© Verkhovets O.S., Martyniuk I.V., Zaika N.V., Okhrimenko T.O. Protection of Modern Operating Systems from Cyber Threats // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 52-59. © This is an open access article under the CC BY 4.0 International license.*

DOI: 10.18372/2225-5036.32.21646

ЗАХИСТ СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМ ВІД КІБЕРЗАГРОЗ

Олексій Верховець[2], Ігор Мартинюк[1,2], Назар Заїка [2,3], Тетяна Охріменко[1,2]

[1] Національний університет «Київський авіаційний інститут», Україна
[2] Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Україна
[3] Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Україна



ВЕРХОВЕЦЬ Олексій Сергійович, аспірант
Рік та місце народження: 1982 рік, м. Ужгород, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут», 2004 рік.
Посада: заступник начальника центру Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації.
Наукові інтереси: інформаційні технології, кібербезпека та захист інформації, комп'ютерна безпека.
Публікації: більше 10 наукових публікацій, серед яких наукові статті, матеріали та тези доповідей на конференціях.
E-mail: balexc.ua@gmail.com
ORCID: 0000-0002-3897-106X



МАРТИНЮК Ігор Вадимович, аспірант
Рік та місце народження: 1988 рік, с. Верхнєдніпровський.
Освіта: Національний авіаційний університет, 2011 рік.; аспірант, Національний університет «Київський авіаційний інститут» з 2024 року.
Посада: інженер Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації з 2023 року.
Наукові інтереси: кібербезпека, моніторинг.
Публікації: більше 10 наукових публікацій, серед яких наукові статті, матеріали та тези доповідей на конференціях.
E-mail: imartyniukiv@gmail.com
ORCID: 0009-0003-5565-0828



ЗАЇКА Назар Валентинович, аспірант
Рік та місце народження: 1990 рік, м. Черкаси, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут», 2014 рік.
Посада: мол. наук. співробітник Державного науково-дослідного інституту технологій кібербезпеки.
Наукові інтереси: комп'ютерні науки.
Публікації: більше 10 наукових публікацій, серед яких монографії, наукові статті, матеріали та тези доповідей на конференціях.
E-mail: nazar2611@gmail.com
ORCID: 0000-0002-5791-8926



ОХРІМЕНКО Тетяна Олександрівна, к.т.н., ст. дослідник
Рік та місце народження: 1990 рік, м. Вінниця, Україна.
Освіта: Національний авіаційний університет, 2012 рік.
Посада: заступник декана з наукової роботи Факультету комп'ютерних наук та технологій, Національний університет «Київський авіаційний інститут»; провідний науковий співробітник ДержНДІ.
Наукові інтереси: інформаційна безпека, реагування на інциденти інформаційної безпеки, квантова криптографія.
Публікації: більше 100 наукових публікацій, серед яких монографії, наукові статті, матеріали та тези доповідей на конференціях, патенти та авторські свідоцтва.
E-mail: t.okhrimenko@npp.kai.edu.ua
ORCID: 0000-0001-9036-6556

Анотація. *У статті досліджено основні аспекти забезпечення безпеки сучасних операційних систем у контексті зростання кіберзагроз. Проаналізовано архітектурні механізми захисту, моделі контролю доступу та підходи до управління привілеями. Розглянуто особливості реалізації безпеки в різних типах операційних систем, зокрема настільних, серверних і мобільних. Окрему увагу приділено використанню принципу мінімальних привілеїв, механізмів довірених обчислень та сучасних методів аналізу даних для виявлення аномальної активності та підвищення кіберстійкості інформаційних систем.*

Ключові слова: *операційні системи, кібербезпека, кіберзагрози, контроль доступу, довірені обчислення, захист інформаційних систем, комп'ютерні системи.*

© Verkhovets O.S., Martyniuk I.V., Zaika N.V., Okhrimenko T.O. Protection of Modern Operating Systems from Cyber Threats // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 52-59. © This is an open access article under the CC BY 4.0 International license.*

Вступ

Операційна система є фундаментальним компонентом інформаційної інфраструктури, оскільки забезпечує управління апаратними ресурсами, координацію виконання програм, міжпроцесну взаємодію та реалізацію механізмів контролю доступу. Саме на рівні операційної системи реалізуються базові функції забезпечення інформаційної безпеки, що визначають рівень захищеності всієї комп'ютерної системи. У сучасних операційних системах застосовується комплекс взаємопов'язаних механізмів захисту, до яких належать автентифікація користувачів, розмежування доступу до системних ресурсів, ізоляція процесів, криптографічні методи захисту інформації та засоби аудиту подій безпеки. Застосування цих механізмів забезпечує можливість контролю доступу до інформаційних ресурсів та зменшує ризики несанкціонованого використання системи [1]. Дослідження архітектур безпеки операційних систем також підкреслюють важливість поєднання програмних і апаратних механізмів захисту, що дозволяє підвищити загальний рівень кіберстійкості інформаційної інфраструктури [2, 3].

Аналіз існуючих досліджень

Операційна система Microsoft Windows реалізує багаторівневу модель безпеки, яка включає систему облікових записів користувачів, механізми розмежування доступу на основі списків контролю доступу (Access Control Lists), ізоляцію процесів та інтегровані засоби захисту мережевої взаємодії. Такі механізми дозволяють реалізовувати політики доступу до системних ресурсів, включаючи файлову систему, процеси та мережеві служби, що є важливим елементом забезпечення безпеки інформаційних систем. Разом із тим широка поширеність цієї операційної системи обумовлює її високу привабливість для кіберзлочинців, що призводить до значної кількості атак і шкідливого програмного забезпечення, орієнтованого на цю платформу [1]. Показовим прикладом масштабної кіберзагрози є атака BlueBorne, що використовувала уразливості у реалізації Bluetooth-стеку. За оцінками дослідників компанії Armis, потенційно вразливими могли бути понад 8,2 млрд пристроїв, які використовують Bluetooth-з'єднання [4].

Операційна система Linux широко застосовується у серверних системах, хмарній інфраструктурі та середовищах критичної інфраструктури. Основою її архітектури безпеки є модель розмежування доступу на основі користувачів і груп, контроль доступу до файлової системи та механізми ізоляції процесів. Додатково використовуються системи розширеного контролю доступу, такі як SELinux або AppArmor, що дозволяють реалізувати принцип мінімальних привілеїв та обмежувати доступ процесів до критичних системних ресурсів [1]. Сучасні дослідження у сфері безпеки ядра Linux спрямовані на підвищення рівня ізоляції системних компонентів. Зокрема у роботі Gravani та ін. запропоновано механізм Protection Keys for Kernelspace (PKK), реалізований у системі IskiOS. Експериментальні результати показали, що використання цього механізму створює приблизно 11 % накладних витрат продуктивності, тоді як додаткове застосування механізму shadow stacks може збільшувати їх до 22 % [5]. Отримані результати свідчать про можливість посилення ізоляції ядра без критичного впливу на продуктивність системи.

Мобільні операційні системи використовують специфічні архітектурні підходи до забезпечення інформаційної безпеки. Зокрема, операційна система Android реалізує модель ізоляції додатків (sandbox), систему дозволів для доступу до системних ресурсів та криптографічні механізми захисту даних. Кожен додаток виконується у власному ізольованому середовищі, що обмежує його взаємодію з іншими компонентами системи без надання відповідних дозволів [6]. Разом із тим дослідники відзначають, що відкрита модель розповсюдження додатків у цій екосистемі створює додаткові ризики поширення шкідливого програмного забезпечення [7]. Для зменшення цих ризиків пропонуються додаткові механізми контролю доступу до системних ресурсів. Одним із прикладів є механізм контролю використання сенсорів у мобільних системах, що дозволяє регулювати передачу прав доступу між взаємодіючими програмами та запобігати несанкціонованому використанню сенсорних даних.

Операційна система iOS застосовує більш централізовану модель забезпечення безпеки, що передбачає суворий контроль розповсюдження програмного забезпечення, криптографічний захист файлової системи та обмежену взаємодію між додатками. Така архітектура дозволяє зменшити ризик поширення шкідливого програмного забезпечення у мобільному середовищі [6]. Порівняльні дослідження мобільних операційних систем показують, що централізований контроль екосистеми програм у iOS забезпечує більш жорсткий механізм перевірки додатків порівняно з відкритою моделлю Android [7]. Водночас навіть така архітектура не гарантує повної захищеності, оскільки складні атаки можуть використовувати раніше невідомі вразливості програмного забезпечення.

Серед найбільш поширених кіберзагроз для операційних систем дослідники виділяють шкідливе програмне забезпечення, експлуатацію вразливостей програмного коду, атаки на міжпроцесну взаємодію та компрометацію мережевих протоколів. У сучасних дослідженнях особлива увага приділяється використанню методів аналізу даних і машинного навчання для виявлення шкідливого програмного забезпечення. Такі підходи дозволяють ідентифікувати нові зразки malware на основі аналізу поведінкових характеристик програмного забезпечення та статистичних моделей виконання програм [8].

Операційні системи можуть класифікуватися за різними критеріями, включаючи кількість

© Verkhovets O.S., Martyniuk I.V., Zaika N.V., Okhrimenko T.O. Protection of Modern Operating Systems from Cyber Threats // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 52-59. © This is an open access article under the CC BY 4.0 International license.*

користувачів, характер виконання завдань та сферу застосування. У науковій літературі зазначається, що поділ операційних систем на однокористувацькі та багатокористувацькі, а також на однозадачні та багатозадачні системи дозволяє визначити їх архітектурні особливості та відповідні механізми безпеки. Багатокористувацькі системи, зокрема Unix-подібні операційні системи та серверні дистрибутиви Linux, повинні реалізовувати більш складні механізми розмежування доступу та управління привілеями, оскільки декілька користувачів можуть одночасно використовувати спільні системні ресурси. Класифікація операційних систем за сферою застосування також має значення для аналізу кіберзагроз. Настільні операційні системи орієнтовані на виконання прикладних програм та взаємодію з користувачем, серверні системи оптимізовані для роботи у мережевих середовищах з великою кількістю підключень, тоді як мобільні операційні системи проектуються з урахуванням енергоспоживання та сенсорних інтерфейсів. Окрему категорію становлять вбудовані операційні системи та системи реального часу (RTOS), які використовуються у промислових системах, робототехніці та транспортній інфраструктурі. Кожна з цих категорій має власні вимоги до безпеки, що безпосередньо впливає на архітектуру механізмів захисту [1].

Метою даної роботи є є систематичний аналіз архітектур безпеки сучасних операційних систем — зокрема Windows, Linux, Android та iOS — у частині вбудованих механізмів контролю доступу, моделей ізоляції процесів, криптографічних засобів захисту інформації та інструментів аудиту подій безпеки, а також дослідження основних категорій кіберзагроз, що експлуатують архітектурні вразливості на рівні операційної системи. Додатково робота спрямована на оцінювання придатності комплексних підходів до управління кіберризиками, визначених міжнародно визнаними стандартами, зокрема NIST SP 800-53, для захисту середовищ операційних систем, а також на виявлення ключових залежностей між класифікацією операційних систем за функціональним призначенням та відповідними вимогами до механізмів їх захисту.

Основна частина дослідження

Порушення безпеки операційних систем

Порушення безпеки операційних систем здебільшого пов’язані з експлуатацією архітектурних слабкостей механізмів управління доступом, обробки файлових ресурсів та автентифікації користувачів. У наукових дослідженнях зазначається, що значна частина атак на операційні системи реалізується через пошук конфіденційної інформації у файловій системі, підбір або компрометацію облікових даних, а також через спроби ескалації привілеїв для отримання доступу до системних ресурсів із підвищеним рівнем довіри [1]. Подібні сценарії атак можуть включати аналіз тимчасових файлів, журналів подій або службових каталогів, що іноді містять інформацію, здатну розкрити структуру системи або механізми її захисту. Дослідження у сфері безпеки операційних систем показують, що такі методи можуть застосовуватися незалежно від конкретної платформи, оскільки вони використовують типові принципи організації доступу до ресурсів, характерні для більшості сучасних операційних систем [2, 3].

Проблематика порушення безпеки інформаційних систем набуває особливого значення у середовищах, пов’язаних із цифровими фінансовими процесами, де компрометація системи може призвести до значних економічних втрат. У дослідженні Rakibuzzaman та ін. розглянуто підходи до оцінювання ризиків у автоматизованих бухгалтерських системах, які функціонують у цифрових фінансових інфраструктурах. Автори аналізують типові загрози, включаючи несанкціонований доступ до фінансових даних, шахрайство та маніпуляції з транзакціями, а також пропонують застосування методів машинного навчання для виявлення ризикової поведінки у фінансових інформаційних системах . У межах дослідження використовуються алгоритми аналізу даних, зокрема підхід Isolation Forest для виявлення аномалій у транзакційних даних, що дозволяє ідентифікувати потенційно небезпечні операції на ранніх етапах їх виконання [9].

Останні дослідження у сфері кібербезпеки також демонструють зростаючу роль методів аналізу поведінки системи у процесі виявлення атак на операційні системи. Використання алгоритмів машинного навчання дозволяє аналізувати поведінкові характеристики програмного забезпечення та мережевої активності з метою ідентифікації шкідливих програм або аномальних дій користувачів. Огляд сучасних підходів до виявлення malware показує, що застосування моделей машинного навчання дає можливість аналізувати великі обсяги даних і виявляти раніше невідомі типи шкідливого програмного забезпечення, які можуть не визначатися традиційними сигнатурними методами [8].

Важливим напрямом підвищення безпеки операційних систем є забезпечення цілісності даних та ефективного контролю доступу до інформаційних ресурсів. У сучасних архітектурах безпеки значна увага приділяється використанню криптографічних механізмів захисту даних, що дозволяє забезпечити конфіденційність інформації навіть у випадку компрометації окремих компонентів системи. Крім того, дослідники підкреслюють важливість регулярного оновлення програмного забезпечення, застосування механізмів ізоляції процесів та реалізації принципу мінімальних привілеїв як ключових елементів захисту операційних систем від експлуатації відомих вразливостей [1, 2].

Впровадження комплексних підходів до управління кіберризиками

Одним із ключових напрямів забезпечення безпеки операційних систем є впровадження

комплексних підходів до управління кіберризиками, що охоплюють як технічні, так і організаційні механізми захисту інформаційних систем. У рекомендаціях National Institute of Standards and Technology (NIST) підкреслюється, що ефективна система захисту повинна поєднувати механізми контролю доступу, аудит подій безпеки, управління конфігураціями та постійний моніторинг стану системи. Зокрема, стандарт NIST Special Publication 800-53 визначає набір базових контролів безпеки, які застосовуються для захисту інформаційних систем, включаючи механізми управління обліковими записами, криптографічний захист інформації, контроль доступу до системних ресурсів та засоби реєстрації подій безпеки [10].

У звітах European Union Agency for Cybersecurity (ENISA) наголошується, що операційні системи є критично важливим компонентом цифрової інфраструктури, оскільки вони забезпечують взаємодію між прикладними програмами, мережевими сервісами та апаратними ресурсами комп'ютерних систем. У звіті Threat Landscape for Supply Chain Attacks зазначається, що компрометація програмних компонентів операційної системи може призвести до отримання зловмисником повного контролю над системою, що робить операційні системи важливою ціллю атак на ланцюги постачання програмного забезпечення [11].

Суттєвим елементом підвищення безпеки операційних систем є застосування механізмів ізоляції програмного середовища. У наукових дослідженнях зазначається, що ізоляція процесів та обмеження доступу програм до системних ресурсів дозволяють зменшити ризик ескалації привілеїв або поширення шкідливого програмного забезпечення після компрометації окремого програмного компонента [1]. Такі підходи широко використовуються у сучасних операційних системах та розглядаються як один із базових принципів побудови захищених програмних середовищ [2].

Окрему увагу в міжнародних стандартах інформаційної безпеки приділяють управлінню доступом до системних ресурсів та забезпеченню цілісності програмного забезпечення. У стандарті ISO/IEC 27002 зазначається, що захист інформаційних систем повинен включати регулярне оновлення операційних систем, обмеження доступу до системних ресурсів відповідно до принципу мінімальних привілеїв та використання криптографічних механізмів для захисту конфіденційної інформації [12]. Реалізація таких заходів дозволяє зменшити ризики експлуатації відомих вразливостей і підвищити загальний рівень кіберстійкості інформаційної інфраструктури.

Важливим напрямом розвитку сучасних систем кіберзахисту є використання методів аналізу поведінки програмного забезпечення та даних журналів подій. У сучасних дослідженнях показано, що застосування алгоритмів машинного навчання дозволяє підвищити ефективність виявлення шкідливого програмного забезпечення та аномальної активності у комп'ютерних системах. Зокрема, огляд сучасних методів виявлення malware демонструє, що використання моделей машинного навчання дає можливість аналізувати великі обсяги системних даних і виявляти нові типи шкідливого програмного забезпечення, які можуть залишатися непоміченими при використанні традиційних сигнатурних підходів [8, 13].

Архітектурні механізми безпеки операційних систем формуються через поєднання декількох взаємодоповнюючих технологій, включаючи автентифікацію користувачів, контроль доступу до ресурсів, ізоляцію процесів та механізми реєстрації подій безпеки. У систематичних оглядах безпеки операційних систем підкреслюється, що ефективність цих механізмів значною мірою залежить від їх інтеграції на рівні ядра операційної системи та використання політик управління привілеями [3]. Такі механізми дозволяють контролювати взаємодію між програмними компонентами системи та обмежувати можливість виконання несанкціонованого програмного коду.

Одним із перспективних напрямів підвищення безпеки операційних систем є використання механізмів довірених обчислень. У дослідженнях, присвячених проектуванню безпечних операційних систем, показано, що інтеграція механізмів довіреного завантаження, перевірки цілісності програмного забезпечення та апаратних коренів довіри дозволяє забезпечити контроль над виконанням програм та запобігати несанкціонованому доступу до системних ресурсів [1, 14]. Використання таких підходів створює основу для формування довіреного середовища виконання програм і підвищує стійкість операційних систем до складних кіберзагроз.

Аспекти захисту сучасних операційних систем

Одним із фундаментальних принципів побудови захищених операційних систем є реалізація принципу мінімальних привілеїв. Його сутність полягає у наданні користувачам та програмним процесам лише тих прав доступу, які необхідні для виконання конкретних функцій. У дослідженнях, присвячених безпеці операційних систем, зазначається, що реалізація механізмів контролю привілеїв та їх перевірки дозволяє зменшити ризик ескалації привілеїв і обмежити потенційні наслідки компрометації системи [3]. Використання такого підходу сприяє більш чіткому розмежуванню доступу до системних ресурсів і підвищує загальний рівень захищеності операційного середовища. Окремим напрямом наукових досліджень є аналіз механізмів захисту операційних систем сімейства Linux. У відповідних роботах розглядаються типові сценарії експлуатації вразливостей та можливі способи їх запобігання, включаючи використання механізмів контролю доступу, систем моніторингу та аналізу подій безпеки [8]. Застосування таких засобів дозволяє виявляти аномальну активність у системному середовищі та підвищувати ефективність реагування на потенційні кіберінциденти.

© Verkhovets O.S., Martyniuk I.V., Zaika N.V., Okhrimenko T.O. Protection of Modern Operating Systems from Cyber Threats // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 52-59. © This is an open access article under the CC BY 4.0 International license.*

Інтенсивний розвиток цифрових сервісів та інформаційних технологій призводить до постійного зростання обсягів електронних даних, що обробляються інформаційними системами. У цих умовах забезпечення безпеки операційних систем набуває критичного значення, оскільки саме вони виступають базовим компонентом інформаційної інфраструктури та забезпечують управління апаратними ресурсами, виконання прикладних програм і контроль доступу до інформаційних ресурсів. У науковій літературі підкреслюється, що сучасні операційні системи повинні реалізовувати комплекс базових механізмів захисту, серед яких автентифікація користувачів, контроль доступу до системних ресурсів, управління привілеями, аудит подій безпеки та механізми контролю цілісності програмного забезпечення [1, 3]. Ефективність реалізації цих механізмів безпосередньо впливає на здатність системи протидіяти несанкціонованому доступу, поширенню шкідливого програмного забезпечення та експлуатації системних вразливостей.

Одним із перспективних напрямів підвищення рівня безпеки операційних систем є використання концепції довірених обчислень (trusted computing). У дослідженнях архітектури безпечних операційних систем зазначається, що інтеграція механізмів довіреного завантаження, перевірки цілісності програмного забезпечення та використання апаратних коренів довіри дозволяє підвищити контроль над виконанням програмного коду та запобігти запуску модифікованих або несанкціонованих компонентів системи [14]. Такі механізми забезпечують перевірку автентичності програмних компонентів операційної системи на етапі завантаження та сприяють формуванню довіреного середовища виконання програм.

Важливим аспектом захисту операційних систем є застосування багаторівневих моделей контролю доступу. У наукових роботах, присвячених проектуванню безпечних операційних систем, підкреслюється, що використання обов'язкового контролю доступу, механізмів аудиту та систем розмежування прав доступу дозволяє обмежити можливості зловмисника у випадку компрометації окремих компонентів системи [1, 2]. Реалізація таких механізмів є важливим елементом архітектури сучасних операційних систем і забезпечує контроль взаємодії між процесами та системними ресурсами.

Проблема захисту операційних систем набуває особливої актуальності у сфері мобільних обчислень. Мобільні пристрої зберігають значні обсяги персональних та службових даних, включаючи фінансову інформацію, документи та комунікації користувачів. У дослідженнях мобільних платформ зазначається, що домінуючими операційними системами на ринку є Android та iOS, які використовують різні архітектурні підходи до забезпечення безпеки [6, 9]. Android застосовує модель ізоляції додатків (sandbox) та систему дозволів для контролю доступу до ресурсів пристрою, тоді як iOS використовує централізовану модель розповсюдження програмного забезпечення та процедури перевірки додатків перед їх публікацією [6]. Відмінності у цих підходах безпосередньо впливають на характер потенційних загроз та способи їх нейтралізації [9]. Узагальнення рівня безпеки операційної системи може розглядатися як функція обчислювальних можливостей платформи, враховуючи регулярності оновлень безпеки, рівня реалізації механізмів trusted computing та кількості актуальних вразливостей. При цьому зростання складності програмно-апаратної архітектури та впровадження багаторівневих механізмів контролю доступу здатні підвищувати рівень захищеності системи, тоді як накопичення невиправлених вразливостей зменшує її стійкість до кіберзагроз. Узагальнена функція залежності рівня захищеності від складності ОС, обчислювальних ресурсів та оновлень, може бути представлена як:

$$S(t)=\alpha\cdot\ln(P(t))+\beta\cdot U(t)+\gamma\cdot C(t)+\lambda\cdot M(t)+\mu\cdot R(t)+\eta\cdot I(t)-\delta\cdot V(t)$$

де:
- S(t) - інтегральний рівень безпеки операційної системи у момент часу t;
- P(t) - обчислювальна потужність та складність програмно-апаратної платформи;
- U(t) - інтенсивність та регулярність оновлень безпеки;
- C(t) - рівень реалізації механізмів контролю доступу та trusted computing;
- V(t) - кількість або критичність виявлених вразливостей;
- M(t) - рівень моніторингу;
- R(t) - механізми резервування;
- I(t) - рівень ізоляції процесів;
- α, β, γ, δ, λ, μ, η - вагові коефіцієнти впливу. Орієнтовні значення приведено у таблиці 1.

Таблиця 1. Вагові коефіцієнти впливу

Параметр	**Опис**	**Позначення**	**Діапазон значень**
Обчислювальна потужність та архітектурна складність системи	Вплив апаратно-програмної складності на реалізацію механізмів захисту	α	0.15 – 0.25
Регулярність оновлень безпеки	Частота та оперативність встановлення security updates	β	0.25 – 0.35
Механізми trusted computing та контролю доступу	Secure Boot, TPM, sandboxing, ACL, MAC	γ	0.25 – 0.40
Кількість та критичність вразливостей	Виявлені CVE, zero-day, невиправлені уразливості	δ	0.30 – 0.45
Рівень журналювання та моніторингу	SIEM, audit logs, поведінковий аналіз	λ	0.10 – 0.20
Резервування та механізми відновлення	Backup, fault tolerance, rollback	μ	0.10 – 0.15
Ізоляція процесів та контейнеризація	VM isolation, namespaces, SELinux/AppArmor	η	0.15 – 0.25

© Verkhovets O.S., Martyniuk I.V., Zaika N.V., Okhrimenko T.O. Protection of Modern Operating Systems from Cyber Threats // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 52-59. © This is an open access article under the CC BY 4.0 International license.*

Вагові коефіцієнти у моделі інтегрального оцінювання безпеки операційних систем визначають відносний вплив окремих механізмів захисту на загальний рівень стійкості системи. Для об'єктів критичної інфраструктури найбільший вплив, як правило, мають своєчасність оновлень безпеки, реалізація механізмів trusted computing та рівень актуальних вразливостей, оскільки саме ці фактори безпосередньо впливають на ймовірність компрометації системи.

Безпека операційних систем також тісно пов'язана із захистом мережевих сервісів та веб-інфраструктури, які функціонують на їх основі. У міжнародних стандартах інформаційної безпеки наголошується на необхідності застосування комплексних механізмів захисту, що включають автентифікацію користувачів, використання криптографічних протоколів, контроль доступу до інформаційних ресурсів та регулярне оновлення програмного забезпечення [10, 12]. Такі заходи спрямовані на зменшення ризиків несанкціонованого доступу та підвищення стійкості інформаційних систем до сучасних кіберзагроз.

У сучасних умовах операційні системи все частіше інтегруються у складні кіберфізичні середовища, що поєднують інформаційні та фізичні компоненти. Такі системи використовуються у промисловості, енергетиці, транспорті та інших сферах критичної інфраструктури. У дослідженнях кібербезпеки зазначається, що інтеграція сенсорних систем, мережевих технологій та програмного забезпечення створює нові потенційні вектори атак, що потребує застосування сучасних механізмів моніторингу та аналізу системної активності. У цьому контексті особливу увагу приділяють використанню методів аналізу даних та машинного навчання для виявлення аномальної поведінки системи [8].

Кіберзагрози та їх вплив на безпеку операційних систем

У сучасному цифровому середовищі інформаційні системи піддаються різним формам кіберзагроз, які умовно поділяють на пасивні та активні атаки. Пасивні атаки спрямовані на перехоплення або аналіз інформаційних потоків без прямого втручання у функціонування системи, тоді як активні атаки передбачають зміну, підміну або знищення інформації, а також вплив на роботу програмних компонентів системи. У дослідженнях безпеки операційних систем зазначається, що ефективна протидія таким загрозам потребує застосування механізмів контролю доступу, управління привілеями, реєстрації подій безпеки та інших засобів моніторингу системної активності [1, 3].

Актуальність досліджень у сфері кібербезпеки значно зростає у складних цифрових екосистемах, де інформаційні системи функціонують у взаємодії з мережевими сервісами та іншими програмними компонентами. У наукових роботах підкреслюється, що поєднання програмних платформ, мережевих технологій та великих обсягів даних створює нові потенційні вектори атак. У цьому контексті дослідники розглядають можливості використання методів аналізу даних і машинного навчання для виявлення шкідливого програмного забезпечення та аномальної поведінки у комп'ютерних системах [8].

Вразливості операційних систем можуть використовуватися для реалізації атак на рівні мережевих сервісів та прикладного програмного забезпечення. У науковій літературі зазначається, що однією з поширених причин компрометації систем є слабкі механізми автентифікації або некоректна конфігурація доступу до системних служб. У таких випадках використання політик управління доступом, механізмів автентифікації та журналювання подій дозволяє підвищити рівень контролю над доступом до системних ресурсів і зменшити ризик несанкціонованих дій користувачів [10, 12].

Подальший розвиток мережевих технологій та концепції Інтернету речей створює додаткові виклики для забезпечення безпеки операційних систем. Збільшення кількості підключених пристроїв призводить до розширення потенційної поверхні атак, що ускладнює процес забезпечення кіберзахисту. У сучасних дослідженнях наголошується, що для підвищення рівня безпеки інформаційних систем доцільно використовувати підходи, засновані на аналізі великих обсягів даних та застосуванні алгоритмів машинного навчання, які дозволяють виявляти аномальні шаблони поведінки у системних процесах і мережевій активності [8, 15].

Окремий напрям досліджень присвячений розробленню архітектур безпечних операційних систем. У роботах, що розглядають принципи проектування захищених системних середовищ, зазначається, що використання механізмів довіреного завантаження, контролю цілісності програмного забезпечення та моделей обов'язкового контролю доступу дозволяє значно підвищити рівень захисту системи від несанкціонованого виконання програмного коду або несанкціонованих дій користувачів [14].

Крім технічних механізмів захисту, важливим елементом забезпечення кібербезпеки є управління кіберризиками на організаційному рівні. У міжнародних стандартах інформаційної безпеки підкреслюється необхідність впровадження комплексних заходів, які включають криптографічний захист інформації, контроль доступу до системних ресурсів, постійний моніторинг безпеки та підготовку планів реагування на інциденти [11, 12]. Застосування таких підходів сприяє підвищенню стійкості інформаційних систем до сучасних кіберзагроз.

Висновки

Забезпечення безпеки операційних систем є багаторівневим завданням, яке передбачає поєднання архітектурних механізмів захисту, політик контролю доступу та процедур управління інформаційною безпекою. До ключових елементів безпечної архітектури операційних систем належать механізми автентифікації користувачів,

розмежування доступу до ресурсів, управління привілеями, аудит подій безпеки та контроль цілісності програмного забезпечення. Ефективність реалізації цих механізмів визначає здатність системи протидіяти несанкціонованому доступу, експлуатацію вразливостей та поширенню шкідливого програмного забезпечення.

Вразливості операційних систем можуть використовуватися для реалізації різних сценаріїв атак, зокрема через компрометацію облікових даних або помилки конфігурації системи. У зв'язку з цим важливого значення набуває застосування принципу мінімальних привілеїв, багаторівневих моделей контролю доступу та механізмів перевірки цілісності програмного забезпечення, які дозволяють обмежити можливості зловмисника навіть у випадку часткової компрометації системи.

Додатковим напрямом підвищення рівня кіберстійкості є використання сучасних методів аналізу даних для виявлення шкідливої або аномальної активності. Застосування алгоритмів машинного навчання дозволяє аналізувати поведінку системи та своєчасно виявляти потенційні загрози у складних інформаційних середовищах. Захист операційних систем потребує комплексного підходу, який поєднує архітектурні механізми безпеки, політики управління доступом, засоби контролю цілісності програмного забезпечення та методи аналізу даних для підвищення загальної кіберстійкості інформаційних систем.

Список літератури

[1] Akhtar Z. B. Securing operating systems: A comprehensive approach to security with best practices and techniques // International Journal of Advanced Network, Monitoring and Controls. 2024. DOI: https://doi.org/10.2478/ijanmc-2024-0010 (дата звернення: 20.01.2026).

[2] Hamdani S. W. A., Abbas H., Janjua A., Shahid W., Amjad M., Malik J., Murtaza M., Atiquzzaman M., Khan A. Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons // ACM Computing Surveys. 2021. DOI: https://doi.org/10.1145/3442480 (дата звернення: 01.03.2026).

[3] Mahfud A. Z., Sabila M. T., Wibowo N. A., Rhamdhan A., Priambodo D. F. A systematic literature review on operating system security // Proceedings of the 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS). 2023. DOI: https://doi.org/10.1109/ICE3IS59323.2023.10335475.

[4] Armis Labs. BlueBorne: The attack vector exposes almost every connected device. URL: https://www.armis.com/blueborne/ (дата звернення: 21.01.2026).

[5] Gravani S., Hedayati M., Criswell J., Scott M. Fast intra-kernel isolation and security with IskiOS. 2019. URL: https://arxiv.org/abs/1903.04654 (дата звернення: 06.02.2026).

[6] Quissanga F. C. Comparative study of information security in mobile operating systems: Android and Apple iOS // Mobile Security and Privacy. IntechOpen, 2023. URL: https://www.intechopen.com/chapters/85754 (дата звернення: 14.01.2026).

[7] Singh A., Taneja A., Kumar A. Comparative analysis of Android and iOS from security viewpoint // Computer Science Review. 2021. DOI: https://doi.org/10.1016/j.cosrev.2021.100372 (дата звернення: 15.02.2026).

[8] Bensaoud A., Kalita J., Bensaoud M. A survey of malware detection using deep learning. 2024. URL: https://arxiv.org/abs/2407.19153 (дата звернення: 05.03.2026).

[9] Rakibuzzaman Md., Sarna S., Mohammed A. A. Risk assessment models for protecting automated accounting systems from cyber threats // Journal of Computer Science and Technology Studies. 2025. DOI: https://doi.org/10.32996/jcsts.2025.7.7.78 (дата звернення: 10.01.2026).

[10] National Institute of Standards and Technology. Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5). DOI: https://doi.org/10.6028/NIST.SP.800-53r5 (дата звернення: 07.03.2026).

[11] ENISA. Threat landscape for supply chain attacks. European Union Agency for Cybersecurity, 2021. URL: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (дата звернення: 27.01.2026).

[12] ISO/IEC. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. URL: https://www.iso.org/standard/75652.html (дата звернення: 17.02.2026).

[13] Petracca G., Grossklags J., McDaniel P., Jaeger T. Regulating access to system sensors in cooperating programs. 2018. URL: https://arxiv.org/abs/1808.05579 (дата звернення: 23.02.2026).

[14] Nie X., Feng D., Che J., Wang X. Design and implementation of security operating system based on truted computing // International Conference on Machine Learning and Cybernetics. 2006. DOI: https://doi.org/10.1109/ICMLC.2006.258997.

[15] Martyniuk I. V., Okhrimenko T. O. Methodology and classification of open-source ML methods for IT monitoring based on the Zabbix system // Ukrainian Scientific Journal of Information Security. 2025. Vol. 31, No. 2. P. 87–92. 2025. DOI: https://doi.org/10.18372/2225-5036.31.20700.

УДК 004.056

Verkhovets O.S., Martyniuk I.V., Zaika N.V., Okhrimenko T.O. Protection of Modern Operating Systems from Cyber Threats

Abstract. *The article examines key aspects of ensuring the security of modern operating systems in the context of increasing cyber threats. Architectural security mechanisms, access control models, and privilege management approaches are analyzed. The study considers security features of different types of operating systems, including desktop, server, and mobile platforms. Particular*

attention is paid to the principle of least privilege, trusted computing mechanisms, and the use of data analysis methods for detecting anomalous activity and improving the cyber resilience of information systems.
Keywords: *operating systems, cybersecurity, cyber threats, access control, trusted computing, information system security, computer systems.*

ВЕРХОВЕЦЬ Олексій Сергійович, аспірант Національного університету «Київський авіаційний інститут»; заступник начальника центру Державного науково-дослідного інституту технологій кібербезпеки.
VERKHOVETS Oleksii, postgraduate student at the National University «Kyiv Aviation Institute», deputy head of the center at the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection.

МАРТИНЮК Ігор Вадимович, аспірант Національного університету «Київський авіаційний інститут», інженер ДержНДІ технологій кібербезпеки.
MARTYNIUK Ihor, postgraduate student at the National University «Kyiv Aviation Institute», engineer at the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection.

ЗАЇКА Назар Валентинович, аспірант Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України; мол. наук. співробітник Державного науково-дослідного інституту технологій кібербезпеки.
ZAIKA Nazar, postgraduate student of the Institute of Modeling Problems in Energy named after G.E. Pukhov National Academy of Sciences of Ukraine, junior researcher at the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection.

ОХРІМЕНКО Тетяна Олександрівна, кандидат технічних наук, старший дослідник, заступник декана з наукової роботи, Національний університет «Київський авіаційний інститут».
OKHRIMENKO Tetiana, Ph.D., senior researcher, deputy dean for research, National University «Kyiv Aviation Institute».

Дата надходження:	Дата прийняття:	Дата публікації:
02.03.2026	07.04.2026	22.04.2026