КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.813
УДК 004.56

Штонда Роман Михайлович
начальник науково-дослідного відділу
Військовий інститут телекомунікацій
та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-5986-0847
roman.shtonda@viti.edu.ua

Паламарчук Світлана Анатоліївна
головна наукова співробітниця
Військовий інститут телекомунікацій
та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-7483-9165
palam_sv@ukr.net

Бокій Олена Володимирівна
наукова співробітниця
Військовий інститут телекомунікацій
та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0009-0006-3459-5665
olenabokiy1971@gmail.com

Терещенко Тетяна Павлівна
старша наукова співробітниця
Військовий інститут телекомунікацій
та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0002-9659-7897
tetiana.tereshchenko@viti.edu.ua

Черниш Юлія Олександрівна
старша наукова співробітниця
Військовий інститут телекомунікацій
та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0002-6626-5656
yuliia.chernysch@viti.edu.ua

КОМПЛЕКСНА МЕТОДИКА ОЦІНЮВАННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ АНТИВІРУСНИХ ПРОГРАМНИХ ЗАСОБІВ

Анотація. У сучасних умовах інтенсивного розвитку інформаційно-комунікаційних технологій та стрімкого зростання кількості кіберзагроз, захист кінцевих пристроїв та інформаційно-комунікаційних систем організацій набуває критичного значення. У зв'язку з цим антивірусні програмні засоби залишаються ключовим інструментом у забезпеченні кіберзахисту від шкідливого програмного забезпечення та сценаріїв цілеспрямованих атак. Однак, для вибору оптимального антивірусного програмного засобу важливо мати об'єктивний і комплексний підхід до оцінки їхніх функціональних можливостей. Метою цієї статті є розробка Комплексної методики оцінювання функціональних можливостей антивірусного програмного забезпечення. Запропонована методика враховує широкий спектр тестів, що моделюють типові та нетипові вектори проникнення шкідливого програмного забезпечення: від заражених ZIP-архівів, фішингових листів, змін системних файлів (hosts, реєстру) до виявлення Beacon-активності, автозавантажуваних скриптів, обфускованих PowerShell-команд, макросів Office-документів тощо. У дослідженні оцінюються чотири популярні антивірусні програмні засоби: ESET Endpoint Security, Avast Business Antivirus, Zillya та Windows Defender. У межах експерименту дослідницька група провела оцінювання функцій кожного антивірусного програмного засобу за 21 критерієм. Оцінювання здійснювалось у балах (0–2) із відповідною вагою критичності (1 — критична, 0.8 — висока, 0.5 — середня). Методика дозволяє визначити загальний рівень функціональності та ефективність у відсотковому

значенні. Це дозволяє об'єктивно підходити до вибору антивірусного програмного засобу залежно від характеру інформаційної інфраструктури та рівня ризику. Запропонований підхід є універсальним і придатним до адаптації під інші платформи та умови, а також може бути розширений для взаємодії з системами класу Endpoint Detection and Response (Extended Detection and Response). Результати дослідження підтверджують важливість комплексного підходу до кіберзахисту, з урахуванням особливостей сучасних кібератак.

Ключові слова: антивірусний програмний засіб; кібератаки; кібербезпека; кіберзахист; кіберінциденти; кінцевий пристрій.

ВСТУП

З кожним роком все більше кінцевих пристроїв користувачів, що підключені до електронних комунікаційних мереж (далі — ЕКМ) та інформаційно-комунікаційних систем (далі — ІКС) піддаються цілеспрямованим атакам, що впливає на кіберзахист ІКС організацій та тягне за собою порушення надійності їх функціонування. Метою цілеспрямованих атак зазвичай є отримання несанкціонованого доступу до інформації, що обробляється та циркулює в ІКС організацій та установ [1].

Левову частку щодо забезпечення кіберзахисту ІКС організацій і установ, в тому числі кінцевих пристроїв, становлять антивірусні програмні засоби (далі — АВПЗ). В Україні АВПЗ, яке дозволено для використання в організаціях та установах визначається Державною службою спеціального зв'язку та захисту інформації України (далі — ДССЗЗІ України) та вноситься в перелік засобів технічного захисту інформації, які мають експертний висновок про відповідність вимогам технічного захисту інформації (далі — Перелік) [2]. Цей Перелік періодично уточнюється та змінюється.

Постановка проблеми. Однією із найактуальніших проблем — є кібератаки на кінцеві пристрої користувачів та ІКС організацій і установ [3]. В сучасних підходах, дану проблему в тій чи іншій мірі вирішують Security Operations Center (далі — SOC) та аналітики з їх складу, за допомогою підходів із кіберзахисту [4]. На кінцевих пристроях користувачів, що можуть бути заражені шкідливим програмним забезпеченням (далі — ШПЗ) та на яких можуть бути реалізовані цілеспрямовані атаки, окрім різних клієнтських агентів систем виявлення та реагування на кіберінциденти, в обов'язковому порядку інсталюється, налаштовується та підтримується в оновленому стані АВПЗ. Широке коло сучасних антивірусних програм потребує оптимального їх вибору.

Аналіз останніх досліджень і публікацій. В даному напрямку працюють науковці провідних вузів України та світу. Серед таких наукових публікацій можливо виділити роботу авторського колективу в складі Шевченко С.М., Складаний П.М. та Марценюк М.С. [5]. В публікації автори проаналізували основні загрози інформаційній безпеці у сфері інформаційних технологій. Окремо зроблено наголос на те, що АВПЗ є найбільш ефективним засобом захисту проти ШПЗ. Здійснено порівняльний аналіз основних характеристик (визначено 13 характеристик) антивірусних програм.

В публікації авторського колективу в складі Антоненко Н.В., Дігтяр Я.С. та Крикун Н.О., розкрито актуальні питання використання сучасних методів боротьби з комп'ютерними вірусами. Детально розглянуто різноманітні методи виявлення шкідливих програм в контексті вимог комп'ютерної безпеки [6]. Особливу увагу в публікації приділено механізму зараження окремих комп'ютерів.

Також слід відмітити публікацію авторського колективу в складі Фесьоха В.В., Кисиленко Д.Ю. та Нестеров О.М. [7]. Автори розглядають завдання аналізу спроможності існуючих АВПЗ та покладених в їх основу методів до виявлення нового

шкідливого програмного забезпечення в інформаційних системах критичної інфраструктури. Описані властивості нового ШПЗ з метою пошуку найбільш відповідного йому класу комп'ютерних вірусів. Наведено характеристику методів виявлення ШПЗ. Запропоновано напрями удосконалення існуючих АВПЗ щодо підвищення адаптивності до виявлення нових класів ШПЗ.

Мета статті. Метою даної статті є розроблення Комплексної методики оцінювання функціональних можливостей АВПЗ, на прикладі наступних продуктів: Avast Business Antivirus, ESET Endpoint Security, Zillya та Windows Defender.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Комплексна методика оцінювання функціональних можливостей АВПЗ призначена для перевірки можливостей АВПЗ, що забезпечують кіберзахист операційних систем сімейства Windows на кінцевих пристроях в ІКС організацій і установ.

Тестування можливостей АВПЗ здійснюється за наступними складовими методики:

- перевірка можливостей щодо інсталяції, видалення, та роботи в системі;
- перевірка можливостей виявлення заражених ZIP-архівів;
- перевірка можливостей виявлення фішингових вкладень в Outlook/Thunderbird;
- перевірка можливостей виявлення підроблених SSL-сертифікатів;
- перевірка можливостей щодо реакції на запуск AutoIT-скрипта;
- перевірка захисту системного реєстру від модифікацій;
- перевірка можливостей щодо захисту файлу hosts від змін;
- перевірка можливостей поведінкового блокування кейлогера;
- перевірка можливостей виявлення обфусцированих PowerShell-скриптів;
- перевірка можливостей блокування обходу міжмережевого екрану через Netcat/Ncat;
- перевірка можливостей виявлення Beacon-активності C2;
- перевірка реакції виявлення на вбудований скрипт у PDF-файлах;
- перевірка можливостей захисту від спроб завершення процесу роботи АВПЗ;
- перевірка можливостей виявлення спроб видалення Shadow Copy;
- перевірка можливостей блокування встановлення шкідливого драйвера .sys;
- перевірка можливостей виявлення шкідливого макроса у Word/Excel;
- перевірка можливостей реагування на запізніле завантаження DLL;
- перевірка можливостей виявлення запуску в sandbox-середовищі;
- перевірка можливостей поведінкового захисту при запуску програмних рішень із тимчасової папки;
- перевірка можливостей відстеження змін у системних бібліотеках .dll;
- перевірка можливостей виявлення DNS-тунелювання.

Першочерговим кроком слід отримати чи придбати ліцензії у виробників АВПЗ в нашому випадку це:

Avast Business Antivirus — компанії AVAST Software s.r.o;

ESET Endpoint Security — компанії ESET;

Zillya — компанії Zillya;

Windows Defender — компанії Microsoft.

Більшість виробників надають безкоштовну пробну версію свого продукту терміном на один місяць. А такий як Windows Defender є спеціальним програмним забезпеченням, що входить до операційної системи Windows на умовах ліцензії.

Дослідний зразок для проведення оцінювання наведено на рис. 1.

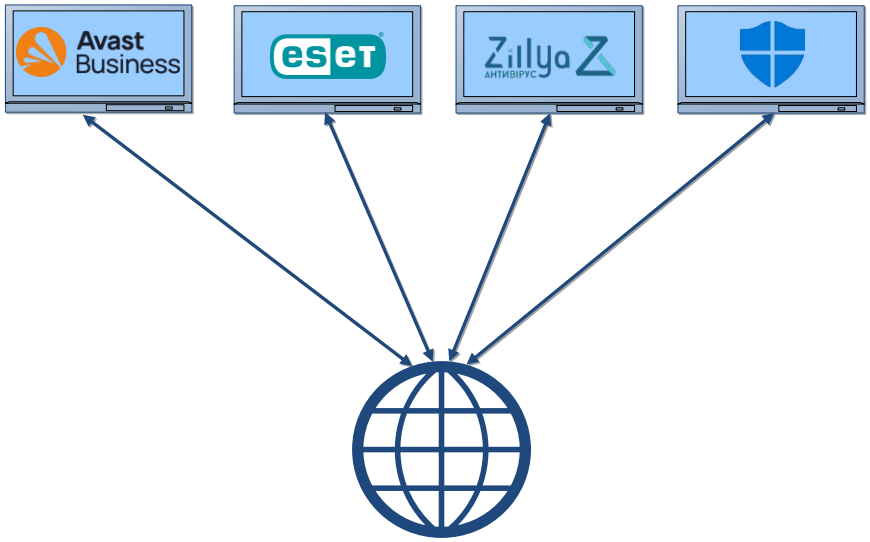

Рис. 1. Дослідний зразок для проведення оцінювання АВПЗ

Проведено інсталяцію АВПЗ на чисті операційні системи сімейства Windows, що встановлені на кінцевих пристроях.

Оновлено бази сигнатур перед початком тестування.

Після моделювання кіберзагроз здійснювалося експертне оцінювання реагування тим чи іншим АВПЗ. Відповідно до розробленої Комплексної методики функціональні можливості АВПЗ оцінюється наступним чином [4]:

– 2 бали — АВПЗ успішно проходить перевірку за складовою методики;
– 1 бал — АВПЗ частково проходить перевірку за складовою методики;
– 0 балів — АВПЗ не проходить перевірку за складовою методики.

Ступінь критичності перевірки визначається коефіцієнтами наступним чином [4]:

– критична — коефіцієнт 1 ($К_1$);
– висока — коефіцієнт 0,8 ($К_2$);
– середня — коефіцієнт 0,5 ($К_3$).

Результати оцінювання АВПЗ на кінцевих пристроях із операційною системою Windows 10 Pro наведені в табл. 1.

Таблиця 1

Результати оцінювання АВПЗ на кінцевих пристроях із операційною системою Windows 10 Pro

№ з/п	Найменування перевірки (складова методики)	Критичність	Avast Business Antivirus	ESET Endpoint Security	Zillya	Windows Defender
1.	Інсталяція, видалення, та роботи в системі	Критична	2	2	2	2
2.	Виявлення заражених ZIP-архівів	Висока	2	2	2	2
3.	Виявлення фішингових вкладень в Outlook/Thunderbird	Висока	2	2	1	2
4.	Виявлення підроблених SSL-сертифікатів	Критична	2	2	0	1

ISSN 2663 - 4023

№ з/п	Найменування перевірки (складова методики)	Критичність	Avast Business Antivirus	ESET Endpoint Security	Zillya	Windows Defender
5.	Реакція на запуск AutolT-скрипта	Середня	1	1	0	1
6.	Захист системного реєстру від модифікацій	Висока	2	2	1	2
7.	Захист файлу hosts від змін	Висока	2	2	0	2
8.	Поведінкове блокування кейлогера	Критична	2	2	0	2
9.	Виявлення обфусцированих PowerShell-скриптів	Висока	1	1	0	1
10.	Блокування обходу міжмережевого екрану через Netcat/Ncat	Середня	1	1	0	1
11.	Виявлення Beacon-активності C2	Критична	1	2	0	1
12.	Реакція виявлення на вбудований скрипт у PDF-файлах	Висока	2	2	1	2
13.	Захист від спроб завершення процесу роботи АВПЗ	Критична	2	2	0	2
14.	Виявлення спроб видалення Shadow Copy	Висока	2	2	0	2
15.	Блокування встановлення шкідливого драйвера .sys	Критична	2	2	0	2
16.	Виявлення шкідливого макроса у Word/Excel	Висока	2	2	1	2
17.	Реагування на запізніле завантаження DLL	Середня	1	1	0	1
18.	Виявлення запуску в sandbox-середовищі	Середня	2	2	0	2
19.	Поведінковий захист при запуску програмних рішень із тимчасової папки	Висока	2	2	0	2
20.	Відстеження змін у системних бібліотеках .dll	Висока	2	2	0	2
21.	Виявлення DNS-тунелювання	Критична	1	1	0	1

Оцінка відповідності технічним вимогам (Коефіцієнт ефективності $К_Е$) АВПЗ для кожного із них розраховується за формулою 1:

$$К_Е = n \times \left(\sum_{\text{критична}} \times К_1 + \sum_{\text{висока}} \times К_2 + \sum_{\text{середня}} \times К_3 \right) \quad (1)$$

де n — часткова доля кінцевих пристроїв з операційною системою Windows 10 Pro із АВПЗ в цілому n=1;

$\sum$ критична — це загальна кількість балів по функціях з позначкою критична;

$\sum$ висока — це загальна кількість балів по функціях з позначкою висока;

$\sum$ середня — це загальна кількість балів по функціях з позначкою середня.

Провівши розрахунки за формулою 1 відповідно до Комплексної методики оцінювання функціональних можливостей АВПЗ, отримано:

ESET Endpoint Security — 30,7 балів;

Avast Business Antivirus — 29,7 балів;
Windows Defender — 28,7 балів;
Zillya — 6,8 балів.

На рис. 2 зазначена діаграма оцінювання функціональних можливостей АВПЗ за результатами розрахунків.

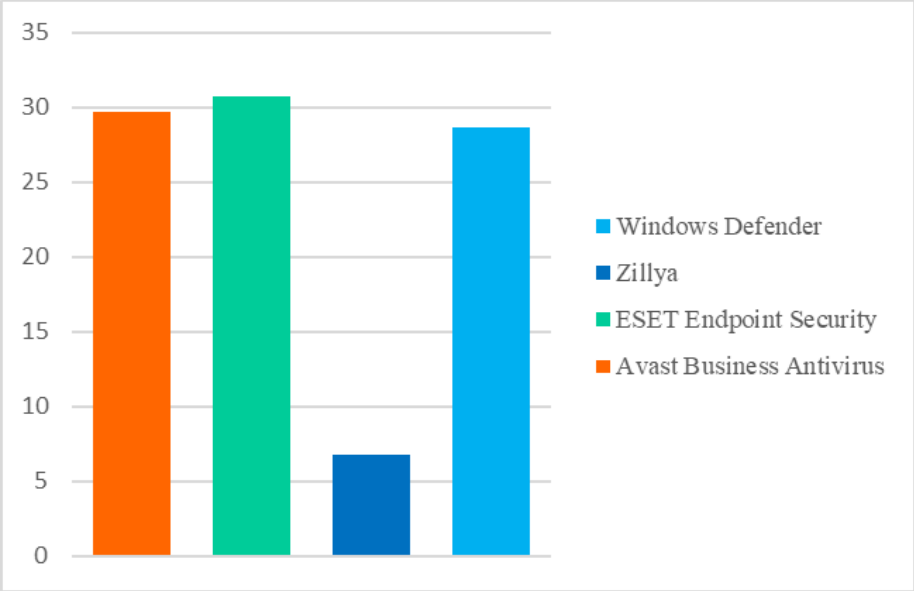

Рис. 2 Діаграма оцінювання функціональних можливостей АВПЗ

Кількісні дані з табл. 1 мають наступний характер як зазначено в табл. 2.

Таблиця 2

Кількісні дані реагування АВПЗ на ШПЗ

АВПЗ	Успішна перевірка	Частково успішна перевірка	Неуспішна перевірка
Avast Business Antivirus	15	6	0
ESET Endpoint Security	16	5	0
Zillya	2	4	15
Windows Defender	14	6	0

Для визначення у відсотковому відношенні коефіцієнту ефективності виявлення кіберзагроз ($К_{Е\%}$) АВПЗ Avast Business Antivirus, ESET Endpoint Security, Zillya та Windows Defender застосовуємо результати, що зазначені в табл. 2 та формулу 2.

$$К_{Е\%} = \frac{ПВ}{ПВ + ЧВ + НВ} \times 100\% \quad (2)$$

де ПВ — кількість виявлених АВПЗ кіберзагроз;
ЧВ — кількість частково виявлених АВПЗ кіберзагроз (умовно враховувати як 0,5 ЧВ);
НВ — кількість не виявлених АВПЗ кіберзагроз.

Таким чином, провівши розрахунки, розглянуті АВПЗ забезпечують захист кінцевих пристроїв у наступному відношенні:
ESET Endpoint Security — на 86%;
Avast Business Antivirus — на 83%;
Windows Defender — на 82%;
Zillya — на 11%.

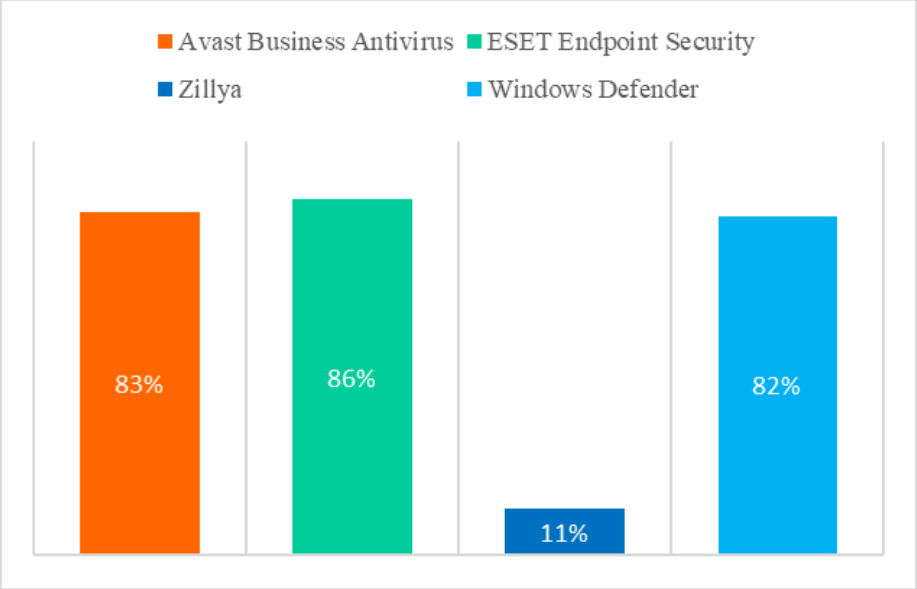

Рис. 3. Ефективність АВПЗ

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розроблена Комплексна методика оцінювання функціональних можливостей АВПЗ дозволяє провести належним чином вибір АВПЗ, в залежності від оцінених ризиків ІКС.

За результатами проведених досліджень найвищу ефективність по відношенню до інших АВПЗ показав ESET Endpoint Security, що становить 86%. Також непогані показники показали Avast Business Antivirus та Windows Defender, що склало 83% та 82% відповідно. Zillya, навпаки, продемонстрував низький рівень ефективності — 11%. Windows Defender продемонстрував, що навіть стандартні рішення операційних систем сімейства Windows можуть бути конкурентоспроможними за умови правильного налаштування, особливо для малих і середніх організацій та установ.

Рекомендовано використовувати ESET Endpoint Security та Avast Business Antivirus на об’єктах критичної інфраструктури та організаціях і установах державної власності. Windows Defender є оптимальним рішенням для використання на кінцевих пристроях в ІКС з обмеженим набором спеціального програмного забезпечення. Zillya доцільно застосовувати лише для захисту домашніх кінцевих пристроїв, за умови низького ризику кібератак та кіберінцидентів.

Подальшими дослідженнями є вивчення взаємодії даних АВПЗ із програмними рішеннями Endpoint Detection and Response (Extended Detection and Response).

Боремося з кібертерором разом! Разом до перемоги! Слава Україні!

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *State Service for Special Communications and Information Protection of Ukraine. Access Denied.* (n. d.) https://cip.gov.ua/ua/news/cert-ua-poperedzhaye-pro-kiberzagrozu-cilespryamovani-ataki-z-vikoristannyam-programi-viddalenogo-dostupu-superops-rmm
2. *State Service for Special Communications and Information Protection of Ukraine. Access Denied.* (n. d.) https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi

3. Oleksenko, V., Shtonda, R., Chernish, Y., & Maltseva, I. (2022). Modern approaches to cybersecurity provision in radio relay lines of communication. *Electronic professional scientific publication "Cybersecurity: education, science, technology", 1(17)*, 57–64. https://doi.org/10.28925/2663-4023.2022.17.5764
4. Shtonda, R., Cherednychenko, O., Fomkin, D., Bokiy, O., & Kutsaev, P. (2025). Methodology for testing the capabilities of endpoint detection and response (extended detection and response) software solutions. *Electronic professional scientific publication "Cybersecurity: education, science, technology", 3(27)*, 380–389. https://doi.org/10.28925/2663-4023.2025.27.737
5. Shevchenko, S., Skladannyi, P., & Martseniuk, M. (2019). Analysis and research of the characteristics of antivirus software standardized in ukraine. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 4(4),* 62–71. https://doi.org/10.28925/2663-4023.2019.4.6271
6. Antonenko, N., Digtyar, Ya., & Krykun, N. (2022). Modern methods of combating computer viruses. *Economy and society, (43).* https://doi.org/10.32782/2524-0072/2022-43-51
7. Fesokha V., Kysylenko D., & Nesterov O. (2023). Analysis of the capacity of existing anti-virus protection systems and their based methods for detecting new malware in military information systems. *Communication, informatization and cybersecurity systems and technologies, 3(3).* https://doi.org/10.58254/viti.3.2023.16.143

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Roman Shtonda
Head of Research Department
Kruty Heroes Military Institute of Telecommunications
and Information Technology, Kyiv, Ukraine
ORCID ID: 0000-0001-5986-0847
roman.shtonda@viti.edu.ua

Svitlana Palamarchuk
Chief Research Fellow
Kruty Heroes Military Institute of Telecommunications
and Information Technology, Kyiv, Ukraine
ORCID ID: 0000-0001-7483-9165
palam_sv@ukr.net

Olena Bokii
Research associate
Kruty Heroes Military Institute of Telecommunications
and Information Technology, Kyiv, Ukraine
ORCID ID: 0009-0006-3459-5665
olenabokiy1971@gmail.com

Tetiana Tereshchenko
Senior Research Fellow
Kruty Heroes Military Institute of Telecommunications
and Information Technology, Kyiv, Ukraine
ORCID ID: 0000-0002-9659-7897
tetiana.tereshchenko@viti.edu.ua

Yuliya Chernish
Senior Research Fellow
Kruty Heroes Military Institute of Telecommunications
and Information Technology, Kyiv, Ukraine
ORCID ID: 0000-0002-6626-5656
yuliia.chernysch@viti.edu.ua

COMPREHENSIVE METHODOLOGY FOR EVALUATING THE FUNCTIONAL CAPABILITIES OF ANTIVIRUS SOFTWARE

Abstract. In today's conditions of intensive development of information and communication technologies and rapid growth of the number of cyber threats, protection of end devices and information and communication systems of organizations is becoming critical. In this regard, antivirus software remains a key tool in ensuring cyber protection against malicious software and targeted attack scenarios. However, to choose the optimal antivirus software, it is important to have an objective and comprehensive approach to assessing their functionality. The purpose of this article is to develop a Comprehensive Methodology for Evaluating the Functional Capabilities of Antivirus Software. The proposed methodology takes into account a wide range of tests that simulate typical and atypical vectors of malware penetration: from infected ZIP archives, phishing emails, changes to system files (hosts, registry) to detection of Beacon activity, auto-start scripts, obfuscated PowerShell commands, Office document macros, etc. The study evaluates four popular antivirus software products: ESET Endpoint Security, Avast Business Antivirus, Zillya, and Windows Defender. As part of the experiment, the research team evaluated the functions of each antivirus software product according to 21 criteria. The evaluation was carried out in points (0–2) with the corresponding criticality weight (1 — critical, 0.8 — high, 0.5 — medium). The methodology allows you to determine the overall level of functionality and efficiency in percentage terms. This allows you to objectively approach the choice of antivirus software depending on the nature of the information infrastructure and the level of risk. The proposed approach is universal and suitable for adaptation to other platforms and conditions, and can also be expanded to interact with

Endpoint Detection and Response (Extended Detection and Response) class systems. The results of the study confirm the importance of a comprehensive approach to cyber protection, taking into account the specifics of modern cyberattacks.

Keywords: antivirus software; cyberattacks; cybersecurity; cyberprotection; cyberincidents; endpoint device.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *State Service for Special Communications and Information Protection of Ukraine. Access Denied.* (n. d.) https://cip.gov.ua/ua/news/cert-ua-poperedzhaye-pro-kiberzagrozu-cilespryamovani-ataki-z-vikoristannyam-programi-viddalenogo-dostupu-superops-rmm
2. *State Service for Special Communications and Information Protection of Ukraine. Access Denied.* (n. d.) https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi
3. Oleksenko, V., Shtonda, R., Chernish, Y., & Maltseva, I. (2022). Modern approaches to cybersecurity provision in radio relay lines of communication. *Electronic professional scientific publication "Cybersecurity: education, science, technology", 1(17),* 57–64. https://doi.org/10.28925/2663-4023.2022.17.5764
4. Shtonda, R., Cherednychenko, O., Fomkin, D., Bokiy, O., & Kutsaev, P. (2025). Methodology for testing the capabilities of endpoint detection and response (extended detection and response) software solutions. *Electronic professional scientific publication "Cybersecurity: education, science, technology", 3(27),* 380–389. https://doi.org/10.28925/2663-4023.2025.27.737
5. Shevchenko, S., Skladannyi, P., & Martseniuk, M. (2019). Analysis and research of the characteristics of antivirus software standardized in ukraine. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 4(4),* 62–71. https://doi.org/10.28925/2663-4023.2019.4.6271
6. Antonenko, N., Digtyar, Ya., & Krykun, N. (2022). Modern methods of combating computer viruses. *Economy and society, (43).* https://doi.org/10.32782/2524-0072/2022-43-51
7. Fesokha V., Kysylenko D., & Nesterov O. (2023). Analysis of the capacity of existing anti-virus protection systems and their based methods for detecting new malware in military information systems. *Communication, informatization and cybersecurity systems and technologies, 3(3).* https://doi.org/10.58254/viti.3.2023.16.143