УДК 004.056.5:004.42:004.75

СИСТЕМНИЙ АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У КОРПОРАТИВНИХ МЕРЕЖАХ

Світличний В.А.,[1] к.т.н., доц.; Груба В.В.[2]
[1,2] Харківський національний університет внутрішніх справ
Україна, Кам'янець-Подільський
[1] vit.svet@ukr.net; [2] valeriyanaa20@gmail.com

Анотація. *Під час дослідження розглянуто основні методи виявлення шкідливого програмного забезпечення (ШПЗ) у корпоративних мережах: сигнатурний, евристичний, поведінковий та комбінований. Проведено системний аналіз їхніх переваг і недоліків з урахуванням актуальних кіберзагроз. Визначено перспективні напрями розвитку систем виявлення ШПЗ.*
Ключові слова: *шкідливе програмне забезпечення; системний аналіз; корпоративна мережа; виявлення загроз; поведінковий метод.*

Вступ. Сучасні корпоративні мережі все активніше зазнають складних і цілеспрямованих кібератак, що ставлять під загрозу конфіденційність, цілісність і доступність інформаційних ресурсів. Одним із головних аспектів забезпечення кібербезпеки є оперативне виявлення шкідливого програмного забезпечення, яке часто слугує початковим етапом більшості атак [1]. Звичайні методи захисту, що базуються виключно на сигнатурному аналізі, більше не можуть забезпечити достатню ефективність у боротьбі з сучасними поліморфними та безфайловими атаками [2]. Потреба в інноваційних підходах до виявлення шкідливого ПЗ, зокрема таких, що ґрунтуються на поведінковому аналізі та машинному навчанні, зростає щодня, оскільки зловмисники постійно вдосконалюють свої методи обходу традиційних засобів захисту. Через це стає актуальним проведення системного аналізу існуючих методів виявлення, що дає змогу оцінити їхню ефективність, взаємозалежність і доцільність застосування в контексті корпоративних середовищ.

Мета дослідження. Проведення системного аналізу існуючих підходів до виявлення шкідливого програмного забезпечення в корпоративних мережах з урахуванням сучасних викликів кіберзагроз і постійного ускладнення методів атак. Для реалізації цієї мети передбачено:

– проаналізувати наявні підходи до виявлення ШПЗ (сигнатурний, евристичний, поведінковий, комбінований) з позицій ефективності, продуктивності та адаптивності [1;3];

– визначити чинники, що впливають на результативність роботи систем виявлення у корпоративному середовищі;

– дослідити можливості інтеграції технологій машинного навчання у системи моніторингу безпеки [5];

– обґрунтувати напрями вдосконалення комбінованих підходів, що поєднують сигнатурний та поведінковий аналіз для динамічної ідентифікації загроз [2;4].

Основна частина. Методи виявлення шкідливого програмного забезпечення у корпоративних мережах відіграють ключову роль у забезпеченні комплексного захисту. Їх підбір залежить від архітектури мережі, масштабу інфраструктури, природи загроз і наявних ресурсів. У результаті аналізу всі методи можна умовно класифікувати на чотири основні групи [1].

Сигнатурні методи ґрунтуються на зіставленні вмісту файлів, мережевого трафіку чи виконуваних процесів із базою відомих сигнатур шкідливих об’єктів. Їхніми перевагами є висока швидкість роботи, точність та низький рівень хибнопозитивних спрацювань [1]. Водночас ці методи ефективні лише проти вже відомих зразків ШПЗ. Вони не виявляють нові, поліморфні або безфайлові атаки, які активно модифікують свій код або взагалі не залишають слідів у файловій системі [2]. Для корпоративних мереж сигнатурні засоби можуть виконувати роль базового фільтра, але не можуть бути єдиним рівнем захисту.

Евристичні методи аналізують структуру, логіку та поведінкові ознаки програм, щоб визначити потенційно шкідливу активність [3]. Вони можуть виявляти невідомі зразки ШПЗ завдяки аналізу підозрілих шаблонів, наприклад спроб прихованого запису в системні каталоги, змін реєстру або несанкціонованих мережевих з’єднань. Однак евристика часто потребує глибокого налаштування та може породжувати хибні спрацювання, особливо у великих корпоративних середовищах із нестандартними бізнес-процесами.

Поведінкові методи базуються на безперервному моніторингу активності процесів у режимі реального часу. Вони аналізують події, взаємодію між процесами, системними службами та мережею, щоб фіксувати аномалії [4]. Такий підхід дозволяє виявляти невідомі та складні загрози, зокрема zero-day атаки. Поведінкові системи часто інтегруються з інструментами машинного навчання, що дозволяє автоматично оновлювати моделі виявлення [5]. Основними викликами залишаються значне навантаження на ресурси та потреба у кваліфікованих фахівцях для налаштування правил реагування [4;5].

Комбіновані методи поєднують елементи сигнатурного, евристичного та поведінкового аналізу, а також використовують статистичні та інтелектуальні алгоритми для зниження рівня хибнопозитивних спрацювань [5]. Такі рішення найчастіше реалізовані у вигляді систем виявлення та запобігання вторгнень (IDS/IPS), систем моніторингу кінцевих точок (EDR) та платформ розширеного захисту (XDR). Їхня перевага полягає у здатності адаптуватися до нових типів атак і взаємодіяти з іншими елементами корпоративної інфраструктури безпеки [1;5].

До сучасних прикладів практичного застосування комбінованих методів належать рішення: CrowdStrike Falcon [6], Cisco Secure Endpoint [7] та Microsoft Defender for Endpoint [8]. Вони інтегрують сигнатурний, поведінковий і машинно-навчальний підходи, що забезпечує адаптивне реагування на нові типи атак і глибоку аналітику інцидентів у реальному часі.

У корпоративних мережах найкращі результати демонструють поведінкові та комбіновані системи, доповнені алгоритмами машинного навчання для виявлення нетипових дій користувачів і процесів [5]. Окрім цього, важливим чинником ефективності є правильне налаштування політик безпеки, сегментація мережі, централізоване управління журналами подій та інтеграція систем виявлення з SIEM-рішеннями [4]. Такий підхід забезпечує не лише виявлення загроз, а й формування повної картини інциденту в масштабах усієї мережі.

Висновки. Проведене дослідження дозволяє зробити допущення що жоден окремий метод виявлення не забезпечує повного захисту від шкідливого ПЗ у корпоративному середовищі. На наш погляд, найбільш ефективними є інтегровані рішення, що комбінують сигнатурний, евристичний та поведінковий підходи, доповнені технологіями машинного навчання [5]. Подальші дослідження повинні бути спрямовані на розроблення адаптивних моделей виявлення, здатних реагувати на невідомі типи атак у реальному часі, а також на вдосконалення методів автоматичного аналізу великих обсягів телеметричних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
[2] Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware-analysis techniques and tools. *ACM Computing Surveys*, 44(2), 1–42. https://doi.org/10.1145/2089125.2089128
[3] Šrndić, N., & Laskov, P. (2014). Practical evasion of a learning-based classifier: A case study. *IEEE Symposium on Security and Privacy*, 197–211. https://doi.org/10.1109/SP.2014.20
[4] Mohaisen, A., & Alrawi, O. (2015). Unveiling Zeus: Automated classification of malware samples. In *Proceedings of the 22nd Network and Distributed System Security Symposium (NDSS)*. https://www.ndss-symposium.org/wp-content/uploads/2017/09/06_4_1.pdf
[5] Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. *Computers & Security*, 81, 123–147. https://doi.org/10.1016/j.cose.2018.11.001
[6] CrowdStrike. (2025). *CrowdStrike Falcon Platform Overview*. https://www.crowdstrike.com/en-us/platform/
[7] Cisco. (2025). *Cisco Secure Endpoint – Advanced Endpoint Protection*. https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html
[8] Microsoft. (2025). *Microsoft Defender for Endpoint documentation*. https://learn.microsoft.com/en-us/defender-endpoint/

Svitlychnyi V.A., Hruba V.V.

Systematic analysis of malware detection methods in corporate networks

Abstract. *The study examined the main methods of detecting malicious software (Malware) in corporate networks: signature, heuristic, behavioral and combined. A systematic analysis of their advantages and disadvantages was conducted, taking into account current cyber threats. Promising directions for the development of malware detection systems were identified.*

Keywords: *malware, system analysis, corporate network, threat detection, behavioral method.*