DOI: 10.58254/viti.3.2023.16.143

УДК 004.056.57

доктор філософії Фесьоха В. В. ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
Кисиленко Д. Ю. ORCID: 0000-0001-5491-6231 (ВІТІ ім. Героїв Крут)
доктор філософії Нестеров О. М. ORCID: 0000-0001-5092-6205 (ВІТІ ім. Героїв Крут)

АНАЛІЗ СПРОМОЖНОСТІ ІСНУЮЧИХ СИСТЕМ АНТИВІРУСНОГО ЗАХИСТУ ТА ПОКЛАДЕНИХ У ЇХНЮ ОСНОВУ МЕТОДІВ ДО ВИЯВЛЕННЯ НОВОГО ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У ВІЙСЬКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У статті вирішується завдання аналізу спроможності існуючих антивірусних систем та покладених у їх основу методів до виявлення нового шкідливого програмного забезпечення в інформаційних системах критичної інфраструктури, зокрема сектору сил оборони держави. Зазначено, що офіційні дані розробників антивірусних систем часто не підтверджують задекларований рівень точності виявлення нового шкідливого програмного забезпечення на практиці. До того ж, у більшості випадків задекларований показник точності виявлення нового шкідливого програмного забезпечення є вищим за аналогічний показник виявлення відомого шкідливого програмного забезпечення, що свідчить про тестування розглянутих антивірусних систем у специфічних умовах, занадто відмінних від реальних.

Описано властивості нового шкідливого програмного забезпечення з метою пошуку найбільш відповідного йому класу комп'ютерних вірусів. Класи поліморфних (олігоморфних) та метаморфних вірусів демонструють найбільш повну відповідність зазначеним властивостям, що дозволяє стверджувати про їх значну частку у застосуванні нового шкідливого програмного забезпечення.

Наведено характеристику методів виявлення шкідливого програмного забезпечення, які завдяки своїм властивостям спроможні певною мірою адаптуватися до метаморфної (поліморфної) їх природи. Найбільш повну відповідність демонструють методи, в основу яких покладено теорію нечіткої логіки.

Запропоновано напрям удосконалення існуючих антивірусних систем щодо підвищення адаптивності до виявлення нових (поліморфних, метаморфних) класів шкідливого програмного забезпечення. Отримані результати доцільно розглядати, як підґрунтя для реалізації нових підходів до виявлення шкідливого програмного забезпечення з метою ідентифікації раніше невідомих його екземплярів, що дозволить значно підвищити ефективність забезпечення кібербезпеки сучасних інформаційних систем та мереж.

Ключові слова: *шкідливе програмне забезпечення, комп'ютерний вірус, поліморфні віруси, метаморфні віруси, антивірус, нечітка логіка, кіберзахист.*

V. Fesokha, D. Kysylenko, O. Nesterov Analysis of the capacity of existing anti-virus protection systems and their based methods for detecting new malware in military information systems.

The article solves the task of analyzing the ability of existing anti-virus systems and the methods based on them to detect new malicious software in information systems of critical infrastructure, in particular, the sector of the state defense forces. It is noted that the official data of the developers of antivirus systems often do not confirm the declared level of accuracy of detecting new malicious software in practice. In addition, in most cases, the declared accuracy rate of detecting new malware is higher than the similar rate of detection of known malware, which indicates that the antivirus systems in question are tested in specific conditions that are too different from real ones.

The properties of new malicious software are described in order to find the most suitable class of computer viruses. Classes of polymorphic (oligomorphic) and metamorphic viruses demonstrate the most complete compliance with the specified properties, which allows us to assert their significant share in the use of new malicious software.

The characteristics of malicious software detection methods are given, which due to their properties are able to adapt to a certain extent to their metamorphic (polymorphic) nature. Methods based on the theory of fuzzy logic demonstrate the most complete correspondence.

The direction of improvement of the existing anti-virus systems in order to increase the adaptability to the detection of new (polymorphic, metamorphic) classes of malicious software is proposed. The obtained results should be considered as a basis for the implementation of new approaches to the detection of malicious software in order to identify previously unknown instances of it, which will allow to significantly increase the effectiveness of ensuring cyber security of modern information systems and networks.

Keywords: *malware, computer virus, polymorphic viruses, metamorphic viruses, antivirus, fuzzy logic, cyber protection.*

Актуальність та постановка завдання в загальному вигляді. В існуючих умовах ведення кібервійни залишає не вирішеним завдання ефективного кіберзахисту інформаційних систем (ІС) критичної інфраструктури держави, зокрема ІС військового призначення, оскільки багато в чому забезпечення національної безпеки, захист територіальної цілісності та управління військами реалізується їх засобами [1].

Об'єктивно, сторона кібервпливу завжди має перевагу, оскільки ентропія комплексу її заходів для сторони кіберзахисту є досить високою, що у свою чергу, не дозволяє досягти хоча б ситуації паритету у процесі протиборства у кіберпросторі в режимі реального часу. Одним із основних підходів до реалізації описаної переваги є застосування нового шкідливого програмного забезпечення (ШПЗ), боротьба з яким, як правило, можлива не раніше стадії ліквідації його наслідків, а численні факти деструктивного впливу на ІС демонструють неспроможність існуючих систем антивірусного захисту виявляти та протидіяти їм достатньою мірою, внаслідок чого зростають вимоги до існуючих антивірусних програм [2].

За даними [3] міжнародної компанії AV-TEST (незалежна організація, яка вивчає та оцінює антивірусне ПЗ та пакети безпеки для популярних операційних систем (ОС) за різними критеріями) за останнім часом приріст нових комп'ютерних вірусів сягає нових рекордів. Зокрема для ОС Windows з'явилося близько 70 мільйонів нових зразків ШПЗ, що значно перевищує показник ОС macOS, для якої було зафіксовано лише близько 12 000 нових вірусів. Для ОС Linux зловмисники створили близько 2 мільйонів шкідливих програм. Причому динаміка появи нових видів (типів) ШПЗ ілюструє зміну вектора його застосування з добування криптовалюти на вимагання коштів від постраждалих, внаслідок деструктивної діяльності ШПЗ, а з початку 2022 року значно зріс відсоток інформаційно-руйнівного впливу на критичну інфраструктуру України з боку росії з метою викрадення інформації, що є особливо пріоритетним для забезпечення кібербезпеки ІТ-інфраструктури сил оборони і безпеки держави під час воєнного стану.

Нижче наведено стислий опис деяких деструктивних впливів на інформаційні сервіси різних держав засобами ШПЗ, які набули широкого розголосу протягом останнього часу.

1. 02 березня 2022 року фахівці центру виявлення загроз Threat Intelligence Center корпорації Microsoft виявили небезпечний вірус, так званий "FoxBlade" ("Fox" – лисиця і "Blade" – клинок), націлений на фінансові установи та міністерства України. Згідно із заявою [4] даний вірус реалізував деструктивний вплив на цифрову інфраструктуру України, зокрема банки, військові об'єкти, державні установи та промислові підприємства. Шляхом видалення даних із комп'ютерів, підключених до мережі Інтернет.

2. 02 червня 2022 року низку державних організацій України було атаковано ШПЗ Cobalt Strike Beacon, що призвело до численних перебоїв у їх роботі на певний час. Розповсюдження ШПЗ здійснювалося засобами електронної пошти через файл "Зміни оплата праці з нарахуваннями.docx". Відкриття файлу ініційовувало завантаження та виконання шкідливого скрипту засобами додатка MS Office. Також реалізація деструктивного впливу зловмисниками передбачала застосування експлойтів, сценарії яких використовували вразливість Microsoft Trident – функціонального ядра браузера Internet Explorer. Наявні системи антивірусного захисту не змогли перешкодити цьому деструктивному впливу [5].

3. 10 жовтня 2022 року компанії в Україні та Польщі було атаковано засобами ШПЗ Prestige [6]. Програма отримує доступ до облікових записів користувачів з метою шифрування файлів, додає розширення "enc", а також вимагає викуп в обмін на інструмент для розшифровування. Microsoft виділила кілька особливостей вірусу Prestige, які раніше не зустрічалися експертам з кібербезпеки. Незважаючи на подібні методи розгортання, кампанія Prestige відрізняється від недавніх руйнівних кібератак з використанням AprilAxe (ArguePatch)/CaddyWiper або Foxblade (HermeticWiper), які протягом останніх двох тижні до інциденту стосувалися кількох критично важливих об'єктів інфраструктури України. Вірус використовує бібліотеку CryptoPP C++ для шифрування AES кожного відповідного файлу. У процесі шифрування одна версія програми-вимагача використовує наступний

запрограмований відкритий ключ RSA X509 (кожна версія Prestige може мати унікальний відкритий ключ).

4. 17 грудня 2022 року урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA отримано інформацію щодо розповсюдження засобами електронної пошти (з використанням скомпрометованої електронної адреси одного зі співробітників оборонного відомства), а також, мессенджерів, повідомлення щодо необхідності оновлення сертифікатів у системі "Delta" (спеціалізоване програмне забезпечення (ПЗ) для ситуаційної обізнаності про противника). ШПЗ у розширенні pdf повністю імітувало легітимні дайджести одного з підрозділів, але містило посилання на zip-архів зі шкідливим вмістом. При переході за посиланням на комп'ютер завантажувався архів, який містив виконуваний файл деструктивного впливу, що захищений за допомогою VMProtect (спосіб захисту від аналізу та зламу). Після запуску виконуваного файлу на комп'ютері створювалося декілька dll-файлів з метою імітації процесу встановлення сертифіката. У результаті на комп'ютері здійснювався запуск ШПЗ RomCom, яке, у свою чергу, забезпечувало виконання інших шкідливих програм: FateGrab (викрадення файлів) та StealDeal (отримання та збереження даних браузерів у відповідних файлах з метою їх подальшої несанкціонованої передачі [7].

5. 10 лютого 2023 року російська хакерська група, яка стояла за руйнівними кібератаками з використанням ШПЗ WhisperGate, знову націлилась на українські організації з метою крадіжки інформації засобами нового ШПЗ [8]. Зловмисники націлені в першу чергу на Україну, але також атакували країни – члени НАТО в Північній Америці та Європі. ШПЗ маскується під програми-вимагачі, але робить цільові пристрої повністю непрацездатними та нездатними відновлювати файли, навіть якщо виплачується викуп. Під час нової хвилі кібератак зловмисники використовують раніше невідоме ШПЗ для крадіжки інформації під назвою Graphiron, яке використовувалося принаймні до середини січня 2023 року.

6. 20 березня 2023 за інформацією Держспецзв'язку [9], російські хакери поширюють шкідливі файли за допомогою безкоштовного доступу на торент-трекерах. Зокрема, якщо встановити такі файли на комп'ютер, зловмисники отримують доступ до вмісту комп'ютера й довгий час залишаються непомітними. У Держспецзв'язку зазначають, що жертвою хакерів можуть стати пересічні українці, які встановлюють неліцензійне програмне забезпечення (ПЗ) з неофіційних джерел та торентів.

Описані факти обумовлюють актуальність проведення подальших наукових досліджень щодо підвищення ефективності існуючих систем антивірусного захисту ІС військового призначення у процесі виявлення нового ШПЗ.

Аналіз останніх публікацій. Дослідженню ефективності застосування методів виявлення ШПЗ з метою пошуку напрямків вдосконалення існуючих систем антивірусного захисту присвячена значна кількість робіт [6–9], аналіз основних із яких викладено нижче.

У роботі [10] запропоновано підхід до аналізу методів виявлення ШПЗ на основі виокремлення критеріїв класифікації, які дозволять підвищити ефективність та достовірність виявлення нового ШПЗ: характер отриманих даних, ознаки, що виступають об'єктом пошуку та дослідження, методи аналізу, алгоритм прийняття рішень, очікуваний результат та оцінка класифікації. Даний підхід розширює існуючу класифікацію методів виявлення ШПЗ, однак не дозволяє класифікувати їх по найбільш повній відповідності характеристикам, властивим новому ШПЗ.

У роботі [11] виконано дослідження сигнатурного та евристичного методів виявлення ШПЗ. Наведено порівняльну характеристику методів машинного навчання, графічної візуалізації, евристичних методів виявлення ШПЗ та систематизовано їх за значеннями точності пошуку. Для ефективного виявлення нового ШПЗ запропоновано комбінувати всі сучасні методи, способи і засоби, враховуючи особливості їх використання. Даний підхід не дозволяє краще зрозуміти принципи застосування нового ШПЗ.

У роботі [12] розглянуто динаміку розвитку ШПЗ, а також здійснено огляд ряду методів виявлення програм, які можуть становити загрозу для комп'ютерних систем. Проаналізовано сигнатурні та поведінкові підходи. Окреслено недоліки існуючого методологічного апарату.

Основну увагу приділено евристичним методам на основі викликів API, N-грам та опкодів. Визначено шляхи подальших досліджень у напрямі комплексування досліджених методів з графами контролю потоків (CFG) та використання методів штучного інтелекту. Даний підхід також не дозволяє краще зрозуміти принципи застосування нового ШПЗ.

У роботі [13] наведений детальний огляд типів шкідливих програм, досліджуються та порівнюються методи їх аналізу та виявлення. Серед особливостей нового ШПЗ зазначено їх здатність до самомодифікації. Запропоновано підхід до виявлення поліморфного ШПЗ на основі поєднання переваг евристичних методів та методів машинного навчання. Даний підхід не дозволяє краще зрозуміти принципи застосування нового ШПЗ у повній мірі, оскільки не враховує усю множину властивостей нового ШПЗ.

Наявність недоліків у наведених наукових працях, а також численні факти вдалих спроб здійснення деструктивного впливу [4–9] на ІС демонструють неспроможність існуючих систем антивірусного захисту в силу обмеженості покладених у їх функціональне ядро алгоритмів, способів, моделей, методів та методик ідентифікації ШПЗ виявляти та протидіяти їм повною (достатньою) мірою, внаслідок чого зростають вимоги до існуючих систем антивірусного захисту ІС.

У зв'язку з цим, виникає завдання аналізу спроможності існуючих систем антивірусного захисту та покладених у їх основу методів виявлення ШПЗ до виявлення нових його екземплярів у військових ІС.

Метою статті є аналіз спроможності існуючих систем антивірусного захисту та покладених у їх основу методів виявлення ШПЗ до ідентифікації нового ШПЗ у військових ІС.

Спроможність рейтингових антивірусних систем до виявлення нового ШПЗ. Під спроможністю антивірусних систем та покладених у їх основу методів до виявлення нового ШПЗ будемо розуміти точність його виявлення.

Відповідно до офіційних даних [14–19] розробників популярного антивірусного ПЗ спроможність запропонованих ними програмних систем до виявлення екземплярів відомого ШПЗ є майже бездоганною за показником точності (не нижче 95 %), тоді як виявлення нових типів ШПЗ, зокрема вірусів, демонструє точність не нижче 98 %. Однак офіційні дані розробників антивірусного ПЗ часто не підтверджують задекларований рівень точності та/або достовірності виявлення нового ШПЗ на практиці, про що свідчить вищезазначена фактологія [4–9]. До того ж у більшості випадків задекларований показник точності виявлення нового ШПЗ є вищим за аналогічний показник виявлення відомого ШПЗ, що неприпустимо, оскільки метод сигнатурного аналізу, який покладено у основу їх модулів виявлення відомого ШПЗ є ефективнішим. В таблиці 1 наведено офіційну характеристику спроможності популярних антивірусних програм до виявлення відомого і нового ШПЗ [14–19].

Таблиця 1

Стисла характеристика спроможності популярних антивірусних програм до виявлення відомого і нового ШПЗ

№ з/п	Найменування антивірусного ПЗ	Відоме ШПЗ		Нове ШПЗ		
		Методи виявлення	Точність (%)	Методи виявлення	Точність «0-day» (%)	Точність виявлення нового ШПЗ (%)
1	Avira Antivirus	Сигнатурний аналіз Евристичний аналіз	95	Машинне навчання	99,6	–
2	ESET NOD 32	Сигнатурний аналіз Аналіз поведінки	100	Машинне навчання Евристичний аналіз	98	–
3	Panda	Сигнатурний аналіз Аналіз поведінки	99,7	Нейронні мережі	100	–
4	Avast Free Antivirus	Сигнатурний аналіз Аналіз поведінки	99,8	Нейронні мережі Евристичний аналіз	100	–

Avira Antivirus декларується як одна з кращих антивірусних програм для захисту кінцевих пристроїв. За результатами досліджень інституту AV-Test Avira отримала нагороду 2022 року в тестовій категорії "Найкращий захист споживачів під Windows". Захист споживачів від ШПЗ під управлінням платформи Windows є пріоритетним завданням, адже це найбільша група користувачів у світі [14; 15].

ESET NOD 32 є антивірусним ПЗ, що використовується для захисту кінцевих пристроїв від різних типів загроз. Має широкі можливості сканування файлів перед їх виконанням, що дає змогу певною мірою виявляти та блокувати навіть нові загрози [16]. Використовується у ІС та мережах Збройних Сил України.

Антивірусна програма ***Panda*** декларується як краща програма для захисту у реальному часі. Додаткові функції: захист від фішингу, захист Wi-Fi, фаєрвол, захист від програм-вимагачів та захист USB-пристроїв. Особливості: мінімальний вплив на систему [17].

Avast Free Antivirus декларується як одна з кращих програм антивірусного захисту із найменшим завантаженням ОС. Додаткові функції: інструменти управління паролями, оптимізація системи та VPN [18]. Антивірус Avast після отримання нагород в трьох тестових категоріях: "Найкращий захист для споживачів під Windows", "Найкращий захист Android для споживачів", "Найкращий захист macOS для споживачів " визнаний найкращим продуктом в галузі ІТ-безпеки 2022 року [19].

На основі проведеного аналізу популярних систем антивірусного захисту за спроможністю до виявлення відомого і нового ШПЗ можна зробити такі висновки:

1. Задекларована спроможність розглянутих систем антивірусного захисту є майже бездоганною, що досягається засобами покладених у їх основу методів виявлення ШПЗ, проте цей факт потребує додаткового вивчення. Так, декларація спроможності виявлення нових типів ШПЗ представлена статистикою виявлення вірусів нульового дня (0-day), тоді як вірус нульового дня та новий вірус – кардинально різні поняття. Новий комп'ютерний вірус – новий тип ШПЗ, який, як правило, становить собою модифікацію існуючого вірусу (поліморфізм/метаморфізм) з новими функціями або абсолютно нове ШПЗ, яке реалізує раніше невідомі способи (алгоритми) здійснення інформаційно-руйнівного впливу. Вірус 0-day – вразливість у ПЗ, яка ще не була виявлена розробниками антивірусних програм.

2. Ураховуючи багаторічний світовий досвід наукової спільноти щодо виявлення ШПЗ, отримані показники точності наведених результатів в аспекті виявлення нового ШПЗ у порівняно з відомим ШПЗ свідчать про тестування розглянутих антивірусних систем у специфічних умовах, занадто відмінних від реальних.

3. У зв'язку з відсутністю офіційних даних про результати виявлення нового ШПЗ [14–19], а також пошуку причин недостатньої ефективності застосування існуючих систем антивірусного захисту [4–9] виникає необхідність дослідження властивостей застосування нового ШПЗ, а також методів, спроможних його виявляти.

Дослідження властивостей нового ШПЗ. Характерні особливості нового ШПЗ можуть змінюватися залежно від його типу та вектора впливу на об'єкт атаки. Серед 22 типів ШПЗ [20] найпоширенішим є *комп'ютерні віруси* (англ. computer virus) – спеціалізовані програми, що володіють здатністю до самовідтворення і, як правило, здатні здійснювати дії, які можуть порушити функціонування комп'ютерної системи і/або зумовити порушення її політики безпеки.

У зв'язку з цим, пропонується порівняльний аналіз існуючих типів комп'ютерних вірусів за наступними критеріями на предмет відповідності властивостям нового ШПЗ:

нові методи інфікування;

шифрування власного коду (тіла) для захисту від виявлення та аналізу;

нові методи обходу антивірусних програм та інших відомих заходів (політик) захисту;

збільшення функціональності;

підвищення ефективності маскування;

використання технологій штучний інтелекту, блокчейну;

використання нових вразливостей ПЗ (0-day) тощо.

Дослідження характерних ознак наведено множини типів комп'ютерних вірусів на предмет відповідності вищезазначеним властивостям нового ШПЗ показало найбільш повну відповідність властивостей з поліморфними (олігоморфними) та метаморфними вірусами. Так, всі перераховані віруси є представниками типу, що відрізняється від решти типів алгоритмом дій та реалізують: нові методи обходу антивірусних програм та інших заходів відомих захисту у тому числі шляхом шифрування власного коду для захисту від виявлення та аналізу. У таблиці 2 наведено результати аналізу властивостей комп'ютерних вірусів.

Таблиця 2

Результати аналізу властивостей існуючих комп'ютерних вірусів

Віруси	**Нові методи інфікування**	**Шифрування власного коду**	**Нові методи обходу засобів захисту**	**Збільшення функціональності**	**Підвищення ефективності маскування**	**Використання передових технологій**	**Використання нових вразливостей ПЗ (0-day)**
1	2	3	4	5	6	7	8
За деструктивними можливостями							
Безпечні	–	–	–	+	–	–	–
Нешкідливі	–	–	–	+	–	–	–
Небезпечні	–	–	–	+	–	–	–
Руйнівні	+	–	–	+	–	–	+
За способом зараження							
Резидентні	+	–	–	+	–	–	+
Нерезидентні	+	–	–	+	–	–	+
За середовищем існування							
Файлові	+	–	–	+	–	+	–
Мережеві	+	–	–	+	–	+	+
Завантажувальні	–	–	–	+	–	–	+
Flash-віруси	–	–	–	+	–	–	–
Макровіруси	–	–	–	+	–	–	–
За особливостями алгоритму дій							
1	2	3	4	5	6	7	8
«Стелс»-віруси (віруси-невидимки)	+	–	+	+	+	–	+
Паразитичні	+	–	–	+	–	–	–
Поліморфні (олігоморфні)	+	+	+	+	+	+	+
Метаморфні	+	–	+	+	+	+	+
Віруси-супутники	+	–	–	–	–	–	–

Так, у випадку самомодифікації поліморфного (олігоморфного) ШПЗ частина його коду змінюється [20], зберігаючи початковий алгоритм неушкодженим (вектор і тіло програми), в якому закладено основний сценарій реалізації деструктивної діяльності. На рисунку 1 представлено узагальнену структуру поліморфних вірусів.

Рис. 1. Типова структура поліморфного вірусу

Виявлення такого типу вірусів можливе лише після розробки його сигнатури, а факт незмінності функціонального призначення тіла вірусу, що реалізує його вектор, дає підставу для виявлення нового ШПЗ на основі ідентифікації спільних структур вже класифікованих їх типів. Поліморфні та метаморфні віруси становлять основну частку нового ШПЗ, оскільки нові комп'ютерні віруси у своїй більшості являють собою модифіковані версії існуючого ШПЗ [21].

Метаморфні віруси можуть змінювати свою структуру і код таким чином, що вони стають абсолютно новим вірусом, який не може бути виявлено антивірусною програмою за сигнатурою попереднього екземпляра (перетворення коду, мутація, зміна порядку виконання). На рисунку 2 наведено узагальнену типову структуру метаморфних вірусів.

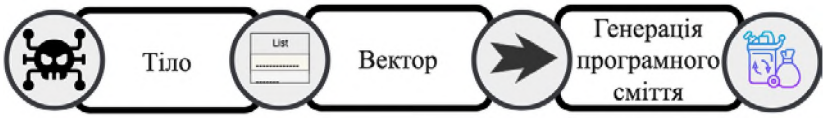

Рис. 2. Типова структура метаморфного вірусу

У зв'язку з наявністю властивості метапрограмування з метою уникнення виявлення антивірусними системами поліморфні (олігоморфні) та метаморфні віруси є особливо небезпечними для комп'ютерних систем та мереж військового призначення. До того ж поліморфні та метаморфні віруси становлять основну частку нового ШПЗ, оскільки нові комп'ютерні віруси у своїй більшості являють собою модифіковані версії існуючого ШПЗ [18].

Оцінка спроможності виявлення нового ШПЗ існуючими методами. Із множини існуючих підходів до аналізу ШПЗ найбільш доцільним є динамічний аналіз, оскільки дозволяє виявляти деструктивну діяльність різних програм безпосередньо під час виконання. Динамічний аналіз ШПЗ виділяє методи, спроможні певною мірою виявляти нове ШПЗ, завдяки властивості адаптації [22]. Крім того, внаслідок зростання вимог до антивірусних систем [22], порівняння методів виявлення ШПЗ має ґрунтуватись на властивостях верифікованості та спроможності до виявлення нового ШПЗ: *наявність невідомих унікальних характеристик, рівень хибних спрацьовувань, розмитість досліджуваних даних* (табл. 3).

Таблиця 3

Результати аналізу методів виявлення нового ШПЗ за визначеними критеріями

Метод	**Верифікованість**	**Спроможність виявляти нове ШПЗ за характеристиками**		
		Наявність невідомих унікальних характеристик	**Рівень хибних спрацьовувань**	**Шум (розмитість) досліджуваних даних**
Поведінкові методи:				
Спектральний аналіз	–	низька	середній	низька
Фрактальний аналіз	–	низька	низький	низька
Аналіз ентропії	+	низька	середній	середня
На основі знань:				
Графи сценаріїв	+	низька	середній	низька
Методи на сплайнах	–	низька	середній	середня
Евристичний аналіз	+	середня	низький	середня
Статистичний аналіз	–	низька	середній	середня
Експертні системи	+	низька	низький	низька
Методи штучного інтелекту:				
Нейронні мережі	–	середня	низький	середня
Генетичні алгоритми	–	середня	низький	низька
Нечітка логіка	+	середня	низький	висока
Імунні системи	–	середня	низький	середня
Опорні вектори	–	низька	середній	низька
Роєві алгоритми	+	середня	низький	низька
Методи машинного навчання:				
Алгоритми регресії	–	низька	середній	середня
Кластеризація	–	низька	середній	середня
Байєсівські мережі	–	низька	середній	середня
Байєсівський метод	–	низька	середній	середня

На основі проведеного аналізу методів виявлення нового ШПЗ можна зробити такий висновок.

Жоден з досліджуваних методів в силу своїх властивостей неспроможний у повному обсязі забезпечити виявлення одного з найнебезпечніших типів ШПЗ – комп'ютерних вірусів, здатних до метапрограмування власного коду з метою реалізації способу приховування від існуючих антивірусних систем. До такого типу вірусів належать поліморфні (олігоморфні) і метаморфні віруси. Так, кожен із класів існуючих методів (на основі знань, штучного інтелекту, машинного навчання, поведінкові) спроможний вирішувати це завдання тією чи іншою мірою, проте в умовах певних обмежень. Результати порівняльного аналізу за описаними критеріями демонструють, що серед них можливо виділити методи, які показали найбільш повну їм відповідність, – методи на основі теорії нечіткої логіки. Так, формалізація неточних знань та виконання наближених міркувань в області виявлення ШПЗ дозволяє виявляти його деструктивну діяльність в умовах певної нечіткості інформації про стан ІС з можливістю адаптації до виявлення подібних типів ШПЗ.

Напрям удосконалення існуючих систем. На сьогодні існує дві стратегії до виявлення нового ШПЗ [22]: виявлення аномальної діяльності на підставі аудиту сценаріїв функціонування, виявлення з урахуванням набутого досвіду боротьби з відомим ШПЗ. Для ефективного виявлення нового ШПЗ доцільно використовувати другий підхід, заснований на досвіді боротьби з уже відомим ШПЗ, оскільки кількість нових його екземплярів, які характеризуються принципово новою множиною ознак, досить мала.

Пріоритетним напрямом удосконалення існуючого антивірусного ПЗ є доповнення існуючого функціоналу методом, в основу якого покладено теорію нечіткої логіки. Причому застосування обраного методу має передбачати визначення поліморфної (метаморфної) компоненти ШПЗ для кожного відомого його типу, що забезпечить ефективне виявлення нового ШПЗ на основі ідентифікації поліморфних (метаморфних) структур уже існуючих вірусів в умовах деякої неточності (розмитості) інформації про стан ІС.

Висновки. У статті вирішується завдання аналізу спроможності існуючих антивірусних систем та покладених у їх основу методів до виявлення нового шкідливого програмного забезпечення. Офіційні дані розробників антивірусних систем часто не підтверджують задекларований рівень точності виявлення нового шкідливого програмного забезпечення на практиці, що свідчить про тестування розглянутих антивірусних систем у специфічних умовах, занадто відмінних від реальних.

Проведено аналіз існуючих типів ШПЗ, серед них виділено поліморфні (олігоморфні) та метаморфні віруси, як особливо небезпечне ШПЗ для сучасних комп'ютерних систем. Поліморфні та метаморфні віруси становлять основну частку нового ШПЗ, оскільки нові комп'ютерні віруси у своїй більшості являють собою модифіковані версії існуючого ШПЗ.

Результати аналізу методів виявлення ШПЗ демонструють, що серед них можливо виділити методи, які показали найбільш повну відповідність поставленим до них вимогам (адаптивність, верифікованість, наявність невідомих унікальних характеристик, рівень хибних спрацьовувань, розмитість досліджуваних даних), – методи на основі теорії нечіткої логіки.

Запропоновано напрям удосконалення існуючих антивірусних систем щодо підвищення спроможності до виявлення нових типів шкідливого програмного забезпечення. Причому застосування обраного методу має передбачати визначення поліморфної (метаморфної) компоненти ШПЗ для кожного відомого його класу, що дозволить виявляти нове ШПЗ на основі ідентифікації поліморфних (метаморфних) структур уже існуючих вірусів в умовах деякої неточності (розмитості) інформації про стан ІС.

Таким чином, отримані результати є підґрунтям для реалізації нових підходів до виявлення нового ШПЗ, що дасть можливість підвищити ефективність кібербезпеки військових ІС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII: станом на 17.08.2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Фесьоха В. В., Кисиленко Д. Ю., Турчак О. Р. Перспективи удосконалення існуючих рішень виявлення шкідливого програмного забезпечення в інформаційних системах військового призначення. Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: матеріали II міжнар.наук.-практ. конф., 01 грудня 2022. Київ: ВІТІ ім. Героїв Крут. С. 216.

3. ГайдамашкоО. Кількість шкідливих програм для Windows у 5000 разів вища, ніж на macOS. *24 Канал.* URL: https://24tv.ua/tech/2022-rotsi-dlya-windows-stvorili-70-milyoniv-virusiv_n2226891.

4. Smith B. Digital technology and the war in Ukraine - Microsoft On the Issues. *Microsoft On the Issues*. URL: https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattack.

5. Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon та експлойтів до вразливостей CVE-2021-40444 і CVE-2022-30190 (CERT-UA#4753). *cert.gov.ua*. URL: https://cert.gov.ua/article/40559.

6. New "Prestige" ransomware impacts organizations in Ukraine and Poland - Microsoft Security Blog. *Microsoft Security Blog*. URL: https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

7. Кібератака на користувачів системи DELTA з використанням шкідливих програм RomCom/FateGrab/StealDeal (CERT-UA#5709). *cert.gov.ua*. URL: https://cert.gov.ua/article/3349703.

8. Page C. Russian 'WhisperGate' hackers are using new data-stealing malware to target Ukraine. *TechCrunch*. URL: https://techcrunch.com/2023/02/08/whispergate-hackers-data-stealing-malware-ukraine/.

9. Викриття: (Російські спецслужби розповсюджують шкідливе програмне забезпечення за допомогою торент-трекерів). *#DisinfoChronicle. Кремлівська дезінформація щодо військового наступу на Україну – Детектор медіа.* URL: https://disinfo.detector.media/post/rosiiski-spetssluzhby-poshyriuiut-shkidlyve-prohramne-zabezpechennia-za-dopomohoiu-torent-trekeriv.

10. Савенко О. С. Критерії класифікації методів виявлення шкідливого програмного забезпечення. *Вісник Хмельницького національного університету.* № 1. С. 23–27.

11. Жульковська І. І., Плужник А. В., Жульковський О. А. Сучасні методи виявлення шкідливих програм. *Математичне моделювання.* № 1. С. 46–54.

12. Лисенко С. М., Щука Р. В. Аналіз методів шкідливого програмного забезпечення в комп'ютерних системах. *Вісник Хмельницького національного університету*. № 2. С. 101–107.

13. Rabia Tahir. A Study on Malware and Malware Detection Techniques. I.J. Education and Management Engineering, p. 20–30.

14. Поліщук Н. Avira огляд 2023: чи варто купувати? *WizCase*. URL: https://uk.wizcase.com/antivirus/avira.

15. Selinger M. AV-TEST Award 2022 for Avira. *AV-TEST |Unabhängige Tests von Antiviren- & Security-Software*. URL: https://www.av-test.org/en/news/av-test-award-2022-for-avira/.

16. Унікальна технологія ESET для сучасного захисту. *ESET*. URL: https://www.eset.com/ua/about/technology/.

17. Олеч Ю. Огляд антивірусу Panda у 2023: чи варто купувати?. *WizCase*. URL: https://uk.wizcase.com/antivirus/panda.

18. Поліщук Н. Avast огляд 2023: чи варто купувати?. *WizCase*. URL: https://uk.wizcase.com/antivirus/avast.

19. Selinger M. AV-TEST Award 2022 for Avast. *AV-TEST|Unabhängige Tests von Antiviren- & Security-Software*. URL: https://www.av-test.org/en/news/av-test-award-2022-for-avast/.

20. Tunggal A. T. 22 Types of Malware and How to Recognize Them in 2023 | UpGuard. *Third-Party Risk and Attack Surface Management Software | UpGuard*. URL: https://www.upguard.com/blog/types-of-malware.

21. Zero-day polymorphic cyberattacks detection using fuzzy inference system / V. V. Fesokha et al. *Austrian Journal of Technical and Natural Sciences*. p. 8–13. URL: https://doi.org/10.29013/ajt-20-5.6-8-13.

22. Субач І., Фесьоха В., Фесьоха Н. Фесьоха Н. О. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі. *Information Technology and Security*. 2017. Т. 5, № 1. С. 29–41.