УДК 004.056

Я. Л. Алєксєєв
Г. В. Крайнічук (Шелепало)

ЕВОЛЮЦІЯ ТА МЕХАНІЗМИ РОБОТИ СУЧАСНИХ АНТИВІРУСНИХ СИСТЕМ

Вінницький національний технічний університет

Анотація. *У роботі досліджено еволюцію та сучасні механізми роботи антивірусних систем. Розглянуто базову класифікацію програм захисту, статичний та динамічний аналіз, роль поведінкового аналізатора, а також інтеграцію машинного навчання та аналітики поведінки користувачів (UEBA). Проаналізовано трансформацію антивірусів у комплексні платформи (EPP, EDR, XDR) на прикладі протидії вірусам-вимагачам.*

Ключові слова: антивірусна система, UEBA, поведінковий аналіз, машинне навчання, безфайлові загрози, AMSI, EDR, XDR.

Abstract. *The work examines the evolution and modern mechanisms of antivirus systems. The basic classification of security programs, static and dynamic analysis, the role of a behavioral analyzer, as well as the integration of machine learning and user and entity behavior analytics (UEBA) are considered. The transformation of antiviruses into comprehensive platforms (EPP, EDR, XDR) is analyzed on the example of countering ransomware.*

Keywords: antivirus, UEBA, behavioral analysis, machine learning, fileless threats, AMSI, EDR, XDR.

Вступ

Проблема захисту інформації виникла одночасно зі створенням перших обчислювальних машин. Історія комп'ютерних вірусів має глибоке коріння, починаючи з 1949 року, коли Джон фон Нейман запропонував теоретичну модель автоматів, здатних до самовідтворення. Відтоді шкідливе програмне забезпечення еволюціонувало від аматорських експериментів до потужної зброї злочинних угруповань. Сучасні загрози, такі як троянські програми, мережеві хробаки та програми-вимагачі, здатні завдавати багатомільярдних збитків інфраструктурі та бізнесу.

Основна проблема сучасного етапу розвитку кібербезпеки полягає в тому, що кількість та складність загроз зростають експоненціально. Традиційні підходи до захисту, які були ефективними ще десять років тому, сьогодні виявляються безсилими перед атаками "нульового дня" (zero-day), поліморфним кодом та загрозами, згенерованими за допомогою штучного інтелекту. Саме тому сучасні антивірусні системи змушені були еволюціонувати з простих програм-сканерів у надзвичайно складні екосистеми.

Дане дослідження має на меті розкрити еволюцію та механізми роботи сучасних антивірусних систем, від класичного сканування до впровадження алгоритмів штучного інтелекту та розгортання багаторівневих платформ класу EDR та XDR. Ця робота слугує комплексним оглядом сучасних методів протидії кіберзагрозам.

Результати дослідження

Актуальність дослідження еволюції та механізмів роботи сучасних антивірусних систем зумовлена тим, що захист комп'ютерних систем постійно змінюється у відповідь на появу більш складних кібератак, які часто функціонують приховано, працюючи виключно в оперативній пам'яті й не залишаючи слідів на фізичних накопичувачах [5]. На початкових етапах розвитку антивірусного програмного забезпечення захист будувався на основі відокремлених утиліт, серед яких базовим компонентом були сканери, що здійснювали пошук загроз за допомогою сигнатур – унікальних цифрових відбитків відомих вірусів [1, 2]. Хоча сигнатурний аналіз відзначався стовідсотковою точністю виявлення відомого шкідливого коду, він виявився абсолютно безсилим перед модифікованими чи новими загрозами, що змусило розробників доповнювати системи моніторами для перевірки файлів у реальному часі, а також ревізорами, вакцинами та фагами для лікування

інфікованих файлів [4]. На сучасному етапі розвитку індустрії безпеки ці розрізнені інструменти еволюціонували у комплексні модульні системи, які забезпечують ешелоновану цифрову гігієну користувача через мережу незалежних екранів для перевірки файлової системи, електронної пошти, веб-трафіку, батьківського контролю та менеджерів автозапуску [5].

З огляду на стрімке зростання кількості та автоматизацію створення нових унікальних вірусів, виникла потреба в оцінці не лише статичної структури файлу, а й його потенційних намірів під час виконання. Впровадження евристичного аналізу дозволило оцінювати структуру файлів за імовірнісними алгоритмами та виявляти підозрілі шаблони дій ще до запуску програми, проте справжня революція відбулася з появою динамічних поведінкових аналізаторів, які оцінюють реальні операції процесів безпосередньо в процесі їхнього виконання та миттєво блокують деструктивну активність [7]. Для перевірки підозрілих файлів було впроваджено технологію ізольованих віртуальних середовищ – «пісочниць», де програми запускаються у віртуальному вакуумі без ризику для операційної системи [6]. Цей прогрес змусив зловмисників змінити тактику та розробити безфайлові загрози (Fileless Malware), які взагалі не записують свій код на жорсткий диск, а виконуються лише в оперативній пам'яті шляхом експлуатації легітимних системних інструментів, таких як PowerShell або WMI, за концепцією "Living off the Land" [5]. Оскільки ці утиліти необхідні для штатного функціонування системи, антивіруси не можуть їх заблокувати. Інфікування зазвичай відбувається через макроси в документах, які приховано запускають PowerShell для завантаження коду в пам'ять , а для закріплення в системі після перезавантаження використовуються записи в системному реєстрі або постійні підписки на події в репозиторії WMI, що дозволяє зловмисникам зберігати постійний безфайловий доступ із найвищими системними правами [4, 6].

Для протидії безфайловим атакам та аналізу скриптів безпосередньо в оперативній пам'яті компанія Microsoft інтегрувала в Windows інтерфейс Antimalware Scan Interface, який виступає посередником між скриптовими рушіями, такими як PowerShell, та встановленим антивірусним ПЗ. Основний механізм роботи AMSI полягає в тому, що він перехоплює шкідливий код у "голому" вигляді безпосередньо в оперативній пам'яті за долю секунди до його виконання і передає цей буфер антивірусному ядру для детального аналізу через систему стандартних функцій, таких як AmsiInitialize, AmsiScanBuffer та AmsiResultIsMalware. Однак у процесі протистояння хакери розробили методи обходу цього захисту, найпопулярнішим з яких є перепрограмування пам'яті (In-Memory Patching), коли зловмисники знаходять функцію AmsiScanBuffer у завантаженій бібліотеці amsi.dll і перезаписують її інструкції таким чином, щоб вона завжди повертала антивірусу результат про повну безпеку коду. Окрім цього, використовуються апаратні пастки CPU та виконання коду у середовищах, які не підтримуються AMSI [6]. Щоб нейтралізувати ці обхідні шляхи, сучасні захисні платформи будують ешелоновану оборону, комбінуючи провайдер AMSI із незалежними сканерами командного рядка, які аналізують текст команд на предмет аномалій ще до передачі скриптовим рушіям , а також обмежують можливості зловмисників за допомогою технологій контролю додатків (WDAC), які переводять консолі у режим обмеженої функціональності (Constrained Language Mode) та захищають ядро за допомогою цілісності коду на основі гіпервізора [5].

Сучасні масштаби кіберзагроз змусили індустрію інтегрувати в захисні системи алгоритми штучного інтелекту та машинного навчання, які автоматично вираховують рівень ризику для невідомих файлів за тисячами характеристик і самостійно виявляють приховані аномалії в мережевому трафіку [7]. Для захисту від компрометації легітимних акаунтів застосовуються системи аналітики поведінки користувачів та сутностей (UEBA), які створюють динамічні профілі активності співробітників і автоматично блокують облікові записи у разі виявлення нетипових дій (наприклад, масового скачування баз даних у нічний час з незвичної геолокації) [3]. На корпоративному рівні класичні антивіруси остаточно поступилися місцем платформам виявлення та реагування на кінцевих точках (EDR), які працюють як "чорні скриньки" і фіксують усю системну телеметрію для проведення розслідувань [6]. У контексті протидії вірусам-вимагачам (Ransomware) платформи EDR використовують поведінкові екрани та файли-приманки для зупинки шифрування на ранніх стадіях, а також автоматично ізолюють заражені вузли від локальної мережі, що разом із бекапами за правилом «3-2-1» нівелює загрозу шантажу [8]. Найбільш перспективним вектором розвитку є перенесення захисту на апаратний рівень процесора за допомогою технологій на кшталт Intel Threat Detection Technology (Intel TDT), яка використовує низькопровідникову телеметрію та алгоритми машинного навчання на рівні мікроархітектури CPU для створення апаратних відбитків шкідливої поведінки. Це дозволяє виявляти безфайлові віруси та загрози нульового дня безпосередньо під час виконання інструкцій у кремнієвому кристалі, унеможливлюючи будь-яке програмне маскування чи обхід

системних перевірок [5, 7]. При цьому для збереження продуктивності системи важкі обчислення з глибокого сканування пам'яті (Advanced Memory Scanning) делегуються на вбудований графічний процесор (GPU).

Таким чином, архітектурна еволюція захисного програмного забезпечення демонструє фундаментальний перехід від реактивної моделі ідентифікації відомих сигнатур до проактивного прогнозування та динамічного аналізу намірів програми [1, 2]. Сучасні антивірусні системи трансформувалися зі звичайних локальних утиліт у глобальні ешелоновані екосистеми (EDR/XDR), які поєднують у собі програмний моніторинг операційної пам'яті (AMSI), аналітику поведінки користувачів, машинне навчання, хмарні бази кіберрозвідки та апаратні датчики процесора [3, 5, 6]. Подальший розвиток захисних рішень відбуватиметься у площині повної предиктивної автономності та глибинної інтеграції з мікропроцесорною архітектурою, що дозволить блокувати найскладніші атаки ще до моменту завантаження операційної системи.

Висновки

Проведене дослідження підтверджує, що сучасні антивірусні системи здійснили перехід від застарілого сигнатурного сканування до комплексних систем проактивного захисту. Стрімке зростання складності кібератак, зокрема поява безфайлових загроз та вірусів-вимагачів, змусило індустрію впровадити концепцію ешелонованої оборони. Сьогодні фундаментом кібербезпеки є платформи класу EDR та XDR, ефективність яких забезпечується синергією динамічного поведінкового аналізу, ізоляції коду у віртуальних середовищах, перехоплення інструкцій в оперативній пам'яті (AMSI) та використання аналітики на базі штучного інтелекту (UEBA).

Найбільш перспективним вектором розвитку індустрії безпеки є перенесення захисних механізмів на апаратний рівень. Використання мікроархітектурної телеметрії процесорів дозволяє ідентифікувати загрози нульового дня безпосередньо під час виконання інструкцій у кремнієвому кристалі, що унеможливлює спроби програмного обходу чи маскування. Таким чином, механізми роботи сучасних антивірусів невпинно ускладнюються, а їхній подальший еволюційний крок прямує до повної предиктивної автономності та здатності нейтралізувати деструктивні дії ще до того, як вони завдадуть шкоди інфраструктурі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бурячок В. Л., Толюпа С. В., Семінько В. В. Інформаційна та кібербезпека: підручник. Київ: ДУТ, 2015. 584 с.
2. Ігнатьєва О. В. Інформаційна безпека й основні загрози захисту комп'ютерів. URL: https://ignatevaolesy.narod.ru/files/Ignateva-2010.pdf (дата звернення: 31.05.2026).
3. Ковальчук В. Дослідження та принципи побудови системи поведінкового аналізу користувачів за допомогою концепції UEBA. URL: https://kntu.kr.ua/file/content/28047/v-kovalchuk-doslidzhennia-ta-pryntsypy-pobudovy-systemy-povedinkovoho-analizu-korystuvachiv-za-dopomohoyu-kontseptsii-ueba-str-229-240-.pdf (дата звернення: 31.05.2026).
4. Корченко О. Г., Гнатюк С. О., Сейлова Н. А. Системи захисту інформації: навч. посіб. Київ: НАУ, 2017. 256 с.
5. Ланде Д. В., Фурашев В. М. Основи інформаційної та кібербезпеки: навч. посіб. Київ: НТУУ «КПІ», 2020. 345 с.
6. Опірський І. Р. Захист інформації в корпоративних мережах: монографія. Львів: Вид-во Львівської політехніки, 2021. 210 с.
7. Смірнов О. А., Смірнова Т. О. Системи виявлення вторгнень та поведінковий аналіз в кібербезпеці // Захист інформації. 2023. Т. 25, № 1. С. 45–52.
8. Щербаков О. В., Коваленко А. А. Методи та засоби протидії програмам-вимагачам (Ransomware) у корпоративних мережах // Безпека інформаційних систем. 2022. № 3. С. 112–119.

Алєксєєв Ярослав Леонідович бакалавр групи 2БС-24, кафедра захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: alieksieiev.yaroslav@gmail.com

Крайнічук (Шелепало) Галина Василівна – доцент кафедри захисту інформації, кандидат фізико-математичних наук, кафедра захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: hv.shelepalo@vntu.edu.ua

Alekseev Yaroslav Leonidovych – bachelor of group 2BS-24, Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: alieksieiev.yaroslav@gmail.com

Krainichuk (Shelepalo) Halyna Vasylivna – Associate Professor of the Department of Information Protection, Candidate of Physical and Mathematical Sciences, Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: hv.shelepalo@vntu.edu.ua