

УДК 004.421.1:004.415

Багатко А.С.¹, Коновалов О.Ю.²

¹ здобувач вищої освіти, Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

² доц. Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій

ВІРТУАЛЬНІ ПІСОЧНИЦІ ДЛЯ АНАЛІЗУ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Віртуальні пісочниці набули статусу ключового інструменту кібербезпеки, дозволяючи дослідження шкідливого програмного забезпечення без ризику для основної інфраструктури. Їхній принцип ґрунтується на створенні ізольованого середовища, де зловмисний код, зокрема віруси, трояни та шпигунські програми, може виконуватися для аналізу. Це забезпечує можливість отримувати детальну картину функціонування загроз, включаючи їхні методи обходу систем безпеки та шкідливий вплив на операційну систему.

Основою побудови пісочниць є технології віртуалізації або емуляції, які гарантують повну ізоляцію від продуктивного середовища. У рамках цього підходу створюються віртуальні машини, кожна з яких має власну операційну систему, мережеві конфігурації та налаштування апаратного забезпечення, що можна змінювати залежно від потреб дослідження.[1] Такі можливості дозволяють моделювати різноманітні сценарії для перевірки, наприклад, здатності загроз до самопоширення, завантаження додаткових компонентів чи адаптаційних тактик приховування своєї діяльності.

Важливою характеристикою віртуальних пісочниць є підтримка моментальних знімків середовища (snapshots), що дозволяє оперативно повертатися до початкового стану після завершення дослідження. Це не лише мінімізує затрати часу, але й допомагає уникнути накопичення залишкових даних від попередніх тестів. Завдяки такій функціональності фахівці можуть неодноразово аналізувати одні й ті самі загрози у змінених умовах, відстежуючи варіації їхньої поведінки залежно від налаштувань середовища.

Однак шкідливе ПЗ часто розробляється із вбудованими механізмами виявлення віртуалізованого оточення, щоб уникнути детального аналізу. Як наслідок, важливою задачею стає розробка реалістичних умов, які не видають пісочницю як штучне середовище. Це передбачає маскування гіпервізора, використання правдоподібних параметрів обладнання та імітацію активності користувача – заходи, що ускладнюють розпізнавання оточення з боку шкідливого коду.

Крім того, сучасні віртуальні пісочниці можуть працювати в автоматичному режимі. У такій моделі система самостійно запускає

підозрілий файл і фіксує всі його дії: створення процесів, внесення змін до реєстру, модифікацію файлів або спроби встановити зв'язок із зовнішніми серверами.[2] Це дозволяє швидко формувати технічний профіль загрози та порівнювати його зі стандартними шаблонами атак, що значно прискорює процес реагування на кіберінциденти.

Для аналітиків стає критично важливо не лише стежити за активністю шкідливого програмного забезпечення, але й глибоко розуміти механізми його функціонування. Інтеграція віртуальних пісочниць з системами моніторингу мережевого трафіку та інструментами для аналізу API-викликів дає змогу отримати багатогранну картину поведінки загрози, охоплюючи як локальні зміни в операційній системі, так і взаємодію з віддаленими командними серверами.

Швидкий розвиток шкідливого ПЗ змушує постійно адаптувати технології віртуальних пісочниць. Сучасні зловмисні програми здатні змінювати свою поведінку залежно від системних налаштувань, геолокації або навіть затримувати активацію до певного часу.[3] Це стимулює дослідників вдосконалювати свої інструменти, впроваджуючи емуляцію користувацьких дій, симуляцію робочого оточення та створення динамічних профілів для більш точного аналізу загроз.

Разом із розвитком віртуальних машин активно вдосконалюються й хмарні пісочниці, що пропонують можливість паралельного аналізу значної кількості зразків. Це стає критично важливим для організацій, які щоденно стикаються зі сотнями або навіть тисячами підозрілих файлів. Завдяки хмарним рішенням забезпечується масштабованість, централізоване управління та доступність результатів аналізу для різних відділів.

Віртуальні пісочниці відіграють ключову роль у сучасному кіберзахисті, й одним із їхніх важливих аспектів є автоматизація процесів аналізу. Сучасні платформи пропонують скриптове керування, що забезпечує запуск потенційно шкідливих файлів під заданими сценаріями, фіксацію їхньої поведінки та порівняння отриманих даних із базами відомих загроз.[4] Цей підхід значно скорочує час, необхідний для виявлення ризиків, а також мінімізує ймовірність людських помилок.

Не менш важливим завданням є інтеграція віртуальних пісочниць із корпоративними системами безпеки. Ідеальним варіантом механізму є автоматичне передавання результатів аналізу до систем управління подіями та інформацією безпеки (SIEM), а також до платформ для захисту кінцевих точок (EDR). Це створює самодостатній цикл: підозрілий файл перевіряється у пісочниці, результати використовуються для вдосконалення захисту мережі, а вся інфраструктура отримує можливість швидше реагувати на потенційні загрози.

Майбутнє цього напрямку передбачає подальше впровадження штучного інтелекту, удосконалення прихованої емуляції та створення більш масштабованих рішень для корпоративного використання. Завдяки цьому пісочниці перетворюються з простого інструменту аналізу на ключовий елемент комплексного кіберзахисту.[5]

Загалом, віртуальні пісочниці є незамінним інструментом для аналізу шкідливого програмного забезпечення. Вони створюють безпечне середовище для досліджень, допомагають виявляти новітні техніки атак і сприяють розробці більш ефективних методів захисту. Хоча їх впровадження супроводжується значними витратами і технічними викликами, їхня роль у сучасній кібербезпеці залишається фундаментальною і лише збільшуватиметься в умовах безперервної еволюції загроз.

СПИСОК ВИКОРИСТОНОЇ ЛІТЕРАТУРИ

1. Нафієв А., Родіонов А. Система динамічного аналізу шкідливого програмного забезпечення на основі інтроспекції віртуальних машин та методів машинного навчання. Problems in programming. URL: <https://pp.isoftware.kiev.ua/index.php/ojs1/article/download/570/621> (дата звернення: 30.09.2025).
2. Ільїн М. Вступ до аналізу шкідливого програмного забезпечення. Київський політехнічний інститут. URL: https://www.infosec-kpi.in.ua/assets/files/crdf_slides.pdf (дата звернення: 30.09.2025).
3. Sandbox або пісочниця – незамінний компонент інформаційної безпеки. IT Specialist. URL: <https://my-itspecialist.com/sandbox-or-sandbox-is-an-essential-component-of-information-security> (дата звернення: 30.09.2025).
4. Хмарна пісочниця - аналізує і виявляє складні загрози. ESET. URL: https://www.eset.com/ua/about/newsroom/blog/business-security/analiz-v-oblachnoy-pesochnitse-kak-uluchshit-vyyavleniye-ugroz/?srsltid=AfmBOooAH8VUromil5lCYE3xFGpViF17T-GZQpTo3EmhfhgGDG_4YSVB (дата звернення: 30.09.2025).
5. Єгоров С., Шкварницька Т. Розширений метод аналізу шкідливого програмного забезпечення з метою створення сигнатур. Вісник Університету «Україна» Серія Інформатика, обчислювальна техніка та кібернетика. URL: https://visn-it.uu.edu.ua/old_site/files/2020/16.pdf (дата звернення: 30.09.2025).