УДК 004.05(045)
DOI https://doi.org/10.32782/IT/2025-1-12

Євгенія ІВАНЧЕНКО
доктор технічних наук, професор, директор Навчально-наукового інституту кібербезпеки та захисту інформації, Державний університет інформаційно-комунікаційних технологій, вул. Солом'янська, 7, Київ, Україна, 03110
***ORCID:** 0000-0003-3017-5752*

Ігор АВЕРІЧЕВ
кандидат економічних наук, доцент кафедри технічних систем кіберзахисту, Державний університет інформаційно-комунікаційних технологій, вул. Солом'янська, 7, Київ, Україна, 03110
***ORCID:** 0009-0008-9766-0115*

Євген КИХТЕНКО
аспірант, Державний університет інформаційно-комунікаційних технологій, вул. Солом'янська, 7, Київ, Україна, 03110

Бібліографічний опис статті: Іванченко, І., Аверічев, І., Кихтенко, Є. (2025). Дослідження механізмів підвищення ефективності захисту комп`ютерної мережі від поліморфних комп`ютерних вірусів. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 82–90, doi: https://doi.org/10.32782/IT/2025-1-12

ДОСЛІДЖЕННЯ МЕХАНІЗМІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ КОМП`ЮТЕРНОЇ МЕРЕЖІ ВІД ПОЛІМОРФНИХ КОМП`ЮТЕРНИХ ВІРУСІВ

***Мета роботи** – провести комплексний аналіз механізму підвищення ефективності захисту комп'ютерної мережі від поліморфних комп'ютерних вірусів, визначити переваги та недоліки компонентів, що входять до цього механізму, та запропонувати адаптивні підходи для протидії сучасним загрозам. Основна увага приділяється розробці інноваційних методів, які здатні ефективно протистояти поліморфним вірусам, що мають здатність змінювати свій код для уникнення виявлення традиційними антивірусними системами.*

***Методологія** дослідження полягає в розробці механізму аналізу поліморфних загроз, який ґрунтується на виявленні шаблонів змінності та статистичному аналізі поведінкових характеристик програм. Для підвищення ефективності захисту запропоновано використання методів поведінкового аналізу та алгоритмів машинного навчання, зокрема нейронних мереж, що дозволяють динамічно моделювати та виявляти аномальну активність в комп'ютерній мережі. Цей підхід дозволяє розпізнавати невідомі зразки шкідливих програм, враховуючи їх поліморфну природу, що є ключовим для протидії сучасним кіберзагрозам.*

***Наукова новизна** дослідження полягає в інтеграції адаптивних підходів, таких як поведінковий аналіз та машинне навчання, для ефективного розпізнавання невідомих зразків поліморфних вірусів. Це дозволяє враховувати їх здатність до зміни коду та уникнення виявлення традиційними антивірусними програмами. Запропонований механізм ґрунтується на використанні нейронних мереж для динамічного моделювання поведінки програм, що дозволяє швидко реагувати на нові загрози та адаптуватися до змін у коді вірусів. Це значно підвищує точність виявлення та знижує ризик помилкових спрацьовувань.*

***Висновки** дослідження підтверджують ефективність запропонованого механізму в протидії поліморфним вірусам завдяки динамічному підходу до виявлення аномальної активності. Реалізація таких методів дозволяє значно підвищити рівень захисту комп'ютерних мереж, зробивши їх більш стійкими до стрімкої еволюції сучасних кіберзагроз. Отримані результати свідчать про те, що використання машинного навчання та нейронних мереж є перспективним напрямом для розвитку систем кібербезпеки. Такі системи можуть ефективно протистояти невідомим загрозам, що особливо актуально у сучасних умовах, коли кількість і складність кібератак постійно зростають. У подальшому планується оптимізація запропонованого механізму для його інтеграції в реальні системи захисту комп'ютерних мереж, що дозволить забезпечити високий рівень безпеки та мінімізувати втрати від кібератак.*

***Ключові слова:** кібербезпека, кіберпростір, поліморфні віруси, нейронні мережі, адаптивний аналіз, виявлення загроз, поведінковий аналіз, алгоритми захисту.*

Yevheniia IVANCHENKO
Doctor of Technical Sciences, Professor, Director of the Educational and Scientific Institute of Cybersecurity and Information Protection of the State University of Information and Communication Technologies, 7, Solomyanska Str., Kyiv, Ukraine, 03110, e.ivanchenko@duikt.edu.ua
ORCID: *0000-0003-3017-5752*

Ihor AVERICHEV
Candidate of Economic Sciences, Associate Professor of the Department of Technical Cyber Defense Systems, State University of Information and Communication Technologies, 7, Solomyanska Str., Kyiv, Ukraine, 03110, iaverichev19@gmail.com
ORCID: *0009-0008-9766-0115*

Yevhen KYKHTENKO
Postgraduate Student, State University of Information and Communication Technologies, 7, Solomyanska Str., Kyiv, Ukraine, 03110

To cite this article: Ivanchenko, Ye., Averichev, I., Kykhtenko, Ye. (2025). Doslidzhennia mekhanizmiv pidvyshchennia efektyvnosti zakhystu komp`iuternoi merezhi vid polimorfnykh komp`iuternykh virusiv [Research on mechanisms to improve the efficiency of computer network protection against polymorphic computer viruses]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 82–90, doi: https://doi.org/10.32782/IT/2025-1-12

RESEARCH ON MECHANISMS TO IMPROVE THE EFFICIENCY OF COMPUTER NETWORK PROTECTION AGAINST POLYMORPHIC COMPUTER VIRUSES

The objective *of this undertaking is to execute a comprehensive assessment of the methodologies used to enhance the robustness of a computer network's defenses against polymorphic computer viruses. This involves identifying both the strengths and weaknesses inherent in the individual components comprising this protective mechanism, and ultimately proposing adaptive strategies to counteract contemporary threats. A primary focus will be placed on developing novel methods designed to effectively combat polymorphic viruses, which possess the ability to alter their code to evade detection by conventional antivirus systems.*

The novelty of the research *resides in the integration of adaptive methodologies, specifically behavioral analysis and machine learning techniques, to robustly identify previously unseen polymorphic virus samples. This is achieved by accounting for their inherent code mutation capabilities, preventing detection by conventional antivirus solutions. The suggested mechanism utilizes neural networks for the dynamic modeling of software behavior. This approach facilitates prompt response to emerging threats and the ability to adapt to changes within viral code. The outcome is a substantial increase in detection accuracy alongside a reduced occurrence of false positives.*

The study's findings *validate the proposed mechanism's effectiveness against polymorphic viruses, leveraging a dynamic approach for anomaly detection. Implementing these methods greatly enhances the security of computer networks, fortifying them against the rapid evolution of current cyber threats. The outcomes suggest that employing machine learning and neural networks is a promising avenue for advancements in cybersecurity systems. Such systems can effectively counter unknown threats, a critical need in the present environment where cyberattacks are escalating in number and complexity. Future efforts will focus on optimizing the suggested mechanism for its integration into actual network defense systems, ultimately ensuring high security levels and minimizing losses due to cyberattacks.*

Key words: *cybersecurity, cyberspace, polymorphic viruses, neural networks, adaptive analysis, threat detection, behavioral analysis, defense algorithms.*

Вступ. У сучасному світі динамічного розвитку інформаційних технологій захист комп'ютерних мереж стає ключовим завданням для забезпечення кібербезпеки. Серед численних загроз особливу небезпеку становлять поліморфні комп'ютерні віруси, які здатні змінювати свій код при кожному зараженні нової системи. Така властивість ускладнює їх виявлення традиційними методами захисту, що базуються на сигнатурному аналізі. Актуальність проблеми підвищується через зростання частоти використання поліморфного шкідливого програмного забезпечення у кібератаках, спрямованих на мережеву інфраструктуру підприємств, державних установ та окремих користувачів.

Сучасні дослідження в галузі кібербезпеки демонструють, що підвищення ефективності захисту можливе завдяки впровадженню адаптивних підходів, зокрема методів поведінкового аналізу та алгоритмів машинного навчання

(B. Zhurakovskyi, I. Averichev, I. Shakhmatov, 2023; А. Корченко, 2019). У статті запропоновано механізм виявлення та нейтралізації поліморфних вірусів, який базується на аналізі їх поведінкових характеристик та статистичних моделей аномальної активності. Такий підхід дозволяє протидіяти невідомим загрозам, забезпечуючи вищий рівень безпеки комп'ютерних мереж.

Постановка проблеми. З розвитком цифрових технологій та зростанням обсягів інформаційних потоків комп'ютерні мережі дедалі частіше стають об'єктами кібератак, які використовують нові, складніші види шкідливого програмного забезпечення. Одним із найсерйозніших викликів є поліморфні комп'ютерні віруси, які здатні адаптувати свій код для уникнення виявлення традиційними антивірусними системами. Їхня особливість полягає у використанні механізмів динамічної модифікації, що дозволяє ефективно обходити сигнатурний та статичний аналіз. Це значно ускладнює роботу спеціалістів з кібербезпеки та потребує впровадження нових підходів до захисту мережевих систем (С. Казмірчук, А. Корченко, Т. Паращук, 2018).

Існуючі методи захисту, такі як сигнатурні бази, статичний аналіз або простий евристичний підхід, мають обмежену ефективність у боротьбі з поліморфними загрозами. Водночас використання методів поведінкового аналізу, адаптивних алгоритмів та штучного інтелекту набуває все більшого значення для своєчасного виявлення та нейтралізації нових видів шкідливого програмного забезпечення. Проте наразі існує недостатня кількість оглядових досліджень, які б систематизували сучасні підходи до боротьби з поліморфними вірусами. Тому постає необхідність у ґрунтовному аналізі стану проблеми, огляді актуальних методів захисту та визначенні перспективних напрямів для їхнього подальшого розвитку (І. Терейковський, А. Корченко, Т. Паращук, Є. Педченко, 2018; K. Alieyan, 2016).

Аналіз останніх досліджень і публікацій. Використання шкідливого програмного забезпечення зростає з кожним днем, створюючи проблеми для користувачів комп'ютерних систем. Новими сферами застосування для отримання вигоди та переваг є військова та політична, в тому числі раніше фінансова (електронний ресурс, 2025).

Військові доктрини багатьох країн передбачають розвиток військових кіберпідрозділів, які розробляють і застосовують зброю масового ураження для нанесення матеріальних збитків інфраструктурі інших країн. Використання руйнівної технології ШПЗ дозволяє здійснювати віддалені атаки без необхідності наближення до цілі.

Особливу увагу слід приділяти захисту від атак в різних секторах країни, які можуть паралізувати критично важливу інфраструктуру та фінансовий сектор на тривалий час. Крім того, поява нових фінансових інструментів, таких як альтернативні валюти, стимулює злочинців до подальшої розробки шкідливого програмного забезпечення (ШПЗ) з метою отримання прибутку. При цьому шкідливе програмне забезпечення використовує обчислювальні потужності не тільки свої, але й інших користувачів, підключених до глобальної мережі. Тому своєчасне виявлення шкідливого програмного забезпечення є нагальним питанням для організацій та бізнесу.

Інформаційна сфера, яка є головною, впливає на стан соціально-політичної, економічної сфери діяльності. Складність процесів, які відбуваються в розподілених інформаційних системах (РІС), постійно зростає. Це призводить до того, що РІС застосовується для обміну інформацією та розв'язання різного типу завдань у всіх сферах людської діяльності, які можуть стати об'єктом зловживань.

В основі сучасної розподіленої інформаційної системи містяться засоби інформації, комунікаційні сервери, сервери вторинної і третинної інформації, різного типу процесори обробки інформації, обчислювальні комплекси системи, пристрої передачі інформації. Кожна розподілена інформаційна система має свої особливості, які обумовлені сферою її застосування.

Важливість і відповідальність задач, розв'язуваних за допомогою розподілених систем у реальному масштабі часу, обумовили високі вимоги до надійності цих систем, у яких, найчастіше, неможливо проведення технічного обслуговування під час функціонування і відмова всієї розподіленої інформаційної системи, або її окремих компонентів може привести до негативних наслідків. Крім того, зростає необхідність підвищення ефективності РІС, оскільки помилки, які можуть бути допущені призводять до суттєвих негативних наслідків.

Здатність розподіленої інформаційної системи виконувати необхідні функції та їх поведінку характеризується властивістю функціональної стійкості. Це означає, що зі структури виключаються несправні елементи, структура перебудовується, а параметри системи коригуються для пристосування.

Таким чином, аналіз вимог до розподілених інформаційних систем та існуючих наукових методів показує, що на сьогоднішній день

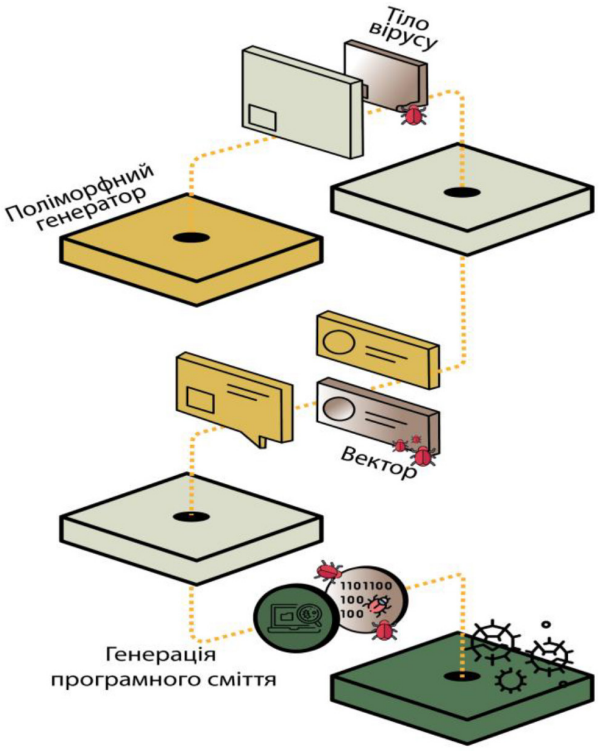

Рис. 1. Типова структура поліморфних вірусів

загострилось протиріччя між необхідністю забезпечення інформаційної системи властивістю функціональної стійкості в сенсі робастності системи відносно програмних збоїв, відмов, які утворилися в результаті кібернетичних атак з однієї сторони та недосконалістю існуючих наукових та інженерних методів забезпечити захист від кібернетичних загроз.

На сьогодні головними питаннями є оцінка продуктивності і якості, а також оптимізація існуючих або запланованих корпоративних мереж. Наприклад, у випадку самомодифікації поліморфних (олігоморфних) ІПС змінюються частини коду, але оригінальні алгоритми (вектори і тіло програми) залишаються недоторканими (M.Antonakakis, 2017).

Розглянемо типові структури поліморфних вірусів та метаморфних вірусів.

На рис. 1 представлено типова структура поліморфних вірусів.

Метаморфні віруси можуть змінювати свою структуру або код (трансформація коду, мутація, зміна порядку виконання) так, що вони стають абсолютно новими вірусами, які не можуть бути виявлені антивірусними програмами за сигнатурами попередніх екземплярів.

На рис. 2 представлено типова структура метаморфних вірусів.

Ефективність корпоративної мережі залежить від низки факторів, серед яких вибір протоколів передачі даних, операційних систем мережі та їх конфігурації, організація розподілених обчислювальних процесів, а також захист і відновлення після збоїв у роботі. Від цього залежить низка факторів, зокрема розподіл файлів баз даних, організація розподілених обчислювальних процесів, а також захист, підтримка і відновлення в разі збоїв або поломок (L.Adleman, 1988).

Протягом десятиліття старі методи і засоби комунікації відійдуть у минуле, поступившись місцем мережевим комунікаціям. Саме тому вкрай важливо володіти знаннями в галузі мережевих технологій.

Веб-сервер у корпоративній мережі може надавати користувачам послуги, подібні до тих, що надаються в Інтернеті, такі як гіпертекстові сторінки (включаючи текст, гіперпосилання, графіку і звук), надання ресурсів, запитуваних веб-клієнтами (L.Adleman, 1983). Корпоративні мережі є географічно розподіленими, вони об’єднують офіси, підрозділи та інші організації, які знаходяться на значній відстані один від одного.

Поки пакети даних знаходяться в окремих мережах або підмережах, проблема маршрутизації вирішується за допомогою методів, специфічних для інтерфейсів цих мереж. Маршрутизація – це завдання пошуку маршруту між комп’ютером, що надсилає дані, та комп’ютером, що їх отримує. В моделі зв’язаної IP-мережі це завдання зводиться, в першу чергу, до пошуку маршруту до шлюзу між мережами. IP-маршрутизація – це коли дані потрібно передати між різними мережами з різними інтерфейсами (M.Akiyamn, 2007).

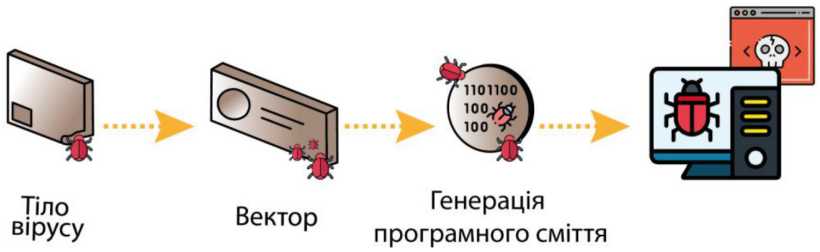

Рис. 2. Типова структура метаморфних вірусів

Якщо мережі одержувача і відправника з'єднані безпосередньо, дані повинні проходити через шлюзи, які з'єднують мережі. Якщо ці мережі не з'єднані шлюзом, дані повинні проходити через мережі між відправником і одержувачем і шлюз, що їх з'єднує. Коли дані досягають шлюзу в мережі одержувача, технологія маршрутизації цієї мережі спрямовує дані до одержувача. Щоб знайти маршрут до комп'ютера призначення, система зберігає таблицю маршрутизації, яку протокол мережевого рівня використовує для вибору відповідного мережевого інтерфейсу (S.Alqurashi, 2017).

Інформація про маршрутизацію зберігається у двох таблицях: перша – для маршрутів до хоста, друга – для маршрутів до мережі. Такий підхід дозволяє використовувати універсальний механізм маршрутизації як в розподілених мережах, так і в мережах типу «точка-точка». При визначенні маршруту модуль мережевого протоколу (IP) спочатку переглядає таблицю хостів, а потім таблицю мережі. Якщо пошук не вдається, використовується маршрут за замовчуванням.

Рішення про маршрутизацію можуть ґрунтуватися на різних показниках або комбінаціях показників. Програмні реалізації алгоритмів маршрутизації обчислюють вартість маршруту для визначення оптимального шляху до пункту призначення. Існує багато підходів до проблеми пошуку оптимального маршруту в мережі, які реалізовані в протоколах, що виконують маршрутизацію, таких як протоколи внутрішніх шлюзів (S. Alqurashi, 2017).

Найпоширеніші алгоритми це алгоритми вектора відстані та найкоротшого шляху. Це означає, що провайдери, які надають послуги клієнтам у вигляді доступу до Інтернету, повинні відповідати вимогам, щоб гарантувати якість обслуговування абонентів.

Інформація про перевантаження кабелю використовується в процесі маршрутизації. Тому необхідно розробити набори задач, які можуть бути інтегровані в системи управління комп'ютерними мережами як системи оптимізації навантаження на мережу. Інтеграція може бути здійснена безпосередньо шляхом встановлення набору задач як окремого модуля або віддалено шляхом підключення до віддаленого RMI-сервера та виклику його функцій. Сервер, що керує мережею, повинен збирати інформацію про поточний стан системи і передавати її на обробку в набір задач.

Формат передачі даних xml був обраний для збільшення швидкості передачі інформації через Інтернет. Після обробки отриманої інформації та визначення нового маршруту для існуючого, модуль комплексу задач надсилає на сервер відповідь у форматі xml, що містить дані про маршрут.

Вибір методу інтеграції залежить від розміру мережі та ресурсів, доступних для обчислювальних операцій. Чим більша мережа, тим більше даних потрібно обробити, щоб знайти рішення, і тим більше даних потрібно передати інформаційним технологіям. Якщо сервер, що керує мережею, має достатньо ресурсів для виконання обчислювальних операцій, має сенс встановити модулі для набору завдань безпосередньо на сервері, зменшивши витрати на передачу інформації. Однак, якщо сервер не має необхідної потужності, краще встановити потужний віддалений сервер для виконання складних завдань і виконання обчислювальних операцій з пошуку нових маршрутів у мережі.

Наразі маршрутизація в комп'ютерних мережах здійснюється за допомогою різних алгоритмів, які можна поділити на адаптивні та неадаптивні, глобальні та централізовані, статичні та динамічні (M. Alazab, 2016).

До сучасних алгоритмів маршрутизації ставляться такі вимоги:

– точність;
– простота;
– надійність;
– стійкість;
– справедливість;
– оптимальність.

Не всі сучасні алгоритми відповідають цим вимогам. Предиктивна інформаційна технологія дозволяє динамічно покращувати поточне навантаження в комп'ютерних мережах, незалежно від обраного для мережі алгоритму маршрутизації. Завдання полягає в тому, щоб зменшити відносну перевантаженість мережі, незалежно від алгоритму маршрутизації, який використовується для визначення шляхів передачі даних в мережі.

На рис. 3. представлено життєвий цикл поліморфного вірусу.

Наразі поліморфні віруси є складним явищем, яке важко діагностувати.

Поліморфні віруси покладаються на механізми мутації, щоб змінювати свої процедури дешифрування кожного разу, коли вони заражають машину.

Однак розширені антивірусні програми, які використовують евристичний аналіз, виявляють нові загрози, такі як поліморфні віруси. При цьому ретельно вивчається структура потенційної загрози, логіка програмування та зміст небажаного коду, незвичних інструкцій і поведінка загрози (Ponochovny P., 2024).

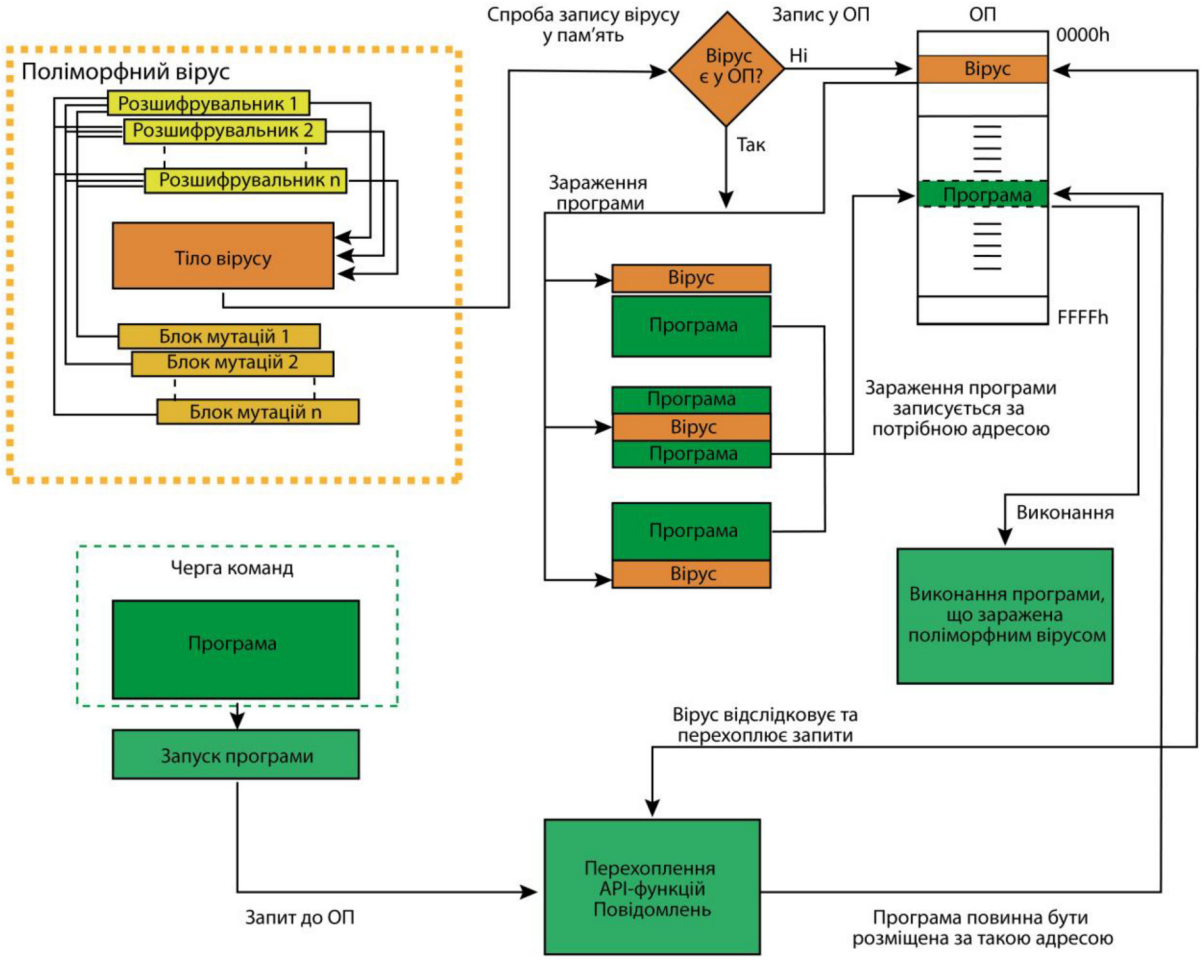

Рис. 3. Життєвий цикл поліморфних вірусів

Комп'ютерний вірус можна просто визначити як програму, яка заражає інші програми або системи шляхом їх модифікації для зловмисних цілей. Зараз злочинці використовують віруси, щоб заволодіти комп'ютерами нічого не підозрюючих користувачів. Пристрої заражені вірусом використовуються для створення ботнетів для розповсюдження спаму, виконання розподіленої відмови в обслуговуванні та викрадення даних ідентифікації. Комп'ютерні віруси змінилися від простого показу дратівливих повідомлень на екрані до впливу на репутацію компанії та впливу на прибутки бізнесу.

Зараз існує велика різноманітність антивірусних програм, які намагаються вирішити поширену проблему вірусів у комп'ютерних системах. Незважаючи на антивірусну індустрію на ринку, вірусні атаки не сповільнюються. Наприклад антивірусні рішення лабораторії McAfee повідомили про 69 277 289 унікальних шкідливих вірусів у 2023 році. Статистика показує зростання на 1631,9 % протягом року, тобто між 2022 і 2023 роками. Звіт Symantec повідомляє про загрози інтернет-безпеки та показує 125 % збільшення кількості вразливостей нульового дня між 2022 і 2023 роками (Guerid H., 2013).

Для того щоб вирішити проблеми вірусів у комп'ютерних системах використовують уніфікований доступ до обчислювальних ресурсів, який має назву Грід обчислення. Грід – це узгоджене, відкрите і стандартизоване середовище, яке розподіляє обчислювальні ресурси і ресурси зберігання даних, безпечно і скоординовано в рамках єдиної корпоративної мережі. Які територіально розподілені і забезпечують надійний та уніфікований доступ до обчислювальних ресурсів. Вони організовані на основі застарілої моделі набору персональних комп'ютерів, підключених до ієрархічної локальної мережі (LAN), в якій знаходяться сервери (Guharoy R., 2017).

На рис. 4 представлено уніфікований доступ до обчислювальних ресурсів.

Грід-обчислення використовуються в комерційних інфраструктурах для вирішення трудомістких завдань. Таким чином, традиційні рішення безпеки можуть нелегко вловити їх, оскільки вони не використовують статичний, незмінний код. Використання складних

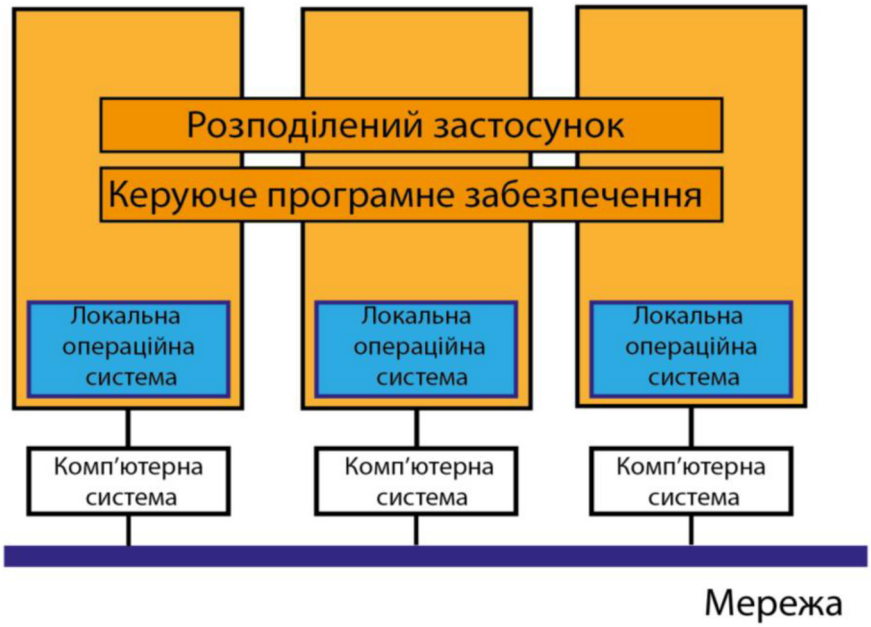

Рис. 4. Уніфікований доступ до обчислювальних ресурсів

механізмів мутації, які генерують мільярди процедур дешифрування, ще більше ускладнює їх виявлення.

Висновки. В роботі досліджується сучасний стан проблеми захисту комп'ютерних мереж від поліморфних вірусів, що є одним із найскладніших викликів у сфері кібербезпеки. З'ясовано, що традиційні підходи до виявлення шкідливого програмного забезпечення, зокрема сигнатурний аналіз і статичний підхід є малоефективними у боротьбі з динамічно змінними загрозами. Це пов'язано з тим, що поліморфні віруси здатні змінювати свій код та уникати виявлення стандартними антивірусними системами.

Аналіз показав, що за рахунок методів поведінкового аналізу та нейронних мереж можливо виявляти як відомі, так і невідомі зразки шкідливого програмного забезпечення, враховуючи їх поліморфну природу. Реалізація таких підходів сприятиме створенню більш безпечного інформаційного середовища та забезпеченню надійного захисту мережевих систем від новітніх викликів кібербезпеки. І в подальшому буде використовуватися для підвищення ефективності захисту комп'ютерної мережі від поліморфних комп'ютерних вірусів.

Перспективними напрямами подальших досліджень є вдосконалення алгоритмів аналізу поліморфних загроз, інтеграція методів машинного навчання у системи реального часу та розробка комплексних засобів захисту, які враховують особливості сучасних кіберзагроз.

ЛІТЕРАТУРА:

1. Using the Latest Methods of Cluster Analysis to Identify Similar Profiles in Leading Social Networks. Bohdan Zhurakovskyi, Ihor Averichev and Ivan Shakhmatov. Information Technology and Implementation (Satellite) Conference Proceedings, 21 November, 2023. URL: https://ceur-ws.org/Vol-3646/Paper_12.pdf

2. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 URL: https://nubip.edu.ua/sites/default/files/u34/monografiya_korchenko_anna_1.pdf

3. С. Казмірчук, А. Корченко, Т. Паращук, «Аналіз систем виявлення вторгнень». Захист інформації, Т. 20, № 4, с. 259–276, 2018. https://doi.org/10.18372/2225-5036.24.13431

4. І. Терейковський, А. Корченко, Т. Паращук, Є. Педченко, «Аналіз відкритих систем виявлення вторгнень». Безпека інформації Т. 24, № 3, с. 201–216, 2018. https://doi.org/10.18372/2225-5036.24.13431

5. Alieyan K. An overview of DDoS attacks based on DNS / K. Alieyan, M. M. Kadhum, M. Anbar, S. Ul. Rehman, N. KA. Alajmi. 2016 International Conference on Information and Communication Technology Convergence (ICTC). – Jeju Island (South Korea), October 19, 2016. Pp. 276–280.

6. Інформаційне агентство Уніан. Bloomberg: Китай міг вбудувати шпигунські чіпи у сервери Apple і Amazon URL: https://www.unian.ua/world/10286736-bloomberg-kitay-mig-vbuduvati-shpigunski-chipi-u-serveri-apple-i-amazon.html

7. Antonakakis M. Understanding the mirai botnet. M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, Yi. Zhou. 26th {USENIX} Security Symposium ({USENIX} Security 17)(Vancouver, BC). 2017. Pp. 1093–1110.

8. Adleman L. An Abstract Theory of Computer Viruses. Proceedings of the Conference on the Theory and Application of Cryptography. Santa Barbara, CA (USA), 21–25 August, 1988. Pp. 354–374.

9. Adleman L. A method for obtaining digital signatures and public-key cryptosystems / L. Adleman, R. Rivest, A. Shamir. Proceedings of the Communications of the ACM – Special 25-th Anniversary Issue. Vol. 26. 1983. Pp. 1–3.

10. Akiyama M. A proposal of metrics for botnet detection based on its cooperative behavior / M. Akiyama, T. Kawamoto, M. Shimamura, T. Yokoyama, Y. Kadobayashi, S. Yamaguchi. International Symposium on Applications and the Internet Workshops (SAINTW'07), Hiroshima (Japan) January 15–19, 2007. Pp. 82–85.

11. Alqurashi S. A Comparison of Malware Detection Techniques Based on Hidden Markov Model / S. Alqurashi, O. Batarfi. *Journal of Information Security*. 2016. Vol. 7. Pp. 215–223.

12. Alqurashi S. A comparison between API call sequences and opcode sequences as reflectors of malware behavior/ S. Alqurashi, O. Batarfi. 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST) (London, UK). 11.12.2017 Pp. 105–110.

13. Alazab M. Spam and criminal activity / M. Alazab, R. Broadhurst. Trends and Issues in Crime and Criminal Justice (Australian Institute of Criminology). December 3, 2016. Vol. 526 Pp. 1–20.

14. Ponochovny P. Low-speed http ddos attack prevention model for end users. *Cybersecurity: education, science, technique*. 2024. Vol. 2, no. 26. P. 291–304. https://doi.org/10.28925/2663-4023.2024.26.695

15. Guerid H. Privacy-preserving domain-flux botnet detection in a large scale network / H. Guerid, K. Mittig, A. Serhrouchni. Proceedings of the 2013 Fifth International Conference on Communication Systems and Networks. Bangalore (India), January 7–10, 2013. Pp. 1–9.

16. Guharoy R. A theoretical and detail approach on grid computing a review on grid computing applications / R. Guharoy et al. Proceedings of 8th Annual Industrial Automation and Electromechanical Engineering Conference. Bangkok (Thailand), August 16–18, 2017. Pp. 142–146.

REFERENCES:

1. Using the Latest Methods of Cluster Analysis to Identify Similar Profiles in Leading Social Networks. Bohdan Zhurakovskyi, Ihor Averichev and Ivan Shakhmatov. Information Technology and Implementation (Satellite) Conference Proceedings, 21 November, 2023. Retrieved from: https://ceur-ws.org/Vol-3646/Paper_12.pdf

2. Korchenko, A. (2019). Metody identyfikatsiyi anomal'nykh staniv dlya system vyyavlennya vtorhnen. [Methods for identifying abnormal conditions for intrusion detection systems]. Monohrafiia, Kyiv, TsP «Komprynt», Retrieved from: https://nubip.edu.ua/sites/default/files/u34/monografiya_korchenko_anna_1.pdf

3. Kazmirchuk, S., Korchenko, A., Parashchuk, T. 92018). Analiz system vyyavlennya vtorhnen [Analysis of intrusion detection systems]. Zakhyst informatsii, T. 20, № 4, c. 259–276, https://doi.org/10.18372/2225-5036.24.13431

4. Tereikovskyi, I., Korchenko, A., Parashchuk, T., Pedchenko, Ye. (2018). Analiz vidkrytykh system vyyavlennya vtorhnen [Analysis of open intrusion detection systems]. Bezpeka informatsii T. 24, № 3, c. 201–216, https://doi.org/10.18372/2225-5036.24.13431

5. Alieyan, K. (2016). An overview of DDoS attacks based on DNS/ K. Alieyan, M. M. Kadhum, M. Anbar, S. Ul. Rehman, N. KA. Alajmi. 2016 International Conference on Information and Communication Technology Convergence (ICTC). Jeju Island (South Korea), October 19, Pp. 276–280.

6. Informatsiine ahentstvo Unian. Bloomberg: Kytai mih vbuduvaty shpyhunski chipy u servery Apple i Amazon [UNIAN News Agency. Bloomberg: China could have embedded spy chips in servers Apple i Amazon] Retrieved from: https://www.unian.ua/world/10286736-bloomberg-kitay-mig-vbuduvati-shpigunski-chipi-u-serveri-apple-i-amazon.html

7. Antonakakis, M. 92017). Understanding the mirai botnet. M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, Yi. Zhou. 26th {USENIX} Security Symposium ({USENIX} Security 17)(Vancouver, BC). Pp. 1093–1110.

8. Adleman, L. (1988). An Abstract Theory of Computer Viruses. Proceedings of the Conference on the Theory and Application of Cryptography. Santa Barbara, CA (USA), 21–25 August, Pp. 354–374.

9. Adleman, L.A. (1983). method for obtaining digital signatures and public-key cryptosystems / L.Adleman, R.Rivest, A.Shamir. Proceedings of the Communications of the ACM – Special 25-th Anniversary Issue. Vol. 26. Pp. 1–3.

10. Akiyama, M.A. (2007). proposal of metrics for botnet detection based on its cooperative behavior / M.Akiyama, T.Kawamoto, M.Shimamura, T.Yokoyama, Y.Kadobayashi, S.Yamaguchi. International Symposium on Applications and the Internet Workshops (SAINTW'07), Hiroshima (Japan) January 15–19, Pp. 82–85. [in Japan].

11.Alqurashi S.A. (2016). Comparison of Malware Detection Techniques Based on Hidden Markov Model / S.Alqurashi, O.Batarfi. *Journal of Information Security*. Vol. 7. Pp. 215–223.

12. Alqurashi, S.A. (2017). comparison between API call sequences and opcode sequences as reflectors of malware behavior/ S.Alqurashi, O.Batarfi. 12th International Conference for Internet Technology and Secured Transactions (ICITST) (London, UK). 11.12.2017. Pp. 105–110.

13. Alazab, M. (2016). Spam and criminal activity / M.Alazab, R.Broadhurst. Trends and Issues in Crime and Criminal Justice (Australian Institute of Criminology). – December 3,. Vol. 526, Pp. 1–20.

14. Ponochovny, P. (2024). Low-speed http ddos attack prevention model for end users. *Cybersecurity: education, science, technique*. Vol. 2, no. 26. P. 291–304. https://doi.org/10.28925/2663-4023.2024.26.695.

15. Guerid, H. (2013). Privacy-preserving domain-flux botnet detection in a large scale network / H.Guerid, K.Mittig, A.Serhrouchni. Proceedings of the 2013 Fifth International Conference on Communication Systems and Networks. Bangalore (India), January 7–10, Pp. 1–9.

16. Guharoy, R. (2017). A theoretical and detail approach on grid computing a review on grid computing applications / R.Guharoy et al. Proceedings of 8th Annual Industrial Automation and Electromechanical Engineering Conference. Bangkok (Thailand), August 16–18, Pp. 142–146.