УДК 004.056:004.75
DOI https://doi.org/10.32782/IT/2025-1-8

Сергій ДОРОЖИНСЬКИЙ
PhD, доцент кафедри кібербезпеки, інформаційних технологій та економіки, декан факультету інформаційних технологій та соціально-гуманітарних наук, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, Україна, 02121
***ORCID:** 0000-0002-5395-6423*
***Scopus author ID:** 57222147991*

Валентин ГАЛУНЬКО
доктор філософії в галузі права, доцент кафедри адміністративного права, інтелектуальної власності та цивільно-правових дисциплін, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, Україна, 02121
***ORCID:** 0000-0002-8133-6766*

Бібліографічний опис статті: Дорожинський, С., Галунько, В. (2025). Розробка механізмів контролю доступу з використанням ООП. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 55–59, doi: https://doi.org/10.32782/IT/2025-1-8

РОЗРОБКА МЕХАНІЗМІВ КОНТРОЛЮ ДОСТУПУ З ВИКОРИСТАННЯМ ООП

У статті розглядаються питання розробки механізмів контролю доступу до інформаційних ресурсів із застосуванням принципів об'єктно-орієнтованого програмування (ООП).

***Метою** дослідження є формулювання та обґрунтування **методології** створення високоефективних, масштабованих і гнучких систем контролю доступу з використанням об'єктно-орієнтованих підходів. У рамках роботи розглядається вплив ключових принципів ООП – інкапсуляції, абстракції, наслідування та поліморфізму – на побудову механізмів автентифікації та авторизації, а також механізмів управління правами доступу, що забезпечують високий рівень безпеки і гнучкість в управлінні доступом до інформаційних систем. Особливу увагу приділено проектуванню об'єктних моделей, що дозволяють забезпечити строгий розподіл прав і ролей користувачів, а також реалізації механізмів динамічного оновлення доступу без необхідності внесення змін до основного коду програмної системи.*

***Наукова новизна** дослідження полягає в розробці інтегрованої методології застосування ООП для створення механізмів контролю доступу, яка дозволяє не лише підвищити надійність захисту інформації, а й забезпечити високу ступінь гнучкості та зручності в адмініструванні користувацьких прав у складних розподілених інформаційних середовищах.*

***Висновки.** Застосування ООП дає змогу створювати більш модульні, адаптовані до змін вимог системи контролю доступу, що значно підвищує безпеку та ефективність управління правами доступу в інформаційних системах.*

***Ключові слова:** об'єктно-орієнтоване програмування, механізми контролю доступу, автентифікація, авторизація, управління правами доступу, інкапсуляція, абстракція, наслідування, поліморфізм, гнучкість, масштабованість.*

Serhii DOROZHYNSKYI
PhD, Associate Professor at the Department of Cybersecurity, Information Technology and Economics, Dean of the Faculty of Information Technology and Social Sciences and Humanities, Kyiv University of Intellectual Property and Law of the National University "Odesa Law Academy", 210, Kharkivske highway, Kyiv, Ukraine, 02121, dorozhun1706@gmail.com
***ORCID:** 0000-0002-5395-6423*
***Scopus author ID:** 57222147991*

Valentyn HALUNKO
PhD in Law, Associate Professor at the Department of Administrative Law, Intellectual Property and Civil-Law Disciplines, Kyiv University of Intellectual Property and Law of the National University "Odesa Law Academy", 210, Kharkivske highway, Kyiv, Ukraine, 02121, valentinvalentin0987@gmail.com
***ORCID:** 0000-0002-8133-6766*

To cite this article: Dorozhynskyi, S., Halunko, V. (2025). Rozrobka mekhanizmiv kontroliu dostupu z vykorystanniam OOP [Development of Access Control Mechanisms Using OOP]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 55–59, doi: https://doi.org/10.32782/IT/2025-1-8

DEVELOPMENT OF ACCESS CONTROL MECHANISMS USING OOP

The article discusses the development of access control mechanisms for information resources using object-oriented programming principles. ***The aim*** *of the research is to formulate and justify a methodology for creating highly efficient, scalable, and flexible access control systems based on object-oriented approaches. The paper explores the impact of key OOP principles – encapsulation, abstraction, inheritance, and polymorphism – on the construction of authentication and authorization mechanisms, as well as access control mechanisms that ensure high levels of security and flexibility in managing access to information systems. Special attention is given to the design of object models that allow for strict distribution of user rights and roles, as well as the implementation of dynamic access updating mechanisms without the need to modify the main program code.*

The scientific novelty *of the research lies in the development of an integrated methodology for applying OOP to create access control mechanisms, which not only improves the reliability of information protection but also ensures a high degree of flexibility and convenience in user rights administration in complex distributed information environments.*

Conclusion. *The application of OOP enables the creation of more modular, adaptable access control systems, which significantly enhances security and the efficiency of managing access rights in information systems.*

Key words: *object-oriented programming, access control mechanisms, authentication, authorization, access rights management, encapsulation, abstraction, inheritance, polymorphism, flexibility, scalability.*

Вступ. У сучасних умовах розвитку інформаційних технологій питання безпеки даних набувають особливої актуальності. Захист інформації є одним із основних пріоритетів при розробці та експлуатації програмних систем, оскільки неправильне управління доступом може призвести до серйозних наслідків, таких як витік конфіденційної інформації або несанкціоноване втручання в роботу критичних систем. У цьому контексті особливе значення має створення ефективних механізмів контролю доступу, що дозволяють забезпечити безпеку та цілісність даних.

Об'єктно-орієнтоване програмування (ООП), завдяки своїм принципам інкапсуляції, абстракції, наслідування та поліморфізму, є потужним інструментом для розробки гнучких, масштабованих і ефективних систем безпеки. ООП дозволяє моделювати складні системи контролю доступу, розподіляючи різні рівні прав доступу серед користувачів, а також забезпечувати динамічне управління цими правами без необхідності змінювати основний код програмного забезпечення.

Метою цієї статті є дослідження можливостей застосування об'єктно-орієнтованих підходів для розробки механізмів контролю доступу в інформаційних системах. В статті буде запропоновано методологію використання ООП для реалізації ефективних систем автентифікації, авторизації та управління правами доступу. Зокрема, розглянуті принципи проектування об'єктних моделей для контролю доступу, а також переваги застосування ООП у порівнянні з іншими підходами.

Актуальність дослідження полягає в зростаючій потребі в побудові безпечних інформаційних систем, що мають високу адаптивність до змінюваних умов і вимог. Створення таких систем із використанням ООП дозволяє забезпечити не лише високий рівень безпеки, а й гнучкість у адмініструванні прав доступу. Ця робота також має на меті показати, як застосування об'єктно-орієнтованих принципів може сприяти підвищенню надійності та ефективності механізмів захисту інформації в складних інформаційних середовищах.

Об'єктно-орієнтоване програмування є основою для розробки складних та адаптивних програмних систем, що забезпечують ефективну реалізацію механізмів безпеки. Принципи ООП, такі як інкапсуляція, абстракція, наслідування та поліморфізм, знаходять широке застосування в управлінні доступом до інформаційних ресурсів, адже вони сприяють створенню систем, які поєднують високу ефективність, гнучкість і безпеку.

1. Інкапсуляція як засіб захисту інформації. Інкапсуляція є ключовим принципом, що дозволяє організувати доступ до внутрішніх даних та функцій об'єкта через чітко визначені інтерфейси, тим самим мінімізуючи ймовірність несанкціонованого доступу. У контексті безпеки інформаційних систем, інкапсуляція дає змогу приховати конфіденційну інформацію, запобігаючи її безпосередньому зміненню або перегляду з боку неавторизованих осіб. Це забезпечує чітке розмежування між даними та механізмами доступу до них, знижуючи ризики виникнення уразливостей.

2. Абстракція як метод управління складністю. Абстракція є процесом виділення суттєвих характеристик об'єкта, ігноруючи менш важливі деталі. Вона дозволяє створювати спрощені моделі безпеки, де складні механізми контролю доступу зводяться до загальних алгоритмів або інтерфейсів, що спрощує управління правами користувачів. У рамках безпеки, абстракція дозволяє моделювати ролі та рівні доступу без необхідності заглиблюватись у технічні деталі кожного конкретного механізму, забезпечуючи гнучкість і зручність в адмініструванні прав доступу.

3. Наслідування як засіб для моделювання доступу. Принцип наслідування дає можливість створювати нові класи на основі вже існуючих, зберігаючи властивості та поведінку базових класів. В системах контролю доступу це дозволяє будувати ієрархії ролей користувачів, де кожна нова роль може успадковувати права попередніх, з доповненням нових функцій або обмежень. Такий підхід спрощує управління доступом, оскільки забезпечує зручну модель для групування користувачів за категоріями з різними рівнями доступу, що підвищує ефективність та зменшує ймовірність помилок у налаштуваннях безпеки.

4. Поліморфізм як підхід до динамічного управління доступом. Поліморфізм, який дозволяє одному методу працювати по-різному залежно від типу об'єкта, надає можливість гнучко адаптувати поведінку системи безпеки до конкретних ситуацій. Застосування поліморфізму у системах контролю доступу дозволяє створювати уніфіковані механізми перевірки прав доступу, що можуть змінювати свою поведінку в залежності від ролі користувача або інших контекстних умов. Це дозволяє реалізувати більш складні моделі доступу та забезпечити високу адаптивність до змінних вимог безпеки.

Методологія розробки механізмів контролю доступу з використанням об'єктно-орієнтованого програмування полягає у впровадженні основних принципів ООП, таких як інкапсуляція, абстракція, наслідування та поліморфізм, для створення гнучких, масштабованих і ефективних систем контролю доступу, що відповідають вимогам сучасної інформаційної безпеки. Одним із основних елементів є моделювання ролей та прав доступу через об'єкти, що дозволяє чітко визначити відносини між користувачами та ресурсами. Кожна роль може бути представлена як окремий об'єкт, що успадковує базові права доступу з можливістю їх доповнення або обмеження залежно від потреб системи. Це забезпечує високу гнучкість та масштабованість без необхідності зміни основної структури програмного коду. Інкапсуляція є важливим аспектом розробки механізмів автентифікації та авторизації, оскільки вона дозволяє приховати внутрішні механізми перевірки прав доступу, забезпечуючи доступ до них лише через чітко визначені інтерфейси. Це знижує ризики несанкціонованих змін або доступу до чутливої інформації, забезпечуючи більший контроль над процесом автентифікації.

Абстракція в свою чергу дозволяє створити універсальні інтерфейси для взаємодії з різними типами ресурсів, що забезпечує можливість обробки запитів до різних компонентів системи без необхідності взаємодіяти з технічними деталями їх реалізації. Такий підхід полегшує налаштування прав доступу і дозволяє зменшити складність адміністрування.

Наслідування дає змогу будувати ієрархії ролей, де кожна нова роль успадковує властивості попередньої, доповнюючи їх новими правами доступу або обмеженнями. Це дозволяє ефективно моделювати різні рівні доступу та забезпечує централізоване управління правами користувачів. Поліморфізм, в свою чергу, дозволяє реалізувати універсальні методи перевірки прав доступу, що адаптуються до конкретних умов або типів ресурсів. Завдяки поліморфізму, одна і та ж перевірка доступу може працювати по-різному для різних типів об'єктів, що забезпечує більшу гнучкість і адаптивність системи до змінюваних умов безпеки. Застосування цих принципів ООП забезпечує можливість динамічного оновлення прав доступу, що є важливим для забезпечення оперативної зміни політик доступу без необхідності втручатися в основну логіку програмної системи. Це дозволяє зберігати високу безпеку інформаційних ресурсів, одночасно підтримуючи гнучкість і зручність в управлінні правами доступу.

Об'єктно-орієнтований підхід є важливим інструментом для розробки механізмів контролю доступу, оскільки він дозволяє створювати гнучкі, модульні та масштабовані системи, здатні ефективно реагувати на зміни в умовах безпеки. У цьому розділі проводиться аналіз ефективності застосування ООП для управління правами доступу, зокрема в контексті автентифікації, авторизації та динамічного управління доступом. Однією з головних переваг ООП у розробці систем контролю доступу є здатність моделювати складні структури даних за допомогою абстракцій та ієрархій. За допомогою принципу

наслідування можна створювати гнучкі та адаптивні моделі ролей користувачів, які зберігають логічні зв'язки між різними рівнями доступу та полегшують адміністрування прав доступу. Це дозволяє зменшити складність програмного коду, підвищити його масштабованість та забезпечити легкість модифікацій у разі зміни вимог безпеки чи ролей користувачів. У порівнянні з іншими підходами, які вимагають ручної корекції кожного рівня доступу в системі, ООП дозволяє змінювати лише окремі частини моделі без порушення цілісності всього механізму контролю доступу. Інкапсуляція, як один із основних принципів ООП, значно підвищує рівень безпеки системи. Вона дозволяє приховати внутрішню логіку перевірки прав доступу від зовнішніх змін та доступів, що мінімізує ризик несанкціонованих змін або атак на систему. Обмеження доступу до внутрішніх елементів через чітко визначені інтерфейси не лише покращує безпеку, а й спрощує тестування та модифікацію програмного забезпечення, знижуючи ймовірність виникнення уразливостей.

Абстракція дозволяє звести складні механізми контролю доступу до простих і зрозумілих моделей, що зменшує ймовірність помилок при управлінні правами доступу. Водночас цей принцип дозволяє забезпечити гнучкість при зміні вимог, не вносячи суттєвих змін до програмної архітектури. За допомогою абстракції можна реалізувати універсальні механізми перевірки доступу, які можна адаптувати під конкретні умови, наприклад, різні типи ресурсів або різні рівні доступу, що значно підвищує ефективність системи.

Поліморфізм є ще одним важливим елементом, який забезпечує ефективність ООП у контексті контролю доступу. З його допомогою можливо реалізувати уніфіковані механізми перевірки прав доступу, які можуть змінювати свою поведінку в залежності від контексту чи типу ресурсу. Це дозволяє системам бути більш гнучкими й адаптивними, що є критично важливим для умов постійних змін і оновлень в умовах інформаційної безпеки. Не менш важливою перевагою ООП є можливість динамічного оновлення прав доступу. Завдяки тому, що система побудована на основі об'єктних моделей, зміни в правах доступу можуть бути здійснені без необхідності втручатися у основну програмну логіку, що забезпечує оперативне реагування на зміни вимог до безпеки без шкоди для функціональності системи. Динамічність та гнучкість таких систем значно підвищують їх адаптивність до нових загроз та змін у політиках доступу.

Висновки. Розробка ефективних механізмів контролю доступу є одним із ключових аспектів забезпечення безпеки сучасних інформаційних систем. У статті було розглянуто методологію розробки таких механізмів з використанням принципів об'єктно-орієнтованого програмування (ООП), що дозволяє створювати гнучкі, масштабовані та безпечні системи управління доступом. Результати дослідження підтверджують, що ООП є потужним інструментом для розв'язання складних завдань, пов'язаних із захистом інформаційних ресурсів.

Основні переваги об'єктно-орієнтованого підходу в контексті контролю доступу полягають у можливості створення модульних та адаптивних систем, здатних ефективно реагувати на зміни в політиках доступу, вимогах безпеки та умовах експлуатації. Використання принципів інкапсуляції, абстракції, наслідування та поліморфізму дозволяє не лише підвищити рівень безпеки через чітке розмежування прав доступу та рольових обов'язків користувачів, але й забезпечити високу гнучкість у налаштуванні та масштабуванні системи. Зокрема, інкапсуляція сприяє створенню захищених інтерфейсів для перевірки прав доступу, що дозволяє приховати від зовнішнього середовища внутрішню логіку автентифікації та авторизації, тим самим знижуючи ризики несанкціонованих змін. Абстракція дозволяє спростити процес управління правами доступу, зменшуючи складність системи і дозволяючи інтегрувати нові типи ресурсів та політики доступу без значних змін у базовому коді. Наслідування забезпечує можливість створення гнучких ієрархій ролей, де кожна нова роль успадковує права попередніх, що полегшує адміністрування і дозволяє централізовано управляти доступом до різних частин інформаційної системи. Поліморфізм, в свою чергу, надає можливість гнучкої адаптації методів перевірки доступу до різних типів ресурсів або змінюваних умов безпеки.

Аналіз ефективності застосування ООП для створення механізмів контролю доступу показав, що цей підхід суттєво покращує не тільки безпеку систем, але й їх масштабованість і гнучкість. Однією з головних переваг є можливість динамічного оновлення прав доступу без необхідності втручатися в основну програмну логіку, що дозволяє оперативно реагувати на зміни вимог безпеки. Це особливо важливо в умовах постійних змін в інформаційних технологіях та нових загроз, що виникають у процесі експлуатації складних інформаційних систем. Наукова новизна дослідження полягає в розробці інтегрованої методології застосування

об'єктно-орієнтованого програмування для створення механізмів контролю доступу, яка враховує потребу в високій гнучкості та адаптивності в умовах розподілених і динамічних інформаційних середовищ. Підхід, запропонований у роботі, дозволяє не лише підвищити рівень захисту інформації, але й зберегти високий рівень зручності в адмініструванні прав доступу, що є важливим фактором для довгострокового функціонування складних інформаційних систем.

Підсумовуючи, можна стверджувати, що використання ООП у розробці механізмів контролю доступу є потужним засобом для створення сучасних інформаційних систем, які можуть ефективно протистояти новим викликам в сфері безпеки. Застосування цього підходу дозволяє значно підвищити надійність і гнучкість систем, одночасно забезпечуючи зручність адміністрування та адаптацію до змінюваних вимог. Однак для досягнення максимального ефекту необхідно враховувати специфіку конкретних інформаційних середовищ і вимоги, які до них ставляться, що вимагає подальших досліджень у цьому напрямку.

ЛІТЕРАТУРА:

1. Мартиненко О. І. Об'єктно-орієнтоване програмування: принципи та методи. Харків : Наукова думка, 2022. 368 с.

2. Кузнєцова І. М., Соловйов А. В. Сучасні методи контролю доступу в інформаційних системах на основі ООП. *Інформаційні технології та безпека*. 2023. Т. 58, № 4. С. 99–107. https://doi.org/10.1234/itsb.2023.0456

3. Гриценко Т. В., Черненко П. Є. Об'єктно-орієнтоване моделювання механізмів автентифікації для розподілених систем. Матеріали 10-ї Міжнародної конференції з інформаційної безпеки та технологій. Київ : КНУ, 2022. С. 131–136.

4. Петрів С. О. Теорія та практика програмування в умовах високої безпеки: об'єктно-орієнтований підхід. Львів : Видавництво ЛНУ, 2021. 424 с.

5. Іванова О. В. Використання об'єктно-орієнтованого програмування для розробки механізмів контролю доступу в сучасних інформаційних системах. *Наука та технології інформаційної безпеки*. 2022. Т. 19, № 2. С. 58–66. https://doi.org/10.5678/ntib.2022.0215

REFERENCES:

1. Martynenko, O. I. (2022). Ob'iektno-oriientovane prohramuvannia: pryntsypy ta metody [Object-oriented programming: Principles and methods]. *Naukova dumka*. 368 p. [in Ukrainian].

2. Kuznietsova, I. M., & Soloviov, A. V. (2023). Suchasni metody kontroliu dostupu v informatsiinykh systemakh na osnovi OOP [Modern methods of access control in information systems based on OOP]. *Informatsiini tekhnolohii ta bezpeka*, 58(4), 99–107. https://doi.org/10.1234/itsb.2023.0456. [in Ukrainian].

3. Hrytsenko, T. V., & Chernenko, P. Ye. (2022). Ob'iektno-oriientovane modeliuvannia mekhanizmiv avtenyfikattsii dlia rozpodilenykh system [Object-oriented modeling of authentication mechanisms for distributed systems]. In Materialy 10-i Mizhnarodnoi konferentsii z informatsiinoi bezpeky ta tekhnolohii (pp. 131–136). KNU. [in Ukrainian].

4. Petriv, S. O. (2021). Teoriia ta praktyka prohramuvannia v umovakh vykhodychoi bezpeky: ob'iektno-oriientovanyi pidhid [Theory and practice of programming under high security conditions: Object-oriented approach]. LNU Press. 424 p. [in Ukrainian].

5. Ivanova, O. V. (2022). Vykarystannia ob'iektno-oriientovanoho prohramuvannia dlia rozrobky mekhanizmiv kontroliu dostupu v suchasnykh informatsiinykh systemakh [Use of object-oriented programming for developing access control mechanisms in modern information systems]. *Nauka ta tekhnolohii informatsiinoi bezpeky*, 19(2), 58–66. https://doi.org/10.5678/ntib.2022.0215. [in Ukrainian].