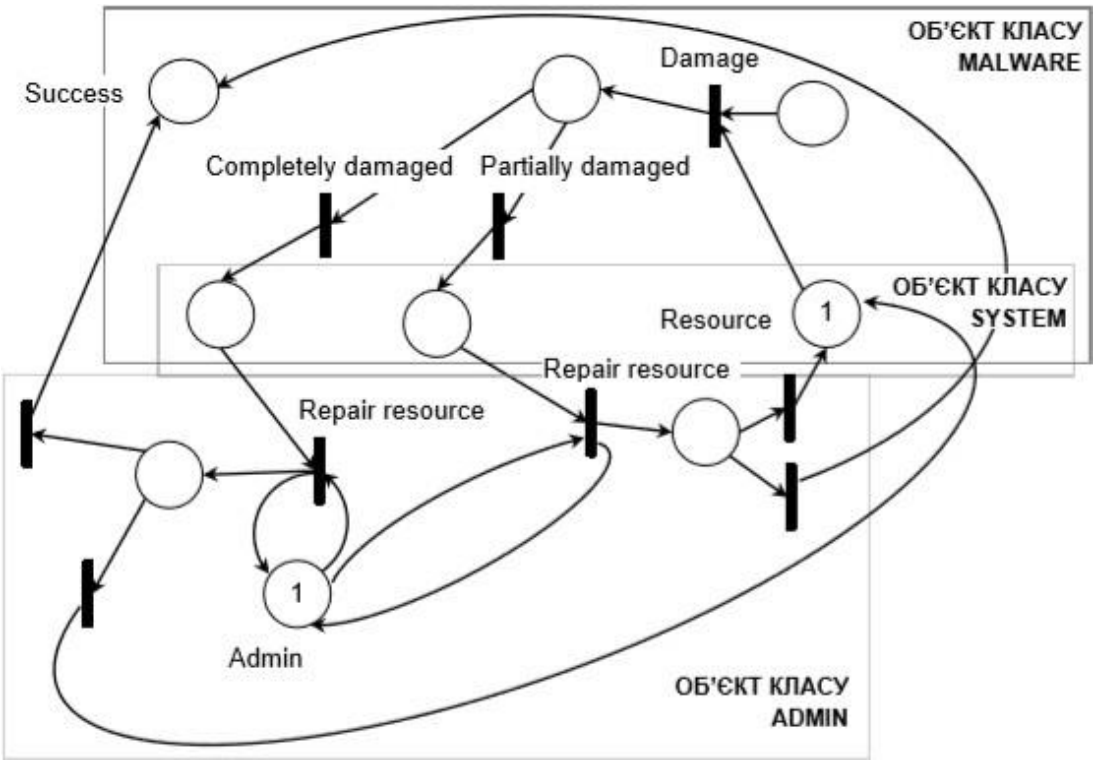

Рисунок 3.7 - Деталізація ушкодження обчислювального ресурсу

Моделювання сценарію кіберзагрози на прикладі вірусу SpyEye за описаними діями в UML діаграмі станів має три етапи:

– дії хакера з вірусом, шкідливі дії у мережі, продаж вірусу . і результат імітації діяльності;

– дії користувача комп'ютером в умовах до інфікування і після;

– інфікування вірусом.

Імітація дії хакера з вірусом зображені на рисунку 3.8.

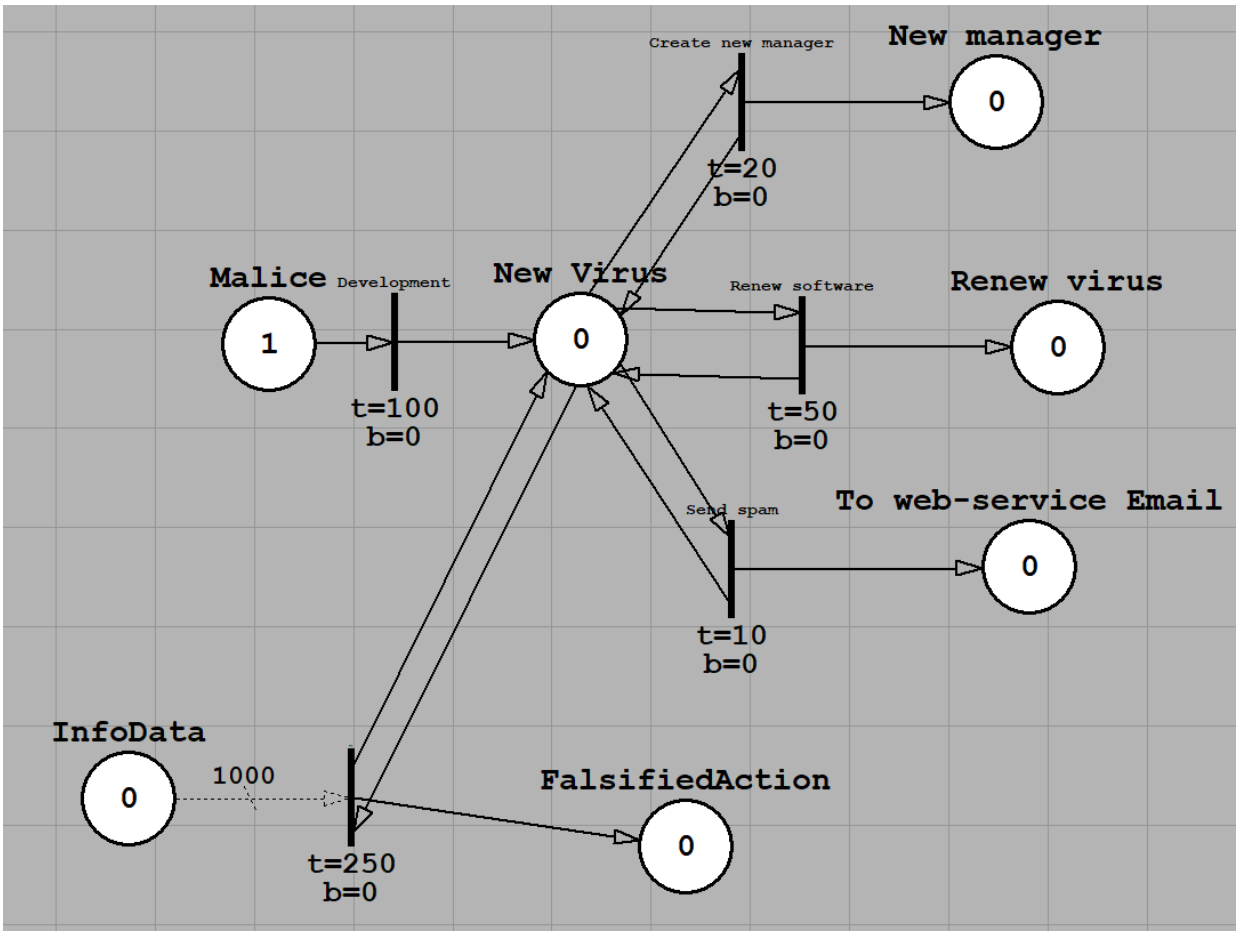

Рисунок 3.8 - Модель у стані вхідних параметрів перед імітацією. Імітація дій хакера з вірусом

В імітаційній моделі можна спостерігати що умовний користувач вже інфікований і отримав усі оновлення вірусу та його модулі. Далі він починає відправляти звіти до адміністративної панелі вірусу.

Імітація в умовах до інфікування вірусом пристрою користувача і після інфікування відображено на рисунку 3.9. На рисунках 3.10 та 3.11 буде відображено процес моделювання дій користувача та результат роботи цієї моделі.

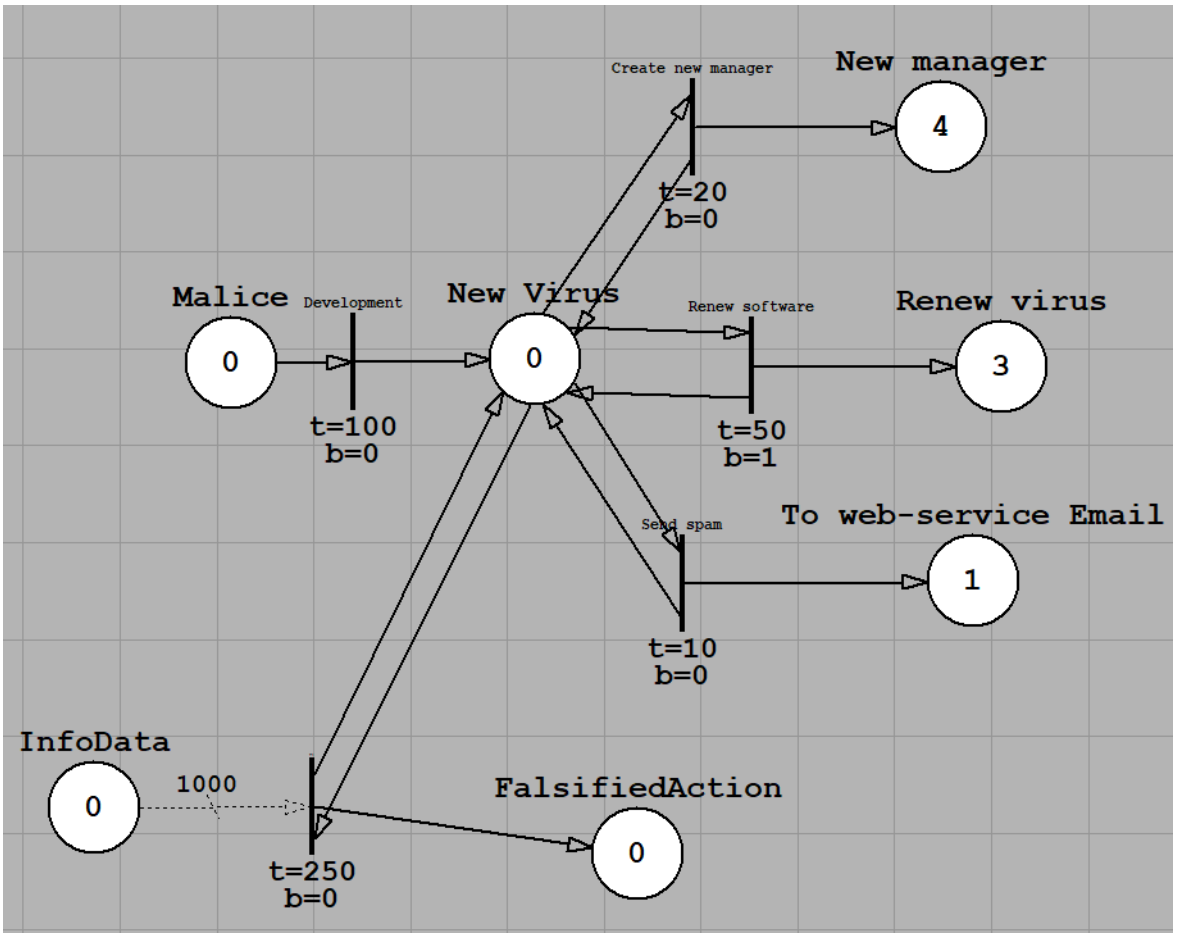

Рисунок 3.9 - Результат при імітації

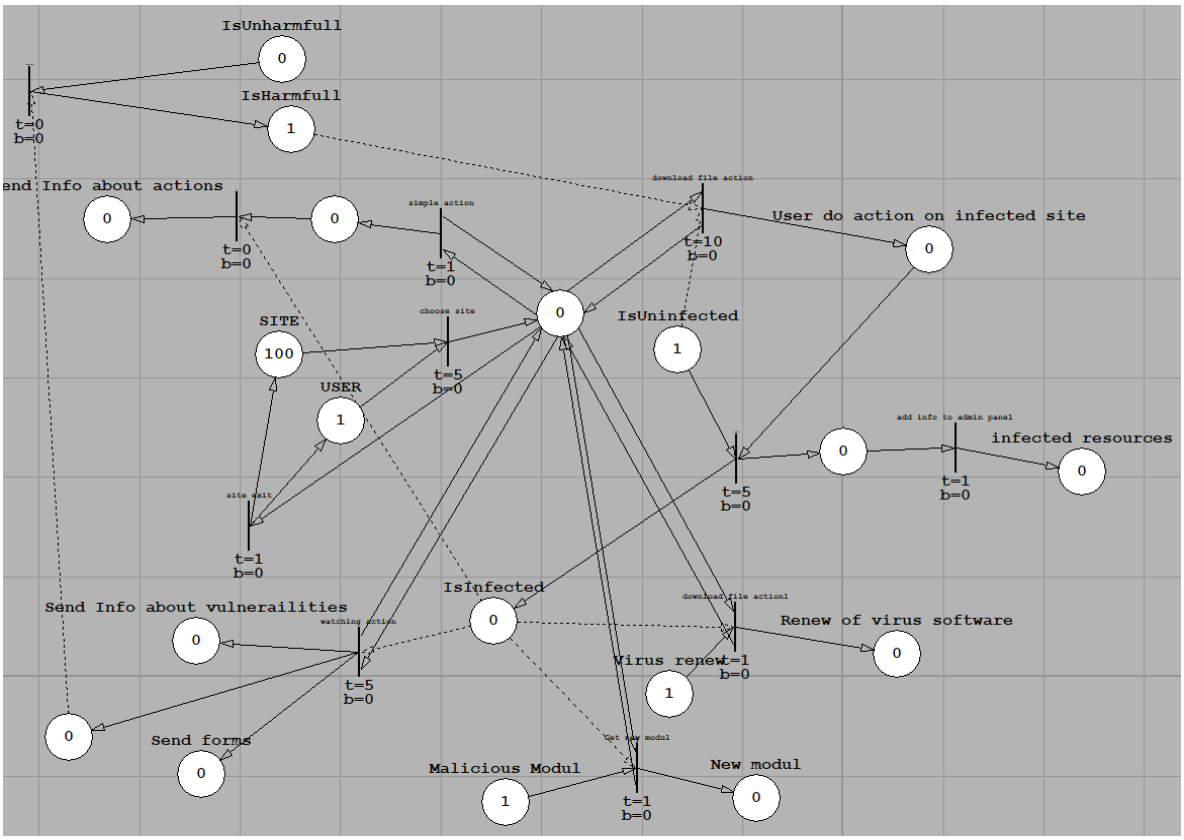

Рисунок 3.10 - Вхідні дані для моделювання дій користувача

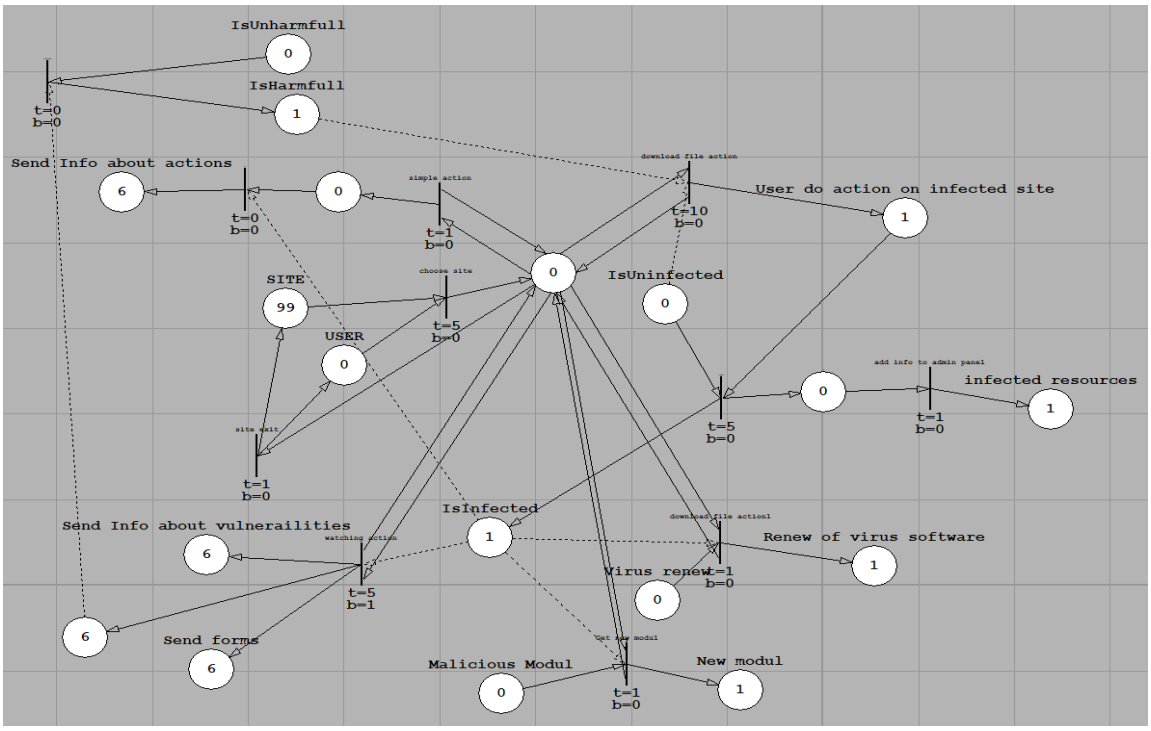

Рисунок 3.11 - Результат роботи моделі дій користувача

На рисунку 3.12 представлено імітаціну модель з умовами ураження користувача і перехоплення даних з ураженого пристрою.

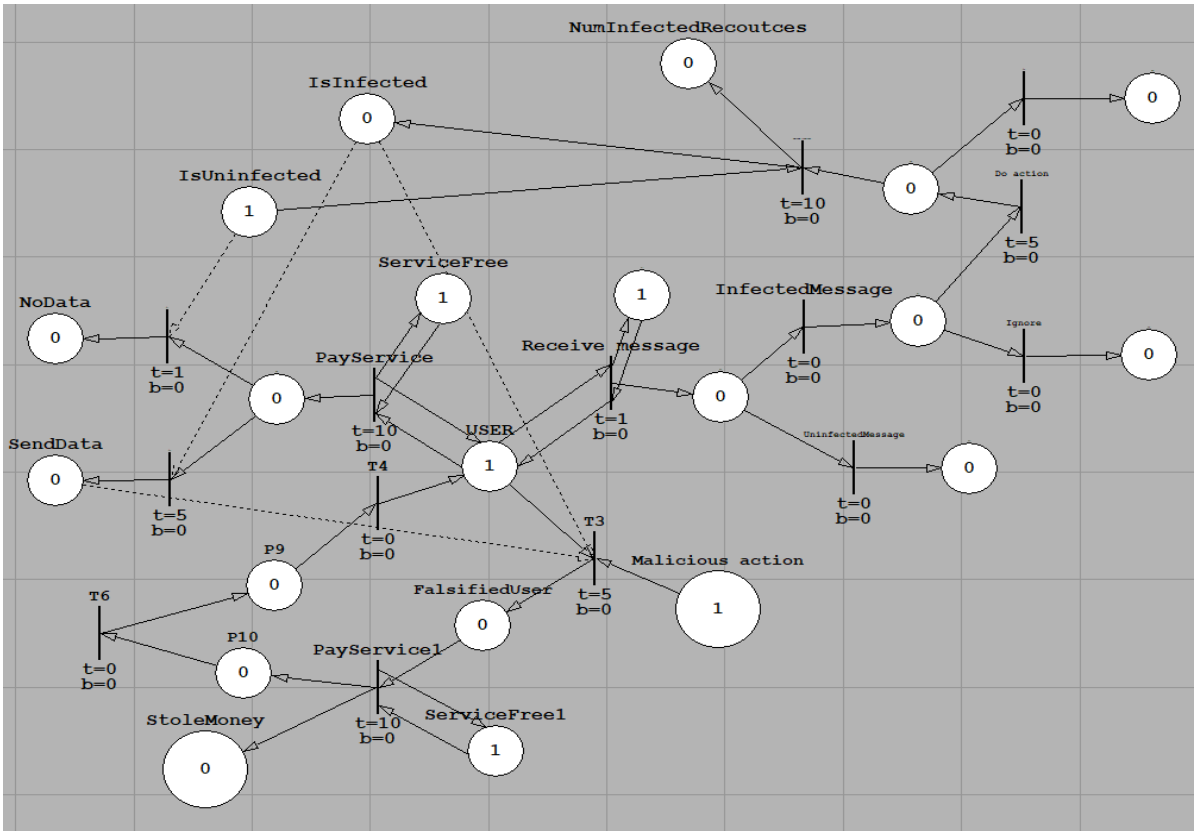

Рисунок 3.12 - Вхідні дані імітація дій користувача перед інфікуванням

На зображенні 3.13 відбувається імітація міскування хакера під корстувача для виконання дій на банківському ресурсі.

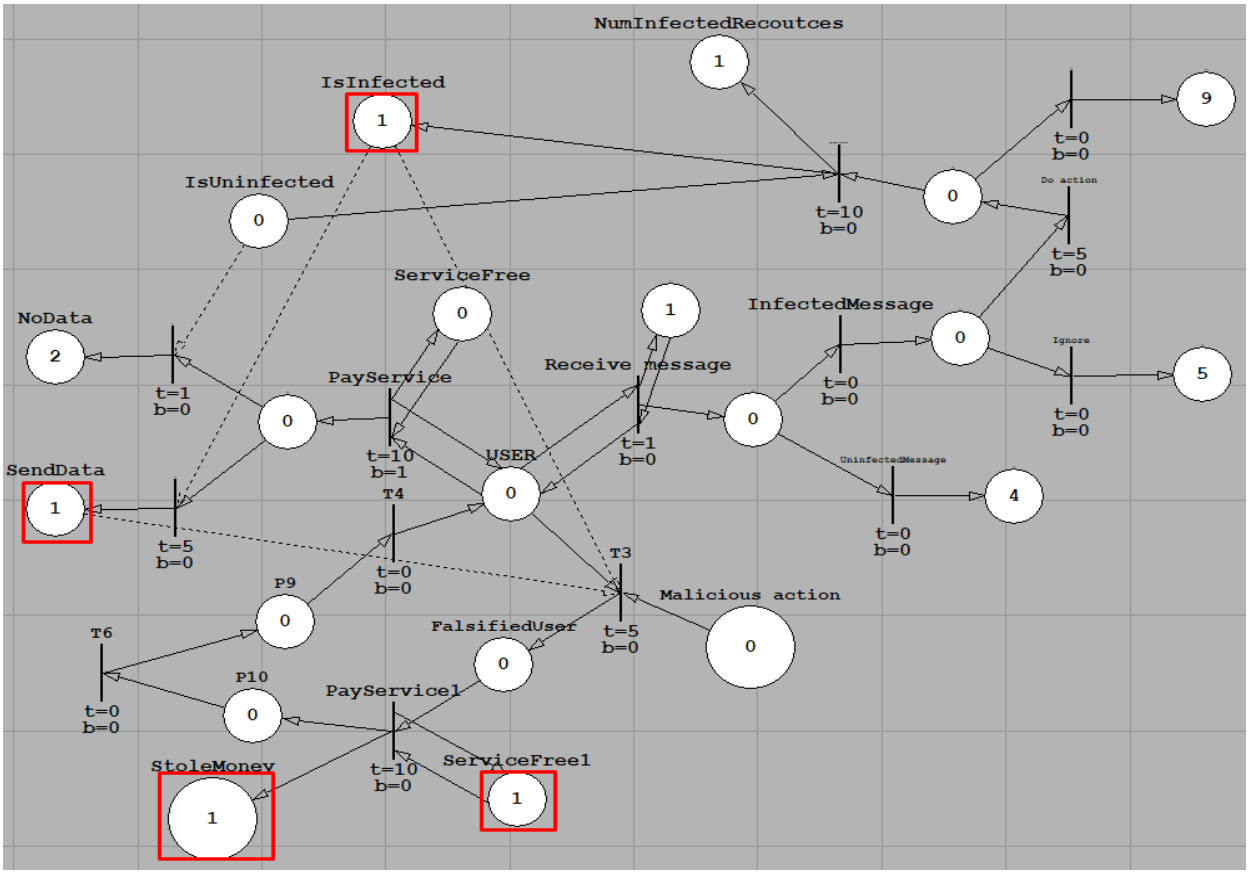

Рисунок 3.13 - Результат після моделювання дій користувача і маскування хакера під користувача

На зображенні 3.14 після отримання результатів моделювання, створюємо графік для описання за яким часом комп’ютер буде уражений. Час представляємо як абстрактну величину у експериментальних умовах.

При збільшенні часових проміжків графік не зманюється і тенденція залишається як і у першому прикладі що можна побачити на рисунку 3.15.

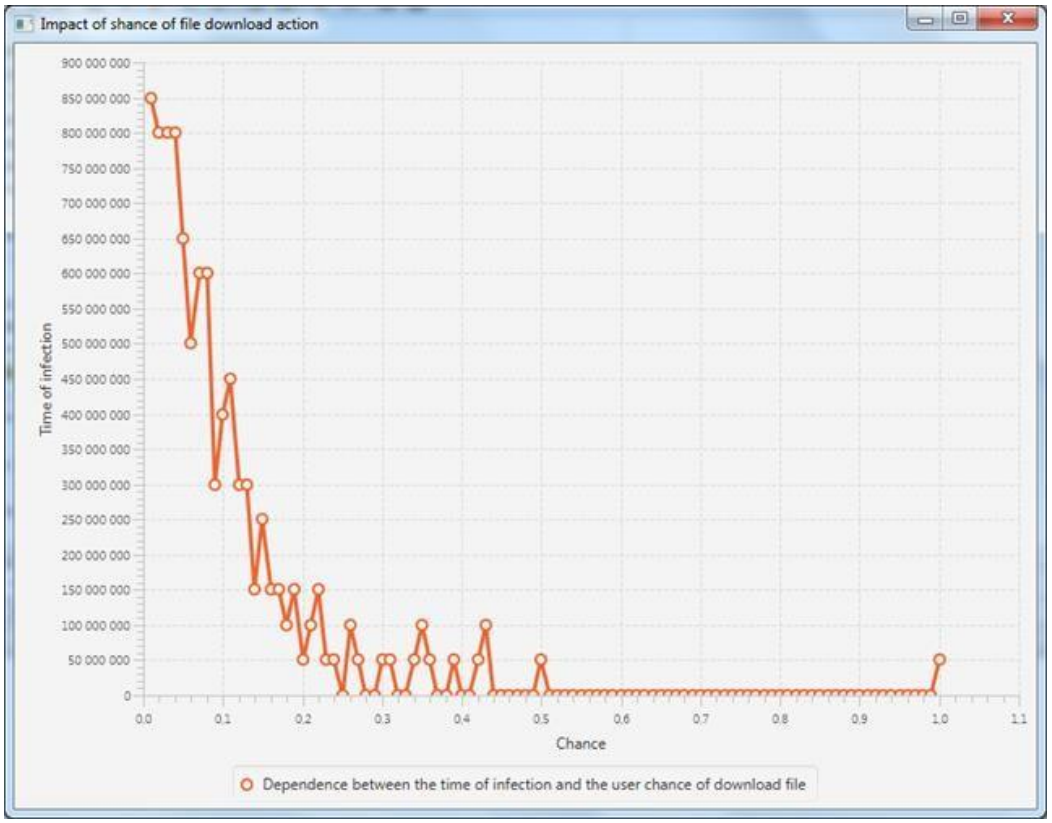

Рисунок 3.14 - Графік аналізу швидкості ураження від шансу завантажити файл

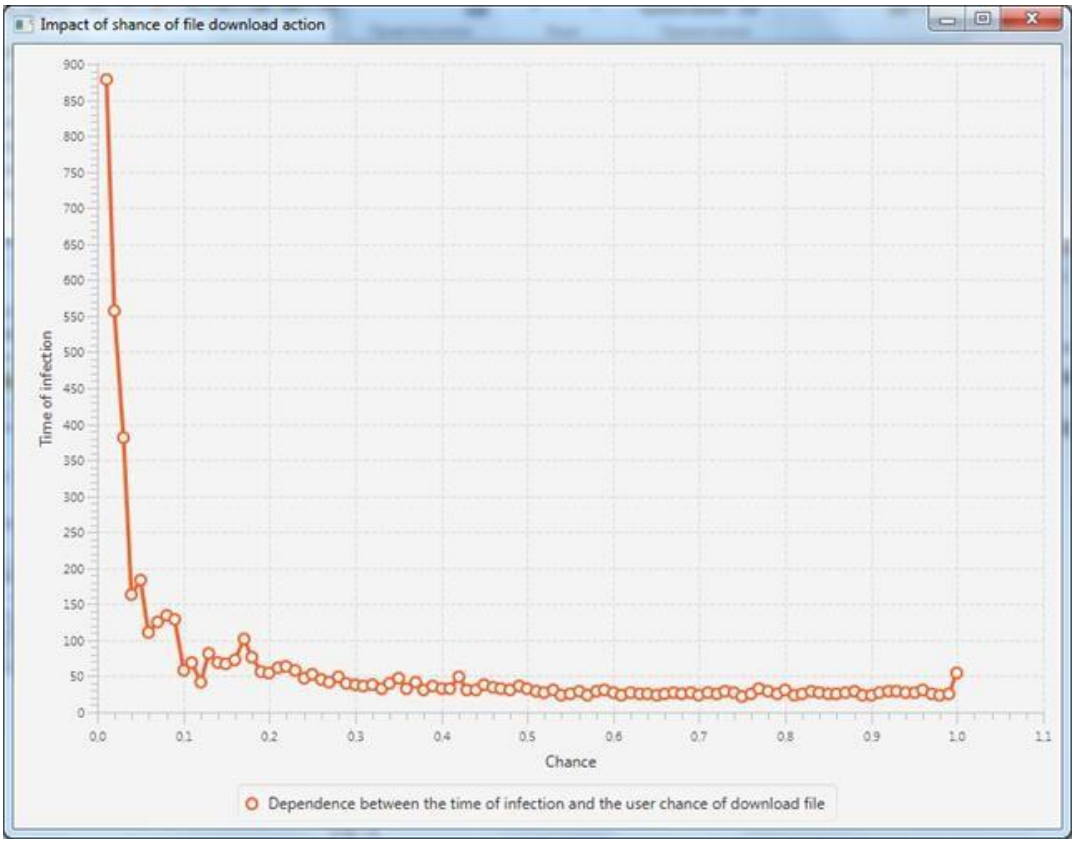

Рисунок 3.15 - Графік аналізу швидкості ураження від шансу завантажити файл у часовому діапазоні 100 секунд

За результатами моделювання графіків можна зробити висновок що при збільшенні шансу на відкриття зараженого файлу, або переходу на спам повідомлення з вірусом, зменшується час зараження ІС вірусом. З шансом відкриття файлу в 20% час ураження системи буде довгим, при шансі 25% і більше час ураження суттєво зменшується[14]. Якщо шанс завантаження файлу вище 50% відсотків то можливість того що ІС залишитися неушкодженою – зникає. Створені графіки підтверджують вірність побудови моделей і логічність вищевказаних тверджень.

3.3 Використання алгоритму Мережі Петрі для моделювання сценарію кіберзагрози вірусом SpyEye

За допомогою опису етапів процесів кіберзагроз UML діаграмою процесів, були змодельовані сценарій кібератак використовуючи Петрі-об’єтне моделювання стохастичних мереж Петрі.

Змодельований сценарій кіберзагроз за етапами:

– Хакер розповсюджує вірус в мережі Інтернет;

– Користувач заходить на інфікований ресурс, завантажує вірус;

– Вірус виконує інфікування пристрою (комп’ютера);

– Вірус викрадає / модифікує персональну інформацію і передає її хакеру;

– Хакер використовує персональну інформацію виконуючи злочин.

Моделі побудовані з урахуванням усього життєвого циклу вірусу.

На основі моделей є можливість оцінити кроки розповсюдження вірусу і можливі наслідки[15]. З використанням отриманих даних після моделювання, створений графік оцінки шансів для ураження приладів, за допомогою якого можна оцінити, що логічна модель правильно побудована і імітує реальний результат кіберзагрози. На основі дослідження визначені етапи кіберзагрози і їх подальші кроки шкідливих дій.

ВИСНОВКИ

В наш час питання захисту інформації стали важливими як ніколи, про це свідчить не лише зростаюча статистика збитків світової економіки від діяльності хакерів, котрі вже перейшли планку в триліон доларів загалом. Крім фінансових збитків хакери також можуть проводити цілком успішні атаки на об’єкти та компанії державного значення для тієї чи іншої країни, що в черговий раз підкреслює важливість вивчення методів роботи зловмисників та можливості протидії їм. Одним із таких методів є процес моделювання діяльності хакерів що дозволяють виявити потенційні вразливості системи та завчасно підготувати методи протидії для інформаційної системи.

Для подальшого моделюванню сценарію вірусу був використаний алгоритм стохастичних Петрі мереж і Петрі-об’єктний підхід моделювання. Вперше побудована модель сценарію життєвого циклу вірусу з використанням алгоритму мереж Петрі дала змогу змоделювати усі етапи поширення вірусу. За отриманими результатами було змодельована поведінка вірусу і складений графік шансу ураження приладу від дій користувача комп’ютером чи приладом Інтернет речей.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Cybercrimes URL: https://www.ixbt.com/live/offtopic/problemy-kiberbezopasnosti-v-nashe-vremya.html (дата звернення: 09.09.2023)

2. Modern cybercrimes URL: https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html (дата звернення: 17.09.2023)

3. Cybercrime threads URL: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/ (дата звернення: 29.09.2023)

4. Cybersecurity issues URL: https://online.maryville.edu/blog/cybersecurity-issues/ (дата звернення: 05.10.2023)

5. Economic impact URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf (дата звернення: 06.10.2023)

6. Cybercrimes in economics URL: https://www.linkedin.com/pulse/impact-cybercrime-individuals-businesses-society-join-welance (дата звернення: 15.10.2023)

7. Карпінський М.П. Атаки на відмову в обслуговуванні комп'ютерних мереж / М. П. Карпінський, У. О. Яциковська, А. В. Балик, М. Александер // Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі. – 2014. – № 806. – С. 94-99

8. Стеценко И.В. Дослідження дискретно-подійних систем з використанням технології Петрі-об’єктного моделювання // Управляющие системы и машины. – Киев, 2014. – №5 (253). - С.77-85.

9. Проектування графічного модуля програмного забезпечення Петрі-об’єктного моделювання систем / І. В. Стеценко, О. В. Василевська //

Вісник Черкаського державного технологічного університету. Сер. : Технічні науки. - 2013. - № 2. - С. 13-18.

10. Лоу А. Имитационное моделирование. Классика CS : Пер. с англ. / Аверилл М. Лоу, В. Дэвид Кельтон. – 3-е изд. – Киев : Издательская группа BHV, 2004. – 847 с.

11. Стеценко І. В. Проектування графічного модуля програмного забезпечення Петрі-об'єктного моделювання систем / І. В. Стеценко, О. В. Василевська // Вісник Черкаського державного технологічного університету. – Черкаси : ЧДТУ, 2013. – № 2. – С. 13-18.

12. Стеценко І. В. Імітаційне моделювання систем управління засобами сіток Петрі / І. В. Стеценко, А. А. Данилюк // Вісник Черкаського державного технологічного університету. – Черкаси, 2005. – № 3. – С. 293-295.

13. Огородников Д.В., дтн, доц, Стеценко. І.В. Моделювання Сценарію Кібератаки На Основі Атаки «Petya», «Notpetya» Безпека. Відмовостійкість. Інтелект ICSFTI2018, Київ, 10-12 травня. 2018. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 415 с.

14. Murata T. Petri Nets: Properties, Analysis and Applications / Tadao Murata // Proceedings of the IEEE. – 1989. – Vol. 77, No. 4. – P. 541-580.