КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кібербезпеки та комп'ютерної інженерії

(назва випускової кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

на тему:
Управління доступом під час реалізації компонентів

інформаційно-комунікаційних систем

Коротка Мілена Сергіївна

(прізвище, ім'я та по батькові здобувача повністю)

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кібербезпеки та комп'ютерної інженерії

(назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Делембовський М.М.

„____" _____20____року

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Управління доступом під час реалізації компонентів інформаційно-комунікаційних систем

(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності.Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач Коротка Мілена Сергіївна

(прізвище, ім'я та по батькові повністю)

125 «Кібербезпека»

(спеціальність)

Безпека інформаційних та комунікаційних систем

(освітня програма)

Група БІКС-22

Керівник Ізмайлова О.В.

(прізвище та ініціали)

доцент кафедри кібербезпеки та комп'ютерної інженерії, кандидат технічних наук

(вчене звання, науковий ступінь)

Рецензент_____

(прізвище та ініціали)

Ідентичність підтверджую

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій
Випускова кафедра: кібербезпеки та комп'ютерної інженерії
Ступінь вищої освіти: бакалавр
Спеціальність: 125 «Кібербезпека»
Освітня програма: Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри
Делембовський М.М.
„___" _____20___року

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Коротка Мілена Сергіївна
(прізвище, ім'я та по батькові здобувача)

1. Тема роботи «Управління доступом під час реалізації компонентів інформаційно-комунікаційних систем»

затверджена наказом ректора КНУБА № 576/52/-15/13.2/26 від «14» травня 2026 року
2. Керівник роботи
доцент кафедри кібербезпеки та комп'ютерної інженерії, кандидат технічних наук Ізмайлова Ольга Василівна
(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)

3. Термін подання здобувачем роботи до захисту 30 травня 2026
4. Зміст пояснювальної записки за розділами:
Р. 1. Теоретико-методологічні основи управління доступом в інформаційно-комунікаційних системах
Р. 2. Аналіз механізмів управління доступом у сучасних інформаційно-комунікаційних системах
Р. 3. Шляхи вдосконалення управління доступом під час реалізації компонентів інформаційно-комунікаційних систем

5. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1	03.05.2025
Розділ 2	15.05.2026
Розділ 3	25.05.2026
Остаточне оформлення роботи	01.06.2026
Направлення роботи для перевірки на плагіат	08.06.2026
Попередній захист роботи	08.06.2026
Направлення роботи на рецензування	08.06.2026

6. Дата видачі завдання 10.02.2026

Керівник Ізмайлова О.В. _____

Здобувач Коротка М.С. _____

Анотація

Коротка М. С. *Управління доступом в інформаційно-комунікаційних системах. Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 125 «Кібербезпека та захист інформації». — Київський Національний університет будівництва і архітектури — Київ, 2026. — 85 с., 3 розділи, список використаних джерел із 31 найменування.*

Кваліфікаційну роботу присвячено дослідженню теоретичних і практичних аспектів управління доступом в інформаційно-комунікаційних системах. Метою роботи є аналіз сучасних механізмів управління доступом та розробка рекомендацій щодо підвищення ефективності захисту інформаційних ресурсів шляхом удосконалення процесів автентифікації, авторизації та контролю дій користувачів.

У роботі розглянуто сутність і принципи управління доступом, здійснено класифікацію основних моделей контролю доступу, проаналізовано нормативно-правове забезпечення та стандарти інформаційної безпеки у сфері управління доступом. Проведено аналіз механізмів управління доступом на прикладі інформаційної системи «Нотаріус», досліджено сучасні технології та інструменти контролю доступу.

Запропоновано модель ефективного управління доступом, що передбачає впровадження багаторівневої системи автентифікації та авторизації, автоматизацію контролю доступу, моніторинг дій користувачів і використання сучасних засобів захисту інформації. Розроблені рекомендації спрямовані на підвищення рівня інформаційної безпеки, мінімізацію ризиків несанкціонованого доступу та забезпечення надійного функціонування інформаційно-комунікаційних систем.

Ключові слова: *управління доступом, інформаційно-комунікаційні системи, інформаційна безпека, автентифікація, авторизація, контроль доступу, моніторинг користувачів, захист інформації.*

Abstract

Korotka M. S. *Access Management in Information and Communication Systems. Qualification Thesis for the Bachelor's Degree in Specialty 125 "Cybersecurity and Information Protection". — Kyiv National University of Construction and Architecture — Kyiv, 2026. — 85 pages, 3 chapters, list of references containing 31 sources.*

The qualification thesis is devoted to the study of theoretical and practical aspects of access management in information and communication systems. The purpose of the study is to analyze modern access management mechanisms and develop recommendations for improving the protection of information resources through the enhancement of authentication, authorization and user activity control processes.

The paper examines the essence and principles of access management, classifies the main access control models, and analyzes the regulatory framework and information security standards in the field of access management. An analysis of access management mechanisms was conducted using the "Notarius" information system as a case study, and modern technologies and tools for access control were investigated.

An effective access management model is proposed, which includes the implementation of a multi-level authentication and authorization system, automation of access control, user activity monitoring, and the use of modern information protection tools. The developed recommendations are aimed at increasing the level of information security, minimizing the risks of unauthorized access, and ensuring the reliable operation of information and communication systems.

Keywords: *access management, information and communication systems, information security, authentication, authorization, access control, user monitoring, information protection.*

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	ПІБ *Коротка Мілена Сергіївна Korotka Milena Serhiivna*		
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	«Управління доступом під час реалізації компонентів інформаційно-комунікаційних систем» « Access Management in the Implementation of Information and Communication System Components»		
Освітній ступінь	Бакалавр		
Факультет	Автоматизації і інформаціних технологій		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 «Кібербезпека»		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	Ізмайлова Ольга Василівна		
Обсяг роботи:	*Поснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	88	3	18
Розділ 1	Теоретико-методологічні основи управління доступом в інформаційно-комунікаційних системах.		
Розділ 2	Аналіз механізмів управління доступом у сучасних інформаційно-комунікаційних системах на прикладі бази дослідження «Нотаріус».		
Розділ 3	Шляхи вдосконалення управління доступом під час реалізації компонентів інформаційно-комунікаційних систем.		
Висновки по роботі	Проведено аналіз теоретичних засад управління доступом в інформаційно-комунікаційних системах, розглянуто основні моделі контролю доступу, нормативно-правове забезпечення та міжнародні стандарти інформаційної безпеки. Досліджено особливості реалізації механізмів управління доступом на прикладі інформаційної системи «Нотаріус», проаналізовано сучасні технології автентифікації, авторизації та контролю доступу користувачів.		

	Розроблено модель ефективного управління доступом, що передбачає впровадження багаторівневої автентифікації та авторизації, автоматизацію контролю доступу, моніторинг дій користувачів і вдосконалення механізмів захисту інформації. Запропоновані рекомендації спрямовані на підвищення рівня інформаційної безпеки та мінімізацію ризиків несанкціонованого доступу.
Ключові слова:	управління доступом, інформаційно-комунікаційні системи, інформаційна безпека, автентифікація, авторизація, контроль доступу, багатофакторна автентифікація, моніторинг користувачів.
Keywords:	access management, information and communication systems, information security, authentication, authorization, access control, multi-factor authentication, user monitoring.

Здобувач Коротка М. С. _____/ _____

Керівник Ізмайлова О.В. _____/ _____

ЗМІСТ

ВСТУП

Актуальність дослідження. Стрімкий розвиток інформаційних технологій у XXI столітті суттєво трансформує всі сфери суспільного життя, зокрема інформаційно-комунікаційні системи, які стають основою функціонування сучасних організацій. В умовах цифровізації зростає роль захисту інформації та ефективного управління доступом до неї, оскільки саме ці процеси забезпечують конфіденційність, цілісність та доступність даних, що є ключовими характеристиками інформаційної безпеки.

Зміни в інформаційному середовищі зумовлюють необхідність удосконалення теоретико-методологічних підходів до управління доступом, що дозволяє своєчасно реагувати на загрози, мінімізувати ризики несанкціонованого доступу та забезпечувати належний рівень захисту інформаційних ресурсів. Особливого значення набуває впровадження сучасних моделей управління доступом, які враховують специфіку інформаційно-комунікаційних систем, їхню архітектуру та динамічний характер функціонування. Актуальність дослідження зумовлена тим, що зростання обсягів інформації, розширення використання хмарних технологій, мобільних пристроїв та розподілених систем супроводжується підвищенням рівня кіберзагроз, що, у свою чергу, вимагає формування ефективних механізмів управління доступом, які базуються на сучасних методах автентифікації, авторизації та контролю дій користувачів.

Розвиток інформаційно-комунікаційних технологій також сприяє ускладненню структури інформаційних систем, що потребує впровадження комплексних підходів до управління доступом із використанням інтелектуальних технологій, автоматизації процесів та аналізу поведінкових факторів користувачів. У сучасних умовах управління доступом стає не лише технічним, а й стратегічним інструментом забезпечення інформаційної безпеки організацій.

Велика увага серед науковців приділяється питанням інформаційної безпеки, зокрема управлінню доступом, проте існує потреба у подальшому розвитку теоретико-методологічних засад цієї проблематики. Серед дослідників, які зробили вагомий внесок у розвиток теорії інформаційної безпеки та управління доступом, слід відзначити таких учених, як Р. Лампсон, Д. Денінг, В. Столлінгс, а також вітчизняних науковців: В. Бурячок, О. Корченко, В. Хорошко, С. Гнатюк та інших. Незважаючи на значну кількість наукових праць, окремі аспекти управління доступом в інформаційно-комунікаційних системах залишаються недостатньо дослідженими, особливо в контексті сучасних викликів цифрової трансформації.

Метою роботи є дослідження теоретико-методологічних основ управління доступом в інформаційно-комунікаційних системах.

Для досягнення поставленої мети визначено такі **завдання**:

- розкрити сутність та значення управління доступом в інформаційно-комунікаційних системах;
- охарактеризувати основні моделі та механізми управління доступом;
- проаналізувати сучасні підходи до забезпечення інформаційної безпеки;
- дослідити нормативно-правове забезпечення управління доступом в Україні;
- визначити особливості застосування сучасних технологій у процесах управління доступом;
- сформувати теоретико-методичні рекомендації щодо удосконалення управління доступом в інформаційно-комунікаційних системах.

Об’єктом дослідження є процес управління доступом в інформаційно-комунікаційних системах.

Предметом дослідження є теоретико-методологічні засади, методи та підходи до управління доступом в інформаційно-комунікаційних системах.

Методи дослідження. У процесі дослідження використовувалися такі методи: діалектичний, системний і структурно-логічний; методи аналізу і синтезу; порівняльний та узагальнення; абстрагування; метод моделювання; а також графічний метод для наочного представлення результатів дослідження.

Теоретико-методологічною основою дослідження є положення сучасної теорії інформаційної безпеки, наукові праці вітчизняних і зарубіжних учених, міжнародні стандарти у сфері кібербезпеки, а також нормативно-правові акти України, що регламентують питання захисту інформації та управління доступом.

Наукова новизна полягає в уточненні теоретичних положень управління доступом в інформаційно-комунікаційних системах, а також у вдосконаленні підходів до організації контролю доступу з урахуванням сучасних кіберзагроз і розвитку інформаційних технологій.

Практичне значення отриманих результатів полягає у можливості їх використання для підвищення рівня інформаційної безпеки в організаціях, удосконалення політик управління доступом, а також у впровадженні ефективних механізмів контролю доступу в інформаційно-комунікаційних системах різного рівня складності.

Структура роботи. Робота складається із вступу, трьох розділів, висновків, списку використаних джерел. Загальний обсяг роботи становить 77 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ УПРАВЛІННЯ ДОСТУПОМ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

1.1. Поняття, сутність та основні принципи управління доступом

Комунікативні процеси виступають суттєвим елементом існування соціуму та діяльності організацій, зокрема в сучасних нестабільних умовах, коли значна частина персоналу працює у віддаленому форматі. Обсяг відомостей і потоки даних зростають унаслідок інтенсивної взаємодії та обміну інформацією. Комунікаційна діяльність реалізується завдяки функціонуванню засобів інформаційної взаємодії, відповідної інфраструктури й ресурсної бази, потреба у захисті яких посилюється через стрімку цифровізацію та переведення послуг у електронний формат.

Засоби контролю доступу є складовим елементом інформаційних систем і охоплюють, зокрема, такі технології, як багатофакторна автентифікація, що підвищує рівень безпеки, надаючи додаткові гарантії того, що доступ отримує саме авторизований користувач. Система управління доступом вимагає безперервного вдосконалення у зв’язку з новими викликами, серед яких особливе місце посідає перехід до хмарних технологій, адже інформація більше не зберігається виключно в локальних мережах, а розміщується у розподіленому хмарному середовищі.

Крім того, контроль доступу виконує важливу функцію запобігання внутрішнім загрозам, оскільки значна кількість інцидентів інформаційної безпеки спричиняється діями працівників організацій, як умисними, так і випадковими. Дієва система розмежування доступу дає змогу обмежувати повноваження співробітників у межах їхніх посадових обов’язків, унеможливлюючи доступ до даних, що не пов’язані з їхньою професійною діяльністю. Сукупність зазначених викликів зумовлює необхідність

подальшого вдосконалення механізмів управління доступом до інформаційних ресурсів та забезпечення їх надійного й безперервного захисту.

Система управління доступом не може функціонувати як незмінна структура, оскільки потребує постійного вдосконалення з урахуванням нових викликів і загроз інформаційній безпеці. У процесі її реалізації необхідно враховувати інтенсивне впровадження сучасних технологій, зокрема хмарних обчислень, Інтернету речей (IoT) та штучного інтелекту, які, з одного боку, розширюють можливості обробки даних, а з іншого – генерують додаткові ризики для їх захисту. У сучасних умовах інформація зберігається не лише в межах локальних мереж, але й у розподілених середовищах, що значно ускладнює забезпечення її безпеки. За таких обставин ефективне управління доступом забезпечує контрольованість захисту інформаційних ресурсів незалежно від їх фізичного розташування [17].

Функціонування системи управління доступом має ґрунтуватися на сукупності принципів, які забезпечують її результативність та здатність до адаптації. Одним із ключових є принцип мінімізації привілеїв, відповідно до якого кожному користувачеві або інформаційній системі надається виключно той рівень доступу, який є необхідним для виконання визначених функціональних обов’язків, що сприяє зниженню ризику помилкових дій або навмисних порушень. Не менш важливим є принцип розподілу обов’язків, який передбачає делегування критично важливих функцій між різними суб’єктами з метою запобігання надмірній концентрації повноважень в одних руках. Запобігання загрозам інформаційній безпеці підприємства виступає ключовим завданням фахівця з кібербезпеки, реалізація якого можлива за умови обґрунтованого вибору моделі управління доступом, що відповідає специфіці діяльності та особливостям функціонування організації. Формування ефективного механізму управління доступом до інформаційних ресурсів сприятиме підвищенню рівня захищеності інформаційного середовища підприємства [7].

У сучасній науковій літературі поняття управління доступом трактується як комплексна багаторівнева система організаційних, правових і технічних заходів, спрямованих на регулювання процесів надання, обмеження та контролю прав суб'єктів щодо використання інформаційних ресурсів. Такий підхід відображає інтегративну природу управління доступом, що поєднує як нормативно-правові механізми, так і інструменти інформаційно-комунікаційних технологій.

Згідно з положеннями Закону України «Про інформацію», інформація визнається об'єктом правових відносин і підлягає захисту від несанкціонованого доступу, знищення, модифікації чи поширення. У цьому процесі управління доступом виступає ключовим інструментом реалізації державної інформаційної політики. Як зазначає І. Арістова, ефективність функціонування державних інституцій значною мірою залежить від належної організації доступу до інформаційних ресурсів, що передбачає чітке нормативне регулювання, розмежування повноважень та встановлення відповідальності за порушення режиму доступу [6].

Розглядаючи управління доступом як елемент системи державного управління, В. Мороз підкреслює, що інформаційні ресурси є стратегічним об'єктом управління, а отже, доступ до них повинен здійснюватися на основі визначених принципів, з урахуванням їх цінності, значущості та рівня ризику. Управління доступом виконує функцію впорядкування інформаційних потоків і забезпечення їх раціонального використання [7].

З позицій кібернетичного підходу, сформульованого Н. Вінером, управління доступом інтерпретуємо як процес регулювання інформаційних потоків у системі через механізми зворотного зв'язку. Такий підхід дозволяє розглядати доступ не лише як статичну характеристику, а як динамічний процес, що адаптується до змін зовнішнього середовища, загроз і поведінки користувачів [10].

У працях сучасних дослідників у сфері інформаційної безпеки управління доступом визначається як базова складова систем захисту інформації. Зокрема, Д. Лубко та М. Мірошниченко розглядають його як систему процедур і технологій, що включає ідентифікацію, автентифікацію та авторизацію користувачів з метою забезпечення основних властивостей інформаційної безпеки – конфіденційності, цілісності та доступності даних. Аналогічної позиції дотримуються І. Карпович, О. Гладка та Я. Наконечна, які наголошують, що ефективне управління доступом є ключовим фактором мінімізації ризиків у інформаційних системах.

У контексті сучасних кіберзагроз значення управління доступом суттєво зростає. Так, Л. Байс та співавтори підкреслюють, що більшість атак на інформаційні системи пов’язані саме з порушенням механізмів контролю доступу, що свідчить про необхідність їх постійного вдосконалення. А. Ахмад та інші дослідники звертають увагу на те, що сучасні цілеспрямовані кіберзагрози (APT-атаки) передбачають використання складних стратегій обходу систем доступу, що вимагає впровадження адаптивних і інтелектуальних моделей контролю [9].

Особливої актуальності проблема управління доступом набуває в умовах розвитку новітніх технологій, таких як хмарні обчислення, мобільні мережі та Інтернет речей. Зокрема, Р. Нарендра, С. Тадапанені та М. Сабрі наголошують, що у хмарних середовищах контроль доступу ускладнюється через розподілений характер інфраструктури та відсутність фізичного контролю над даними. А. Свамі підкреслює, що впровадження мереж 5G і 6G створює нові виклики у сфері управління доступом, пов’язані з високою швидкістю передачі даних і великою кількістю підключених пристроїв [12].

У свою чергу, В. Дудикевич, Г. Микитин та інші дослідники акцентують увагу на особливостях управління доступом у кіберфізичних системах та системах Інтернету речей, де порушення доступу може призвести не лише до

інформаційних, а й до фізичних наслідків, що зумовлює необхідність інтеграції механізмів безпеки на всіх рівнях функціонування таких систем [14].

Важливим аспектом є також людський фактор у системі управління доступом. Т. Коробейнікова та А. Ямнич зазначають, що значна частина інцидентів інформаційної безпеки пов'язана з помилками або навмисними діями персоналу, що актуалізує необхідність впровадження політик контролю доступу, орієнтованих на поведінкові характеристики користувачів [18].

З правової точки зору, управління доступом тісно пов'язане із забезпеченням захисту персональних даних, що регламентується Законом України «Про захист персональних даних». Як підкреслює М. Василенко, ефективна реалізація механізмів доступу є необхідною умовою дотримання вимог законодавства у сфері кібербезпеки та захисту інформації [17].

Крім того, І. Сопілко у своїх дослідженнях наголошує на необхідності гармонізації підходів до управління доступом із міжнародними стандартами інформаційної безпеки, що забезпечує підвищення рівня захищеності інформаційно-комунікаційних систем у глобальному середовищі. Управління доступом є складною багатокомпонентною системою, яка забезпечує регулювання взаємодії суб'єктів із інформаційними ресурсами на основі встановлених правил, процедур і технологій. Воно виступає ключовим елементом системи інформаційної безпеки, що забезпечує захист інформації від несанкціонованого доступу та сприяє ефективному функціонуванню інформаційно-комунікаційних систем в умовах сучасних викликів [21].

Змістовне наповнення сутності управління доступом розкривається через сукупність взаємопов'язаних процесів, до яких належать ідентифікація, автентифікація, авторизація, а також облік і аудит дій суб'єктів. Ідентифікація передбачає встановлення унікальності суб'єкта доступу в інформаційній системі шляхом присвоєння відповідного ідентифікатора, що дозволяє відрізнити одного користувача або процес від іншого. Автентифікація, у свою чергу, забезпечує підтвердження достовірності заявленої ідентичності

суб’єкта за допомогою відповідних механізмів (паролів, біометричних даних, токенів тощо). Авторизація визначає обсяг і межі прав доступу суб’єкта до ресурсів системи відповідно до встановлених політик, ролей або атрибутів, тим самим забезпечуючи диференціацію доступу залежно від функціональних обов’язків і рівня довіри. Важливим елементом є також облік і аудит, що передбачають фіксацію дій користувачів і процесів у системі з метою подальшого контролю, аналізу та виявлення можливих порушень безпеки.

У наукових дослідженнях підкреслюється, що ефективне функціонування систем управління доступом є необхідною умовою протидії сучасним кіберзагрозам. Зокрема, у працях Л. Байса та співавторів зазначається, що значна частина атак на інформаційні системи пов’язана з компрометацією механізмів доступу, що обумовлює необхідність їх постійного вдосконалення та адаптації до нових умов функціонування [8].

У свою чергу, А. Ахмад та інші дослідники наголошують на стратегічному характері сучасних кіберзагроз, які реалізуються у вигляді складних багатоетапних атак, спрямованих на поступове отримання несанкціонованого доступу до критичних ресурсів. У зв’язку з цим системи управління доступом повинні враховувати не лише технічні параметри безпеки, а й поведінкові характеристики користувачів, що передбачає використання адаптивних і контекстно-орієнтованих механізмів контролю [17].

Особливого значення управління доступом набуває в умовах розвитку кіберфізичних систем та Інтернету речей, де інформаційні процеси тісно інтегровані з фізичними об’єктами. Як зазначають В. Дудикевич, Г. Микитин та інші науковці, порушення доступу в таких системах може спричинити не лише інформаційні втрати, але й призвести до матеріальних збитків або загроз для життя і здоров’я людей, що зумовлює необхідність комплексного підходу до організації управління доступом, що передбачає поєднання технічних, організаційних і правових механізмів захисту [14].

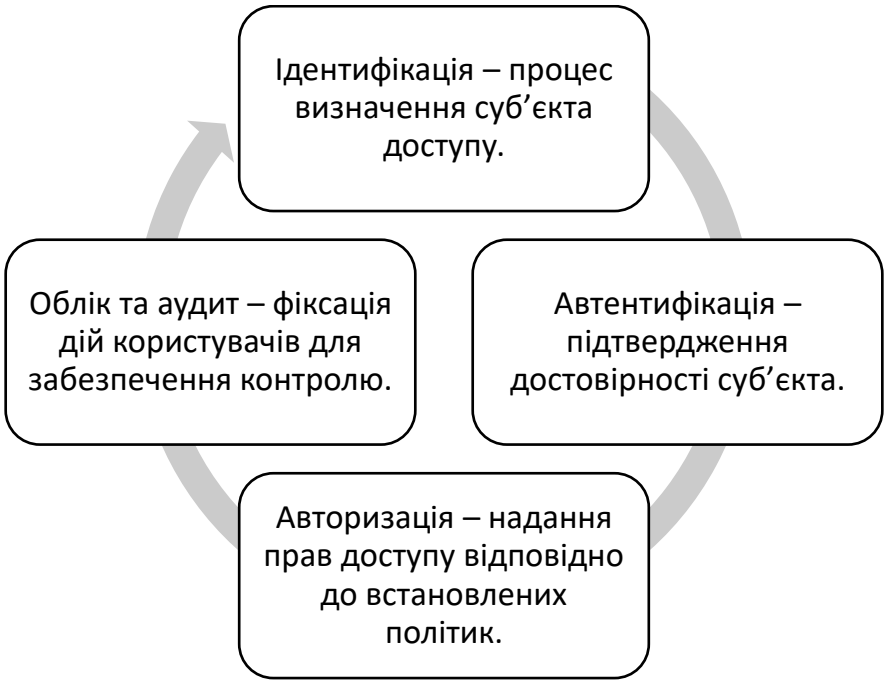

Рисунок 1.1. – Сутність управління доступом

Таким чином, сутність управління доступом полягає не лише у формальному розподілі прав доступу, але й у забезпеченні цілісної, динамічної та адаптивної системи контролю взаємодії суб’єктів і об’єктів інформаційного середовища. Така система має враховувати сучасні виклики інформаційної безпеки, забезпечувати баланс між доступністю інформації та її захистом, а також відповідати вимогам ефективного функціонування інформаційно-комунікаційних систем у цифровому суспільстві.

Управління доступом виступає невід’ємною складовою системи інформаційної безпеки та відіграє ключову роль у забезпеченні належного рівня захисту інформаційних ресурсів у сучасних інформаційно-комунікаційних системах. Його функціональне призначення полягає у регулюванні процесів доступу суб’єктів до об’єктів інформаційної інфраструктури шляхом встановлення чітко визначених правил, процедур і політик безпеки, що забезпечують контроль за використанням інформації відповідно до визначених повноважень.

У межах системи інформаційної безпеки управління доступом забезпечує реалізацію базових принципів захисту інформації, зокрема конфіденційності, цілісності та доступності даних. Передусім воно спрямоване на захист конфіденційної інформації від несанкціонованого ознайомлення, що досягається шляхом обмеження доступу лише для авторизованих користувачів відповідно до їхніх функціональних обов'язків. Водночас ефективні механізми управління доступом сприяють запобіганню витоку даних, що є особливо актуальним в умовах зростання обсягів обробки інформації та розширення каналів її передавання.

Управління доступом забезпечує мінімізацію ризиків несанкціонованого доступу, який може виникати як унаслідок зовнішніх кіберзагроз, так і через внутрішні фактори, пов'язані з діяльністю персоналу. У цьому контексті важливим є впровадження багаторівневих механізмів контролю доступу, що поєднують технічні засоби (автентифікація, авторизація), організаційні заходи (розподіл ролей, політики безпеки) та правові інструменти регулювання.

Важливою функцією управління доступом є також забезпечення відповідності діяльності інформаційних систем вимогам чинного законодавства у сфері захисту інформації та персональних даних. Дотримання нормативно-правових актів, зокрема законодавства України про інформацію та захист персональних даних, передбачає впровадження чітких процедур контролю доступу, що гарантують правомірність обробки та використання інформації.

Наукові дослідження підтверджують визначальну роль управління доступом у забезпеченні безпеки інформаційного середовища. Так, за висновками В. Кравчука, ефективно організована система управління доступом є основою безпечного функціонування мережі Інтернет, оскільки саме вона забезпечує контроль за взаємодією користувачів із мережевими ресурсами та запобігає реалізації більшості кіберзагроз. У свою чергу, Р. Городиський, О. Вавріченко та М. Стрельбицький акцентують увагу на

зростанні ризиків витоку інформації через сучасні канали зв’язку, зокрема супутникові та бездротові мережі, що значно ускладнює процеси контролю доступу та потребує впровадження більш досконалих механізмів захисту [16].

Основні принципи управління доступом становлять концептуальну основу побудови ефективної системи захисту інформації та визначають логіку організації взаємодії суб’єктів із інформаційними ресурсами. Їх дотримання забезпечує належний рівень інформаційної безпеки, сприяє мінімізації ризиків несанкціонованого доступу та підвищує стійкість інформаційно-комунікаційних систем до сучасних загроз.

Одним із базових є принцип мінімальних привілеїв, який передбачає надання користувачам виключно тих прав доступу, що є необхідними для виконання їхніх службових обов’язків. Реалізація цього принципу дозволяє суттєво обмежити потенційні можливості зловживання правами доступу, знизити рівень внутрішніх загроз і мінімізувати наслідки можливих інцидентів безпеки. Кожен суб’єкт отримує лише мінімально достатній набір повноважень, що унеможливлює надмірний доступ до критичних ресурсів.

Тісно пов’язаним із попереднім є принцип необхідності знання (need-to-know), відповідно до якого доступ до інформації надається виключно за умови наявності обґрунтованої службової потреби, що означає, що навіть за наявності формальних повноважень користувач може отримати доступ лише до тієї інформації, яка безпосередньо необхідна для виконання конкретних завдань. Такий підхід забезпечує додатковий рівень захисту конфіденційних даних і сприяє обмеженню їх поширення в межах організації.

Важливим принципом є також принцип розмежування доступу, який передбачає чіткий розподіл прав доступу між різними користувачами, групами або ролями. Його реалізація базується на ієрархії повноважень та функціональному розподілі обов’язків, що дозволяє уникнути концентрації критичних прав у межах одного суб’єкта, що підвищує рівень контролю за використанням інформаційних ресурсів і знижує ризик несанкціонованих дій.

Не менш значущим є принцип багаторівневого захисту, який передбачає застосування декількох взаємодоповнюючих механізмів контролю доступу. Такий підхід ґрунтується на ідеї створення декількох бар'єрів безпеки, кожен з яких ускладнює можливість несанкціонованого проникнення до системи. Практична реалізація цього принципу може включати поєднання різних методів автентифікації, зокрема використання паролів, одноразових кодів, біометричних даних та інших засобів ідентифікації. Багаторівневий підхід забезпечує підвищену надійність системи захисту навіть у разі компрометації одного з її елементів.

Особливе місце у системі принципів управління доступом займає принцип підзвітності, який передбачає обов'язкову фіксацію та контроль усіх дій суб'єктів доступу в інформаційній системі. Реалізація цього принципу забезпечує можливість проведення аудиту, виявлення порушень та встановлення відповідальності за неправомірні дії. У сучасних умовах, коли значна частина інцидентів інформаційної безпеки пов'язана з людським фактором, значення підзвітності суттєво зростає. Зокрема, як зазначають Т. Коробейнікова та А. Ямнич, персонал організації виступає одним із ключових джерел ризиків, що обумовлює необхідність постійного моніторингу його дій та впровадження ефективних механізмів контролю [18].

Отже, управління доступом є ключовим елементом забезпечення інформаційної безпеки, що поєднує технічні, організаційні та правові механізми. Його сутність полягає у регулюванні доступу до інформаційних ресурсів на основі визначених принципів та моделей. Сучасні виклики, пов'язані з розвитком цифрових технологій, вимагають постійного вдосконалення систем управління доступом, впровадження інноваційних підходів та адаптації до нових загроз. Ефективне управління доступом виступає необхідною умовою стабільного функціонування інформаційно-комунікаційних систем та гарантією захисту інформації в умовах цифрового суспільства.

1.2. Класифікація моделей управління доступом

Моделі управління доступом є фундаментальним інструментом забезпечення інформаційної безпеки в сучасних інформаційно-комунікаційних системах. Вони визначають сукупність формалізованих правил і механізмів, відповідно до яких регулюється доступ суб'єктів до об'єктів системи. Основною метою застосування таких моделей є гарантування конфіденційності, цілісності та доступності інформації, а також запобігання несанкціонованим діям користувачів або програмних процесів.

У загальному вигляді модель управління доступом можна розглядати як абстрактне представлення політики безпеки, що встановлює, хто (суб'єкт) і за яких умов має право виконувати певні дії над ресурсами системи (об'єктами). Суб'єктами, як правило, виступають користувачі, процеси або програми, тоді як об'єктами є файли, бази даних, пристрої чи інші інформаційні ресурси. Таким чином, модель доступу формує основу для реалізації механізмів авторизації та контролю доступу в операційних системах, мережах і прикладних середовищах.

До ключових властивостей моделей управління доступом належить, передусім, їх відповідність реальній системі, що моделюється, що означає, що модель повинна адекватно відображати структуру, взаємозв'язки та особливості функціонування інформаційної системи, враховуючи типи користувачів, характер ресурсів та політику безпеки організації. Недостатня адекватність моделі може призвести до появи вразливостей або, навпаки, до надмірного обмеження доступу, що негативно впливатиме на ефективність роботи системи [7].

Другою важливою властивістю є простота та абстрактність моделі. Вона повинна бути достатньо зрозумілою для реалізації та аналізу, не містити зайвої складності й водночас забезпечувати необхідний рівень формалізації.

Надмірно складні моделі важко впроваджувати, супроводжувати та перевіряти на наявність помилок, що знижує їх практичну цінність [9].

Серед основних підходів до організації управління доступом виділяють матричні та багаторівневі моделі. Матричні моделі базуються на представленні прав доступу у вигляді таблиці (матриці), де рядки відповідають суб'єктам, стовпці – об'єктам, а комірки містять набір дозволених операцій. Багаторівневі моделі, у свою чергу, орієнтовані на ієрархічну організацію доступу відповідно до рівнів секретності або довіри [10].

Однією з класичних матричних моделей є модель Лемпсона, яка стала основою для подальшого розвитку теорії контролю доступу. У цій моделі визначальним елементом є матриця доступу, що задає права взаємодії між суб'єктами та об'єктами. Суб'єкти розглядаються як активні елементи системи, які ініціюють запити на доступ, тоді як об'єкти є пасивними ресурсами, до яких здійснюється доступ. Водночас особливістю моделі є те, що суб'єкти можуть виступати також і об'єктами, що дозволяє описувати більш складні взаємодії в системі. Важливою перевагою моделі Лемпсона є можливість динамічного передавання прав доступу, що означає, що права можуть змінюватися в процесі функціонування системи, що забезпечує гнучкість управління доступом і дозволяє адаптувати систему до змінних умов. Однак така гнучкість водночас ускладнює контроль і аналіз безпеки [11].

Попри свою концептуальну простоту та універсальність, модель Лемпсона має низку недоліків. По-перше, матриця доступу в реальних системах є значною мірою розрідженою, оскільки більшість суб'єктів не взаємодіє з більшістю об'єктів, що призводить до неефективного використання пам'яті при явному зберіганні матриці. По-друге, модель не враховує потоки інформації між об'єктами, що унеможливлює аналіз витоку інформації або непрямих каналів передачі даних [4].

З метою подолання зазначених обмежень було запропоновано низку модифікацій матричної моделі, зокрема використання списків управління

доступом та списків повноважень суб’єктів. Списки управління доступом (Access Control Lists, ACL) передбачають зберігання для кожного об’єкта переліку суб’єктів, які мають до нього доступ, із зазначенням відповідних прав. Такий підхід дозволяє значно зменшити обсяг пам’яті, необхідний для зберігання інформації про доступ, оскільки фіксуються лише фактично існуючі зв’язки між суб’єктами та об’єктами. Крім того, ACL забезпечують зручний механізм отримання інформації про те, хто має доступ до конкретного ресурсу, що є важливим для адміністрування та аудиту безпеки. Водночас використання списків управління доступом має і певні недоліки. Зокрема, виникають труднощі при визначенні всіх об’єктів, до яких має доступ конкретний суб’єкт, оскільки ця інформація розподілена між багатьма списками. Також ускладнюється відстеження обмежень, залежностей і політик безпеки на рівні всієї системи [5].

Іншим підходом є використання списків повноважень суб’єктів, або так званих профілів доступу. У цьому випадку для кожного суб’єкта формується перелік об’єктів, до яких він має доступ, із зазначенням дозволених операцій. Такий підхід є зручним для аналізу діяльності конкретного користувача або процесу, а також широко застосовується в системах аудиту, зокрема в операційних системах сімейства Microsoft Windows NT. Перевагами списків повноважень є економія пам’яті та можливість швидкого отримання інформації про доступи конкретного суб’єкта. Однак, аналогічно до ACL, цей підхід має обмеження: зокрема, складність визначення всіх суб’єктів, які мають доступ до певного об’єкта, що може ускладнювати адміністрування системи [7].

Ще одним важливим напрямом розвитку моделей управління доступом є атрибутні підходи. Атрибутна схема базується на призначенні суб’єктам і об’єктам певних характеристик (атрибутів), які визначають їх властивості та рівень доступу. Рішення про надання доступу приймається на основі аналізу цих атрибутів відповідно до заданих правил політики безпеки.

Особливістю атрибутних моделей є те, що матриця доступу не зберігається у явному вигляді. Натомість вона формується динамічно під час кожного запиту на доступ, що дозволяє значно підвищити гнучкість системи. Такий підхід широко використовується в операційних системах сімейства UNIX, де доступ до файлів визначається на основі атрибутів користувачів і ресурсів (наприклад, прав читання, запису та виконання). Атрибутні моделі мають низку переваг, серед яких – масштабованість, гнучкість і можливість реалізації складних політик безпеки. Водночас вони потребують більш складних механізмів обробки запитів і можуть створювати додаткове навантаження на систему. Управління доступом у сучасних технологіях набуває особливого значення у зв'язку зі стрімким розвитком цифрового середовища, розширенням мережевої інфраструктури та зростанням кількості підключених пристроїв. Трансформація інформаційно-комунікаційних систем, зумовлена впровадженням хмарних обчислень, мобільних мереж нового покоління та Інтернету речей, обумовлює необхідність переосмислення традиційних підходів до контролю доступу та впровадження більш гнучких, адаптивних і контекстно-орієнтованих моделей безпеки [17].

У процесі хмарних обчислень управління доступом ускладнюється через розподілений характер інфраструктури, віртуалізацію ресурсів і відсутність чіткого фізичного контролю над даними. Як зазначають Р. Нарендра, С. Тадапанені та М. Сабрі, хмарні середовища характеризуються високим рівнем динамічності, що потребує впровадження посиленого контролю доступу з урахуванням багаторівневої архітектури та багатокористувацького режиму функціонування. У таких умовах особливої актуальності набувають моделі управління доступом, які враховують не лише роль користувача, але й контекст доступу, зокрема місцезнаходження, час, тип пристрою та інші параметри. Крім того, важливим є забезпечення ізоляції даних різних користувачів і організацій, що функціонують у межах єдиного хмарного

середовища, а також впровадження механізмів централізованого моніторингу та аудиту доступу [6].

Розвиток мобільних мереж, зокрема впровадження технологій п’ятого та шостого поколінь (5G і 6G), створює нові виклики у сфері управління доступом, що пов’язані з високою швидкістю передачі даних, низькою затримкою та значним збільшенням кількості підключених користувачів і пристроїв. А. Свамі підкреслює, що такі мережі забезпечують принципово новий рівень взаємодії між об’єктами цифрового середовища, що, у свою чергу, потребує вдосконалення механізмів автентифікації та авторизації. Зокрема, зростає потреба у впровадженні децентралізованих систем управління доступом, здатних функціонувати в умовах високої мобільності користувачів і постійної зміни параметрів мережевого середовища. Особливу увагу слід приділяти захисту каналів передачі даних і запобіганню несанкціонованому доступу в умовах відкритих і гетерогенних мереж [12].

У свою чергу, розвиток Інтернету речей (IoT) зумовлює появу нових підходів до управління доступом, що враховують специфіку взаємодії великої кількості пристроїв з обмеженими обчислювальними ресурсами. Як зазначають В. Дудикевич, Г. Микитин, Л. Бортнік та Т. Стосик, IoT-системи характеризуються високим рівнем масштабованості, динамічності та гетерогенності, що значно ускладнює реалізацію традиційних моделей доступу. У таких умовах виникає потреба у впровадженні адаптивних моделей управління доступом, які здатні автоматично змінювати політики безпеки залежно від контексту функціонування системи, типу пристрою та рівня потенційної загрози. Крім того, особливу увагу необхідно приділяти забезпеченню безпеки на рівні пристроїв, мережі та прикладних сервісів, що вимагає комплексного підходу до організації контролю доступу [11].

Отже, моделі управління доступом відіграють ключову роль у забезпеченні безпеки інформаційних систем. Вибір конкретної моделі залежить від вимог до безпеки, масштабів системи, характеру оброблюваної

інформації та інших факторів. Матричні моделі забезпечують простоту та наочність, але мають обмеження щодо ефективності та масштабованості. Атрибутні підходи, у свою чергу, надають більшу гнучкість і адаптивність, проте потребують складнішої реалізації. Комплексне поєднання різних моделей дозволяє створювати ефективні системи управління доступом, здатні забезпечити належний рівень захисту інформації в умовах сучасних технологічних викликів.

1.3. Нормативно-правове забезпечення та стандарти інформаційної безпеки у сфері управління доступом

Нормативно-правове забезпечення та стандарти інформаційної безпеки у сфері управління доступом становлять комплексну систему правових, організаційних і технічних засобів, спрямованих на захист інформаційних ресурсів держави, організацій і громадян від несанкціонованого доступу, розголошення, модифікації чи знищення. У сучасних умовах цифровізації суспільства особливого значення набуває формування цілісної та узгодженої системи правового регулювання інформаційної безпеки, яка забезпечує належний рівень захисту даних у різних сферах суспільного життя.

Основою правового регулювання інформаційної безпеки в Україні є Конституція України, яка закріплює базові права та свободи людини і громадянина, зокрема право на інформацію, її вільне збирання, зберігання, використання та поширення. Водночас Конституція встановлює обмеження щодо реалізації цих прав у випадках, передбачених законом, з метою захисту національної безпеки, громадського порядку, здоров’я населення та прав інших осіб. Таким чином, уже на конституційному рівні визначено баланс між свободою доступу до інформації та необхідністю її захисту.

Важливе місце в системі нормативно-правового забезпечення займає Закон України «Про інформацію» від 2 жовтня 1992 року. Цей закон визначає

основні принципи інформаційних відносин, види інформації, а також гарантії її захисту. Особливу увагу приділено інформації з обмеженим доступом, до якої належать конфіденційна, службова та таємна інформація. Закон регламентує умови доступу до інформації, а також встановлює відповідальність за порушення законодавства у цій сфері. У процесі управління доступом цей нормативний акт визначає правові підстави для обмеження доступу до інформаційних ресурсів і встановлює загальні вимоги до їх захисту.

Ключовим елементом сучасної системи національної безпеки є Закон України «Про національну безпеку України» від 2018 року, який визначає основи державної політики у сфері безпеки. Цей закон формує інституційну основу забезпечення національної безпеки, включаючи інформаційну складову. У ньому визначено, що інформаційна безпека є складовою частиною національної безпеки і передбачає захист інформаційного простору держави від зовнішніх і внутрішніх загроз. Закон також регламентує діяльність органів державної влади у сфері забезпечення безпеки, що включає контроль доступу до інформації [4].

Стратегічні напрями розвитку інформаційної безпеки визначаються у Стратегії національної безпеки України, затвердженій Указом Президента України № 392/2020. У цьому документі інформаційна безпека розглядається як один із ключових пріоритетів державної політики. Стратегія визначає основні загрози інформаційній безпеці, серед яких кіберзагрози, інформаційні атаки, дезінформація, а також встановлює завдання щодо вдосконалення системи захисту інформації, у тому числі механізмів управління доступом [6].

Окреме значення має Доктрина інформаційної безпеки України, затверджена Указом Президента України у 2017 році. Документ визначає концептуальні засади формування та реалізації державної політики у сфері інформаційної безпеки. У Доктрині акцентується увага на необхідності забезпечення надійного захисту інформаційних ресурсів, розвитку системи

кіберзахисту, а також удосконалення механізмів контролю доступу до інформації. Вона визначає інформаційну безпеку як стан захищеності національних інтересів у інформаційній сфері, що досягається шляхом впровадження комплексних заходів [7].

Суттєву роль у правовому регулюванні відіграє Закон України «Про основні засади забезпечення кібербезпеки України» від 2017 року. Цей закон визначає правові та організаційні основи забезпечення кібербезпеки, встановлює повноваження державних органів у цій сфері, а також визначає суб'єктів забезпечення кібербезпеки. У процесі управління доступом особливого значення набувають положення щодо ідентифікації, автентифікації та авторизації користувачів, а також контролю доступу до інформаційних систем. Закон спрямований на формування ефективної системи захисту інформаційних ресурсів від кіберзагроз.

Не менш важливим є Закон України «Про Національну програму інформатизації», який визначає загальнодержавні напрями розвитку інформаційного суспільства та впровадження інформаційних технологій. У редакції 2022 року цей закон враховує сучасні виклики цифрової трансформації та передбачає розвиток механізмів захисту інформації, у тому числі впровадження сучасних систем управління доступом. Програма інформатизації сприяє гармонізації національних стандартів із міжнародними вимогами у сфері інформаційної безпеки.

Окрему групу нормативно-правових актів становлять документи, що регулюють технічний захист інформації. В Україні діє система нормативних документів, які встановлюють вимоги до захисту інформації в інформаційно-комунікаційних системах, зокрема державні стандарти, методичні рекомендації та нормативні акти уповноважених органів. Такі документи визначають технічні та організаційні заходи, спрямовані на забезпечення конфіденційності, цілісності та доступності інформації.

У сфері управління доступом технічні стандарти відіграють ключову роль, оскільки вони регламентують механізми реалізації політик безпеки на рівні інформаційних систем. Зокрема, стандарти визначають вимоги до систем ідентифікації та автентифікації користувачів, засобів розмежування доступу, журналювання подій, а також захисту каналів передачі даних. Вони забезпечують уніфікований підхід до реалізації політик безпеки та сприяють сумісності різних інформаційних систем.

Важливу роль у формуванні стандартів інформаційної безпеки відіграють міжнародні нормативні документи, які імплементуються в національне законодавство України. Серед них можна виділити стандарти серії ISO/IEC, зокрема ISO/IEC 27001, який визначає вимоги до систем управління інформаційною безпекою, та ISO/IEC 27002, який містить практичні рекомендації щодо впровадження заходів безпеки. Такі стандарти широко використовуються для побудови ефективних систем управління доступом і забезпечення комплексного захисту інформації [12].

У контексті управління доступом особливе значення має поєднання правових і технічних механізмів. Правове регулювання визначає загальні принципи, права та обов’язки суб’єктів інформаційних відносин, тоді як технічні стандарти забезпечують практичну реалізацію цих принципів у вигляді конкретних механізмів і засобів захисту. Такий комплексний підхід дозволяє створити ефективну систему управління доступом, яка враховує як організаційні, так і технологічні аспекти [23].

Сучасна система нормативно-правового забезпечення інформаційної безпеки в Україні характеризується постійним розвитком і адаптацією до нових викликів. Зокрема, зростання кіберзагроз, розвиток хмарних технологій, мобільних мереж та інтернету речей потребують удосконалення механізмів контролю доступу та захисту інформації. У зв’язку з цим важливим є гармонізація національного законодавства з міжнародними стандартами, а також впровадження сучасних підходів до управління доступом, таких як

багатофакторна автентифікація, рольова модель доступу та атрибутні політики [22].

Таким чином, нормативно-правове забезпечення інформаційної безпеки у сфері управління доступом є складною багаторівневою системою, що включає конституційні норми, закони України, підзаконні акти, державні та міжнародні стандарти. Воно формує правові та організаційні основи для забезпечення надійного захисту інформаційних ресурсів і є невід'ємною складовою сучасної системи інформаційної безпеки держави. Ефективна реалізація цих положень є необхідною умовою для забезпечення стабільного функціонування інформаційного суспільства та захисту національних інтересів України.

Висновки до розділу 1

У результаті дослідження теоретико-методологічних основ управління доступом в інформаційно-комунікаційних системах встановлено, що управління доступом є одним із ключових елементів забезпечення інформаційної безпеки, спрямованим на захист інформаційних ресурсів від несанкціонованого використання, зміни або знищення. Визначено, що основною метою управління доступом є надання користувачам лише тих прав і повноважень, які необхідні для виконання їхніх функціональних обов'язків, із дотриманням принципів конфіденційності, цілісності та доступності інформації.

Досліджено сутність та основні принципи управління доступом, серед яких особливе значення мають принцип мінімальних привілеїв, принцип розмежування повноважень, необхідність автентифікації та авторизації користувачів, а також принцип безперервного контролю та моніторингу доступу. Встановлено, що ефективність системи захисту значною мірою залежить від правильного поєднання організаційних, програмних та технічних заходів контролю доступу.

Проаналізовано основні моделі управління доступом, зокрема дискреційну (DAC), мандатну (MAC), рольову (RBAC) та атрибутно-орієнтовану (ABAC). Визначено, що кожна з моделей має власні переваги та особливості застосування залежно від специфіки інформаційної системи. Встановлено, що найбільш поширеною у сучасних корпоративних та державних інформаційних системах є рольова модель управління доступом, яка забезпечує ефективне розмежування прав користувачів та спрощує адміністрування системи безпеки. Разом із тим сучасні тенденції розвитку інформаційних технологій зумовлюють зростання популярності атрибутно-орієнтованих та адаптивних моделей доступу, що враховують контекст взаємодії користувача із системою.

Досліджено нормативно-правове забезпечення та міжнародні стандарти у сфері управління доступом. Встановлено, що організація доступу до інформаційних ресурсів повинна здійснюватися відповідно до вимог законодавства України у сфері захисту інформації та персональних даних, а також міжнародних стандартів інформаційної безпеки, зокрема серії ISO/IEC 27000. Визначено, що впровадження вимог стандартів забезпечує системний підхід до управління ризиками інформаційної безпеки та підвищує рівень захищеності інформаційно-комунікаційних систем.

Таким чином, проведений теоретичний аналіз дозволив сформувати науково-методичне підґрунтя для подальшого дослідження особливостей реалізації механізмів управління доступом у практичній діяльності інформаційних систем. Отримані результати стали основою для аналізу існуючих підходів до організації доступу, оцінки їх ефективності та розроблення рекомендацій щодо вдосконалення систем захисту інформації в умовах сучасних кіберзагроз.

РОЗДІЛ 2. АНАЛІЗ МЕХАНІЗМІВ УПРАВЛІННЯ ДОСТУПОМ У СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

2.1. Загальна характеристика бази дослідження «Нотаріус»

У сучасних умовах розвитку інформаційно-комунікаційних систем (ІКС) особливого значення набуває забезпечення ефективного управління доступом до інформаційних ресурсів, що обумовлено зростанням обсягів оброблюваних даних, підвищенням вимог до їх конфіденційності, цілісності та доступності, а також активізацією кіберзагроз. Особливої актуальності зазначена проблема набуває у сфері надання юридичних та нотаріальних послуг, де обробляється значний масив персональних і правових даних.

Базою дослідження виступає інформаційна система, що акумулює відомості про суб’єктів нотаріальної діяльності, зокрема приватного нотаріуса Охріменко Наталію Сергіївну, зареєстровану у місті Прилуки Чернігівської області. Дана система містить персональні дані, контактну інформацію, відомості про реєстрацію нотаріуса, а також перелік наданих послуг. Джерелом отримання інформації є автоматизовані реєстри, зокрема Єдиний реєстр нотаріусів України, що інтегрується з аналітичними платформами типу YouControl.

Функціонування подібних систем передбачає необхідність реалізації комплексних механізмів управління доступом, оскільки інформація, що обробляється, має різні рівні чутливості. До таких даних належать персональні відомості, контактна інформація, професійні реквізити та інформація про діяльність нотаріуса. У зв’язку з цим система повинна забезпечувати диференційований доступ до ресурсів залежно від категорії користувачів.

Загалом у досліджуваній інформаційній системі виділяємо кілька основних категорій користувачів: *адміністратори системи, нотаріуси як суб’єкти професійної діяльності, а також зовнішні користувачі, які*

здійснюють пошук інформації. Кожна з цих категорій має різні права доступу, що реалізується за допомогою відповідних механізмів контролю. Для узагальнення характеристик користувачів та рівнів доступу доцільно представити їх у вигляді таблиці 2.4.

Таблиця 2.1. Категорії користувачів системи «Нотаріус» та рівні доступу

Категорія користувачів	**Рівень доступу**	**Основні можливості**
Адміністратор	Повний доступ	Управління системою, редагування даних, аудит
Нотаріус	Обмежений (професійний)	Оновлення власних даних, робота з реєстрами
Зовнішній користувач	Публічний доступ	Перегляд відкритої інформації

**Джерело: складено автором*

Аналіз наведеної таблиці свідчить, що в основі організації доступу лежить принцип розмежування прав відповідно до функціональних обов’язків користувачів. Такий підхід відповідає моделі рольового контролю доступу (RBAC), яка широко використовується у сучасних інформаційних системах. У процесі досліджуваної системи механізми управління доступом реалізуються через поєднання кількох технологічних підходів, серед яких ключовими є автентифікація, авторизація та аудит дій користувачів. Автентифікація забезпечує перевірку особи користувача перед наданням доступу до системи, що є критично важливим для запобігання несанкціонованому доступу. У більшості випадків застосовується парольна автентифікація, однак сучасні вимоги безпеки передбачають необхідність впровадження багатофакторної автентифікації.

Авторизація в системі реалізується шляхом визначення прав доступу до інформаційних ресурсів на основі ролі користувача. Наприклад, зовнішній користувач має доступ лише до загальнодоступної інформації, тоді як нотаріус може працювати з власними даними та здійснювати професійну діяльність у межах системи. Адміністратор, у свою чергу, має повний контроль над усіма компонентами системи.

Для більш детального аналізу механізмів управління доступом доцільно розглянути основні технології, що використовуються у сучасних ІКС (табл.2.2.)

Таблиця 2.2. Основні механізми управління доступом у сучасних ІКС

Механізм	**Сутність**	**Застосування у системі «Нотаріус»**
Автентифікація	Перевірка особи користувача	Вхід до системи нотаріусів та адміністраторів
Авторизація	Надання прав доступу	Розмежування доступу до даних
RBAC	Рольове управління доступом	Ролі: адміністратор, нотаріус, користувач
Фіксація	Фіксація дій користувачів	Контроль змін та доступу
Шифрування	Захист даних під час передачі та зберігання	Захист персональних даних

**Джерело: складено автором*

Як видно з таблиці, у системі застосовується комплексний підхід до забезпечення безпеки, що передбачає використання як організаційних, так і технічних заходів. Особливу увагу слід приділити фіксації, яка дозволяє відстежувати дії користувачів та забезпечує можливість проведення аудиту у разі виникнення інцидентів безпеки.

Важливим аспектом є також захист персональних даних, що обробляються в системі. Оскільки база містить конфіденційну інформацію, необхідно забезпечити її захист шляхом використання криптографічних методів, зокрема шифрування даних під час передачі (TLS) та зберігання, що дозволяє мінімізувати ризики витоку інформації та забезпечити відповідність вимогам законодавства у сфері захисту персональних даних.

Разом із тим, аналіз показує, що сучасні системи управління доступом повинні враховувати не лише статичні характеристики користувачів, але й контекст їхньої діяльності. У зв'язку з цим перспективним є впровадження атрибутної моделі доступу (ABAC), яка дозволяє враховувати додаткові параметри, такі як місцезнаходження користувача, час доступу або тип пристрою. Для узагальнення переваг і недоліків різних підходів до управління доступом доцільно подати порівняльну характеристику (табл.2.3).

Таблиця 2.3. Порівняння підходів до управління доступом

Підхід	Переваги	Недоліки
RBAC	Простота, ефективність	Обмежена гнучкість
ABAC	Гнучкість, адаптивність	Складність впровадження
Zero Trust	Високий рівень безпеки	Високі вимоги до інфраструктури

**Джерело: складено автором*

Узагальнюючи результати аналізу, слід зазначити, що система «Нотаріус» реалізує базові механізми управління доступом, які відповідають сучасним вимогам інформаційної безпеки. Водночас існує потенціал для подальшого вдосконалення, зокрема шляхом впровадження багатофакторної автентифікації, розширення можливостей фіксації та використання більш гнучких моделей доступу.

Таким чином, ефективне управління доступом у сучасних інформаційно-комунікаційних системах є комплексним завданням, що потребує поєднання різних технологій та підходів. Аналіз бази дослідження «Нотаріус» показав,

що навіть у відносно простих системах необхідно забезпечувати багаторівневий захист, що включає автентифікацію, авторизацію, аудит та захист даних. Подальший розвиток таких систем пов’язаний із впровадженням інтелектуальних технологій, автоматизацією процесів управління доступом та переходом до концепції Zero Trust, що дозволить підвищити рівень безпеки та ефективність функціонування інформаційних систем.

Поглиблений аналіз механізмів управління доступом у системі «Нотаріус» дозволяє розглянути їх не лише з позиції функціонального забезпечення, а й з точки зору ефективності, стійкості до загроз та відповідності сучасним стандартам інформаційної безпеки. Саме тому ми вважали доцільно оцінити систему за такими критеріями, як рівень захищеності, гнучкість управління доступом, масштабованість та здатність до адаптації в умовах змін інформаційного середовища.

Одним із ключових показників ефективності системи управління доступом є її здатність протидіяти несанкціонованому доступу. У досліджуваній системі базовий рівень захисту забезпечується через механізми автентифікації та авторизації, однак їх ефективність значною мірою залежить від політик безпеки, що застосовуються. Наприклад, використання лише парольної автентифікації створює потенційні ризики, пов’язані з підбором паролів, фішинговими атаками або витоком облікових даних. У зв’язку з цим доцільним є впровадження багатофакторної автентифікації, що дозволяє значно підвищити рівень захисту шляхом використання додаткових факторів перевірки.

Не менш важливим аспектом є гнучкість системи управління доступом, яка визначає її здатність адаптуватися до змін у структурі користувачів та умов доступу. У системі «Нотаріус» переважно реалізовано рольовий підхід (RBAC), який забезпечує базову зручність адміністрування, однак має обмеження щодо врахування контекстних факторів. У сучасних умовах доцільним є поступовий перехід до більш гнучких моделей, зокрема

атрибутного контролю доступу, що дозволяє враховувати додаткові параметри, такі як геолокація користувача, час доступу або тип використовуваного пристрою.

Окремої уваги потребує питання масштабованості системи, що є критично важливим у контексті розширення функціональності та збільшення кількості користувачів. Система «Нотаріус», як частина інтегрованого інформаційного середовища, повинна забезпечувати можливість обробки зростаючих обсягів даних без втрати продуктивності та безпеки. У цьому аспекті важливу роль відіграє використання централізованих механізмів управління доступом, а також інтеграція з іншими державними реєстрами та інформаційними системами.

Крім того, слід враховувати аспект аудиту та моніторингу доступу, який є невід'ємною складовою сучасних систем безпеки. Фіксація дій користувачів дозволяє не лише відстежувати поточну активність, але й здійснювати ретроспективний аналіз у разі виникнення інцидентів. Водночас ефективність цього механізму залежить від повноти та якості зібраних даних, а також від наявності інструментів їх аналізу. У сучасних умовах доцільним є використання систем аналітики, що базуються на технологіях машинного навчання, які дозволяють виявляти аномальні дії та потенційні загрози.

Для узагальнення оцінки ефективності механізмів управління доступом у системі «Нотаріус» доцільно представити результати аналізу у вигляді таблиці. Аналіз представлених у таблиці даних свідчить про те, що система загалом відповідає базовим вимогам безпеки, однак потребує вдосконалення у напрямі підвищення адаптивності та стійкості до сучасних кіберзагроз. Зокрема, одним із перспективних напрямів є впровадження концепції Zero Trust, яка передбачає постійну перевірку кожного запиту доступу незалежно від джерела. Також важливим напрямом розвитку є впровадження безпарольних методів автентифікації, які базуються на використанні

біометричних даних або криптографічних ключів, що дозволяє не лише підвищити рівень безпеки, але й покращити зручність користування системою.

Таблиця 2.4. **Оцінка ефективності механізмів управління доступом у системі «Нотаріус»**

Критерій	Поточний стан	Рівень оцінки	Рекомендації щодо вдосконалення
Автентифікація	Переважно парольна	Середній	Впровадження MFA
Авторизація	Рольова модель (RBAC)	Достатній	Інтеграція елементів ABAC
Фіксація даних	Наявне	Достатній	Розширення аналітики
Захист даних	Частково реалізований	Середній	Повне шифрування даних
Гнучкість	Обмежена	Середній	Контекстний доступ
Масштабованість	Задовільна	Достатній	Хмарні рішення

**Джерело: складено автором*

У процесі інтеграції з іншими інформаційними системами важливим є використання стандартизованих протоколів управління доступом, що забезпечують взаємодію між різними платформами, що особливо актуально для державних інформаційних систем, які повинні функціонувати у єдиному інформаційному просторі.

Таким чином, проведений розширений аналіз механізмів управління доступом у системі «Нотаріус» дозволяє зробити висновок, що, незважаючи на наявність базових механізмів захисту, існує необхідність їх подальшого вдосконалення відповідно до сучасних вимог інформаційної безпеки. Основними напрямами розвитку є підвищення рівня автентифікації, впровадження гнучких моделей доступу, розширення можливостей моніторингу та інтеграція інтелектуальних технологій аналізу даних, що

забезпечить підвищення ефективності функціонування системи в умовах зростання кіберзагроз.

2.2. Огляд сучасних технологій та інструментів управління доступом

У сучасних умовах стрімкої цифровізації суспільства та активного впровадження інформаційних технологій у всі сфери діяльності особливого значення набуває проблема забезпечення інформаційної безпеки. Одним із ключових її компонентів виступає управління доступом до інформаційних ресурсів, що спрямоване на регулювання взаємодії користувачів із системами, даними та сервісами. Зростання кількості кіберзагроз, поширення хмарних технологій, мобільних пристроїв та віддаленої роботи актуалізують необхідність розробки та впровадження сучасних підходів до контролю доступу, які забезпечують як захист даних, так і зручність користування інформаційними системами.

Управління доступом визначається як сукупність методів, технологій та політик, що забезпечують ідентифікацію, автентифікацію та авторизацію користувачів у межах інформаційної системи. В основі сучасних підходів лежить концепція управління ідентичностями та доступом (Identity and Access Management, IAM), яка передбачає комплексне управління цифровими ідентичностями користувачів, їхніми правами та рівнями доступу протягом усього життєвого циклу. Основною метою IAM є забезпечення того, щоб доступ до ресурсів отримували лише авторизовані суб’єкти відповідно до встановлених політик безпеки.

Ключовими складовими управління доступом є процеси ідентифікації, автентифікації та авторизації (див.табл.2.1). Ідентифікація передбачає визначення користувача у системі, зазвичай за допомогою унікального ідентифікатора, такого як логін або електронна адреса. Автентифікація є наступним етапом і полягає у підтвердженні особи користувача шляхом

перевірки певних факторів, до яких належать знання (пароль), володіння (токен, мобільний пристрій) або біометричні характеристики (відбиток пальця, розпізнавання обличчя). Особливого значення набуває багатофакторна автентифікація, яка передбачає використання двох або більше факторів одночасно, що суттєво підвищує рівень безпеки та ускладнює несанкціонований доступ до системи.

Після успішної автентифікації здійснюється авторизація, яка визначає рівень доступу користувача до ресурсів системи. Авторизація базується на політиках безпеки, що регламентують дозволені дії, доступні ресурси та обмеження, пов’язані з контекстом доступу, таким як місцезнаходження користувача, час доступу або тип пристрою. У сучасних інформаційних системах авторизація дедалі частіше реалізується з урахуванням контекстних факторів, що дозволяє забезпечити більш гнучкий і адаптивний контроль доступу.

Таблиця 2.5. Основні процеси управління доступом та їх характеристика

Процес	Сутність процесу	Основні методи реалізації
Ідентифікація	Визначення користувача в системі	Логін, ID, електронна пошта
Автентифікація	Підтвердження особи користувача	Паролі, OTP, біометрія, токени
Авторизація	Надання прав доступу до ресурсів	Політики доступу, ролі, атрибути

**Джерело: складено автором*

Суттєву роль у системах управління доступом відіграють моделі контролю доступу, які визначають принципи надання прав користувачам.

Однією з найбільш поширених моделей є рольова модель контролю доступу (Role-Based Access Control, RBAC), яка передбачає надання прав

доступу на основі ролей, що відповідають функціональним обов'язкам користувачів. Такий підхід спрощує адміністрування доступу та дозволяє ефективно управляти правами великої кількості користувачів. Водночас RBAC має обмежену гнучкість, що проявляється у складності врахування контекстних умов доступу.

З метою подолання обмежень RBAC було розроблено атрибутну модель контролю доступу (Attribute-Based Access Control, ABAC), яка базується на використанні набору атрибутів користувача, ресурсу та середовища. У цій моделі рішення про надання доступу приймається на основі аналізу сукупності параметрів, що дозволяє реалізувати більш гнучкі та динамічні політики безпеки. Незважаючи на високий рівень адаптивності, впровадження ABAC пов'язане зі значною складністю, що потребує ретельного проєктування та підтримки політик доступу.

Окрім зазначених моделей, у практиці застосовуються також дискреційна (DAC) та мандатна (MAC) моделі контролю доступу. Дискреційна модель передбачає можливість власника ресурсу самостійно визначати права доступу інших користувачів, тоді як мандатна модель базується на централізованому управлінні доступом відповідно до встановлених рівнів секретності. У сучасних інформаційних системах часто використовується комбінований підхід, що поєднує елементи різних моделей для досягнення оптимального балансу між безпекою та зручністю.

Розвиток інформаційних технологій сприяв появі нових підходів до організації доступу, серед яких особливе місце займає технологія єдиного входу (Single Sign-On, SSO). Вона дозволяє користувачеві проходити автентифікацію один раз і отримувати доступ до кількох взаємопов'язаних систем без необхідності повторного введення облікових даних. Це підвищує зручність користування системами та зменшує ризик використання слабких паролів, однак водночас потребує додаткових заходів захисту, оскільки

компрометація облікового запису може призвести до доступу до великої кількості ресурсів.

Таблиця 2.6. Порівняльна характеристика моделей управління доступом

Модель	Принцип роботи	Переваги	Недоліки
RBAC	Доступ на основі ролей	Простота, зручність адміністрування	Обмежена гнучкість
ABAC	Доступ на основі атрибутів	Гнучкість, адаптивність	Складність реалізації
DAC	Доступ визначається власником ресурсу	Гнучкість	Низький рівень контролю
MAC	Централізоване управління доступом	Високий рівень безпеки	Жорсткість, складність впровадження

**Джерело: складено автором*

Розвиток інформаційних технологій сприяв появі нових підходів до організації доступу, серед яких особливе місце займає технологія єдиного входу (Single Sign-On, SSO). Вона дозволяє користувачеві проходити автентифікацію один раз і отримувати доступ до кількох взаємопов’язаних систем без необхідності повторного введення облікових даних. Це підвищує зручність користування системами та зменшує ризик використання слабких паролів, однак водночас потребує додаткових заходів захисту, оскільки компрометація облікового запису може призвести до доступу до великої кількості ресурсів.

Важливим елементом сучасних систем управління доступом є управління привілейованими обліковими записами (Privileged Access Management, PAM), яке спрямоване на контроль доступу користувачів із розширеними правами. Привілейовані облікові записи мають високий рівень

ризику, оскільки їх компрометація може призвести до серйозних наслідків для інформаційної системи. Тому сучасні рішення PAM передбачають використання механізмів тимчасового доступу, моніторингу дій користувачів та запису сесій.

Однією з найважливіших тенденцій у розвитку систем управління доступом є впровадження концепції Zero Trust, яка базується на принципі повної відсутності довіри до будь-якого користувача чи пристрою незалежно від їхнього розташування у мережі. У рамках цієї концепції кожна спроба доступу до ресурсу підлягає перевірці, а рішення про надання доступу приймається на основі аналізу контекстних факторів. Такий підхід дозволяє значно підвищити рівень безпеки, особливо в умовах використання хмарних сервісів та віддаленого доступу.

Сучасні системи управління доступом активно інтегруються з різноманітними протоколами та стандартами, серед яких важливе місце займають OAuth 2.0, OpenID Connect та SAML. Ці технології забезпечують безпечну передачу даних автентифікації між різними системами та дозволяють реалізувати єдину систему доступу до розподілених ресурсів. Використання таких протоколів є особливо актуальним у середовищах, де застосовуються хмарні сервіси та мікросервісна архітектура.

Значну роль у розвитку систем управління доступом відіграє використання хмарних технологій. Хмарні IAM-рішення забезпечують централізоване управління доступом, високу масштабованість та гнучкість, що дозволяє організаціям швидко адаптуватися до змін у середовищі. Водночас використання хмарних сервісів ставить нові вимоги до безпеки, зокрема щодо захисту даних та контролю доступу у розподілених середовищах.

Важливим напрямом розвитку є також автоматизація процесів управління доступом, яка передбачає використання спеціалізованих інструментів для створення, зміни та видалення облікових записів, а також

управління правами користувачів. Автоматизація дозволяє зменшити вплив людського фактору, підвищити ефективність адміністрування та забезпечити відповідність політикам безпеки. Особливо актуальним є використання підходу Policy-as-Code, який дозволяє описувати політики доступу у вигляді програмного коду.

Разом із тим, впровадження сучасних систем управління доступом супроводжується низкою викликів, серед яких слід виділити складність інтеграції різних систем, необхідність забезпечення відповідності нормативним вимогам, а також дефіцит кваліфікованих фахівців у сфері кібербезпеки. Крім того, важливим залишається питання балансу між рівнем безпеки та зручністю користування системами, оскільки надмірно жорсткі обмеження можуть негативно впливати на продуктивність користувачів.

Таблиця 2.7. Сучасні технології та інструменти управління доступом

Технологія / інструмент	**Основне призначення**	**Переваги**
SSO	Єдиний вхід до кількох систем	Зручність, зменшення кількості паролів
MFA	Багатофакторна автентифікація	Високий рівень безпеки
PAM	Управління привілейованими обліковими записами	Контроль адміністраторів
Zero Trust	Безперервна перевірка доступу	Максимальний рівень захисту
IAM системи	Комплексне управління доступом	Централізація та автоматизація

**Джерело: складено автором*

Таким чином, сучасні технології та інструменти управління доступом являють собою складну багаторівневу систему, що поєднує різноманітні

підходи, моделі та технічні рішення. Ефективне управління доступом передбачає комплексне використання різних технологій, таких як багатофакторна автентифікація, рольові та атрибутні моделі доступу, концепція Zero Trust, а також автоматизація процесів та використання сучасних протоколів взаємодії. Подальший розвиток цієї сфери пов'язаний із впровадженням інтелектуальних систем аналізу, розширенням можливостей безпарольної автентифікації та поглибленням інтеграції з хмарними середовищами, що дозволить забезпечити високий рівень безпеки інформаційних ресурсів у умовах постійного зростання кіберзагроз.

2.3. Аналіз реалізації управління доступом на базі дослідження

Реалізація управління доступом у сучасних інформаційно-комунікаційних системах доцільно розглядати не лише через формально задекларовані механізми, а передусім через практичні сценарії взаємодії користувачів із системою та обробки даних. База дослідження «Нотаріус» дозволяє проаналізувати, яким чином відбувається фактичне забезпечення доступу до інформації, як формуються обмеження та які потенційні вразливості виникають у процесі експлуатації.

Однією з ключових особливостей реалізації доступу у досліджуваній системі є поділ інформаційного простору на публічний та обмежений сегменти. Публічний сегмент забезпечує відкритий доступ до загальної інформації про нотаріуса, включаючи контактні дані, місце здійснення діяльності та перелік послуг. Такий підхід відповідає принципам відкритості державних реєстрів та забезпечує доступ громадян до необхідної інформації без додаткової автентифікації. Водночас обмежений сегмент передбачає доступ до внутрішніх даних, що потребує проходження процедури входу до системи.

Фактична реалізація доступу базується на сценаріях взаємодії користувачів із системою. Кожен сценарій передбачає певну послідовність дій, що включає ініціацію запиту, обробку запиту системою та надання або відмову в доступі. Доцільно виділити типові сценарії доступу, які представимо у таблиці 2.8.

Таблиця 2.8. Сценарії реалізації доступу у системі «Нотаріус»

Сценарій доступу	Умови доступу	Результат доступу
Перегляд відкритої інформації	Відсутність автентифікації	Повний доступ до публічних даних
Вхід нотаріуса до системи	Введення облікових даних	Доступ до внутрішніх функцій
Оновлення даних	Авторизований доступ	Можливість редагування інформації
Адміністративні дії	Розширені права доступу	Повний контроль над системою

**Джерело: складено автором*

Аналіз сценаріїв доступу свідчить про наявність чітко структурованої логіки взаємодії, однак водночас виявляє певні обмеження. Зокрема, відсутність додаткових перевірок у публічному доступі створює ризики масового збору даних (data scraping), що є актуальною проблемою для відкритих реєстрів. У свою чергу, процес автентифікації не передбачає багаторівневої перевірки, що знижує стійкість системи до атак, пов’язаних із компрометацією облікових даних.

Особливу увагу слід приділити аналізу потоків доступу до даних, які визначають, як саме інформація передається між користувачем і системою. У досліджуваній системі ці потоки мають лінійний характер, що спрощує реалізацію, але водночас обмежує можливості гнучкого контролю. Відсутність

динамічної оцінки ризиків під час кожного запиту означає, що система не адаптується до змін у поведінці користувача.

Важливим також є аналіз поведінкових аспектів доступу. Сучасні системи безпеки дедалі частіше враховують поведінкові характеристики користувачів, що дозволяє виявляти аномальні дії. У системі «Нотаріус» така функціональність відсутня, що означає неможливість автоматичного виявлення підозрілої активності, наприклад, багаторазових спроб входу або доступу з незвичних локацій.

З метою оцінки рівня реалізації доступу доцільно розглянути її через призму потенційних загроз (табл.2.9)

Таблиця 2.9. Аналіз загроз, пов'язаних із реалізацією доступу

Тип загрози	**Джерело виникнення**	**Потенційні наслідки**
Компрометація облікових даних	Слабка автентифікація	Несанкціонований доступ
Масовий збір інформації	Відкритий доступ	Використання даних третіми особами
Внутрішні порушення	Надмірні права доступу	Зміна або видалення даних
Відсутність моніторингу	Недостатній аудит	Несвоєчасне виявлення загроз

**Джерело: складено автором*

Отримані результати свідчать про те, що основні ризики пов'язані не з відсутністю механізмів доступу як таких, а з особливостями їх реалізації. Зокрема, система функціонує за принципом статичного доступу, коли права користувача визначаються один раз і не змінюються залежно від контексту. У сучасних умовах це є обмеженням, оскільки не дозволяє враховувати динамічні фактори ризику.

Додатковим аспектом аналізу є оцінка зручності використання системи, що безпосередньо впливає на поведінку користувачів. Надмірно складні механізми доступу можуть призводити до зниження продуктивності, тоді як надто прості до зниження рівня безпеки. У досліджуваній системі спостерігається орієнтація на зручність користування, що є позитивним фактором, однак потребує додаткового підсилення безпекових механізмів.

У контексті інтеграції з іншими інформаційними системами важливим є забезпечення єдиної політики доступу. Відсутність централізованого управління може призводити до дублювання облікових записів та ускладнення контролю. У системі «Нотаріус» така інтеграція має обмежений характер, що знижує ефективність управління доступом у масштабах інформаційного середовища.

Для узагальнення особливостей реалізації доступу доцільно представити їх у вигляді таблиці.

Таблиця 2.10. Особливості реалізації управління доступом у системі

Характеристика	**Особливість реалізації**	**Оцінка ефективності**
Тип доступу	Комбінований (публічний/закритий)	Достатній
Гнучкість	Обмежена	Середня
Адаптивність	Відсутня	Низька
Захист від загроз	Частковий	Середній
Зручність використання	Висока	Високий

**Джерело: складено автором*

Таким чином, проведений аналіз реалізації управління доступом у системі «Нотаріус» дозволяє зробити висновок, що вона забезпечує базову функціональність доступу та відповідає вимогам відкритості інформації,

однак має низку обмежень, пов’язаних із відсутністю адаптивних механізмів, недостатнім рівнем захисту та обмеженою інтеграцією. Ключовою особливістю є орієнтація на статичні механізми контролю доступу, що не враховують сучасні тенденції розвитку кібербезпеки. У зв’язку з цим подальший розвиток системи повинен бути спрямований на впровадження адаптивних підходів, розширення можливостей моніторингу та підвищення рівня автентифікації, що дозволить забезпечити більш високий рівень захищеності інформаційних ресурсів.

Висновки до розділу 2

У результаті проведеного аналізу механізмів управління доступом у сучасних інформаційно-комунікаційних системах встановлено, що забезпечення контрольованого доступу до інформаційних ресурсів є одним із ключових чинників ефективного функціонування систем, особливо у сферах, пов’язаних із обробкою персональних та юридично значущих даних.

Здійснено загальну характеристику бази дослідження «Нотаріус», яка являє собою інформаційну систему, інтегровану з державними реєстрами та орієнтовану на надання відкритого доступу до частини інформації про суб’єктів нотаріальної діяльності. Встановлено, що система поєднує елементи публічного доступу та обмеженого використання, що обумовлює необхідність чіткого розмежування прав доступу та реалізації багаторівневих механізмів захисту.

Проаналізовано сучасні технології та інструменти управління доступом, що застосовуються в інформаційних системах. Визначено, що ефективне управління доступом базується на поєднанні кількох ключових компонентів, зокрема автентифікації, авторизації, управління ідентичностями, а також використанні сучасних технологій, таких як багатофакторна автентифікація, системи єдиного входу, управління привілейованим доступом та концепція

Zero Trust. Встановлено, що сучасні підходи до управління доступом характеризуються переходом від статичних до адаптивних моделей, які враховують контекст доступу та поведінкові характеристики користувачів.

Здійснено аналіз реалізації управління доступом на базі дослідження, що дозволило виявити особливості функціонування системи в реальних умовах. Зокрема, встановлено, що доступ до інформації реалізується за комбінованим принципом, який передбачає відкритий доступ до публічних даних та обмежений доступ до внутрішніх ресурсів. При цьому основний акцент зроблено на забезпеченні зручності користування системою, що є важливим для кінцевих користувачів, однак водночас призводить до певного зниження рівня безпеки.

У ході аналізу виявлено, що реалізація управління доступом у досліджуваній системі має низку обмежень, серед яких недостатній рівень захисту автентифікаційних механізмів, відсутність адаптивного контролю доступу, обмежені можливості моніторингу та аналізу дій користувачів, а також ризики, пов’язані з відкритістю частини інформаційних ресурсів. Встановлено, що система функціонує переважно на основі статичних підходів до управління доступом, що не повністю відповідає сучасним вимогам кібербезпеки. Разом із тим визначено, що існуюча реалізація забезпечує базовий рівень захисту та відповідає мінімальним вимогам до організації доступу в інформаційних системах даного типу. Водночас підвищення ефективності управління доступом можливе шляхом впровадження сучасних технологій, зокрема багатофакторної автентифікації, розширення механізмів журналювання, використання контекстного контролю доступу та інтеграції інтелектуальних систем аналізу поведінки користувачів.

Таким чином, результати проведеного дослідження свідчать про необхідність удосконалення існуючих механізмів управління доступом із урахуванням сучасних тенденцій розвитку інформаційної безпеки. Отримані висновки створюють підґрунтя для розробки практичних рекомендацій щодо

підвищення рівня захищеності інформаційно-комунікаційних систем, що буде розглянуто у наступному розділі роботи.

РОЗДІЛ 3. ШЛЯХИ ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ДОСТУПОМ ПІД ЧАС РЕАЛІЗАЦІЇ КОМПОНЕНТІВ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

3.1. Розробка моделі ефективного управління доступом на базі дослідження

У сучасних умовах цифровізації державного управління та правової сфери особливого значення набуває проблема забезпечення інформаційної безпеки та належного управління доступом до інформаційних ресурсів. Зростання обсягів електронних даних, активне використання автоматизованих реєстрів, а також інтеграція державних інформаційних систем із зовнішніми аналітичними платформами зумовлюють необхідність формування ефективних механізмів контролю доступу до конфіденційної інформації. Особливо актуальним це питання постає у сфері нотаріальної діяльності, оскільки нотаріус у процесі професійної діяльності здійснює обробку значних масивів персональних даних фізичних та юридичних осіб, відомостей про майнові права, спадкові справи, договори, довіреності, реєстраційні документи та іншу юридично значущу інформацію, несанкціонований доступ до якої може спричинити суттєві правові, фінансові та репутаційні наслідки.

Розробка моделі ефективного управління доступом до інформаційних ресурсів нотаріального кабінету є складовою забезпечення комплексної системи інформаційної безпеки. У сучасному інформаційному середовищі управління доступом розглядається як сукупність організаційних, технічних та програмних заходів, спрямованих на регулювання прав користувачів щодо використання інформаційних ресурсів відповідно до визначених повноважень та рівнів доступу. Основною метою таких систем є забезпечення конфіденційності, цілісності та доступності інформації, що відповідає базовим принципам інформаційної безпеки.

Базою дослідження виступає інформаційна система, що акумулює відомості про суб’єктів нотаріальної діяльності, зокрема приватного нотаріуса Охріменко Наталія Сергіївна, зареєстровану у місті Прилуки. Досліджувана система містить персональні дані, контактну інформацію, відомості про реєстрацію нотаріуса, перелік нотаріальних послуг, а також інформацію, що надходить із автоматизованих державних реєстрів. Джерелом отримання інформації є автоматизовані інформаційні системи, зокрема Єдиний реєстр нотаріусів України, які інтегруються з аналітичними платформами типу YouControl. Така інтеграція значно підвищує ефективність пошуку, аналізу та обробки даних, однак одночасно створює додаткові ризики несанкціонованого доступу, витоку інформації та порушення законодавства у сфері захисту персональних даних.

Особливість нотаріальної діяльності полягає у високому рівні відповідальності за збереження конфіденційності інформації. Нотаріус є суб’єктом, який відповідно до законодавства України зобов’язаний забезпечувати нотаріальну таємницю та нерозголошення відомостей, отриманих у процесі здійснення професійної діяльності. У зв’язку з цим ефективна модель управління доступом має враховувати не лише технічні аспекти захисту інформації, але й нормативно-правові вимоги, організаційні процедури та специфіку функціонування нотаріальних інформаційних систем.

У загальному вигляді така система включає серверне програмне забезпечення, базу даних, систему автентифікації користувачів, механізми реєстрації дій користувачів, засоби резервного копіювання та захисту інформації. Інформаційна система взаємодіє з державними реєстрами через захищені канали зв’язку, що забезпечує отримання актуальних відомостей про суб’єктів правовідносин. У межах системи функціонує декілька категорій користувачів: нотаріус, помічник нотаріуса, системний адміністратор, оператор бази даних, а також зовнішні суб’єкти інтеграції. Кожна категорія

користувачів має чітко визначений перелік повноважень, який відповідає їх функціональним обов’язкам.

Однією з ключових проблем у сфері управління доступом є необхідність забезпечення балансу між доступністю інформації та її захистом. Надмірне обмеження доступу ускладнює виконання професійних обов’язків працівників, тоді як недостатній рівень контролю створює загрозу витоку конфіденційних даних. Саме тому наша модель управління доступом базуються на принципі мінімально необхідних привілеїв, відповідно до якого кожен користувач отримує лише той рівень доступу, який є необхідним для виконання його функціональних завдань.

Доцільно розглянути основні моделі управління доступом, що застосовуються у сучасних інформаційних системах. Однією з найбільш поширених є дискреційна модель доступу, яка передбачає можливість власника інформаційного ресурсу самостійно визначати права доступу інших користувачів. Перевагою такої моделі є гнучкість налаштування доступу, однак її недоліком виступає підвищений ризик помилкового надання надмірних повноважень.

Іншою моделлю є мандатне управління доступом, яке базується на використанні рівнів секретності та жорстко регламентованих правил доступу. У межах даної моделі користувач не може самостійно змінювати права доступу, а всі рішення приймаються централізовано відповідно до політики безпеки. Мандатна модель забезпечує високий рівень захисту інформації, однак є складною у впровадженні та адмініструванні.

Для інформаційної системи нотаріального кабінету найбільш доцільним є застосування рольової моделі управління доступом. Рольовий підхід передбачає надання прав доступу не окремим користувачам, а певним ролям, які відповідають службовим функціям працівників. У межах такої системи визначені ролі нотаріуса, помічника нотаріуса, адміністратора системи, аудитора безпеки та інших учасників інформаційного процесу. Кожна роль

містить чітко визначений набір дозволених операцій, що значно спрощує адміністрування системи та підвищує рівень контролю над доступом до інформації.

Розробка ефективної моделі управління доступом для нотаріальної інформаційної системи повинна ґрунтуватися на комплексному підході. Першим етапом є ідентифікація інформаційних активів та визначення рівня їх критичності. До критично важливих активів належать персональні дані клієнтів, електронні копії документів, дані державних реєстрів, електронні цифрові підписи та службова документація. Для кожного типу інформації необхідно визначити рівень конфіденційності та категорію користувачів, які мають право доступу.

Наступним етапом є впровадження механізмів автентифікації та авторизації користувачів. Сучасні інформаційні системи використовують багатофакторну автентифікацію, що передбачає поєднання декількох способів підтвердження особи користувача: парольного захисту, електронного ключа, одноразового коду або біометричної ідентифікації. Використання багатофакторної автентифікації значно знижує ризик несанкціонованого доступу навіть у випадку компрометації одного із факторів автентифікації.

Особливу увагу в моделі управління доступом необхідно приділити журналюванню подій та моніторингу активності користувачів. Усі дії користувачів повинні автоматично фіксуватися у спеціальних журналах подій із зазначенням часу доступу, виконаних операцій та IP-адреси користувача. Це забезпечує можливість проведення аудиту безпеки, виявлення підозрілої активності та оперативного реагування на інциденти інформаційної безпеки. Крім того, журнали подій можуть виступати доказовою базою у випадку порушення законодавства або внутрішніх регламентів установи.

Компонентом ефективної системи управління доступом є резервне копіювання інформації та забезпечення безперервності функціонування системи. У разі технічних збоїв, кібератак або фізичного пошкодження

обладнання система повинна забезпечувати можливість швидкого відновлення даних без втрати критично важливої інформації. Для цього доцільним є використання автоматизованих систем резервного копіювання із збереженням копій у захищених середовищах з обмеженим доступом.

Окремого значення набуває проблема кіберзагроз у сфері нотаріальної діяльності. Сучасні інформаційні системи постійно піддаються ризику фішингових атак, шкідливого програмного забезпечення, несанкціонованого втручання та витоку персональних даних. У зв’язку з цим модель управління доступом повинна передбачати регулярне оновлення програмного забезпечення, використання антивірусного захисту, систем виявлення вторгнень та криптографічних методів захисту інформації.

Важливу роль у забезпеченні ефективності системи управління доступом відіграє людський фактор. Практика свідчить, що значна кількість інцидентів інформаційної безпеки пов’язана не з технічними недоліками системи, а з помилками користувачів, низьким рівнем цифрової грамотності або порушенням внутрішніх регламентів. Саме тому доцільним є проведення регулярного навчання працівників з питань інформаційної безпеки, правил роботи з конфіденційною інформацією та методів протидії соціальній інженерії.

Ми запропонувати концептуальну модель управління доступом для інформаційної системи нотаріального кабінету. Основу такої моделі становить багаторівнева система захисту, яка включає фізичний, мережевий, програмний та організаційний рівні безпеки. На фізичному рівні забезпечується контроль доступу до серверного обладнання та робочих станцій. На мережевому рівні використовуються міжмережеві екрани, VPN-з’єднання та системи шифрування даних. Програмний рівень передбачає реалізацію механізмів автентифікації, авторизації та журналювання подій. Організаційний рівень охоплює нормативні документи, політики безпеки та процедури реагування на інциденти.

Ефективність запропонованої моделі визначається можливістю забезпечення високого рівня захисту інформації при одночасному збереженні функціональності та зручності використання системи. Реалізація рольового підходу до управління доступом дозволяє мінімізувати ризик несанкціонованого використання даних, підвищити контроль за діяльністю користувачів та оптимізувати процес адміністрування системи. Інтеграція механізмів багатофакторної автентифікації, аудиту безпеки та криптографічного захисту створює додатковий рівень захисту від сучасних кіберзагроз.

Запропонована нами концептуальна модель управління доступом до інформаційної системи нотаріального кабінету являє собою багаторівневу систему захисту інформаційних ресурсів, що забезпечує комплексну реалізацію механізмів інформаційної безпеки, контролю доступу та моніторингу діяльності користувачів. Основною метою даної моделі є забезпечення конфіденційності, цілісності та доступності інформації, що обробляється в межах нотаріальної інформаційної системи, а також мінімізація ризиків несанкціонованого доступу, витоку даних та порушення функціонування системи.

Структура моделі базується на принципі багаторівневого захисту, відповідно до якого кожен рівень виконує окремі функції у загальній системі забезпечення інформаційної безпеки. До складу моделі входять організаційний, програмний, мережевий та фізичний рівні захисту, взаємодія яких формує єдине безпечне інформаційне середовище для функціонування нотаріального кабінету. Такий підхід забезпечує комплексний характер системи захисту та дозволяє мінімізувати потенційні вразливості на різних етапах обробки інформації.

Верхній рівень структури представлений користувачами інформаційної системи, які взаємодіють із її функціональними компонентами відповідно до визначених ролей та повноважень. До основних категорій користувачів

належать нотаріус, помічник нотаріуса, адміністратор системи, оператор бази даних та аудитор безпеки. Кожна категорія користувачів характеризується визначеним набором функціональних обов'язків, що обумовлює рівень доступу до інформаційних ресурсів системи. Нотаріус має повний доступ до функціональних можливостей системи та здійснює безпосередню роботу з юридично значущими документами. Помічник нотаріуса отримує доступ лише до окремих модулів та інформаційних ресурсів, необхідних для виконання допоміжних функцій. Адміністратор системи забезпечує технічне супроводження інформаційної системи та управління користувацькими обліковими записами. Оператор бази даних виконує операції з адміністрування та підтримки баз даних, тоді як аудитор безпеки здійснює контроль дотримання політик безпеки та аналіз журналів подій.

Важливим компонентом моделі є інтеграція інформаційної системи нотаріального кабінету із зовнішніми інформаційними ресурсами та державними реєстрами. До таких систем належать Єдиний реєстр нотаріусів України, державні реєстри, аналітичні платформи та інші автоматизовані інформаційні ресурси. Взаємодія із зовнішніми системами забезпечує отримання актуальної інформації, необхідної для здійснення нотаріальної діяльності, однак одночасно створює додаткові ризики інформаційної безпеки. Саме тому модель передбачає використання захищених каналів зв'язку, криптографічних засобів захисту інформації та механізмів контролю автентичності зовнішніх підключень.

Організаційний рівень моделі охоплює нормативно-правову та управлінську складову системи захисту інформації. До його структури входять нормативні документи, політики безпеки, внутрішні регламенти, процедури управління доступом та механізми реагування на інциденти інформаційної безпеки. Нормативні документи визначають правові засади функціонування системи та регламентують порядок обробки персональних даних відповідно до чинного законодавства України. Політики безпеки встановлюють правила

управління доступом, порядок використання інформаційних ресурсів, вимоги до автентифікації користувачів та процедури захисту конфіденційної інформації. Окреме значення мають процедури реагування на інциденти, які передбачають механізми виявлення, аналізу, локалізації та усунення наслідків порушень інформаційної безпеки.

Наступним елементом моделі є програмний рівень, який забезпечує реалізацію механізмів контролю доступу та управління інформаційними потоками. Центральне місце на цьому рівні займають системи автентифікації та авторизації користувачів. Автентифікація забезпечує перевірку особи користувача перед наданням доступу до системи та реалізується за допомогою багатофакторних механізмів підтвердження особи. До основних засобів автентифікації належать парольний захист, використання електронного цифрового підпису, одноразові коди підтвердження та біометричні методи ідентифікації. Поєднання декількох факторів автентифікації суттєво знижує ризик компрометації облікових записів та підвищує загальний рівень захищеності системи.

Після успішної автентифікації система реалізує механізми авторизації, які визначають рівень доступу користувача до інформаційних ресурсів. У запропонованій моделі використовується рольовий підхід до управління доступом, відповідно до якого права користувачів визначаються на основі їх функціональної ролі у системі. Такий підхід дозволяє централізовано управляти правами доступу, спрощує адміністрування системи та забезпечує дотримання принципу мінімально необхідних привілеїв. Відповідно до цього принципу кожен користувач отримує лише той обсяг повноважень, який необхідний для виконання його службових обов’язків.

Важливим компонентом програмного рівня є система журналювання подій та моніторингу активності користувачів. Усі дії користувачів автоматично фіксуються у журналах подій із зазначенням часу доступу, типу виконаної операції, IP-адреси та інших параметрів сеансу роботи. Це

забезпечує можливість проведення аудиту безпеки, аналізу підозрілої активності та оперативного реагування на потенційні загрози. Журнали подій також можуть використовуватися для проведення службових розслідувань у випадку порушення політик безпеки або несанкціонованого використання інформаційних ресурсів.

Мережевий рівень моделі спрямований на забезпечення безпеки передачі інформації між компонентами системи та зовнішніми інформаційними ресурсами. Одним із ключових елементів цього рівня є міжмережевий екран, який здійснює фільтрацію мережевого трафіку та блокує несанкціоновані спроби доступу до системи. Використання міжмережевих екранів дозволяє обмежити доступ до внутрішніх ресурсів системи лише для авторизованих користувачів та мінімізувати ризик зовнішніх кібератак.

Для забезпечення захищеного обміну інформацією модель передбачає використання VPN-з'єднань, які створюють зашифровані канали передачі даних між користувачами та серверною інфраструктурою. Використання VPN-технологій особливо важливе у випадках віддаленого доступу до інформаційної системи, оскільки дозволяє захистити інформацію від перехоплення під час передачі через відкриті мережі зв'язку. Додатковий рівень захисту забезпечується застосуванням криптографічних алгоритмів шифрування даних, які використовуються для захисту каналів зв'язку, баз даних та електронних документів.

У структурі мережевого рівня також передбачено використання систем виявлення та запобігання вторгненням. Такі системи здійснюють постійний аналіз мережевої активності, виявляють аномальні дії користувачів та автоматично реагують на потенційні загрози інформаційній безпеці. Реалізація подібних механізмів дозволяє своєчасно виявляти спроби несанкціонованого доступу, мережеві атаки та інші інциденти, що можуть вплинути на стабільність функціонування інформаційної системи.

Фізичний рівень моделі забезпечує захист матеріальної інфраструктури інформаційної системи нотаріального кабінету. До його складу входять засоби фізичного контролю доступу до приміщень, серверного обладнання та робочих станцій користувачів. Реалізація фізичного захисту передбачає використання систем відеоспостереження, електронних пропускних систем, охоронної сигналізації та обмеження доступу сторонніх осіб до критично важливих об’єктів інфраструктури.

Окрему роль у межах фізичного рівня відіграє серверне обладнання, яке забезпечує функціонування баз даних, обробку інформаційних запитів та зберігання електронних документів. Для забезпечення безперервності функціонування системи передбачено використання резервного копіювання даних та створення захищених сховищ інформації. Автоматизоване резервне копіювання дозволяє мінімізувати ризик втрати інформації у випадку технічних збоїв, кібератак або фізичного пошкодження обладнання.

Завершальним елементом концептуальної моделі виступають базові принципи управління доступом, які визначають загальну логіку функціонування системи захисту інформації. До основних принципів належать конфіденційність, цілісність, доступність, підзвітність, принцип мінімальних привілеїв та безперервне вдосконалення системи безпеки. Принцип конфіденційності передбачає обмеження доступу до інформації виключно для авторизованих користувачів. Принцип цілісності забезпечує захист даних від несанкціонованої зміни або знищення. Доступність гарантує безперервне функціонування інформаційної системи та можливість своєчасного отримання інформації користувачами. Підзвітність реалізується через механізми журналювання та аудиту дій користувачів. Принцип мінімальних привілеїв обмежує права доступу користувачів лише необхідними функціями, а принцип безперервного вдосконалення передбачає регулярне оновлення політик безпеки, моніторинг ризиків та адаптацію системи до нових кіберзагроз.посилання на рисунок,

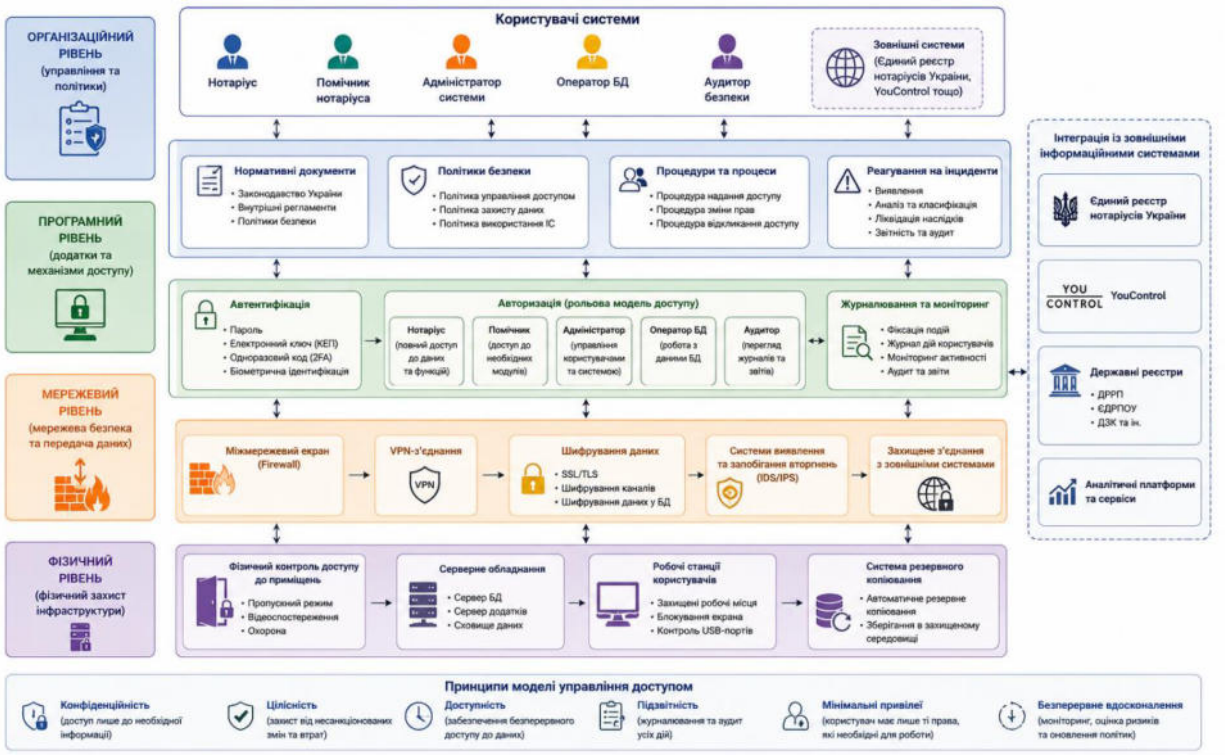

Рисунок 3.1. – Концептуальна модель управління доступом до інформаційної системи нотаріального кабінету

**Джерело: складено автором*

Таким чином, запропонована концептуальна модель управління доступом до інформаційної системи нотаріального кабінету є комплексною багаторівневою системою забезпечення інформаційної безпеки, яка поєднує організаційні, програмні, мережеві та фізичні механізми захисту інформації. Її впровадження дозволяє забезпечити ефективний контроль доступу до інформаційних ресурсів, підвищити рівень захисту персональних даних та мінімізувати ризики інформаційних загроз у процесі здійснення нотаріальної діяльності.

3.2. Впровадження багаторівневої системи автентифікації та авторизації

Важливим напрямом забезпечення інформаційної безпеки є впровадження ефективних механізмів автентифікації та авторизації користувачів, які дозволяють контролювати доступ до інформаційних систем відповідно до визначених повноважень. Інформаційні системи нотаріальних кабінетів містять значні обсяги персональних даних, юридично значущої документації, електронних копій договорів, спадкових справ, довіреностей та інших конфіденційних відомостей, що потребують високого рівня захисту.

Багаторівнева система автентифікації та авторизації являє собою комплекс організаційних, програмних та технічних засобів, спрямованих на перевірку особи користувача, визначення рівня його доступу до інформаційних ресурсів та забезпечення контролю за виконанням операцій у межах інформаційної системи. Основною метою впровадження такої системи є забезпечення конфіденційності, цілісності та доступності інформації, а також мінімізація ризиків несанкціонованого доступу, втрати або модифікації даних.

Процес автентифікації передбачає підтвердження особи користувача перед наданням доступу до системи. Авторизація, у свою чергу, визначає перелік дозволених дій користувача після успішного проходження процедури автентифікації. У сучасних інформаційних системах ці процеси функціонують у тісному взаємозв’язку та утворюють основу системи управління доступом.

У межах інформаційної системи нотаріального кабінету впровадження багаторівневої системи автентифікації та авторизації є необхідною умовою забезпечення належного рівня інформаційної безпеки. Нотаріальна діяльність безпосередньо пов’язана з обробкою персональних даних фізичних та юридичних осіб, що обумовлює необхідність дотримання вимог законодавства України у сфері захисту інформації та персональних даних. Саме тому система

управління доступом повинна враховувати як технічні аспекти захисту інформації, так і специфіку організації нотаріальної діяльності.

Одним із ключових елементів багаторівневої системи захисту є механізм багатофакторної автентифікації. На відміну від традиційної однофакторної автентифікації, яка базується виключно на використанні логіна та пароля, багатофакторний підхід передбачає використання декількох незалежних факторів підтвердження особи користувача. Такий підхід суттєво підвищує рівень захищеності інформаційної системи та мінімізує ризик компрометації облікових записів.

У структурі багатофакторної автентифікації виділяють три основні категорії факторів підтвердження особи: фактор знання, фактор володіння та фактор біометричної ідентифікації.

Таблиця 3.1. Основні фактори багатофакторної автентифікації

Фактор	Характеристика	Приклади
Фактор знання	Інформація, яку знає користувач	Пароль, PIN-код
Фактор володіння	Об’єкт, яким володіє користувач	Токен, смартфон, електронний ключ
Біометричний фактор	Унікальні фізіологічні характеристики	Відбиток пальця, розпізнавання обличчя

**Джерело: складено автором*

Використання декількох факторів автентифікації забезпечує суттєве зниження ризику несанкціонованого доступу навіть у випадку компрометації одного з елементів захисту. Для інформаційної системи нотаріального кабінету найбільш доцільним є поєднання парольного захисту, електронного цифрового підпису та одноразових кодів підтвердження.

Парольний захист є базовим елементом системи автентифікації та використовується для первинної ідентифікації користувача. Ефективність парольного захисту значною мірою залежить від складності паролів, регулярності їх оновлення та дотримання правил безпечного зберігання

облікових даних. Для підвищення рівня безпеки система повинна підтримувати механізми автоматичного блокування облікових записів у випадку багаторазового введення неправильного пароля, а також здійснювати контроль складності паролів відповідно до встановлених політик безпеки.

Важливим компонентом системи автентифікації у нотаріальній діяльності є використання електронного цифрового підпису. Електронний підпис забезпечує не лише ідентифікацію користувача, але й підтвердження юридичної значущості електронних документів. Використання кваліфікованого електронного підпису дозволяє гарантувати автентичність документів, захистити їх від несанкціонованого редагування та забезпечити контроль цілісності інформації.

Одноразові коди підтвердження виступають додатковим рівнем захисту та використовуються для підтвердження особи користувача під час входу до системи або виконання критично важливих операцій. Генерація таких кодів може здійснюватися за допомогою мобільних додатків, SMS-повідомлень або апаратних токенів. Використання одноразових кодів дозволяє мінімізувати ризик несанкціонованого доступу навіть у випадку викрадення пароля користувача.

Після проходження процедури автентифікації система переходить до етапу авторизації користувача. Авторизація визначає перелік дозволених дій та рівень доступу користувача до інформаційних ресурсів системи. У сучасних інформаційних системах найбільш поширеним є рольовий підхід до авторизації, відповідно до якого права доступу визначаються на основі функціональної ролі користувача.

У межах інформаційної системи нотаріального кабінету ми визначаємо декілька основних ролей користувачів.

Таблиця 3.2. Розподіл ролей користувачів у системі

Роль користувача	Основні функції	Рівень доступу
Нотаріус	Робота з документами, реєстрами, підписання документів	Повний доступ
Помічник нотаріуса	Підготовка документів, обробка заяв	Обмежений доступ
Адміністратор системи	Технічне обслуговування системи	Адміністративний доступ
Аудитор безпеки	Контроль журналів подій, аудит безпеки	Доступ до звітів

**Джерело: складено автором*

Рольова модель авторизації забезпечує централізоване управління доступом та дозволяє реалізувати принцип мінімально необхідних привілеїв. Відповідно до цього принципу користувач отримує лише той обсяг повноважень, який необхідний для виконання його функціональних обов’язків. Такий підхід дозволяє мінімізувати ризик несанкціонованого використання інформаційних ресурсів та підвищити рівень контролю за діяльністю користувачів. Усі дії користувачів у системі повинні автоматично фіксуватися у спеціальних журналах подій із зазначенням часу входу до системи, виконаних операцій, IP-адреси користувача та інших параметрів сеансу. Журналювання забезпечує можливість проведення аудиту безпеки, аналізу інцидентів та контролю дотримання політик безпеки. У процесі передавання даних між користувачами та серверною інфраструктурою повинні використовуватися захищені протоколи передачі інформації, зокрема SSL/TLS. Використання криптографічних алгоритмів шифрування дозволяє забезпечити конфіденційність інформації та захистити її від перехоплення під час передачі через мережу. Для підвищення рівня захищеності інформаційної системи також доцільним є використання механізмів адаптивної автентифікації. Суть такого підходу полягає у динамічному аналізі поведінки користувача та

автоматичному підвищенні рівня перевірки у випадку виявлення підозрілої активності. Наприклад, система може вимагати додаткове підтвердження особи у випадку входу з нового пристрою, зміни географічного розташування користувача або спроби виконання нетипових операцій.

Важливим аспектом впровадження багаторівневої системи автентифікації та авторизації є забезпечення безперервності функціонування інформаційної системи. Для цього необхідно використовувати механізми резервного копіювання облікових даних, дублювання серверної інфраструктури та системи аварійного відновлення доступу. У випадку технічних збоїв або кібератак система повинна забезпечувати можливість швидкого відновлення функціонування без втрати критично важливої інформації.

Особливого значення у процесі впровадження системи автентифікації та авторизації набуває людський фактор. Практика свідчить, що значна кількість інцидентів інформаційної безпеки пов’язана з порушенням користувачами правил роботи з інформаційними системами. Саме тому важливим напрямом забезпечення інформаційної безпеки є проведення регулярного навчання працівників щодо правил використання електронних ключів, створення складних паролів, виявлення фішингових повідомлень та дотримання внутрішніх політик безпеки. У процесі впровадження багаторівневої системи автентифікації та авторизації необхідно враховувати вимоги нормативно-правових актів у сфері захисту інформації та персональних даних. Система повинна відповідати принципам законності, пропорційності, конфіденційності та підзвітності. Особливу увагу слід приділяти захисту персональних даних клієнтів нотаріального кабінету, оскільки їх несанкціоноване розголошення може спричинити правові та репутаційні наслідки.

З метою оцінки ефективності впровадженої системи доцільним є проведення регулярного аудиту інформаційної безпеки. Аудит дозволяє

виявити потенційні вразливості, оцінити ефективність механізмів захисту та визначити напрями подальшого вдосконалення системи.

Таблиця 3.3. Основні переваги багаторівневої системи автентифікації та авторизації

Перевага	Характеристика
Підвищення рівня безпеки	Мінімізація ризику несанкціонованого доступу
Контроль дій користувачів	Журналювання та аудит подій
Захист персональних даних	Забезпечення конфіденційності інформації
Гнучке управління доступом	Розподіл прав відповідно до ролей
Відповідність законодавству	Дотримання вимог інформаційної безпеки

**Джерело: складено автором*

Таким чином, впровадження багаторівневої системи автентифікації та авторизації є одним із ключових напрямів забезпечення інформаційної безпеки інформаційної системи нотаріального кабінету. Реалізація багатофакторної автентифікації, рольового підходу до авторизації, механізмів журналювання подій та криптографічного захисту інформації дозволяє забезпечити ефективний контроль доступу до інформаційних ресурсів та мінімізувати ризики інформаційних загроз. Комплексний підхід до організації системи управління доступом сприяє підвищенню рівня захищеності персональних даних, забезпеченню стабільності функціонування інформаційної системи та дотриманню вимог законодавства у сфері інформаційної безпеки.

3.3. Автоматизація контролю доступу та моніторингу дій користувачів

Для інформаційних систем нотаріальної діяльності дане питання має критично важливе значення, оскільки нотаріальні інформаційні ресурси

містять значні обсяги конфіденційної інформації, персональних даних фізичних та юридичних осіб, електронних копій документів, відомостей про майнові права, спадкові справи та інші юридично значущі дані. У зв’язку з цим автоматизація процесів контролю доступу та моніторингу діяльності користувачів виступає одним із ключових напрямів забезпечення інформаційної безпеки інформаційної системи нотаріального кабінету. Впровадження автоматизованої системи контролю доступу та моніторингу дій користувачів є необхідною умовою забезпечення стабільного та безпечного функціонування інформаційної системи нотаріального кабінету.

Автоматизація контролю доступу являє собою сукупність програмних, технічних та організаційних механізмів, спрямованих на автоматичне регулювання доступу користувачів до інформаційних ресурсів відповідно до визначених політик безпеки та рівнів повноважень. Основною метою такої системи є забезпечення конфіденційності інформації, захист від несанкціонованого доступу та контроль за виконанням користувачами дозволених операцій у межах інформаційної системи.

У межах інформаційної системи нотаріального кабінету автоматизація контролю доступу базується на рольовій моделі управління доступом. Дана модель передбачає розподіл користувачів на окремі категорії відповідно до їх функціональних обов’язків та визначення переліку дозволених дій для кожної ролі. Використання рольового підходу дозволяє централізовано управляти правами доступу та мінімізувати ризик надання користувачам надмірних повноважень.

Таблиця 3.4. Основні категорії користувачів інформаційної системи нотаріального кабінету

Категорія користувача	Основні функції	Рівень доступу
Нотаріус	Робота з реєстрами, підписання документів, доступ до персональних даних	Повний
Помічник нотаріуса	Підготовка документів, внесення даних	Обмежений
Системний адміністратор	Адміністрування системи та технічна підтримка	Технічний
Аудитор безпеки	Контроль журналів подій та аудит	Аналітичний

**Джерело: складено автором*

Автоматизована система контролю доступу забезпечує перевірку прав користувача у момент входу до системи та під час виконання кожної операції. Після успішного проходження процедури автентифікації система автоматично визначає роль користувача та надає доступ лише до тих інформаційних ресурсів і функціональних модулів, які відповідають його службовим повноваженням. Такий підхід дозволяє реалізувати принцип мінімально необхідних привілеїв, відповідно до якого користувач отримує лише той рівень доступу, який необхідний для виконання його професійних обов’язків.

У межах інформаційної системи нотаріального кабінету доцільним є поєднання декількох факторів підтвердження особи, зокрема парольного захисту, електронного цифрового підпису та одноразових кодів підтвердження. Використання багатофакторної автентифікації значно підвищує рівень захищеності системи та мінімізує ризик компрометації облікових записів користувачів. Однією з ключових складових автоматизованої системи безпеки є моніторинг дій користувачів. Моніторинг являє собою процес безперервного спостереження за активністю користувачів у межах інформаційної системи з метою виявлення підозрілих або несанкціонованих дій. Усі операції

користувачів автоматично фіксуються у журналах подій із зазначенням часу доступу, IP-адреси, типу операції, об’єкта доступу та результату виконання дії.

Система журналювання подій є інструментом забезпечення підзвітності користувачів та контролю за дотриманням політик безпеки. Автоматичне ведення журналів дозволяє здійснювати аудит діяльності користувачів, аналізувати інциденти інформаційної безпеки та оперативно реагувати на спроби несанкціонованого доступу.

Таблиця 3.5. Інформація, що фіксується у журналі подій

Параметр журналювання	Характеристика
Ідентифікатор користувача	Дані про користувача системи
Час виконання операції	Дата та час доступу
Тип операції	Перегляд, редагування, видалення
IP-адреса	Адреса підключення користувача
Результат операції	Успішне або неуспішне виконання

**Джерело: складено автором*

Особливого значення автоматизований моніторинг набуває у процесі роботи з державними реєстрами та зовнішніми інформаційними системами. Інтеграція інформаційної системи нотаріального кабінету з державними реєстрами передбачає постійний обмін інформацією через захищені канали зв’язку. У зв’язку з цим система моніторингу повинна контролювати не лише дії внутрішніх користувачів, але й процес взаємодії із зовнішніми інформаційними ресурсами. Для підвищення ефективності моніторингу доцільним є використання автоматизованих систем аналізу поведінки користувачів. Такі системи дозволяють виявляти аномальну активність, яка може свідчити про спроби несанкціонованого доступу або компрометацію облікового запису. Наприклад, система автоматично реагує у випадку багаторазових невдалих спроб входу, входу з невідомого пристрою, зміни географічного розташування користувача або виконання нетипових операцій.

Автоматизована система моніторингу реалізовує механізми ризик-орієнтованого аналізу подій, відповідно до яких кожна дія користувача оцінюється за рівнем потенційної загрози. У випадку виявлення підозрілої активності система може автоматично блокувати обліковий запис користувача, вимагати повторну автентифікацію або надсилати повідомлення адміністратору безпеки.

Використання систем централізованого управління обліковими записами користувачів забезпечує автоматичне створення, зміну та блокування користувацьких облікових записів відповідно до кадрових змін або зміни функціональних обов'язків працівників. Автоматизація управління обліковими записами дозволяє мінімізувати ризик помилок адміністрування та забезпечити актуальність політик доступу. Автоматизована система має забезпечувати обмеження доступу до конфіденційної інформації відповідно до ролі користувача, а також здійснювати контроль за операціями копіювання, друку та передачі документів. Для захисту інформації доцільним є використання криптографічних засобів шифрування баз даних та електронних архівів документів. Одним із напрямів удосконалення автоматизованого контролю доступу є впровадження технологій адаптивної безпеки. Суть такого підходу полягає у динамічній зміні рівня захисту залежно від поведінки користувача та поточного рівня ризику. Наприклад, при виконанні критично важливих операцій система може автоматично вимагати додаткову перевірку особи або тимчасово обмежувати доступ до окремих функцій системи.

Особливого значення у процесі автоматизації моніторингу дій користувачів набуває забезпечення відповідності вимогам законодавства у сфері захисту персональних даних. Система повинна гарантувати законність обробки персональних даних, забезпечувати захист конфіденційної інформації та дотримання принципів підзвітності й прозорості. Усі дії користувачів повинні бути документованими та доступними для проведення внутрішнього або зовнішнього аудиту. Система повинна автоматично генерувати аналітичні

звіти про активність користувачів, спроби несанкціонованого доступу, критичні інциденти та порушення політик безпеки. Такі звіти дозволяють оцінювати ефективність функціонування системи захисту інформації та своєчасно виявляти потенційні загрози.

Таблиця 3.6. Основні функції автоматизованої системи моніторингу

Функція	Призначення
Журналювання подій	Фіксація дій користувачів
Аналіз поведінки	Виявлення аномальної активності
Контроль доступу	Перевірка прав користувачів
Формування звітності	Аналіз інцидентів безпеки
Реагування на загрози	Автоматичне блокування або сповіщення

**Джерело: складено автором*

Впровадження автоматизованої системи контролю доступу та моніторингу дій користувачів забезпечує значне підвищення рівня інформаційної безпеки інформаційної системи нотаріального кабінету. Автоматизація процесів управління доступом дозволяє мінімізувати вплив людського фактора, забезпечити оперативне реагування на інциденти безпеки та підвищити ефективність адміністрування інформаційної системи.

Отже, автоматизація контролю доступу та моніторингу дій користувачів є одним із ключових напрямів забезпечення інформаційної безпеки інформаційної системи нотаріального кабінету. Використання рольової моделі управління доступом, багатофакторної автентифікації, автоматизованого журналювання подій та систем аналізу поведінки користувачів дозволяє забезпечити високий рівень захисту конфіденційної інформації та мінімізувати ризики інформаційних загроз. Реалізація комплексної автоматизованої системи контролю доступу сприяє забезпеченню стабільного функціонування інформаційної системи нотаріального кабінету, дотриманню вимог законодавства у сфері захисту інформації та підвищенню ефективності управління інформаційними ресурсами.

3.4. Рекомендації щодо підвищення безпеки доступу на базі дослідження

У процесі дослідження інформаційної системи нотаріального кабінету приватного нотаріуса Охріменко Наталія Сергіївна було встановлено, що ефективність функціонування системи управління доступом безпосередньо залежить від комплексного поєднання організаційних, технічних та програмних засобів захисту інформації. З огляду на специфіку нотаріальної діяльності, яка передбачає обробку персональних даних, електронних документів, відомостей державних реєстрів та конфіденційної юридичної інформації, особливого значення набуває розроблення практичних рекомендацій щодо підвищення рівня безпеки доступу до інформаційних ресурсів.

Одним із ключових напрямів підвищення безпеки доступу є впровадження комплексної багатофакторної автентифікації користувачів. У процесі дослідження було встановлено, що використання лише парольного захисту не забезпечує належного рівня інформаційної безпеки, оскільки паролі можуть бути скомпрометовані внаслідок фішингових атак, використання шкідливого програмного забезпечення або недотримання користувачами правил інформаційної безпеки. Саме тому доцільним є використання декількох незалежних факторів підтвердження особи користувача.

Для інформаційної системи нотаріального кабінету рекомендованим є поєднання таких механізмів автентифікації:

- парольного захисту;
- кваліфікованого електронного підпису;
- одноразових кодів підтвердження;
- біометричної ідентифікації;
- апаратних токенів безпеки.

Використання багатофакторної автентифікації дозволяє суттєво знизити ризик компрометації облікових записів навіть у випадку викрадення одного з елементів автентифікації.

Таблиця 3.7. Рекомендовані механізми підвищення безпеки автентифікації

Механізм захисту	Призначення	Результат
Багатофакторна автентифікація	Додаткова перевірка особи користувача	Зниження ризику несанкціонованого доступу
Електронний цифровий підпис	Підтвердження автентичності документів	Захист електронних документів
Біометрична ідентифікація	Унікальна перевірка користувача	Підвищення точності автентифікації
Апаратні токени	Захист облікових записів	Неможливість віддаленого перехоплення доступу

**Джерело: складено автором*

Наступним важливим напрямом удосконалення системи безпеки є впровадження адаптивного контролю доступу. Традиційні системи авторизації базуються на фіксованому наборі правил доступу, однак сучасні кіберзагрози потребують використання більш гнучких механізмів управління безпекою. Адаптивний контроль доступу передбачає автоматичний аналіз поведінки користувачів та динамічне коригування рівня захисту залежно від поточного рівня ризику.

Наприклад, система автоматично вимагає додаткову автентифікацію у випадках:

- входу з нового пристрою;
- зміни географічного розташування користувача;
- виконання нетипових операцій;
- багаторазових невдалих спроб входу;
- доступу до критично важливих даних.

Використання адаптивних механізмів контролю доступу дозволяє своєчасно реагувати на потенційні загрози та мінімізувати ризик компрометації інформаційної системи. Аспектом підвищення безпеки є удосконалення системи журналювання та моніторингу дій користувачів. Ефективне журналювання подій забезпечує підзвітність користувачів, дозволяє виявляти підозрілу активність та здійснювати аудит інформаційної безпеки. Для підвищення ефективності моніторингу рекомендується впровадження автоматизованих систем аналізу поведінки користувачів, які здатні виявляти аномальні дії та оперативно реагувати на потенційні загрози.

Особливу увагу доцільно приділити автоматичному формуванню повідомлень про інциденти інформаційної безпеки. У разі виявлення підозрілих дій система повинна автоматично:

- блокувати обліковий запис;
- повідомляти адміністратора безпеки;
- створювати запис у журналі подій;
- ініціювати додаткову перевірку користувача.

Такий підхід забезпечує оперативне реагування на інциденти та дозволяє мінімізувати наслідки потенційних кібератак.

Одним із найбільш важливих напрямів підвищення рівня безпеки є захист каналів передачі інформації. Оскільки інформаційна система нотаріального кабінету взаємодіє із зовнішніми реєстрами та інформаційними платформами, особливого значення набуває забезпечення захищеного мережевого з’єднання. Для цього рекомендовано використовувати:

- VPN-з’єднання;
- криптографічні протоколи SSL/TLS;
- міжмережеві екрани;
- системи виявлення вторгнень IDS/IPS;
- сегментацію мережевої інфраструктури.

Застосування сучасних криптографічних алгоритмів дозволяє забезпечити конфіденційність інформації та захистити дані від перехоплення або модифікації під час передачі через мережу.

Таблиця 3.8. Рекомендації щодо захисту мережевої інфраструктури

Захід безпеки	Функціональне призначення
VPN-з'єднання	Захист віддаленого доступу
SSL/TLS шифрування	Захист передачі даних
Firewall	Контроль мережевого трафіку
IDS/IPS системи	Виявлення кібератак
Сегментація мережі	Обмеження поширення загроз

**Джерело: складено автором*

Окремим напрямом удосконалення системи безпеки є забезпечення фізичного захисту серверного обладнання та робочих станцій користувачів. Фізичний доступ до обладнання становить серйозну загрозу інформаційній безпеці, оскільки у випадку несанкціонованого доступу можливе копіювання, пошкодження або викрадення інформації. Саме тому рекомендовано впровадження систем фізичного контролю доступу, відеоспостереження, електронних пропускних систем та засобів резервного копіювання інформації.

Особливо важливим є створення системи резервного копіювання та аварійного відновлення даних. У випадку технічних збоїв, кібератак або фізичного пошкодження обладнання система повинна забезпечувати можливість швидкого відновлення інформації без втрати критично важливих даних. Важливу роль у забезпеченні інформаційної безпеки відіграє людський фактор. Значна частина інцидентів інформаційної безпеки пов'язана з помилками користувачів, недотриманням правил безпеки або використанням слабких паролів. У зв'язку з цим доцільним є проведення регулярного навчання працівників нотаріального кабінету з питань інформаційної безпеки.

Навчання повинно охоплювати:

- правила створення складних паролів;
- безпечне використання електронного підпису;

- виявлення фішингових повідомлень;
- правила роботи з конфіденційною інформацією;
- порядок реагування на інциденти інформаційної безпеки.

Регулярне підвищення рівня цифрової грамотності працівників дозволяє суттєво знизити ризик компрометації інформаційної системи через людський фактор. Наступною рекомендацією є проведення регулярного аудиту інформаційної безпеки. Аудит дозволяє виявляти потенційні вразливості, оцінювати ефективність політик безпеки та визначати напрями подальшого вдосконалення системи управління доступом. У межах аудиту доцільно здійснювати:

- перевірку журналів подій;
- аналіз політик доступу;
- тестування механізмів автентифікації;
- оцінку рівня захищеності мережевої інфраструктури;
- аналіз ризиків інформаційної безпеки.

Особливого значення у сучасних умовах набуває впровадження принципу безперервного вдосконалення системи безпеки. Інформаційні технології та методи кібератак постійно змінюються, тому система захисту інформації повинна регулярно оновлюватися та адаптуватися до нових загроз. Для цього необхідно забезпечити:

- регулярне оновлення програмного забезпечення;
- оновлення антивірусних систем;
- модернізацію засобів криптографічного захисту;
- перегляд політик безпеки;
- моніторинг нових кіберзагроз.

Таблиця 3.9. Комплекс рекомендацій щодо підвищення безпеки доступу

Напрям удосконалення	Основні рекомендації
Автентифікація	Багатофакторний захист
Авторизація	Рольова модель доступу
Моніторинг	Автоматичне журналювання
Мережевий захист	VPN та криптографія
Фізична безпека	Контроль доступу до обладнання
Навчання персоналу	Підвищення цифрової грамотності
Аудит безпеки	Регулярна перевірка системи

**Джерело: складено автором*

Таким чином, результати проведеного дослідження дозволяють сформувати комплекс практичних рекомендацій щодо підвищення рівня безпеки доступу до інформаційної системи нотаріального кабінету. Основними напрямами удосконалення системи захисту є впровадження багатофакторної автентифікації, адаптивного контролю доступу, автоматизованого моніторингу дій користувачів, захищених мережевих технологій та систем резервного копіювання. Реалізація запропонованих заходів дозволить забезпечити високий рівень захисту конфіденційної інформації, мінімізувати ризики інформаційних загроз та забезпечити стабільне функціонування інформаційної системи нотаріального кабінету в умовах сучасного цифрового середовища.

Висновки до розділу 3

Розроблено концептуальну модель ефективного управління доступом до інформаційних ресурсів нотаріального кабінету. Встановлено, що найбільш доцільним підходом до організації системи захисту є використання багаторівневої моделі безпеки, яка охоплює організаційний, програмний, мережевий та фізичний рівні захисту інформації. Доведено, що комплексний характер запропонованої моделі дозволяє забезпечити конфіденційність, цілісність та доступність інформації, а також мінімізувати ризики несанкціонованого доступу до персональних даних і електронних документів. Особливу увагу приділено рольовій моделі управління доступом, яка забезпечує розмежування прав користувачів відповідно до їх функціональних обов'язків та реалізує принцип мінімально необхідних привілеїв.

Досліджено особливості впровадження багаторівневої системи автентифікації та авторизації користувачів у межах інформаційної системи нотаріального кабінету. У результаті дослідження встановлено, що традиційні методи парольного захисту не забезпечують достатнього рівня інформаційної безпеки в умовах сучасних кіберзагроз. У зв'язку з цим обґрунтовано необхідність використання багатофакторної автентифікації, яка поєднує декілька незалежних способів підтвердження особи користувача, зокрема парольний захист, електронний цифровий підпис та одноразові коди підтвердження. Доведено, що впровадження багатофакторної автентифікації суттєво знижує ризик компрометації облікових записів та забезпечує додатковий рівень захисту інформаційної системи. Крім того, визначено переваги рольового підходу до авторизації користувачів, який дозволяє централізовано управляти правами доступу та підвищує ефективність адміністрування системи.

Проаналізовано процес автоматизації контролю доступу та моніторингу дій користувачів. Установлено, що автоматизація процесів управління доступом є важливим напрямом підвищення рівня інформаційної безпеки

нотаріальної інформаційної системи. Визначено, що впровадження автоматизованих механізмів журналювання подій, аналізу поведінки користувачів та контролю доступу дозволяє забезпечити постійний моніторинг активності користувачів та своєчасне виявлення потенційних загроз інформаційній безпеці. Доведено, що використання систем автоматичного реагування на підозрілу активність, зокрема блокування облікових записів та надсилання повідомлень адміністраторам безпеки, сприяє оперативному реагуванню на інциденти та мінімізує ризик несанкціонованого використання інформаційних ресурсів.

Сформовано комплекс рекомендацій щодо підвищення безпеки доступу до інформаційної системи нотаріального кабінету. На основі проведеного дослідження обґрунтовано необхідність впровадження сучасних криптографічних засобів захисту інформації, захищених VPN-з’єднань, систем виявлення вторгнень та механізмів резервного копіювання даних. Визначено важливість забезпечення фізичного захисту серверного обладнання та обмеження доступу до критично важливих компонентів інфраструктури. Окрему увагу приділено проблемі людського фактора у сфері інформаційної безпеки. Встановлено, що проведення регулярного навчання працівників нотаріального кабінету з питань інформаційної безпеки, правил роботи з електронними ключами та методів протидії фішинговим атакам є важливою складовою ефективної системи захисту інформації.

ВИСНОВКИ

У результаті проведеного дослідження теоретичних і практичних аспектів управління доступом в інформаційно-комунікаційних системах встановлено, що ефективне управління доступом є одним із ключових чинників забезпечення інформаційної безпеки та захисту інформаційних ресурсів від несанкціонованого використання, модифікації або знищення. Визначено, що сучасні системи управління доступом повинні базуватися на принципах мінімальних привілеїв, розмежування повноважень, надійної автентифікації та авторизації користувачів, а також безперервного контролю й моніторингу доступу до інформаційних ресурсів.

У ході дослідження проаналізовано основні моделі управління доступом, нормативно-правове забезпечення та міжнародні стандарти інформаційної безпеки, що дозволило сформувати теоретичне підґрунтя для оцінювання сучасних механізмів захисту інформації. Встановлено, що найбільш ефективними є комплексні підходи, які поєднують рольові та адаптивні моделі контролю доступу, а також враховують контекст взаємодії користувача із системою.

На базі дослідження інформаційної системи «Нотаріус» здійснено аналіз особливостей реалізації механізмів управління доступом у сфері обробки персональних та юридично значущих даних. Виявлено, що система забезпечує базовий рівень захисту інформації та поєднує відкритий доступ до публічних даних із обмеженим доступом до внутрішніх ресурсів. Водночас встановлено низку недоліків, зокрема недостатню захищеність автентифікаційних механізмів, відсутність адаптивного контролю доступу, обмежені можливості моніторингу дій користувачів та використання переважно статичних підходів до управління доступом, що не повною мірою відповідають сучасним вимогам кібербезпеки.

На основі отриманих результатів розроблено концептуальну модель ефективного управління доступом до інформаційних ресурсів нотаріального кабінету, яка передбачає використання багаторівневої системи захисту, що охоплює організаційний, програмний, мережевий та фізичний рівні безпеки. Обґрунтовано доцільність застосування рольової моделі управління доступом та принципу мінімально необхідних привілеїв для розмежування прав користувачів.

Доведено ефективність впровадження багатофакторної автентифікації, яка поєднує парольний захист, електронний цифровий підпис та додаткові засоби підтвердження особи користувача. Встановлено, що використання багатофакторної автентифікації суттєво знижує ризик компрометації облікових записів і підвищує загальний рівень захищеності інформаційної системи.

Досліджено можливості автоматизації контролю доступу та моніторингу дій користувачів. Визначено, що впровадження механізмів журналювання подій, аналізу поведінки користувачів, автоматичного виявлення підозрілої активності та реагування на інциденти дозволяє своєчасно виявляти загрози інформаційній безпеці та мінімізувати ризики несанкціонованого доступу до інформаційних ресурсів.

За результатами дослідження сформовано комплекс практичних рекомендацій щодо підвищення безпеки доступу до інформаційної системи нотаріального кабінету, які передбачають використання сучасних криптографічних засобів захисту, VPN-з’єднань, систем виявлення вторгнень, резервного копіювання даних, удосконалення механізмів контролю доступу та регулярного навчання персоналу з питань інформаційної безпеки.

Таким чином, мету дослідження досягнуто, поставлені завдання виконано, а отримані результати підтверджують необхідність впровадження сучасних багаторівневих механізмів управління доступом для підвищення рівня захищеності інформаційно-комунікаційних систем та забезпечення надійного захисту інформаційних ресурсів в умовах зростання кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади: дис. ... д-ра юрид. наук : 12.00.07. Київ, 2002. С. 58–63.

2. Артеменко О. В., Улютіна О. А. Інформаційне право : навч. посіб. Київ : Прінтеко : НУБіП України, 2020. 101 с.

3. Ахмад А., Вебб Дж., Десоуза К. К., Бурман Дж. Стратегічно мотивовані цілеспрямовані кіберзагрози: визначення, процеси, тактики та модель дезінформаційної протидії. *Computers & Security*. 2019. № 86. С. 16–23.

4. Байс Л. Р., Олівейра Р. Р., Барселлос М. П., Гаспарі Л. П., Мадейра Е. Р. Віртуальна безпека мереж: загрози, протидія та виклики. *Journal of Internet Services and Applications*. 2015. Т. 6, № 1. С. 17–23.

5. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.

6. Василенко М. Удосконалення кібербезпеки інформаційно-комунікаційних систем у контексті розвитку інформаційного законодавства. *Проблеми і судження*. 2018. № 3. С. 9–12.

7. Вінер Н. Кібернетика, або керування та зв’язок у тварині і машині. Cambridge : MIT Press, 2019. С. 125–145.

8. Городиський Р., Вавріченко О., Стрельбицький М. Оцінювання загроз витоку інформації через супутникові канали зв’язку. *Наука і техніка сьогодні*. 2024. № 2(30). С. 96–112.

9. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібербезпека підприємства : підручник. Львів : Видавець Марченко Т. В., 2024. С. 56–68.

10. Дудикевич В., Микитин Г., Бортнік Л., Стосик Т. Методологія безпеки кіберфізичних систем та Інтернету речей в умовах інтелектуалізації

інфраструктури. *Комп'ютерні системи та мережі*. 2024. Т. 6, № 1. С. 325–332.

11. Інформаційна безпека держави : підручник / за заг. ред. В. В. Остроухова. Київ : ДНУ «Книжкова палата України», 2016. 264 с.

12. Інформаційна безпека держави : підручник : у 2 т. Т. 1 / В. М. Петрик, М. М. Присяжнюк, Д. С. Мельник та ін.; за заг. ред. В. В. Остроухова. Київ : ДНУ «Книжкова палата України», 2016. 264 с.

13. Коваленко Л. П., Коваленко Б. В. Інформаційне право : підручник / за заг. ред. Л. П. Коваленко. Одеса : Гельветика, 2020. 285 с.

14. Брижко В. М., Фурашев В. М. Інформаційне право та інформаційне законодавство : наук. вид. Харків : Право, 2021. 288 с.

15. Карпович І. М., Гладка О. М., Наконечна Я. А. Аналіз ризиків безпеки інформаційної системи на ІТ-підприємстві. *Наукові записки ТНУ ім. В. І. Вернадського. Серія: Технічні науки*. 2020. С. 236–239.

16. Каткова Т. Г. Інформаційне право. Практикум : навч. посіб. Харків : Право, 2019. 108 с.

17. Коробейнікова Т., Ямнич А. Оцінка ризиків інформаційної безпеки персоналу. *SWorldJournal*. 2023. № 20(01). С. 45–52.

18. Кравчук В. Концепція інформаційної безпеки в мережі Інтернет. *Матеріали 8-ї міжнародної науково-практичної конференції*. 2024. С. 56–68.

19. Кульчій О. О. Інформаційне право : навч.-метод. посіб. Полтава : ПУЕТ, 2015. 193 с.

20. Лубко Д., Мірошниченко М. Ю. Аналіз сучасних підходів і методів у сфері захисту інформації та даних. *Вісник Херсонського національного технічного університету*. 2024. № 1(88). С. 58–64.

21. Мороз В. Інформаційний ресурс як об'єкт державного управління: зміст, принципи та характеристики системи. *Державне управління: удосконалення та розвиток*. 2020. № 1. С. 196–205.

22. Нарендра Р., Тадапанені С., Сабрі М. Проблеми безпеки хмарних обчислень. *SSRN Electronic Journal*. 2020. С. 25–36.

23. Нашинець-Наумова А. Ю. Інформаційне право : навч. посіб. Київ: Київський університет імені Бориса Грінченка, 2020. 136 с.

24. Основи законодавства України про охорону здоров'я : Закон України від 19 листоп. 1992 р. № 2801-XII. URL: zakon.rada.gov.ua (дата звернення: 01.06.2026).

25. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. URL: zakon.rada.gov.ua (дата звернення: 01.06.2026).

26. Про захист персональних даних: Закон України від 1 черв. 2010 р. № 2297-VI. URL: zakon.rada.gov.ua (дата звернення: 01.06.2026).

27. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII. URL: zakon.rada.gov.ua (дата звернення: 01.06.2026).

28. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241. URL: zakon.rada.gov.ua (дата звернення: 01.06.2026).

29. Свамі А. Сучасні мобільні мережі (4G, 5G, 6G). *International Journal of Health Sciences*. 2022. С. 96–112.

30. Сопілко І. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Наукові праці НАУ. Серія: Повітряне і космічне право*. 2021. № 2(59). С. 78–84.

31. Фурашев В. М. Законодавче забезпечення інформаційної безпеки України. *Інформація і право*. 2014. № 1(10). С. 59–67.