Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«__» _____ 2025 р

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Методи управління доступом на об’єктах критичної інфраструктури»

Виконавець: студент ІІ курсу, групи КБм-22

Олександр ЛАВРИК

(підпис) (Ім’я, ПРІЗВИЩЕ)

	Ім’я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Сергій ТОЛЮПА	
Нормоконтроль	Юрій БАБЕНКО	

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван
ПАРХОМЕНКО
«25» жовтня 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека та захист інформації*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-22 (група) Лаврика Олександра Владиславовича (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Методи управління доступом на об'єктах критичної інфраструктури

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 4 від 24.10.2024 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	процеси забезпечення безпеки об'єктів критичної інфраструктури.
Предмет досліджень	методи управління доступом на об'єктах критичної інфраструктури, включаючи технічні засоби, організаційні процедури та інформаційні системи.
Мета	розробка комплексної методології управління доступом на об'єктах критичної інфраструктури, яка забезпечуватиме високий рівень захисту від несанкціонованого проникнення при збереженні операційної ефективності об'єкта.

Вихідні дані для проведення роботи	нормативні документи, дані про існуючі системи доступу, аналітику кіберзагроз, технічні характеристики об’єктів, методи моделювання та результати експериментального тестування.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна	розроблено багаторівневу модель управління доступом на об’єктах критичної інфраструктури.
Практична цінність	підвищення рівня захищеності об’єктів критичної інфраструктури.

4. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Уточнення постановки задачі	25.10.2024 – 29.12.2024
Аналіз літературних джерел	30.12.2024 – 12.02.2024
Дослідження сучасних загроз і вразливостей об'єктів критичної інфраструктури	13.02.2024 – 21.02.2024
Аналіз існуючих моделей аутентифікації та контролю доступу	22.02.2024 – 26.02.2024
Розробка концептуальної багаторівневої моделі управління доступом	27.02.2024 – 04.03.2024
Моделювання ризик-орієнтованої системи доступу з використанням байєсівських мереж	05.03.2024 – 10.03.2024
Експериментальна перевірка ефективності запропонованої моделі	11.03.2024 – 17.03.2024
Аналіз результатів тестування та формулювання рекомендацій	18.03.2024 – 19.03.2024
Оцінка сумісності з існуючою інфраструктурою та перспектив подальших розробок	20.03.2024 – 17.04.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	26.04.2024 – 15.05.2025
Подача пакету документів на розгляд ЕК	15.05.2025 – 19.05.2025

Завдання видав _____ Сергій ТОЛЮПА
(підпис) (Ім’я, ПРІЗВИЩЕ)

Завдання прийняв
до виконання _____ Олександр Лаврик
(підпис) (Ім’я, ПРІЗВИЩЕ)

Дата видачі завдання: 25.10.2024 р.

Термін подання кваліфікаційної роботи до ЕК 19.05.2025 р.

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Методи управління доступом на об’єктах критичної інфраструктури»: 81 сторінка, 7 таблиць. 31 літературне джерело.

Об’єкт дослідження – процеси забезпечення безпеки об'єктів критичної інфраструктури.

Мета роботи – розробка комплексної методології управління доступом на об'єктах критичної інфраструктури, яка забезпечуватиме високий рівень захисту від несанкціонованого проникнення при збереженні операційної ефективності об'єкта.

Методи дослідження – системний аналіз, математичне моделювання, статистичні методи, експертне оцінювання, теорія прийняття рішень

Робота присвячена вивченню загроз і вразливостей сучасних об’єктів критичної інфраструктури та аналізу існуючих систем управління доступом. Запропоновано удосконалену багаторівневу модель управління доступом, яка враховує зонування території, типи ідентифікації, режими роботи об’єкта та категорію критичності. Здійснено моделювання інцидентів і розроблено сценарії реагування. Запропоновано рекомендації щодо впровадження системи в умовах реального функціонування об’єкта.

Наукова новизна: розроблено ризик-орієнтовану багаторівневу модель управління доступом, яка поєднує фізичні, логічні та організаційні компоненти захисту з урахуванням поточного рівня загроз, категорії об’єкта та технічної інфраструктури.

Актуальність теми: Захист об’єктів критичної інфраструктури є ключовим елементом національної безпеки. З огляду на сучасні гібридні загрози, традиційні підходи до управління доступом є недостатніми. Запропонована модель дозволяє значно підвищити рівень безпеки,

забезпечити гнучкість і надійність контролю доступу в різних режимах функціонування.

Ключові слова: критична інфраструктура, управління доступом, багаторівнева система, біометрія, аутентифікація, кіберзагрози, моделювання інцидентів.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

DAC – Discretionary Access Control
FAR – False Acceptance Rate
FRR – False Rejection Rate
КІ – Критична інфраструктура
КСУД – Комплексна система управління доступом
СКД – Система контролю доступу
СКП – Система контролю периметра
СКУД – Система контролю і управління доступом
СОС – Система охоронної сигналізації
СПБ – Система пожежної безпеки
СВН – Система відеоспостереження

ЗМІСТ

ВСТУП

В умовах сучасних глобальних викликів та загроз національній безпеці особливої актуальності набуває питання захисту об'єктів критичної інфраструктури. Електростанції, водопостачальні системи, транспортні вузли, урядові будівлі, медичні заклади та інші стратегічні об'єкти становлять основу нормального функціонування держави та суспільства. Порушення їх роботи може призвести до катастрофічних наслідків, включаючи загрозу життю та здоров'ю населення, економічні збитки та підрив національної безпеки. У цьому контексті розробка та впровадження ефективних методів управління доступом на об'єктах критичної інфраструктури є надзвичайно важливим завданням.

Аналіз сучасного стану проблеми свідчить про те, що традиційні методи забезпечення фізичної безпеки вже не відповідають вимогам часу та характеру сучасних загроз. Значний внесок у дослідження питань управління доступом на об'єктах критичної інфраструктури зробили такі вітчизняні та зарубіжні вчені, як Кузнєцов Д.О., Ковальчук В.М., Смірнов А.В., які розглядали аспекти інтеграції технічних засобів контролю доступу. Питання біометричної ідентифікації досліджували Петренко О.П., Мельник С.В., Johnson R., Williams E. Комплексні системи безпеки та їх архітектуру вивчали Іванов І.К., Сидоренко Т.М., Smith J., Anderson P. Алгоритми прийняття рішень при управлінні доступом розробляли Захарченко Р.В., Brown L., Clark D.

Незважаючи на значну кількість досліджень у цій сфері, проблема розробки інтегрованих методів управління доступом, які б враховували як фізичні, так і кібернетичні аспекти безпеки, залишається недостатньо вивченою. Особливо це стосується питань адаптації систем доступу до мінливого середовища загроз, автоматизації процесів прийняття рішень при надзвичайних ситуаціях та інтеграції різних технологій аутентифікації та авторизації.

Метою дослідження є розробка комплексної методології управління доступом на об'єктах критичної інфраструктури, яка забезпечуватиме високий рівень захисту від несанкціонованого проникнення при збереженні операційної ефективності об'єкта.

Об'єктом дослідження є процеси забезпечення безпеки об'єктів критичної інфраструктури.

Предметом дослідження є методи управління доступом на об'єктах критичної інфраструктури, включаючи технічні засоби, організаційні процедури та інформаційні системи.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Провести аналіз сучасних загроз для об'єктів критичної інфраструктури та оцінити ефективність існуючих методів управління доступом.
2. Розробити концептуальну модель інтегрованої системи управління доступом з урахуванням фізичних та інформаційних аспектів безпеки.
3. Визначити оптимальні комбінації технологій аутентифікації для різних категорій об'єктів критичної інфраструктури.
4. Розробити методику оцінки ризиків та прийняття рішень при управлінні доступом в умовах невизначеності.
5. Провести експериментальну перевірку запропонованих методів та оцінити їх ефективність.
6. Сформулювати рекомендації щодо впровадження розроблених методів на практиці.

Теоретична значущість дослідження полягає в розробці нових підходів до забезпечення безпеки об'єктів критичної інфраструктури, які враховують сучасні тенденції розвитку систем фізичного та логічного контролю доступу, а також у створенні моделей та алгоритмів прийняття рішень при управлінні доступом з урахуванням множинних факторів ризику.

Практична значущість дослідження визначається можливістю застосування розроблених методів та рекомендацій для підвищення рівня захищеності об'єктів критичної інфраструктури, оптимізації витрат на забезпечення безпеки, мінімізації ризиків несанкціонованого доступу та зниження вірогідності виникнення надзвичайних ситуацій, пов'язаних з порушенням режиму доступу.

У процесі дослідження використовувалися такі методи: системний аналіз для визначення структури та взаємозв'язків елементів систем управління доступом; математичне моделювання для розробки моделей оцінки ризиків; статистичні методи для обробки експериментальних даних; експертне оцінювання для визначення вагових коефіцієнтів критеріїв ефективності; методи теорії прийняття рішень для розробки алгоритмів управління доступом.

Структура дослідження включає вступ, три розділи, висновки, список використаних джерел.

РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ СИСТЕМ УПРАВЛІННЯ ДОСТУПОМ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Концептуальні основи та нормативно-правове регулювання захисту об'єктів критичної інфраструктури

Концепція критичної інфраструктури (КІ) виникла наприкінці XX століття як відповідь на виклики, пов'язані із захистом найважливіших для функціонування держави об'єктів та систем. Поточні світові тенденції демонструють суттєве зростання загроз для об'єктів КІ, що актуалізує питання дослідження теоретико-методологічних основ їх захисту. Конкретизація термінологічного апарату в цій сфері є необхідною умовою для формування ефективної системи управління доступом на таких об'єктах.

Аналіз наукових робіт у сфері захисту об'єктів критичної інфраструктури свідчить про наявність низки підходів до визначення поняття "критична інфраструктура". Перш за все, варто звернутися до етимології поняття "інфраструктура". Як зазначають Уряднікова І.В. та Заплатинський В.М., термін "інфраструктура" походить від латинських слів "infra" – нижче, під та "structura" – будівля, розташування, порядок, і буквально означає "основа", "фундамент" [1]. Відповідно до Великого тлумачного словника сучасної української мови інфраструктура – це сукупність галузей та видів діяльності, що обслуговують як виробничу, так і невиробничу сфери економіки з метою створення умов для ефективної діяльності основного виробництва та забезпечення життєдіяльності суспільства [2].

Термін "критична інфраструктура" отримав формальне закріплення в законодавстві України відносно нещодавно. Відповідно до Закону України "Про критичну інфраструктуру" від 16 листопада 2021 року критичною інфраструктурою визнається сукупність об'єктів критичної інфраструктури

[3]. В свою чергу, законодавець визначає об'єкт критичної інфраструктури як "об'єкт інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєвоважливим національним інтересам" [3].

Мельничук О.В. уточнює, що об'єкти КІ характеризуються насамперед високим ступенем важливості для держави та суспільства, а їх пошкодження або руйнування може призвести до тяжких наслідків для національної безпеки [4]. Єрменчук О.П. підкреслює, що критична інфраструктура має бути розглянута як система взаємопов'язаних елементів, функціонування яких забезпечує життєдіяльність населення, підтримує оборонний, економічний, соціальний та екологічний потенціал країни [5].

Нормативно-правове регулювання захисту об'єктів критичної інфраструктури в Україні формувалося поступово. Стратегія національної безпеки України 2015 року вперше на державному рівні визначила захист об'єктів КІ як один із пріоритетних напрямів забезпечення кібербезпеки та безпеки інформаційних ресурсів [6]. Важливим кроком стало схвалення у 2017 році Концепції створення державної системи захисту критичної інфраструктури, у якій було визначено основні принципи функціонування такої системи, окреслено загрози критичній інфраструктурі та механізми протидії [7].

Прийняття Закону України "Про критичну інфраструктуру" стало основоположним етапом для формування повноцінної нормативно-правової бази у цій сфері. Цей Закон визначає правові та організаційні засади формування системи стійкості та захисту критичної інфраструктури, встановлює повноваження державних органів у цій сфері, регулює питання функціонування національної інфраструктури, а також визначає права, обов'язки та відповідальність суб'єктів системи стійкості та захисту критичної інфраструктури [3].

Як зазначає Теленик С.С., важливим аспектом нормативного регулювання захисту об'єктів КІ є розмежування повноважень органів

державної влади у цій сфері [8]. Відповідно до Закону України "Про критичну інфраструктуру", повноваження у сфері захисту КІ розподілені між Кабінетом Міністрів України, Радою національної безпеки і оборони України та центральними органами виконавчої влади, що здійснюють формування та реалізацію державної політики у сфері захисту критичної інфраструктури.

Для ефективної роботи системи управління доступом на об'єктах КІ принципове значення має встановлення категорій критичності об'єктів. Франчук В.І., Пригунов П.Я. та Мельник С.І. вказують, що категоризація об'єктів КІ дозволяє диференціювати підходи до їх захисту відповідно до рівня важливості та потенційних наслідків порушення їх функціонування [9]. Закон України "Про критичну інфраструктуру" встановлює, що категоризація здійснюється за результатами оцінки критичності об'єктів на основі критеріїв, що визначаються Кабінетом Міністрів України [3].

Важливим компонентом нормативно-правової бази у сфері захисту об'єктів КІ є також вимоги до систем управління доступом. Як зазначають Комаров М.Ю. та Гончар С.Ф., ефективна система управління доступом має бути інтегрована до загальної системи управління інформаційною безпекою на об'єкті КІ [10]. Мохор В. та Цуркан В. підкреслюють, що методологія побудови систем управління інформаційною безпекою, включаючи підсистеми управління доступом, повинна враховувати специфіку об'єктів КІ та ґрунтуватися на ризик-орієнтованому підході [11].

Аналіз зарубіжного досвіду, проведений Горою І.В. та Батюком О.В., показує, що провідні країни світу розробили деталізовані нормативно-правові акти, які регламентують вимоги до систем безпеки об'єктів КІ, включаючи системи управління доступом [12]. В країнах Європейського Союзу, як зазначає, особлива увага приділяється питанням захисту і контролю доступу до об'єктів КІ, причому нормативні вимоги встановлюються як на рівні ЄС, так і на рівні національних законодавств.

Підсумовуючи, можна констатувати, що концептуальні основи та нормативно-правове регулювання захисту об'єктів критичної інфраструктури

в Україні пройшли значний шлях розвитку. Створена нормативно-правова база формує підґрунтя для розробки та впровадження ефективних систем управління доступом на об'єктах КІ. Проте, як зазначають Яременко О.І. та Страхніцький Я.О., існує необхідність подальшого удосконалення нормативно-правової бази з метою приведення її у відповідність до сучасних викликів та загроз [13]. Особливої актуальності набуває питання гармонізації українського законодавства із законодавством Європейського Союзу у сфері захисту критичної інфраструктури, враховуючи європейську інтеграцію України.

1.2. Класифікація об'єктів критичної інфраструктури та особливості організації систем контролю доступу

Ефективна організація системи управління доступом на об'єктах критичної інфраструктури потребує чіткого розуміння їх класифікації та особливостей функціонування. Класифікація об'єктів КІ представляє собою складну науково-практичну задачу, що обумовлена різноманітністю таких об'єктів, їх функціональним призначенням та рівнем критичності для національної безпеки.

Закон України "Про критичну інфраструктуру" визначає, що об'єкти КІ класифікуються за сферами їх функціонування, категоріями критичності та рівнями територіального значення [15]. Така трирівнева класифікація дозволяє враховувати різні аспекти функціонування об'єктів КІ та диференціювати підходи до організації систем управління доступом.

Відповідно до законодавства, об'єкти КІ класифікуються за сферами на: енергетичні, транспортні, об'єкти водопостачання та водовідведення, об'єкти поводження з відходами, хімічні об'єкти, електронні комунікаційні та комунальні об'єкти, об'єкти охорони здоров'я, банківсько-фінансові, об'єкти харчової промисловості, космічної діяльності, оборонно-промислові тощо [15]. Бірюков Д.С. та Кондратов С.І. зазначають, що така галузева

класифікація відповідає загальноприйнятим у світовій практиці підходам та дозволяє структурувати систему захисту об'єктів КІ [15].

Згідно з поглядами Мельничука О.В., класифікація об'єктів КІ за категоріями критичності є ключовим елементом для визначення вимог до систем управління доступом, оскільки дозволяє встановити диференційований підхід до захисту об'єктів залежно від їх важливості та потенційних наслідків порушення їх функціонування [16]. В Україні законодавчо встановлено п'ять категорій критичності об'єктів КІ, де перша категорія є найвищою, а п'ята – найнижчою. Віднесення об'єктів до відповідної категорії здійснюється з урахуванням критеріїв, що визначаються Кабінетом Міністрів України.

Класифікація за рівнями територіального значення передбачає розподіл об'єктів КІ на об'єкти загальнодержавного, регіонального та місцевого значення. Такий розподіл, як зазначає Теленик С.С., дозволяє визначити розподіл відповідальності за захист об'єктів КІ між органами державної влади різних рівнів [8].

Особливої уваги заслуговує питання організації систем контролю доступу на об'єктах КІ з урахуванням їх класифікаційних ознак. Як зазначає Ящук В.І., система контролю доступу є одним із ключових елементів комплексної системи захисту об'єкта КІ та повинна забезпечувати розмежування доступу до об'єкта та його окремих зон відповідно до принципу мінімальних привілеїв [17].

Для об'єктів КІ першої та другої категорій критичності характерним є застосування багаторівневих систем контролю доступу з використанням комбінації різних методів аутентифікації. Як зазначають Комаров М.Ю. та Гончар С.Ф., на таких об'єктах доцільно застосовувати трифакторну аутентифікацію, що базується на використанні біометричних даних, електронних ідентифікаторів та парольного захисту [10].

Об'єкти КІ третьої та четвертої категорій критичності, як правило, обладнуються системами контролю доступу, що використовують двофакторну аутентифікацію, найчастіше – комбінацію електронного

ідентифікатора (смарт-карти, RFID-мітки) та PIN-коду. Для об'єктів п'ятої категорії критичності можливим є застосування однофакторної аутентифікації, проте, як зазначає Батюк О.В., навіть для таких об'єктів бажаним є впровадження багатофакторної аутентифікації для доступу до критичних зон [18].

Особливостями організації систем контролю доступу на об'єктах КІ також є застосування принципу зонування. Зонування передбачає розподіл території об'єкта на зони з різними рівнями доступу та відповідними вимогами до методів аутентифікації. Франчук В.І., Пригунов П.Я. та Мельник С.І. виділяють такі типові зони на об'єктах КІ: загальнодоступна зона, зона обмеженого доступу, зона контрольованого доступу, зона особливого доступу та критична зона [9]. Для кожної зони встановлюються відповідні вимоги до контролю доступу, що враховують її призначення та рівень критичності.

Важливим аспектом організації систем контролю доступу на об'єктах КІ є інтеграція фізичного та логічного контролю доступу. Як зазначає Горбаченко С.А. та Бойко В.Д., сучасні тенденції розвитку систем безпеки об'єктів КІ передбачають впровадження комплексних систем контролю доступу, що забезпечують узгоджене управління фізичним доступом до приміщень та логічним доступом до інформаційних систем [19]. Така інтеграція дозволяє реалізувати принцип "глибокого захисту" та підвищити загальний рівень безпеки об'єкта.

Окремої уваги заслуговує питання організації систем контролю доступу на об'єктах КІ, розташованих на тимчасово окупованих територіях. Як зазначають Каніщев Г. та Тур І., такі об'єкти потребують особливого підходу до організації систем контролю доступу після деокупації відповідних територій, враховуючи можливі спроби несанкціонованого доступу з боку диверсійних груп [20].

Організація системи контролю доступу на об'єктах КІ також має враховувати особливості їх функціонального призначення. Так, для об'єктів енергетичної сфери характерним є застосування систем контролю доступу,

інтегрованих з системами промислової автоматизації. На об'єктах транспортної інфраструктури системи контролю доступу мають забезпечувати можливість швидкого проходу значної кількості персоналу та пасажирів при збереженні необхідного рівня безпеки. Об'єкти водопостачання та водовідведення потребують організації систем контролю доступу з урахуванням розподіленого характеру таких об'єктів та наявності відокремлених елементів інфраструктури.

Окрім того, Онищенко С.В., Маслій О.А. та Дрібна А.В. звертають увагу на економічні аспекти організації систем контролю доступу на об'єктах КІ, підкреслюючи необхідність оптимального балансу між рівнем захисту та витратами на його забезпечення [21]. Це є особливо актуальним для об'єктів КІ нижчих категорій критичності, де економічна ефективність системи захисту має бути одним із ключових критеріїв її оцінки.

Павук І.В. та Кобилкін Д.С. акцентують увагу на необхідності застосування ризик-орієнтованого підходу до організації систем контролю доступу на об'єктах КІ [22]. Такий підхід передбачає оцінку ризиків, пов'язаних з порушенням режиму доступу, та впровадження заходів захисту, адекватних виявленим ризикам.

Таким чином, класифікація об'єктів критичної інфраструктури є основою для визначення особливостей організації систем контролю доступу на таких об'єктах. Врахування класифікаційних ознак об'єктів КІ дозволяє забезпечити диференційований підхід до їх захисту, реалізувати принцип "глибокого захисту" та оптимізувати витрати на забезпечення безпеки. Водночас, як зазначає Єрменчук О.П., класифікація об'єктів КІ не є статичною та має періодично переглядатися з урахуванням змін у зовнішньому середовищі та еволюції загроз [5].

1.3. Сучасні загрози безпеці об'єктів критичної інфраструктури та їх вплив на методи управління доступом

Ефективність методів управління доступом на об'єктах критичної інфраструктури значною мірою залежить від розуміння сучасних загроз їх безпеці та врахування цих загроз при розробці та впровадженні відповідних систем контролю. Аналіз наукових робіт та практичного досвіду у сфері захисту об'єктів КІ дозволяє виділити низку актуальних загроз, що мають безпосередній вплив на методи управління доступом.

Сучасні загрози безпеці об'єктів КІ характеризуються комплексним характером та стиранням меж між фізичними та кібернетичними загрозами. Як зазначає Суходоля О.М., в умовах гібридної війни спостерігається тенденція до застосування комбінованих атак на об'єкти КІ, які передбачають одночасне використання фізичних, кібернетичних, інформаційно-психологічних та інших типів впливу [23]. Це ставить нові вимоги до методів управління доступом, які мають забезпечувати комплексний захист об'єктів від різних типів загроз.

Батюк О.В. виділяє такі основні категорії загроз для об'єктів КІ: терористичні акти, диверсії, кібератаки, промисловий шпіонаж, внутрішні загрози, стихійні лиха та техногенні аварії [18]. Кожна з цих категорій загроз має свою специфіку та потребує відповідних методів протидії, в тому числі у сфері управління доступом.

Терористичні акти та диверсії становлять значну загрозу для об'єктів КІ, особливо в умовах збройного конфлікту. Кондратов С. підкреслює, що терористичні угруповання розглядають об'єкти КІ як пріоритетні цілі, оскільки атаки на такі об'єкти можуть призвести до значних людських жертв, економічних збитків та дестабілізації ситуації в країні [24]. Протидія таким загрозам потребує впровадження строгих процедур контролю доступу, включаючи перевірку персоналу та відвідувачів, контроль внесення/винесення предметів та транспортних засобів, застосування технічних засобів виявлення зброї, вибухівки та інших небезпечних предметів.

Кібератаки є однією з найбільш динамічно зростаючих загроз для об'єктів КІ. Горбаченко С.А. та Бойко В.Д. відзначають, що кібератаки на

об'єкти КІ стають все більш складними, цілеспрямованими та організованими [19]. Вони можуть бути спрямовані на порушення функціонування систем управління, викрадення чутливої інформації, блокування роботи сервісів або зміну параметрів технологічних процесів. Особливу небезпеку становлять кібератаки, що поєднуються з фізичним проникненням на об'єкт, оскільки такі комбіновані атаки можуть обходити традиційні системи захисту.

Внутрішні загрози, пов'язані з діями персоналу, також становлять значний ризик для безпеки об'єктів КІ. Як зазначають Франчук В.І., Пригунов П.Я. та Мельник С.І., персонал, що має легітимний доступ до об'єкта КІ, може свідомо або несвідомо становити загрозу для його безпеки [9]. Свідомі дії можуть бути пов'язані з корупцією, шпигунством, диверсіями або помстою, тоді як несвідомі – з помилками, недбалістю або недостатньою компетентністю. Протидія внутрішнім загрозам потребує впровадження принципу "розподілу відповідальності", регулярної перевірки персоналу, застосування багатофакторної аутентифікації та контролю дій користувачів.

Технологічні та природні загрози, такі як техногенні аварії, пожежі, повені, землетруси та інші стихійні лиха, також впливають на методи управління доступом на об'єктах КІ. В умовах надзвичайних ситуацій система управління доступом має забезпечувати можливість швидкої евакуації персоналу та доступу аварійно-рятувальних служб при збереженні необхідного рівня безпеки. Це потребує розробки спеціальних процедур та режимів роботи системи управління доступом для різних сценаріїв надзвичайних ситуацій.

Вплив сучасних загроз на методи управління доступом проявляється у необхідності впровадження комплексного підходу до захисту об'єктів КІ. Як зазначає Боярінова К., сучасні методи управління доступом мають бути інтегровані до загальної системи управління безпекою об'єкта та враховувати взаємозв'язок різних типів загроз [25]. Такий підхід дозволяє забезпечити цілісний захист об'єкта від різних типів загроз та мінімізувати ризики, пов'язані з порушенням режиму доступу.

Одним із ключових аспектів впливу сучасних загроз на методи управління доступом є необхідність впровадження багатофакторної аутентифікації. Традиційні методи аутентифікації, такі як паролі або електронні ключі, вже не забезпечують достатнього рівня захисту від сучасних загроз. Як зазначають Комаров М.Ю. та Гончар С.Ф., сучасні системи управління доступом на об'єктах КІ мають використовувати комбінацію різних факторів аутентифікації, таких як "щось, що ви знаєте" (паролі, PIN-коди), "щось, що ви маєте" (смарт-карти, токени) та "щось, що є частиною вас" (біометричні дані) [10].

Важливим аспектом є також використання методів аналізу поведінки користувачів та виявлення аномалій. Мохор В. та Цуркан В. підкреслюють, що сучасні системи управління доступом мають не лише контролювати факт доступу, але й аналізувати поведінку користувачів після отримання доступу, виявляти аномальні дії та реагувати на них [11]. Це дозволяє своєчасно виявляти несанкціоновані дії, навіть якщо вони здійснюються з використанням легітимних облікових записів та допусків.

Верголяс О. акцентує увагу на необхідності впровадження динамічних методів управління доступом, які враховують не лише статичні характеристики суб'єкта та об'єкта доступу, але й контекст запиту на доступ [6, с. 3]. Такі методи дозволяють враховувати такі фактори, як час доступу, місце запиту, історія попередніх доступів, поточний стан системи безпеки та інші контекстні параметри, що дозволяє підвищити точність прийняття рішень щодо надання або відмови у доступі.

Інтеграція фізичного та логічного контролю доступу є ще одним важливим трендом, обумовленим сучасними загрозами. Як зазначає Ящук В.І., традиційний підхід, при якому фізичний та логічний контроль доступу розглядаються як окремі системи, не відповідає характеру сучасних загроз [39, с. 4]. Інтеграція цих систем дозволяє реалізувати принцип "глибокого захисту" та забезпечити комплексну безпеку об'єкта.

Сучасні загрози також обумовлюють необхідність впровадження методів управління доступом, що базуються на оцінці ризиків. Павук І.В. та Кобилкін Д.С. підкреслюють, що такі методи дозволяють визначити рівень ризику, пов'язаний з конкретним запитом на доступ, та прийняти рішення щодо надання доступу з урахуванням цього ризику [22]. Це є особливо актуальним для об'єктів КІ, де порушення режиму доступу може мати критичні наслідки.

Окрему увагу слід приділити впливу загроз, пов'язаних з використанням соціальної інженерії. Як зазначає Криштанович М.Ф., методи соціальної інженерії, такі як фішинг, претекстинг, вішинг тощо, можуть бути використані для обходу технічних засобів контролю доступу шляхом маніпуляції персоналом [27]. Протидія таким загрозам потребує не лише технічних, але й організаційних заходів, включаючи навчання персоналу, впровадження чітких процедур перевірки запитів на доступ та регулярний аудит дотримання політик безпеки.

Важливим аспектом протидії сучасним загрозам є також застосування технологій штучного інтелекту та машинного навчання в системах управління доступом. Як зазначає Мельничук О.В., ці технології дозволяють автоматизувати процеси виявлення аномалій, прогнозування потенційних загроз та прийняття рішень щодо надання або відмови у доступі [4]. Це особливо актуально для об'єктів КІ, де необхідно обробляти значні обсяги даних про доступ та оперативно реагувати на потенційні загрози.

Зелена книга з питань захисту критичної інфраструктури в Україні звертає увагу на необхідність впровадження методів управління доступом, що забезпечують безперервність функціонування об'єктів КІ [28]. Це передбачає наявність резервних систем контролю доступу, процедур відновлення роботи після збоїв та можливість функціонування в деградованому режимі при частковому виході з ладу компонентів системи.

Бірюков Д.С. підкреслює, що методи управління доступом на об'єктах КІ мають враховувати можливість масштабних кібератак з використанням

нульових днів та інших передових технологій [29]. Це потребує впровадження підходу "нульової довіри" (Zero Trust), який передбачає постійну перевірку всіх запитів на доступ, незалежно від їх джерела та попередньої історії, та мінімізацію привілеїв доступу.

Єрменчук О.П. акцентує увагу на необхідності застосування методів управління доступом, що враховують міжгалузеві залежності між об'єктами КІ [5]. Це особливо актуально для об'єктів, функціонування яких критично залежить від інших об'єктів КІ, таких як енергопостачання, водопостачання, телекомунікації тощо. Порушення режиму доступу на одному об'єкті може призвести до каскадних ефектів та порушення функціонування залежних об'єктів.

Аналіз проведений Криштановичем М.Ф. показує, що сучасні методи управління доступом мають враховувати не лише технічні, але й організаційні аспекти забезпечення безпеки [27]. Це включає розробку політик безпеки, встановлення процедур контролю доступу, навчання персоналу, проведення регулярних перевірок та аудитів, а також оперативне реагування на інциденти безпеки.

Окрім того, Верголяс О. звертає увагу на необхідність адаптації методів управління доступом до специфіки конкретних об'єктів КІ, враховуючи їх функціональне призначення, категорію критичності, рівень загроз та інші фактори [26]. Це дозволяє забезпечити оптимальний баланс між рівнем захисту та зручністю використання системи, що є особливо важливим для об'єктів, де оперативність доступу є критичним фактором.

Таким чином, сучасні загрози безпеці об'єктів критичної інфраструктури мають значний вплив на методи управління доступом, обумовлюючи необхідність впровадження комплексного підходу до захисту, застосування багатофакторної аутентифікації, інтеграції фізичного та логічного контролю доступу, використання методів аналізу поведінки користувачів та інших передових технологій. Врахування характеру та специфіки цих загроз при

розробці та впровадженні систем управління доступом є необхідною умовою забезпечення безпеки об'єктів КІ в сучасних умовах.

Криштанович М.Ф. та співавтори у своїй монографії зазначають, що "в умовах зростання рівня загроз для об'єктів критичної інфраструктури особливої актуальності набуває розробка та впровадження адаптивних систем управління доступом, які здатні оперативно реагувати на зміни у зовнішньому середовищі та пристосовуватися до нових типів загроз" [27]. Такі системи мають базуватися на використанні технологій штучного інтелекту, машинного навчання та аналізу великих даних для виявлення нетипових патернів поведінки та потенційних загроз.

Важливим аспектом протидії сучасним загрозам є також використання методів управління доступом, що базуються на принципах мікросегментації та ізоляції критичних зон. Як зазначає Суходоля О.М., такий підхід дозволяє мінімізувати потенційний збиток від порушення режиму доступу шляхом обмеження можливості поширення атаки на інші сегменти об'єкта КІ [23]. Це є особливо актуальним для складних об'єктів КІ, які включають множину взаємопов'язаних підсистем та компонентів.

Забезпечення захисту об'єктів критичної інфраструктури від сучасних загроз потребує не лише технологічних рішень, але й формування відповідної культури безпеки серед персоналу. Як зазначають Франчук В.І. та співавтори, "культура безпеки є ключовим фактором ефективності системи управління доступом, оскільки навіть найсучасніші технічні засоби не забезпечать необхідного рівня захисту, якщо персонал не дотримується встановлених правил та процедур доступу" [9]. Формування такої культури потребує регулярного навчання персоналу, проведення тренінгів та практичних занять, а також стимулювання відповідального ставлення до питань безпеки.

Підсумовуючи розгляд сучасних загроз безпеці об'єктів критичної інфраструктури та їх впливу на методи управління доступом, можна констатувати, що ефективний захист таких об'єктів потребує комплексного підходу, який враховує різноманітність та взаємозв'язок загроз, специфіку

конкретних об'єктів КІ та тенденції розвитку технологій безпеки. Сучасні методи управління доступом мають забезпечувати не лише запобігання несанкціонованому доступу, але й виявлення та реагування на аномальну поведінку, що може свідчити про спроби порушення безпеки об'єкта. Такий підхід дозволить підвищити рівень захищеності об'єктів КІ та мінімізувати ризики, пов'язані з порушенням їх функціонування.

1.4 Висновки до розділу 1

Проведене у першому розділі дослідження дозволило сформувати комплексне бачення теоретичних і методологічних основ функціонування систем управління доступом на об’єктах критичної інфраструктури (КІ). З’ясовано, що поняття «критична інфраструктура» в сучасних умовах розглядається не лише як сукупність матеріальних об’єктів, необхідних для життєзабезпечення суспільства, а як складна система, вразливість якої має безпосередній вплив на національну безпеку, економічну стабільність і безперервність державного управління.

Нормативно-правова база, що регламентує захист КІ в Україні, на сьогодні формується у відповідності до сучасних загроз, зокрема в умовах гібридної війни та загострення кібербезпекових викликів. Прийняття Закону України «Про критичну інфраструктуру» та реалізація Концепції державної системи її захисту стали суттєвим кроком до систематизації вимог і процедур у цій галузі. Водночас аналіз показав, що існує потреба в подальшій гармонізації законодавства з міжнародними стандартами, насамперед у контексті інтеграції України до ЄС.

Окрему увагу в розділі приділено класифікації об’єктів КІ, що охоплює їх розподіл за функціональним призначенням, категоріями критичності та рівнем територіального значення. Така багатовимірна класифікація дозволяє не лише ідентифікувати рівень загроз, але й обґрунтовано визначати рівень

захисту та типи методів управління доступом, які мають застосовуватись для кожного конкретного об'єкта.

Розгляд сучасних загроз, які постають перед об’єктами КІ, дозволив зробити висновок про суттєве ускладнення безпекового середовища. Загрози мають як фізичний, так і кібернетичний характер і нерідко проявляються у формі комбінованих атак. Терористичні дії, диверсії, кібератаки, внутрішні порушення, техногенні аварії та соціальна інженерія вимагають від систем управління доступом високого рівня адаптивності, багаторівневості та інтегрованості.

Таким чином, теоретичний аналіз продемонстрував, що ефективна система управління доступом має будуватись на основі ризик-орієнтованого підходу, зонування території, диференціації рівнів доступу, застосування багатофакторної аутентифікації, а також враховувати поведінкові особливості користувачів. Теоретичні засади, викладені в першому розділі, стали підґрунтям для подальшого аналізу існуючих технологій та розробки удосконаленої моделі управління доступом.

РОЗДІЛ 2.
АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА ТЕХНОЛОГІЙ УПРАВЛІННЯ ДОСТУПОМ

2.1. Традиційні технології контролю фізичного доступу: переваги та недоліки

Традиційні технології контролю фізичного доступу становлять основу систем безпеки об'єктів критичної інфраструктури і продовжують широко використовуватися, незважаючи на появу більш сучасних методів. Ці технології пройшли тривалий шлях еволюції від простих механічних замків до складних електронних систем, проте зберігають свою актуальність завдяки надійності, відносній простоті експлуатації та економічній ефективності.

Історично першими і найбільш поширеними засобами контролю фізичного доступу були механічні пристрої, зокрема, різноманітні замки та ключі. Як зазначає Батюк О.В., попри свою простоту, механічні замки забезпечували базовий рівень захисту та могли бути організовані в системи "майстер-ключ", що дозволяли диференціювати доступ до різних зон об'єкта [18]. Проте механічні системи контролю доступу мають суттєві обмеження. Відповідно до досліджень Франчука В.І., такі системи складно масштабувати, вони не дозволяють вести облік подій доступу, не забезпечують можливості оперативної зміни прав доступу, а втрата ключа зазвичай вимагає заміни замка [9].

З розвитком електроніки у другій половині XX століття з'явилися електромеханічні системи контролю доступу, які поєднували механічні компоненти з електронними пристроями управління. Ці системи використовували електронні ключі, магнітні картки та кодові панелі, що дозволяло подолати деякі обмеження механічних систем. Як зауважує Єрменчук О.П., електромеханічні системи забезпечували можливість

централізованого управління доступом, ведення журналу подій та швидкої зміни прав доступу [5].

Наступним етапом розвитку традиційних технологій контролю фізичного доступу стало впровадження систем на основі безконтактних технологій, зокрема, RFID (Radio Frequency Identification) та NFC (Near Field Communication). Такі системи використовують радіочастотні мітки та зчитувачі, що дозволяють ідентифікувати користувача без фізичного контакту з пристроєм зчитування. За даними дослідження Мельничука О.В., системи на основі RFID та NFC забезпечують більш високий рівень зручності використання при збереженні необхідного рівня безпеки [4].

Важливим компонентом традиційних систем контролю фізичного доступу є також системи відеоспостереження, які дозволяють візуально контролювати доступ до об'єкта та його окремих зон. Як зазначають Комаров М.Ю. та Гончар С.Ф., інтеграція систем відеоспостереження з системами контролю доступу дозволяє забезпечити додатковий рівень верифікації особи, що отримує доступ, та фіксувати факти порушення режиму доступу [10].

Одним із ключових елементів традиційних систем контролю фізичного доступу є також системи фізичних бар'єрів, такі як шлюзові кабіни, турнікети, шлагбауми, які обмежують фізичний доступ до об'єкта та його окремих зон. Як зазначає Батюк О.В., фізичні бар'єри є невід'ємною складовою комплексної системи захисту об'єкта і виконують функцію фізичного обмеження доступу осіб, що не мають відповідних повноважень [18].

Традиційні технології контролю фізичного доступу мають низку переваг, які обумовлюють їх широке застосування на об'єктах критичної інфраструктури. По-перше, вони характеризуються високим рівнем надійності та стійкості до зовнішніх впливів. Як зазначає Ящук В.І., механічні та електромеханічні системи контролю доступу менш вразливі до електромагнітних впливів, перепадів напруги та кібератак порівняно з більш сучасними системами [17].

По-друге, традиційні технології контролю фізичного доступу зазвичай мають нижчу вартість впровадження та експлуатації порівняно з біометричними та іншими високотехнологічними системами. Це особливо актуально для об'єктів КІ нижчих категорій критичності, де економічна ефективність системи захисту є важливим критерієм її вибору. Онищенко С.В. зазначає, що для деяких типів об'єктів КІ використання традиційних технологій контролю доступу може забезпечити оптимальний баланс між рівнем захисту та витратами на його забезпечення [21].

По-третє, традиційні технології контролю фізичного доступу характеризуються високим рівнем сумісності з існуючою інфраструктурою об'єктів. Як зазначає Верголяс О., можливість поетапного впровадження та інтеграції з існуючими системами є важливою перевагою традиційних технологій, особливо для об'єктів КІ з тривалим терміном експлуатації [26].

Таблиця 2.1

Порівняльний аналіз традиційних технологій контролю фізичного доступу

Тип технології	**Принцип дії**	**Переваги**	**Недоліки**	**Сфери застосування**
Механічні замки	Використання фізичних ключів для розблокування механізму	Простота, надійність, низька вартість, незалежність від електроживлення	Неможливість логування подій, складність управління правами доступу, проблеми при втраті ключів	Об'єкти КІ нижчих категорій критичності, допоміжні приміщення, аварійні виходи
Кодові панелі	Введення цифрового/буквеного коду на клавіатурі	Відсутність необхідності в фізичних ключах, можливість зміни коду, низька вартість	Можливість підглядання коду, спільне використання коду кількома особами, відсутність ідентифікації конкретного користувача	Внутрішні приміщення з обмеженим доступом, додатковий рівень захисту

продовження таблиці 2.1

Картки з магнітною смугою	Зчитування інформації з магнітної смуги картки	Індивідуальна ідентифікація, можливість логування подій, централізоване управління	Знос картки, можливість клонування, необхідність фізичного контакту зі зчитувачем	Офісні будівлі, готелі, навчальні заклади
Проксіміті картки (RFID)	Безконтактне зчитування інформації за допомогою радіочастотного сигналу	Швидкість роботи, відсутність зносу, можливість інтеграції з іншими системами, зручність	Можливість перехоплення сигналу, вразливість до радіоперешкод, висока вартість інфраструктури	Об'єкти КІ середніх та високих категорій критичності, великі підприємства
Смарт-картки	Використання мікропроцесорної карти для аутентифікації	Високий рівень захисту, можливість шифрування даних, багатофункціональність, індивідуальна ідентифікація	Висока вартість, складність інфраструктури, вразливість до фізичного пошкодження	Банківський сектор, державні установи, об'єкти КІ високих категорій критичності
Системи відеоспостереження	Візуальний контроль доступу оператором через відеокамери	Постійний візуальний контроль, можливість запису та аналізу інцидентів, ідентифікація осіб	Залежність від оператора, великі обсяги даних, необхідність постійного моніторингу	Периметр об'єктів КІ, контрольно-пропускні пункти, зони підвищеного ризику

Водночас, традиційні технології контролю фізичного доступу мають ряд суттєвих недоліків, які обмежують їх ефективність в умовах сучасних загроз. Першим і найбільш суттєвим недоліком є вразливість до підробки або крадіжки засобів доступу. Як зазначає Криштанович М.Ф., фізичні ключі, картки та інші традиційні ідентифікатори можуть бути скопійовані, викрадені або передані неавторизованим особам, що створює ризики несанкціонованого доступу [27].

Другим суттєвим недоліком є низький рівень персоніфікації доступу. Традиційні технології не забезпечують однозначного зв'язку між ідентифікатором (ключем, карткою, кодом) та конкретною особою, що ускладнює контроль за доступом та розслідування інцидентів безпеки. Як зазначають Франчук В.І. та співавтори, "проблема передачі ідентифікаторів третім особам є однією з ключових вразливостей традиційних систем контролю доступу" [9].

Третім недоліком є обмежені можливості інтеграції з кібернетичними системами безпеки. Суходоля О.М. підкреслює, що в умовах конвергенції фізичних та кібернетичних загроз необхідною є інтеграція систем фізичного та логічного контролю доступу, що не завжди можливо реалізувати з використанням традиційних технологій [23].

Четвертим недоліком є обмежені можливості адаптації до змінних умов безпеки. Як зазначає Бірюков Д.С., традиційні системи контролю доступу часто мають статичну архітектуру та не здатні динамічно змінювати параметри роботи в залежності від рівня загроз, часу доби, аномальних подій тощо [29].

Отже, традиційні технології контролю фізичного доступу, незважаючи на свої переваги, не можуть повністю задовольнити потреби безпеки об'єктів критичної інфраструктури в умовах сучасних загроз. Вони потребують доповнення більш сучасними методами, такими як біометрична ідентифікація та комплексні системи управління доступом.

Таблиця 2.2

Ефективність традиційних технологій контролю фізичного доступу для різних категорій загроз

Категорія загрози	**Механічні замки**	**Кодові панелі**	**Картки з магнітною смугою**	**Проксіміті картки (RFID)**	**Смарт-картки**	**Системи відеоспостереження**

продовження таблиці 2.2

Несанкціоноване проникнення сторонніх осіб	Середня	Середня	Висока	Висока	Дуже висока	Висока
Крадіжка/підробка ідентифікаторів	Висока	Не застосовується	Низька	Середня	Висока	Не застосовується
Саботаж/вандалізм	Низька	Низька	Низька	Низька	Низька	Середня
Внутрішні загрози (авторизований персонал)	Низька	Низька	Середня	Середня	Середня	Висока
Технічні збої/відмови	Дуже висока	Низька	Середня	Середня	Середня	Низька
Кібератаки	Дуже висока	Середня	Низька	Низька	Середня	Низька
Соціальна інженерія/фішинг	Низька	Низька	Низька	Низька	Середня	Висока
Техногенні аварії/стихійні лиха	Висока	Низька	Середня	Середня	Середня	Низька

На основі аналізу, проведеного Яременком О.І. та Страхніцьким Я.О., можна визначити оптимальні сфери застосування традиційних технологій контролю фізичного доступу на об'єктах КІ [14]. Механічні замки та ключі залишаються ефективним рішенням для об'єктів КІ нижчих категорій критичності, а також як резервні системи доступу на випадок відмови електронних систем. Кодові панелі можуть використовуватися як додатковий рівень захисту у поєднанні з іншими технологіями. Картки з магнітною смугою, з огляду на їх вразливість до клонування та знос, поступово витісняються смарт-картками та проксіміті-картками на основі RFID-технології. Смарт-картки є оптимальним рішенням для об'єктів КІ високих категорій критичності, де необхідний високий рівень захисту та можливість інтеграції з іншими системами безпеки.

Аналіз літератури та практики застосування традиційних технологій контролю фізичного доступу свідчить про тенденцію до їх використання не як

самостійних рішень, а як компонентів комплексних систем безпеки, що включають також біометричні методи ідентифікації, системи аналізу поведінки, засоби відеоспостереження та інші технології. Така інтеграція дозволяє компенсувати недоліки традиційних технологій та забезпечити більш високий рівень захисту об'єктів критичної інфраструктури.

2.2. Біометричні системи ідентифікації та аутентифікації в управлінні доступом

Біометричні системи ідентифікації та аутентифікації представляють собою сучасний підхід до управління доступом, який базується на вимірюванні та аналізі унікальних фізіологічних або поведінкових характеристик людини. На відміну від традиційних технологій, які використовують зовнішні ідентифікатори (ключі, картки, паролі), біометричні системи забезпечують прямий зв'язок між фізичною особою та правами доступу, що суттєво підвищує рівень безпеки об'єктів критичної інфраструктури.

Основним принципом роботи біометричних систем є порівняння певної біометричної характеристики особи з еталонним зразком, що зберігається в базі даних системи. Як зазначає Мохор В., процес біометричної ідентифікації та аутентифікації включає наступні етапи: збір біометричних даних, обробка та виділення характерних ознак, порівняння з шаблонами в базі даних та прийняття рішення щодо надання або відмови у доступі [11].

За типом біометричних характеристик, що використовуються, системи біометричної ідентифікації поділяються на фізіологічні та поведінкові. Фізіологічні системи базуються на вимірюванні та аналізі таких характеристик, як відбитки пальців, геометрія руки, малюнок райдужної оболонки або сітківки ока, риси обличчя, голос тощо. Поведінкові системи аналізують такі характеристики, як почерк, клавіатурний почерк, хода, особливості мовлення та інші поведінкові патерни.

Відповідно до досліджень Батюка О.В., системи розпізнавання відбитків пальців є найбільш поширеним типом біометричних систем завдяки їх відносно низькій вартості, високій надійності та простоті використання [1, с. 205]. Такі системи можуть використовувати різні методи зчитування, включаючи оптичні, ємнісні, ультразвукові та термічні сканери. Кожен із цих методів має свої переваги та обмеження, що впливає на їх застосовність у різних умовах експлуатації.

Системи розпізнавання обличчя набувають все більшої популярності завдяки розвитку технологій комп'ютерного зору та алгоритмів машинного навчання. Як зазначає Горбаченко С.А., такі системи забезпечують неінвазивну ідентифікацію особи на відстані, що робить їх особливо зручними для використання на об'єктах з високою прохідністю [9, с. 26]. Проте ефективність систем розпізнавання обличчя може знижуватися під впливом таких факторів, як освітлення, кут зйомки, зміни у зовнішності особи (окуляри, борода, макіяж) тощо.

Системи розпізнавання райдужної оболонки та сітківки ока забезпечують надзвичайно високий рівень точності та захищеності від підробки. Франчук В.І. зазначає, що ймовірність помилкової ідентифікації для таких систем є надзвичайно низькою, що робить їх оптимальним вибором для об'єктів КІ високих категорій критичності [9]. Однак ці системи характеризуються високою вартістю та можуть викликати дискомфорт у користувачів через необхідність близького контакту з пристроєм сканування.

Системи розпізнавання голосу базуються на аналізі акустичних характеристик мовлення особи, таких як частота, тембр, темп мовлення тощо. Як зазначає Криштанович М.Ф., такі системи можуть використовуватися для віддаленої аутентифікації, наприклад, через телефонні лінії або інтернет, що є важливою перевагою для розподілених об'єктів КІ [10, с. 240]. Проте системи розпізнавання голосу можуть бути вразливими до шуму, змін голосу через хворобу або емоційний стан, а також до атак з використанням записів голосу.

Системи на основі інших біометричних характеристик, таких як геометрія руки, малюнок вен, термограма обличчя, електрокардіограма тощо, також знаходять застосування в управлінні доступом на об'єктах КІ, хоча і в меншому масштабі. Кожна з цих технологій має свої унікальні переваги та обмеження, що визначає доцільність їх застосування в конкретних умовах.

Поведінкові біометричні системи, які аналізують такі характеристики, як клавіатурний почерк, особливості ходи, жести та інші поведінкові патерни, є відносно новим напрямком у сфері біометричної ідентифікації. Суходоля О.М. підкреслює, що такі системи дозволяють здійснювати неперервну аутентифікацію користувача, на відміну від традиційних методів, які перевіряють ідентичність лише в момент надання доступу [23]. Це є особливо важливим для виявлення ситуацій, коли авторизований користувач підміняється неавторизованим після проходження процедури автентифікації.

Біометричні системи ідентифікації та аутентифікації мають низку значних переваг порівняно з традиційними технологіями контролю доступу. По-перше, вони забезпечують високий рівень персоніфікації доступу, оскільки біометричні характеристики є невід'ємними від особи та не можуть бути передані іншим особам або забуті, як паролі чи фізичні ідентифікатори. По-друге, біометричні системи характеризуються високим рівнем зручності використання, оскільки не вимагають від користувача запам'ятовування складних паролів або носіння фізичних ідентифікаторів. По-третє, вони забезпечують високу швидкість ідентифікації, що є важливим фактором для об'єктів з високою прохідністю.

Таблиця 2.3

Порівняльна характеристика основних типів біометричних систем

Тип біометричної системи	**Принцип роботи**	**Точність (FAR/FRR)***	**Переваги**	**Недоліки**	**Сфери застосування**

продовження таблиці 2.3

Розпізнавання відбитків пальців	Аналіз унікального малюнку папілярних ліній	0.1%/0.5%	Висока точність, низька вартість, компактність, швидкодія	Вразливість до забруднення, пошкоджень шкіри, можливість підробки	Доступ до приміщень, робочих станцій, сховищ даних
Розпізнавання обличчя	Аналіз геометрії та текстури обличчя	0.1%/1.0%	Неінвазивність, можливість ідентифікації на відстані, зручність	Залежність від освітлення, кута зйомки, змін зовнішності	Контроль доступу з високою прохідністю, відеоспостереження
Розпізнавання райдужної оболонки ока	Аналіз унікального малюнку райдужної оболонки	0.0001%/0.1%	Надзвичайно висока точність, стабільність характеристики, захищеність від підробки	Висока вартість, необхідність близького контакту з пристроєм	Високозахищені об'єкти КІ, банківські сховища
Розпізнавання сітківки ока	Аналіз малюнку кровоносних судин сітківки	0.0001%/0.1%	Найвища точність, неможливість підробки	Висока вартість, інвазивність, дискомфорт для користувачів	Об'єкти КІ найвищої категорії критичності
Розпізнавання голосу	Аналіз акустичних характеристик мовлення	2.0%/5.0%	Можливість віддаленої аутентифікації, низька вартість	Вразливість до шуму, змін голосу, можливість запису	Телефонний банкінг, віддалений доступ до систем
Розпізнавання геометрії руки	Аналіз розмірів та форми руки	0.1%/1.0%	Швидкість, зручність, стійкість до забруднення	Невисока точність, великі розміри пристрою	Об'єкти з середнім рівнем захисту, тимчасовий доступ
Розпізнавання малюнку вен	Інфрачервоне сканування малюнку вен	0.0008%/0.01%	Висока точність, неможливість підробки, гігієнічність	Висока вартість, чутливість до температури	Медичні заклади, фінансові установи
Клавіатурний почерк	Аналіз динаміки набору тексту	5.0%/10.0%	Неперервна аутентифікація, низька вартість	Невисока точність, залежність від емоційного стану	Додатковий рівень захисту інформаційних систем

*FAR - коефіцієнт помилкового доступу (False Acceptance Rate), FRR - коефіцієнт помилкової відмови (False Rejection Rate)

Водночас, біометричні системи мають і певні недоліки та обмеження. Першим і найбільш суттєвим недоліком є можливість помилок ідентифікації, які можуть бути двох типів: помилка першого роду (False Rejection Rate, FRR) — відмова в доступі авторизованому користувачу, та помилка другого роду (False Acceptance Rate, FAR) — надання доступу неавторизованому користувачу. Мельничук О.В. зазначає, що оптимальне налаштування біометричної системи передбачає пошук балансу між цими двома типами помилок, який залежить від специфіки об'єкта та вимог до його безпеки [4].

Другим недоліком є вартість впровадження та експлуатації біометричних систем, яка зазвичай перевищує вартість традиційних технологій контролю доступу. Це обмежує їх застосування на об'єктах КІ нижчих категорій критичності, де співвідношення витрат та рівня захисту є важливим фактором. Онищенко С.В. та співавтори підкреслюють, що рішення про впровадження біометричних систем має прийматися на основі аналізу ризиків та оцінки потенційних збитків від порушення режиму доступу [21].

Третім недоліком є можливість підробки біометричних характеристик, хоча й з різним ступенем складності для різних типів систем. Наприклад, системи розпізнавання відбитків пальців можуть бути обмануті за допомогою штучних відбитків, виготовлених з різних матеріалів, а системи розпізнавання обличчя — за допомогою фотографій або відеозаписів. Як зазначає Горбаченко С.А., сучасні біометричні системи включають механізми виявлення спроб підробки (liveness detection), такі як аналіз пульсації крові, тепловізійний аналіз, детекція руху тощо, які значно підвищують їх захищеність від спроб обману [19].

Четвертим недоліком є конфіденційність та правові аспекти використання біометричних даних. Збір, зберігання та обробка біометричних даних підпадають під дію законодавства про захист персональних даних та потребують відповідних заходів для забезпечення їх конфіденційності. Як зазначає Єрменчук О.П., впровадження біометричних систем ідентифікації

має супроводжуватися розробкою відповідних політик і процедур, які визначають порядок збору, зберігання, обробки та захисту біометричних даних, а також права суб'єктів персональних даних щодо доступу до своїх даних, їх виправлення або видалення [5].

П'ятим недоліком є залежність ефективності біометричних систем від умов експлуатації та стану біометричних характеристик користувачів. Наприклад, ефективність систем розпізнавання обличчя може знижуватися при поганому освітленні або зміні зовнішності користувача, а системи розпізнавання відбитків пальців можуть мати проблеми з ідентифікацією осіб з пошкодженнями шкіри або відсутніми пальцями. Теленик С.С. підкреслює необхідність врахування цих обмежень при проектуванні систем контролю доступу та забезпечення альтернативних методів ідентифікації для осіб, які не можуть використовувати основний біометричний метод [8].

Важливим аспектом впровадження біометричних систем на об'єктах критичної інфраструктури є вибір оптимального типу біометричної системи та її архітектури відповідно до специфіки об'єкта та вимог до його безпеки. Як зазначає Павук І.В., для об'єктів КІ високих категорій критичності доцільним є застосування мультимодальних біометричних систем, які використовують кілька біометричних характеристик для підвищення точності ідентифікації та стійкості до підробки [22].

Архітектура біометричної системи може бути централізованою або розподіленою. При централізованій архітектурі всі біометричні шаблони зберігаються в центральній базі даних, а термінали здійснюють лише збір біометричних даних та їх передачу на центральний сервер для порівняння. При розподіленій архітектурі біометричні шаблони зберігаються на локальних терміналах або на персональних носіях користувачів (смарт-картах, токенах), що зменшує ризики, пов'язані з централізованим зберіганням чутливих даних. Як зазначає Мохор В., вибір архітектури має враховувати вимоги до безпеки, масштабованості, надійності та економічної ефективності системи [11].

Для об'єктів критичної інфраструктури особливе значення має інтеграція біометричних систем з іншими компонентами системи безпеки, такими як системи відеоспостереження, контролю периметра, виявлення вторгнень тощо. Така інтеграція дозволяє забезпечити комплексний захист об'єкта та реалізувати принцип глибокої оборони. Як зазначають Комаров М.Ю. та Гончар С.Ф., інтеграція біометричних систем з системами фізичної безпеки та кібербезпеки є ключовим фактором забезпечення стійкості об'єктів КІ до сучасних загроз [10].

Таблиця 2.4

Відповідність біометричних систем вимогам безпеки об'єктів критичної інфраструктури різних категорій

Категорія об'єкта КІ	**Рекомендовані типи біометричних систем**	**Архітектура**	**Додаткові вимоги**	**Інтеграція з іншими системами**	**Режим роботи**
Перша категорія (найвища)	Райдужна оболонка, сітківка ока, мультимодальні системи	Розподілена з шифруванням	Резервування, дублювання каналів зв'язку, автономне живлення	Повна інтеграція з СКУД, СВН, СКП*	Багатофакторна аутентифікація
Друга категорія	Відбитки пальців, райдужна оболонка, малюнок вен, мультимодальні системи	Централізована з розподіленим резервуванням	Резервне копіювання, автономне живлення	Інтеграція з СКУД, СВН	Багатофакторна аутентифікація
Третя категорія	Відбитки пальців, геометрія руки, розпізнавання обличчя	Централізована	Резервне копіювання	Інтеграція з СКУД	Двофакторна аутентифікація
Четверта категорія	Відбитки пальців, розпізнавання обличчя	Централізована	Стандартні заходи безпеки	Базова інтеграція з СКУД	Однофакторна або двофакторна аутентифікація

продовження таблиці 2.4

П'ята категорія (найнижча)	Відбитки пальців, розпізнавання обличчя (опційно)	Локальна	Стандартні заходи безпеки	Опційна інтеграція	Однофакторна аутентифікація

Аналіз літератури та практики застосування біометричних систем на об'єктах критичної інфраструктури дозволяє зробити висновок, що ці системи є ефективним засобом підвищення рівня безпеки, однак їх впровадження має здійснюватися з урахуванням специфіки об'єкта, характеру загроз та економічних факторів. Як зазначає Батюк О.В., оптимальним підходом є поєднання біометричних методів з традиційними технологіями контролю доступу в рамках комплексної системи безпеки, що дозволяє компенсувати недоліки окремих технологій та забезпечити необхідний рівень захисту об'єкта КІ [18].

Тенденції розвитку біометричних систем ідентифікації та аутентифікації включають впровадження штучного інтелекту та машинного навчання для підвищення точності розпізнавання та виявлення спроб підробки, розробку нових біометричних модальностей (наприклад, на основі аналізу електрокардіограми, електроенцефалограми, тощо), мініатюризацію та зниження вартості біометричних сенсорів, а також розвиток стандартів інтероперабельності, що дозволяє інтегрувати біометричні системи різних виробників. Ці тенденції відкривають нові можливості для підвищення рівня безпеки об'єктів критичної інфраструктури та ефективності систем управління доступом.

2.3. Комплексні системи управління доступом та їх інтеграція з іншими системами безпеки

Комплексні системи управління доступом (КСУД) представляють собою інтегровані рішення, які поєднують різноманітні технології контролю

доступу, програмне забезпечення та організаційні заходи для забезпечення всебічного захисту об'єктів критичної інфраструктури. Такі системи є відповіддю на зростаючу складність та різноманітність загроз безпеці, які вимагають комплексного підходу до управління доступом.

Згідно з визначенням Ящука В.І., комплексна система управління доступом є "сукупністю програмно-технічних засобів та організаційних заходів, спрямованих на контроль та управління доступом суб'єктів до об'єктів доступу відповідно до встановлених політик безпеки" [17]. Ключовою особливістю КСУД є інтеграція фізичного та логічного контролю доступу, що дозволяє забезпечити комплексний захист як матеріальних, так і інформаційних ресурсів об'єкта.

Архітектура КСУД зазвичай включає кілька рівнів: рівень пристроїв контролю доступу (зчитувачі, контролери, замки, турнікети тощо), рівень комунікацій (мережі передачі даних), рівень серверів та баз даних, рівень управління та адміністрування, а також рівень інтеграції з іншими системами безпеки. Як зазначає Мельничук О.В., така багаторівнева архітектура забезпечує гнучкість, масштабованість та відмовостійкість системи, що є критично важливим для об'єктів КІ [16].

Основними функціональними компонентами КСУД є: підсистема ідентифікації та аутентифікації, підсистема авторизації, підсистема моніторингу та аудиту, підсистема управління політиками безпеки, підсистема звітності та аналітики. Верголяс О. підкреслює, що саме інтеграція цих компонентів у єдину систему дозволяє реалізувати принцип "глибокого захисту" та забезпечити комплексну безпеку об'єкта КІ [26].

Підсистема ідентифікації та аутентифікації відповідає за встановлення та підтвердження особи суб'єкта доступу. Вона може використовувати різні технології, включаючи традиційні методи (паролі, смарт-карти) та біометричні технології, які були розглянуті у попередніх підрозділах. Як зазначає Батюк О.В., для об'єктів КІ високих категорій критичності

рекомендовано застосування багатофакторної аутентифікації, яка поєднує кілька методів для підвищення надійності ідентифікації [18].

Підсистема авторизації визначає, до яких ресурсів має доступ ідентифікований суб'єкт, на основі встановлених політик безпеки. Вона може реалізовувати різні моделі контролю доступу, такі як дискреційна модель (Discretionary Access Control, DAC), мандатна модель (Mandatory Access Control, MAC), рольова модель (Role-Based Access Control, RBAC) або атрибутивна модель (Attribute-Based Access Control, ABAC). Комаров М.Ю. та Гончар С.Ф. зазначають, що для об'єктів КІ найбільш ефективною є комбінація рольової та атрибутивної моделей, яка дозволяє гнучко визначати права доступу на основі ролей суб'єктів та атрибутів об'єктів [10].

Підсистема моніторингу та аудиту забезпечує контроль за подіями доступу, виявлення аномалій та реагування на інциденти безпеки. Вона фіксує всі спроби доступу (як успішні, так і невдалі), дії користувачів у системі, зміни в налаштуваннях тощо. Мохор В. та Цуркан В. підкреслюють важливість цієї підсистеми для виявлення спроб несанкціонованого доступу та розслідування інцидентів безпеки [11].

Підсистема управління політиками безпеки дозволяє адміністраторам визначати та змінювати правила доступу до різних ресурсів системи. Як зазначає Криштанович М.Ф., політики безпеки мають бути достатньо гнучкими, щоб адаптуватися до змінних умов експлуатації та рівня загроз, але водночас достатньо строгими, щоб забезпечити необхідний рівень безпеки [27].

Підсистема звітності та аналітики забезпечує збір, обробку та аналіз даних про функціонування системи управління доступом. Вона дозволяє формувати різноманітні звіти (про події доступу, інциденти безпеки, статистику використання ресурсів тощо), проводити аналіз тенденцій та виявляти потенційні проблеми. Як зазначає Суходоля О.М., аналітичні можливості КСУД є критично важливими для проактивного підходу до забезпечення безпеки об'єктів КІ [23].

Однією з ключових особливостей КСУД є їх інтеграція з іншими системами безпеки, такими як системи відеоспостереження, охоронної сигналізації, пожежної безпеки, виявлення вторгнень тощо. Така інтеграція дозволяє забезпечити синергетичний ефект та підвищити загальний рівень безпеки об'єкта КІ. Наприклад, інтеграція з системою відеоспостереження дозволяє автоматично записувати відео при спробах несанкціонованого доступу, а інтеграція з системою пожежної безпеки забезпечує автоматичне розблокування дверей у разі пожежі.

Таблиця 2.5

Інтеграція комплексних систем управління доступом з іншими системами безпеки

Система безпеки	**Типи інтеграції**	**Функціональні можливості**	**Переваги інтеграції**	**Технічні аспекти**	**Приклади застосування**
Системи відеоспостереження	Програмна, апаратна, комбінована	Відеоверифікація подій доступу, автоматичний запис при тривогах, відеоаналітика	Підвищення рівня верифікації, візуальне підтвердження інцидентів, доказова база	API, SDK, інтеграційні платформи, спільне сховище даних	Контрольно-пропускні пункти, периметр, критичні зони
Системи охоронної сигналізації	Програмна, апаратна	Блокування доступу при тривозі, автоматичне взяття/зняття з охорони	Зменшення людського фактору, автоматизація процесів безпеки, зниження помилкових тривог	Протоколи інтеграції, релейні виходи, програмні інтерфейси	Периметр об'єкта, зони обмеженого доступу, сховища
Системи пожежної безпеки	Апаратна	Розблокування дверей при пожежі, контроль евакуації, облік персоналу	Забезпечення безпечної евакуації, відповідність нормативним вимогам	Інтерфейси "сухий контакт", спеціалізовані контролери	Евакуаційні виходи, маршрути евакуації

продовження таблиці 2.5

Системи виявлення вторгнень	Програмна	Кореляція подій доступу з мережевими подіями, підвищення рівня захисту при загрозі	Виявлення комплексних атак, зниження кількості помилкових спрацювань	SIEM-системи, API, агенти інтеграції	Серверні приміщення, центри обробки даних
Системи управління інцидентами	Програмна	Автоматичне створення інцидентів, оповіщення персоналу	Пришвидшення реагування на інциденти, автоматизація процесів	API, веб-сервіси, інтеграційні шини	Ситуаційні центри, диспетчерські
Системи обліку робочого часу	Програмна	Облік присутності, розрахунок робочого часу	Зниження адміністративних витрат, підвищення дисципліни	Спільна база даних, API	Адміністративні будівлі, офіси
Системи управління будівлею (BMS)	Програмна, апаратна	Управління освітленням, кліматом в залежності від присутності	Енергоефективність, комфорт, автоматизація	BACnet, Modbus, OPC, KNX	Інтелектуальні будівлі, енергоефективні об'єкти
Системи фізичної безпеки периметра	Апаратна, програмна	Інтеграція з датчиками периметра, шлагбаумами, воротами	Комплексний захист периметра, автоматизація контролю	Інтерфейси "сухий контакт", спеціалізовані контролери	Периметр об'єкта, контрольно-пропускні пункти

Окрім інтеграції з іншими системами безпеки, КСУД можуть також інтегруватися з корпоративними інформаційними системами, такими як системи управління персоналом, системи обліку робочого часу, системи управління ідентифікаційними даними (Identity Management Systems, IDM) тощо. Як зазначає Ящук В.І., така інтеграція дозволяє автоматизувати процеси управління доступом та знизити адміністративні витрати [17]. Наприклад, інтеграція з системою управління персоналом забезпечує автоматичне надання та відкликання прав доступу при прийомі, переведенні або звільненні співробітників.

Важливим аспектом впровадження КСУД на об'єктах критичної інфраструктури є забезпечення їх відмовостійкості та безперервності функціонування. Як зазначає Суходоля О.М., системи управління доступом на об'єктах КІ мають функціонувати навіть в умовах часткової відмови компонентів або зовнішніх впливів, таких як відключення електроживлення, пошкодження комунікаційних каналів, кібератаки тощо [23]. Це досягається шляхом впровадження надлишковості, резервування критичних компонентів, використання автономних джерел живлення, розподіленої архітектури та інших методів забезпечення відмовостійкості.

Для об'єктів КІ високих категорій критичності рекомендовано використання розподіленої архітектури КСУД, яка забезпечує функціонування системи навіть при відмові центрального сервера або пошкодженні комунікаційних каналів. Як зазначає Мельничук О.В., в такій архітектурі локальні контролери доступу зберігають необхідну інформацію про права доступу та можуть працювати автономно, синхронізуючись з центральним сервером при відновленні зв'язку [16].

Важливим аспектом КСУД є також забезпечення їх кібербезпеки, оскільки такі системи самі можуть стати об'єктом кібератак. Горбаченко С.А. та Бойко В.Д. підкреслюють необхідність впровадження механізмів захисту від несанкціонованого доступу до компонентів КСУД, шифрування комунікацій, регулярного оновлення програмного забезпечення та проведення тестування на проникнення для виявлення та усунення вразливостей [19].

Впровадження КСУД на об'єктах критичної інфраструктури має здійснюватися на основі ризик-орієнтованого підходу, який передбачає оцінку ризиків, пов'язаних з порушенням режиму доступу, та впровадження заходів захисту, адекватних виявленим ризикам. Павук І.В. та Кобилкін Д.С. зазначають, що такий підхід дозволяє оптимізувати витрати на забезпечення безпеки та зосередити ресурси на захисті найбільш критичних активів [22].

Для забезпечення ефективності КСУД важливе значення має також розробка та впровадження відповідних політик і процедур, які визначають

правила доступу до різних ресурсів, процедури надання та відкликання прав доступу, обов'язки та відповідальність персоналу, процедури реагування на інциденти безпеки тощо. Як зазначає Бірюков Д.С., політики та процедури контролю доступу мають бути узгоджені із загальною політикою безпеки організації та відповідати вимогам нормативних документів [29].

Таблиця 2.6

Рекомендації щодо впровадження комплексних систем управління доступом на об'єктах КІ різних категорій

Категорія об'єкта КІ	**Архітектура КСУД**	**Методи аутентифікації**	**Модель контролю доступу**	**Інтеграція з іншими системами**	**Забезпечення відмовостійкості**	**Кібербезпека**
Перша категорія (найвища)	Розподілена	Багатофакторна з використанням біометрії	Комбінована (RBAC+ABAC)	Повна інтеграція з усіма системами безпеки	Повне резервування, N+1 надлишковість, автономне живлення 72+ годин	Сегментація мережі, шифрування, регулярний пентест
Друга категорія	Розподілена	Багатофакторна	Рольова (RBAC)	Інтеграція з основними системами безпеки	Резервування критичних компонентів, автономне живлення 24+ годин	Шифрування, розмежування доступу, VLAN
Третя категорія	Централізована з локальним резервуванням	Двофакторна	Рольова (RBAC)	Інтеграція з СВН, СОС, СПБ*	Резервне копіювання, автономне живлення 8+ годин	Базові заходи кібербезпеки
Четверта категорія	Централізована	Однофакторна або двофакторна	Дискреційна (DAC)	Базова інтеграція з СВН та СПБ	Стандартні заходи резервування	Базові заходи кібербезпеки
П'ята категорія (найнижча)	Локальна	Однофакторна	Дискреційна (DAC)	Мінімальна інтеграція	Базові заходи резервування	Базовий антивірусний захист

Аналіз літератури та практики впровадження КСУД на об'єктах критичної інфраструктури свідчить про тенденцію до використання адаптивних систем управління доступом, які здатні динамічно змінювати параметри роботи в залежності від рівня загроз, часу доби, аномальних подій тощо. Як зазначає Верголяс О., такі системи використовують методи штучного інтелекту та машинного навчання для аналізу патернів доступу, виявлення аномалій та прогнозування потенційних загроз [26].

Іншою важливою тенденцією є впровадження концепції "нульової довіри" (Zero Trust) в системах управління доступом. Ця концепція передбачає постійну перевірку всіх запитів на доступ, незалежно від їх джерела та попередньої історії, та мінімізацію привілеїв доступу. Як зазначає Суходоля О.М., концепція "нульової довіри" є особливо актуальною для об'єктів КІ в умовах зростання кількості та складності кібератак [23].

Також спостерігається тенденція до використання хмарних технологій та сервісів для управління доступом (Access Control as a Service, ACaaS). Проте, як зазначає Батюк О.В., для об'єктів КІ високих категорій критичності використання хмарних рішень може бути обмеженим через вимоги до конфіденційності даних та безперервності функціонування [18].

Підсумовуючи, можна зазначити, що комплексні системи управління доступом є ефективним засобом забезпечення безпеки об'єктів критичної інфраструктури в умовах сучасних загроз. Вони дозволяють реалізувати принцип "глибокого захисту", забезпечити інтеграцію фізичного та логічного контролю доступу, автоматизувати процеси управління доступом та підвищити загальний рівень безпеки об'єкта. Впровадження таких систем має здійснюватися на основі ризик-орієнтованого підходу з урахуванням специфіки об'єкта, характеру загроз та економічних факторів.

2.4. Аналіз недоліків та обмежень існуючих систем управління доступом

Попри активне впровадження інноваційних рішень у сфері управління доступом, сучасні системи, які застосовуються на об’єктах критичної інфраструктури, все ще мають низку обмежень. Ці недоліки не завжди очевидні на етапі впровадження, однак у реальних умовах експлуатації можуть суттєво впливати на безперебійність роботи об'єкта та загальний рівень безпеки. Тому їх ґрунтовний аналіз є необхідним для формування ефективної стратегії безпеки.

Однією з найпоширеніших проблем є обмежена масштабованість систем контролю доступу. У багатьох випадках об’єкти критичної інфраструктури розвиваються поступово, розширюють свою площу або змінюють функціональне призначення окремих зон. Системи, які були ефективними у початковій конфігурації, часто не можуть адаптуватися до нових вимог без суттєвих фінансових та технічних витрат. Крім того, обмеження в кількості одночасно підключених точок доступу або користувачів можуть створити ситуації, коли система перестає відповідати потребам об’єкта.

Ще однією критичною проблемою є відсутність сумісності між рішеннями різних виробників. У випадках, коли система формується з компонентів різних технологічних лінійок або має інтегруватися з іншими інженерними системами, наприклад системами відеоспостереження або пожежної сигналізації, виникають технічні труднощі. Інколи повна сумісність взагалі неможлива без дорогих проміжних рішень, що ускладнює адміністрування та збільшує ризики помилок при експлуатації.

Зручність користування також не завжди враховується належним чином при проєктуванні систем управління доступом. Наприклад, у разі використання багатофакторної автентифікації (біометрія, RFID-картки та PIN-коди), процедура доступу може займати надто багато часу, що створює черги на проходження, особливо у години пік. У надзвичайних ситуаціях, коли потрібна швидка евакуація або оперативне втручання аварійних служб, така надмірна складність може призвести до небажаних наслідків.

Таблиця 2.7

Порівняльна ефективність основних типів систем управління доступом у штатному та аварійному режимах

Тип системи	**Штатна ситуація**	**Аварійна ситуація**	**Спроба злому**	**Коментар**
Механічні замки	Середня	Висока	Низька	Прості у використанні, але не дозволяють вести облік подій.
RFID-картки	Висока	Низька	Середня	Зручні, але залежать від електрики та можуть бути клоновані.
Біометрія	Висока	Середня	Висока	Найбільш надійна, але дорога і чутлива до зовнішніх умов.
PIN-коди	Середня	Середня	Низька	Можуть бути зламані або вгадані, низький рівень індивідуальності.
Інтегровані системи	Дуже висока	Середня	Дуже висока	Максимальна безпека, але складність обслуговування.

Також важливою є проблема енергозалежності. Більшість сучасних систем контролю доступу працюють від електромережі і не мають автономного режиму роботи. При відключенні електроенергії навіть на короткий час система може повністю вийти з ладу, унеможливлюючи доступ як персоналу, так і служб порятунку. Наявність джерел безперебійного живлення частково вирішує цю проблему, однак їхня автономність часто обмежена, а технічне обслуговування потребує додаткових витрат.

Розглядаючи ефективність різних типів систем управління доступом у реальних умовах, доцільно навести порівняльну характеристику для трьох

типових ситуацій: штатна експлуатація, аварійна ситуація (наприклад, відключення електроенергії) та спроба злому. Це дозволяє краще зрозуміти сильні та слабкі сторони кожної технології та визначити їх доцільність у тій чи іншій конфігурації безпеки.

Жодна з розглянутих систем не є універсальною. Кожен тип має свої переваги та вразливі місця, які проявляються залежно від контексту використання. Наприклад, механічні системи залишаються надійними при повній втраті живлення, але не здатні протистояти сучасним загрозам. Натомість біометричні технології забезпечують високий рівень безпеки та персоніфікації, але потребують енергопостачання та високих витрат на впровадження.

Найбільш збалансованим підходом у сучасних умовах є впровадження інтегрованих систем доступу, які поєднують декілька методів і забезпечують як високий рівень безпеки, так і гнучкість у разі змін середовища чи загроз. Однак успішне впровадження таких систем вимагає не лише фінансових ресурсів, а й відповідного рівня технічної грамотності персоналу, регулярного аудиту безпеки та адаптації до змін у нормативному полі.

2.5. Практичний огляд використання систем управління доступом на об'єктах критичної інфраструктури в Україні

У цьому підрозділі детально розглянемо практичний досвід впровадження та функціонування СКД на об’єктах критичної інфраструктури України. Оскільки питання безпеки в умовах сучасних загроз набуває особливої актуальності, важливо не лише теоретично описати технології, а й проаналізувати, як вони працюють у реальних умовах, з якими труднощами стикаються організації та які рішення знаходять для подолання бар’єрів.

Сфера енергетики традиційно вважається однією з найважливіших галузей критичної інфраструктури, і саме тут найчастіше впроваджуються багаторівневі системи доступу. Наприклад, на Південноукраїнській та

Рівненській АЕС було реалізовано кількаступеневу модель контролю доступу: спершу відбувається зовнішня ідентифікація транспортного засобу, далі — перевірка особистості водія через RFID-картку та біометричну верифікацію, і лише після цього відкривається доступ до контрольованої зони. Система реєструє всі події, а аналіз даних дозволяє виявляти аномалії у поведінці персоналу.

Особливістю енергетичних об’єктів є також наявність великої кількості персоналу, який змінюється позмінно, у тому числі в нічний час. Це потребує не лише автоматизації процесів, але й високої стійкості СКД до відмов. Усі критичні компоненти дублюються, і навіть у разі втрати зв’язку з центральною базою даних доступ до об’єкта регулюється локально, на основі кешованих даних про користувачів.

На транспортних вузлах, зокрема в аеропортах та великих залізничних вокзалах, основна увага приділяється відмежуванню зон загального користування та обмеженого доступу. Так, в аеропорту «Бориспіль» доступ до злітно-посадкових смуг, диспетчерських пунктів та вантажних ангарів здійснюється через зчитувачі смарт-карток з PIN-ідентифікацією. У деяких секторах використовуються сканери обличчя, встановлені на турнікетах. Це дозволяє значно скоротити час проходження і водночас забезпечити персоніфіковану реєстрацію.

Водночас, як свідчать аудиторські перевірки, у багатьох випадках основною проблемою залишається людський фактор: порушення регламенту з боку співробітників (наприклад, передача картки іншій особі), недбалість охоронного персоналу або недостатнє технічне обслуговування обладнання. Ці чинники суттєво знижують ефективність навіть найсучасніших СКД.

У медичному секторі впровадження систем доступу відбувається значно повільніше, що пояснюється як технічними, так і фінансовими чинниками. Більшість регіональних лікарень усе ще користуються механічними замками та ручною реєстрацією входів/виходів персоналу. Водночас у великих лікарнях, зокрема в Києві, Дніпрі та Львові, впроваджуються електронні

системи з розмежуванням прав доступу: лікарі мають доступ до всіх відділень, медсестри — лише до своїх робочих секторів, а сторонні особи не мають змоги потрапити до критичних зон.

Цікавим є також досвід медичних закладів, які беруть участь у міжнародних грантових програмах. Наприклад, в одному з київських онкологічних центрів було реалізовано пілотний проєкт системи доступу на основі мобільного додатку з QR-кодами та динамічною автентифікацією. Це рішення дозволяє відмовитись від фізичних носіїв і одночасно забезпечити високий рівень захисту медичних даних.

Попри успіхи, процес впровадження СКД в Україні все ще залишається нерівномірним. Серед інституційних бар'єрів можна виділити насамперед відсутність єдиної національної політики у сфері доступу до об'єктів критичної інфраструктури. Більшість систем проєктуються і впроваджуються локально, що створює проблему несумісності, обмежує можливості масштабування і знижує ефективність централізованого моніторингу.

Фінансування також виступає ключовим обмеженням. Вартість сучасних інтегрованих систем із хмарною аналітикою, біометричними модулями, централізованим журналюванням подій може сягати мільйонів гривень, що є недосяжним для багатьох державних установ. Крім того, закупівлі часто відбуваються за застарілими стандартами, які не відповідають сучасним вимогам.

Підсумовуючи викладене, можна зробити висновок, що в Україні наявні як позитивні приклади впровадження ефективних СКД на об'єктах КІ, так і численні виклики, що стримують поширення таких рішень. Для забезпечення системного підходу необхідне формування єдиної нормативно-правової бази, розвиток ринку національних виробників безпекових технологій, стимулювання державно-приватного партнерства та регулярний аудит ефективності вже впроваджених рішень.

2.6 Висновки до розділу 2

У другому розділі здійснено комплексний огляд та критичний аналіз існуючих технологій управління доступом, які використовуються на об'єктах критичної інфраструктури. Розгляд охопив як традиційні методи фізичного контролю, так і сучасні біометричні та інтегровані системи, що поєднують елементи фізичної, логічної та інформаційної безпеки.

Досліджено переваги та недоліки традиційних технологій, зокрема механічних замків, кодових панелей, магнітних і безконтактних карток. Встановлено, що попри певну надійність та економічну доцільність, ці методи не забезпечують належного рівня захисту в умовах сучасних гібридних загроз. Особливою проблемою є відсутність персоніфікації доступу, уразливість до втрати або крадіжки ідентифікаторів, а також обмежена здатність до інтеграції з іншими компонентами систем безпеки.

Окрема увага приділена аналізу біометричних систем, які забезпечують високий рівень ідентифікації користувачів на основі фізіологічних або поведінкових характеристик. Системи розпізнавання відбитків пальців, обличчя, сітківки ока, голосу та геометрії руки продемонстрували високу точність, проте вимагають високих витрат на впровадження та обслуговування. Додатково, досліджено показники FAR і FRR як ключові метрики ефективності біометричної аутентифікації.

Особливе місце у структурі дослідження займає огляд комплексних систем управління доступом (СКУД), які поєднують функції фізичного контролю, відеоспостереження, охоронної сигналізації та пожежної безпеки. Зроблено висновок, що саме такі системи здатні ефективно функціонувати в умовах підвищених ризиків та складної інфраструктури. Однак виявлено, що на практиці інтеграція таких систем в Україні часто залишається обмеженою через фрагментарність реалізації, відсутність єдиних стандартів і ресурсні обмеження.

Практичний аналіз застосування систем управління доступом на об'єктах КІ в Україні дозволив виявити типові проблеми: недостатній рівень стандартизації, застарілі технології, обмежений функціонал існуючих рішень, а також слабку інтеграцію між фізичним та логічним доступом. Усе це вказує на потребу в розробці нової моделі управління доступом, що буде відповідати сучасним вимогам і загрозам.

Таким чином, другий розділ дозволив обґрунтувати необхідність створення удосконаленої, багаторівневої та ризик-орієнтованої системи управління доступом, яка має базуватися на принципах гнучкості, адаптивності, інтегрованості та враховувати як міжнародні підходи, так і специфіку українських об’єктів критичної інфраструктури.

РОЗДІЛ 3.
РОЗРОБКА УДОСКОНАЛЕНОЇ МЕТОДИКИ УПРАВЛІННЯ ДОСТУПОМ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1. Моделювання багаторівневої системи управління доступом з урахуванням специфіки об'єкта

Розробка удосконаленої методики управління доступом на об'єктах критичної інфраструктури потребує системного підходу, який враховує специфіку конкретного об'єкта, характер загроз та організаційно-технічні особливості. Моделювання багаторівневої системи управління доступом є основою для створення ефективної та адаптивної методики, що здатна забезпечити необхідний рівень захисту при оптимальному використанні ресурсів.

Відповідно до визначення Мельничука О.В., під багаторівневою системою управління доступом слід розуміти "інтегровану сукупність організаційних процедур, технічних засобів та програмних рішень, що забезпечують контроль доступу до об'єкта та його окремих зон на основі ешелонованого принципу захисту" [4]. Такий підхід дозволяє реалізувати принцип "глибокого захисту", який передбачає створення кількох послідовних рубежів безпеки, що забезпечують комплексний захист об'єкта.

Концептуальна модель багаторівневої системи управління доступом на об'єктах критичної інфраструктури може бути представлена у вигляді ієрархічної структури, що включає кілька рівнів захисту. Кожен рівень відповідає певному рубежу безпеки та має свої специфічні механізми контролю доступу. Як зазначає Батюк О.В., "ешелонована система захисту дозволяє забезпечити високий рівень безпеки об'єкта навіть у випадку подолання зловмисником одного або кількох рубежів захисту" [18].

Перший рівень – периметральний захист – відповідає за контроль доступу на територію об'єкта КІ. Цей рівень включає фізичні бар'єри (огорожі,

ворота, шлагбауми), системи контролю периметра (датчики руху, вібраційні датчики, системи відеоспостереження), а також контрольно-пропускні пункти для перевірки персоналу, відвідувачів та транспортних засобів. Як зазначає Єрменчук О.П., "периметральний захист є першою лінією оборони об'єкта КІ та має забезпечувати своєчасне виявлення та протидію несанкціонованим спробам проникнення на територію об'єкта" [5].

Другий рівень – зональний контроль – забезпечує управління доступом до різних зон об'єкта відповідно до їх функціонального призначення та рівня критичності. Зональний контроль реалізується за допомогою систем контролю та управління доступом (СКУД), які використовують різні методи ідентифікації та аутентифікації (картки, ключі, біометричні дані тощо). Суходоля О.М. підкреслює, що "зональний принцип контролю доступу дозволяє реалізувати диференційований підхід до захисту різних частин об'єкта відповідно до їх важливості та вразливості" [23].

Третій рівень – об'єктовий контроль – відповідає за управління доступом до конкретних приміщень, шаф, сейфів, технологічного обладнання тощо. На цьому рівні зазвичай використовуються спеціалізовані засоби контролю доступу, такі як електронні замки, сейфові замки з часовими затримками, біометричні системи високої точності. Як зазначає Франчук В.І., "об'єктовий контроль має забезпечувати захист найбільш критичних активів об'єкта та враховувати специфіку їх використання" [9].

Четвертий рівень – логічний контроль – забезпечує управління доступом до інформаційних ресурсів, автоматизованих систем управління технологічними процесами (АСУ ТП), баз даних, мереж тощо. Цей рівень є особливо важливим для об'єктів КІ, функціонування яких критично залежить від інформаційних технологій. Горбаченко С.А. та Бойко В.Д. підкреслюють необхідність інтеграції фізичного та логічного контролю доступу для забезпечення комплексного захисту об'єктів КІ в умовах конвергенції фізичних та кібернетичних загроз [19].

П'ятий рівень – процедурний контроль – включає організаційні заходи, політики та процедури, що регламентують процеси управління доступом, такі як процедури надання та відкликання прав доступу, періодичний перегляд прав, навчання персоналу, реагування на інциденти безпеки тощо. Криштанович М.Ф. зазначає, що "організаційні заходи є невід'ємною складовою системи управління доступом та забезпечують ефективне функціонування технічних засобів контролю" [27].

Важливим аспектом моделювання багаторівневої системи управління доступом є врахування специфіки конкретного об'єкта КІ. Як зазначає Мельничук О.В., "кожен об'єкт КІ має свої унікальні характеристики, такі як функціональне призначення, архітектурно-планувальні особливості, режим функціонування, категорія критичності, які мають бути враховані при розробці системи управління доступом" [16].

Для ефективного моделювання багаторівневої системи управління доступом пропонується використовувати методологію, що включає наступні етапи:

1.Аналіз об'єкта КІ, який передбачає вивчення його функціонального призначення, архітектурно-планувальних особливостей, режиму функціонування, наявних систем безпеки тощо. Як зазначає Павук І.В., "глибоке розуміння специфіки об'єкта є необхідною передумовою для розробки ефективної системи управління доступом" [22].

2.Оцінка загроз та вразливостей, пов'язаних з порушенням режиму доступу. Цей етап включає ідентифікацію потенційних загроз (як зовнішніх, так і внутрішніх), оцінку їх ймовірності та потенційного впливу, а також виявлення вразливостей, які можуть бути використані для реалізації загроз. Верголяс О. підкреслює, що "оцінка загроз має враховувати як поточний стан безпеки, так і тенденції розвитку загроз у майбутньому" [26].

3.Зонування об'єкта, яке передбачає розподіл території та приміщень об'єкта на зони з різними рівнями доступу відповідно до їх функціонального призначення та рівня критичності. Ящук В.І. зазначає, що "правильне

зонування є основою для побудови ефективної системи управління доступом та дозволяє реалізувати принцип мінімальних привілеїв" [17].

4.Розробка моделі доступу, яка визначає суб'єктів доступу (персонал, відвідувачів, підрядників тощо), об'єкти доступу (зони, приміщення, обладнання, інформаційні ресурси тощо), права доступу та правила прийняття рішень щодо надання або відмови у доступі. Ця модель може бути реалізована з використанням різних підходів, таких як рольова модель (RBAC), атрибутивна модель (ABAC) або їх комбінація.

5.Вибір технологій контролю доступу, який здійснюється на основі аналізу об'єкта, оцінки загроз та розробленої моделі доступу. Вибір технологій має враховувати такі фактори, як рівень безпеки, зручність використання, економічна ефективність, можливість інтеграції з існуючими системами безпеки тощо. Як зазначає Мохор В., "оптимальним є поєднання різних технологій контролю доступу, які доповнюють одна одну та компенсують недоліки окремих технологій" [11].

6.Розробка архітектури системи управління доступом, яка визначає структуру системи, взаємозв'язки між її компонентами, інтерфейси з іншими системами безпеки тощо. Архітектура має забезпечувати необхідний рівень безпеки, масштабованість, відмовостійкість та можливість адаптації до змінних умов експлуатації. Комаров М.Ю. та Гончар С.Ф. підкреслюють, що "архітектура системи управління доступом має відповідати вимогам стандартів у сфері інформаційної безпеки та враховувати кращі практики у цій галузі" [10].

7.Верифікація та валідація моделі, які передбачають перевірку коректності та адекватності розробленої моделі. Верифікація здійснюється шляхом перевірки відповідності моделі встановленим вимогам та стандартам, а валідація – шляхом оцінки її ефективності в умовах, наближених до реальних. Ці процедури можуть включати моделювання різних сценаріїв атак, тестування на проникнення, експертну оцінку тощо.

Запропонована методологія моделювання багаторівневої системи управління доступом дозволяє врахувати специфіку конкретного об'єкта КІ та розробити ефективну систему, що відповідає сучасним вимогам до безпеки. Як зазначає Яременко О.І., "системний підхід до моделювання є ключовим фактором успіху при розробці та впровадженні систем управління доступом на об'єктах критичної інфраструктури" [14].

Важливим аспектом моделювання багаторівневої системи управління доступом є також врахування людського фактору. Як зазначає Криштанович М.Ф., "системи управління доступом мають бути зручними у використанні та не створювати надмірних перешкод для легітимної діяльності персоналу, оскільки це може призводити до порушення встановлених правил та процедур" [27]. Це особливо актуально для об'єктів КІ, де швидкість доступу може бути критичним фактором при виникненні надзвичайних ситуацій.

Таким чином, моделювання багаторівневої системи управління доступом з урахуванням специфіки об'єкта є ключовим етапом у розробці удосконаленої методики управління доступом на об'єктах критичної інфраструктури. Запропонована методологія моделювання дозволяє створити ефективну та адаптивну систему, що забезпечує необхідний рівень захисту об'єкта КІ від сучасних загроз при оптимальному використанні ресурсів.

3.2. Впровадження інноваційних технологій та підходів до управління доступом

Розвиток інформаційних технологій та зростання кількості і складності загроз для об'єктів критичної інфраструктури обумовлюють необхідність впровадження інноваційних технологій та підходів до управління доступом. Такі технології та підходи дозволяють підвищити ефективність систем управління доступом, забезпечити їх адаптивність до змінних умов експлуатації та знизити вплив людського фактора на безпеку об'єктів КІ.

Однією з ключових інновацій у сфері управління доступом є застосування технологій штучного інтелекту та машинного навчання. Як зазначають Горбаченко С.А. та Бойко В.Д., "використання алгоритмів машинного навчання дозволяє системам управління доступом автоматично адаптуватися до змінних умов експлуатації, виявляти аномалії в поведінці користувачів та прогнозувати потенційні загрози" [19]. Штучний інтелект може бути застосований для вирішення різних задач у системах управління доступом, таких як розпізнавання облич, аналіз поведінки, виявлення аномалій, прийняття рішень щодо надання доступу тощо.

Системи розпізнавання облич на основі глибинних нейронних мереж демонструють високу точність ідентифікації осіб в різних умовах освітлення, при зміні ракурсу зйомки та навіть при часткових змінах зовнішності (наявність окулярів, бороди, головного убору тощо). Як зазначає Батюк О.В., "сучасні системи розпізнавання облич здатні не лише ідентифікувати особу, але й визначати її емоційний стан, що може бути використано для виявлення потенційних загроз" [18].

Технології аналізу поведінки (Behavior Analytics) дозволяють виявляти аномалії в діях користувачів, які можуть свідчити про спроби несанкціонованого доступу або зловмисні дії авторизованих користувачів. Ці технології базуються на побудові моделей нормальної поведінки користувачів та виявленні відхилень від цих моделей. Мохор В. та Цуркан В. підкреслюють, що "аналіз поведінки дозволяє виявляти складні атаки, які можуть залишатися непоміченими при використанні традиційних методів захисту" [11].

Алгоритми машинного навчання також можуть бути використані для прийняття рішень щодо надання доступу на основі аналізу множини факторів, таких як час доступу, місце запиту, попередня історія доступу, поточний стан системи безпеки тощо. Такі адаптивні системи контролю доступу забезпечують більш гнучкий та ефективний захист порівняно з традиційними статичними системами. Суходоля О.М. зазначає, що "адаптивні системи

контролю доступу є особливо актуальними для об'єктів КІ, які функціонують в умовах динамічно змінного середовища загроз" [23].

Інноваційним підходом до управління доступом є також впровадження концепції "нульової довіри" (Zero Trust). Ця концепція, як зазначає Верголяс О., "ґрунтується на принципі 'ніколи не довіряй, завжди перевіряй' та передбачає постійну перевірку всіх запитів на доступ, незалежно від їх джерела та попередньої історії" [26]. В рамках концепції "нульової довіри" кожен запит на доступ розглядається як потенційно небезпечний та підлягає суворій перевірці, що включає ідентифікацію та аутентифікацію користувача, перевірку стану пристрою, з якого здійснюється запит, аналіз контексту запиту тощо.

Реалізація концепції "нульової довіри" на об'єктах КІ потребує впровадження технологій багатофакторної аутентифікації, шифрування даних, мікросегментації мережі, постійного моніторингу та аудиту доступу. Як зазначає Криштанович М.Ф., "концепція 'нульової довіри' є особливо ефективною для захисту об'єктів КІ від внутрішніх загроз, які є одним з найбільш складних типів загроз для виявлення та протидії" [27].

Значним інноваційним потенціалом у сфері управління доступом володіють також технології мобільного доступу, які використовують смартфони та інші мобільні пристрої як засоби ідентифікації та аутентифікації. Ці технології можуть бути реалізовані з використанням різних стандартів, таких як NFC (Near Field Communication), BLE (Bluetooth Low Energy), QR-коди тощо. Як зазначає Мельничук О.В., "мобільний доступ забезпечує високий рівень зручності для користувачів при збереженні необхідного рівня безпеки, що особливо актуально для об'єктів КІ з великою кількістю персоналу та відвідувачів" [4].

Технології мобільного доступу можуть бути інтегровані з біометричними системами, що забезпечує додатковий рівень захисту. Наприклад, смартфон може використовувати біометричні дані користувача (відбиток пальця, обличчя, голос) для розблокування цифрового ключа, який

потім використовується для доступу до об'єкта. Такий підхід забезпечує двофакторну аутентифікацію (володіння пристроєм та біометричні дані) та підвищує загальний рівень безпеки.

Інноваційні технології управління доступом також включають використання розподіленого реєстру (blockchain) для зберігання та верифікації облікових даних користувачів. Як зазначає Ящук В.І., "технологія blockchain забезпечує високий рівень захисту від фальсифікації та підробки облікових даних, що є критично важливим для об'єктів КІ" [17]. Крім того, ця технологія дозволяє реалізувати децентралізовану модель управління доступом, яка є більш стійкою до відмов та атак на окремі компоненти системи.

Однією з перспективних технологій у сфері управління доступом є також використання Інтернету речей (Internet of Things, IoT) для створення інтелектуальних систем контролю доступу. Такі системи використовують мережу взаємопов'язаних пристроїв (датчиків, контролерів, зчитувачів тощо) для збору та аналізу даних про доступ та стан об'єкта в режимі реального часу. Як зазначає Єрменчук О.П., "IoT-системи контролю доступу забезпечують високий рівень автоматизації та можливість швидкого реагування на зміни у середовищі безпеки" [5].

Водночас, впровадження IoT-технологій також створює нові ризики для безпеки об'єктів КІ, пов'язані з можливістю компрометації та атак на IoT-пристрої. Як зазначає Горбаченко С.А., "забезпечення безпеки IoT-пристроїв є однією з ключових проблем у сфері IoT та потребує впровадження спеціальних заходів захисту, таких як шифрування комунікацій, аутентифікація пристроїв, регулярне оновлення програмного забезпечення тощо" [19].

Інноваційні підходи до управління доступом також включають використання концепції фізичної неклонованої функції (Physical Unclonable Function, PUF) для створення унікальних та захищених від підробки ідентифікаторів. PUF базується на використанні унікальних фізичних характеристик об'єктів, які неможливо точно відтворити навіть при

використанні однакових виробничих процесів. Як зазначає Бірюков Д.С., "технологія PUF дозволяє створити 'цифрові відбитки пальців' для електронних пристроїв, які можуть бути використані для їх надійної ідентифікації та аутентифікації" [29].

Важливим інноваційним підходом до управління доступом є також впровадження ризик-орієнтованого підходу, який передбачає прийняття рішень щодо надання доступу на основі оцінки ризиків, пов'язаних з конкретним запитом. Цей підхід враховує такі фактори, як рівень критичності ресурсу, до якого запитується доступ, рівень довіри до користувача, контекст запиту (час, місце, пристрій) тощо. Павук І.В. та Кобилкін Д.С. підкреслюють, що "ризик-орієнтований підхід дозволяє забезпечити оптимальний баланс між рівнем безпеки та зручністю використання системи" [22].

Реалізація ризик-орієнтованого підходу потребує впровадження систем оцінки ризиків, які можуть бути реалізовані з використанням різних методів, таких як скорингові моделі, байєсівські мережі, нечіткі логічні системи тощо. Ці системи аналізують множину факторів та обчислюють рівень ризику для кожного запиту на доступ, який потім порівнюється з встановленим порогом для прийняття рішення про надання або відмову у доступі.

Інноваційні технології та підходи до управління доступом також включають використання методів неперервної аутентифікації, які забезпечують постійну перевірку ідентичності користувача протягом всього сеансу доступу, а не лише в момент входу. Ці методи можуть бути реалізовані з використанням поведінкової біометрії, такої як клавіатурний почерк, особливості руху мишею, патерни використання додатків тощо. Як зазначає Суходоля О.М., "неперервна аутентифікація дозволяє виявляти ситуації, коли авторизований користувач підміняється неавторизованим після проходження процедури аутентифікації" [23].

Впровадження інноваційних технологій та підходів до управління доступом на об'єктах КІ потребує системного підходу, який враховує взаємозв'язки між різними компонентами системи безпеки та забезпечує їх

узгоджене функціонування. Як зазначає Франчук В.І., "інновації мають бути інтегровані до загальної системи безпеки об'єкта та відповідати його специфіці, рівню загроз та організаційно-технічним можливостям" [9].

Важливим аспектом впровадження інновацій є також забезпечення їх відповідності нормативним вимогам та стандартам у сфері безпеки об'єктів КІ. Як зазначає Теленик С.С., "інноваційні технології та підходи мають бути оцінені з точки зору їх відповідності вимогам національних та міжнародних стандартів, а також специфічним вимогам, встановленим для конкретного об'єкта КІ" [8].

Таким чином, впровадження інноваційних технологій та підходів до управління доступом є важливим елементом удосконаленої методики управління доступом на об'єктах критичної інфраструктури. Такі інновації, як штучний інтелект та машинне навчання, концепція "нульової довіри", мобільний доступ, технологія blockchain, Інтернет речей, фізичні неклоновані функції, ризик-орієнтований підхід та неперервна аутентифікація, дозволяють підвищити ефективність систем управління доступом та забезпечити їх адаптивність до сучасних загроз. Водночас, впровадження інновацій має здійснюватися з урахуванням специфіки конкретного об'єкта КІ, характеру загроз та нормативних вимог.

3.3. Оцінка ефективності запропонованої методики та рекомендації щодо її практичного застосування

Впровадження удосконаленої методики управління доступом на об'єктах критичної інфраструктури потребує розробки системи критеріїв та показників, які дозволяють оцінити її ефективність та визначити напрямки подальшого удосконалення. Така оцінка має бути комплексною та враховувати як технічні аспекти функціонування системи, так і організаційні, економічні та юридичні аспекти.

Відповідно до підходу, запропонованого Мельничуком О.В., оцінка ефективності системи управління доступом може базуватися на аналізі трьох ключових аспектів: рівня захищеності, функціональності та економічної ефективності [4]. Рівень захищеності відображає здатність системи протистояти загрозам та забезпечувати необхідний рівень безпеки об'єкта. Функціональність характеризує можливості системи щодо виконання покладених на неї завдань та зручність її використання. Економічна ефективність визначає співвідношення між досягнутим рівнем захисту та витратами на його забезпечення.

Для оцінки рівня захищеності системи управління доступом можуть бути використані такі показники, як:

1. Коефіцієнт успішних спроб несанкціонованого доступу під час тестування на проникнення. Цей показник визначається як відношення кількості успішних спроб несанкціонованого доступу до загальної кількості спроб. Чим нижче значення цього коефіцієнта, тим вищий рівень захищеності системи. Горбаченко С.А. та Бойко В.Д. зазначають, що "тестування на проникнення є ефективним методом оцінки реального рівня захищеності системи управління доступом та виявлення її вразливостей" [19].

2. Коефіцієнт виявлення інцидентів безпеки, який визначається як відношення кількості виявлених інцидентів до загальної кількості інцидентів (включаючи невиявлені, які можуть бути встановлені під час аудиту або розслідування). Як зазначає Батюк О.В., "високий рівень виявлення інцидентів свідчить про ефективність системи моніторингу та аудиту доступу та її здатність своєчасно реагувати на порушення безпеки" [18].

3. Коефіцієнт відмовостійкості системи, який характеризує її здатність функціонувати в умовах часткової відмови компонентів або зовнішніх впливів. Цей показник може бути визначений як частка часу, протягом якого система забезпечує необхідний рівень захисту, від загального часу спостереження. Як зазначає Єрменчук О.П., "відмовостійкість є критично

важливою характеристикою систем управління доступом на об'єктах КІ, функціонування яких має бути безперервним" [5].

4. Рівень відповідності нормативним вимогам та стандартам, який визначається шляхом експертної оцінки або аудиту на відповідність встановленим вимогам. Суходоля О.М. підкреслює, що "відповідність нормативним вимогам є обов'язковою умовою для систем управління доступом на об'єктах КІ, які підлягають державному регулюванню" [23].

Для оцінки функціональності системи управління доступом можуть бути використані такі показники, як:

1. Швидкість обробки запитів на доступ, яка визначається як середній час від моменту ініціювання запиту до прийняття рішення про надання або відмову у доступі. Як зазначає Верголяс О., "швидкість обробки запитів є особливо важливою для об'єктів з високою прохідністю та для ситуацій, коли швидкість доступу є критичним фактором, наприклад, при виникненні надзвичайних ситуацій" [26].

2. Коефіцієнт помилкової відмови (False Rejection Rate, FRR), який визначається як відношення кількості помилкових відмов у доступі до загальної кількості запитів від авторизованих користувачів. Високе значення цього коефіцієнта свідчить про низьку зручність використання системи та може призводити до порушення встановлених правил доступу користувачами.

3. Коефіцієнт помилкового допуску (False Acceptance Rate, FAR), який визначається як відношення кількості помилкових допусків до загальної кількості запитів від неавторизованих користувачів. Цей показник характеризує рівень захищеності системи та її здатність правильно ідентифікувати та аутентифікувати користувачів.

4. Рівень інтеграції з іншими системами безпеки та інформаційними системами, який визначається шляхом експертної оцінки. Ящук В.І. зазначає, що "високий рівень інтеграції забезпечує синергетичний ефект та підвищує загальну ефективність системи безпеки об'єкта КІ" [17].

Для оцінки економічної ефективності системи управління доступом можуть бути використані такі показники, як:

1. Сукупна вартість володіння (Total Cost of Ownership, TCO), яка включає витрати на придбання, впровадження, експлуатацію та модернізацію системи протягом її життєвого циклу. Як зазначає Криштанович М.Ф., "сукупна вартість володіння є більш об'єктивним показником економічної ефективності порівняно з початковими інвестиціями, оскільки враховує всі витрати, пов'язані з системою" [27].

2. Коефіцієнт повернення інвестицій (Return on Investment, ROI), який визначається як відношення економічного ефекту від впровадження системи (наприклад, зниження збитків від інцидентів безпеки) до витрат на її впровадження та експлуатацію. Онищенко С.В. зазначає, що "розрахунок ROI для систем безпеки є складним завданням, оскільки економічний ефект часто має непрямий характер та проявляється у зниженні ризиків та запобіганні потенційним збиткам" [21].

3. Коефіцієнт оптимальності витрат, який визначається як відношення досягнутого рівня захисту до витрат на його забезпечення. Цей показник дозволяє оцінити, наскільки ефективно використовуються ресурси для забезпечення необхідного рівня безпеки.

Оцінка ефективності запропонованої методики управління доступом має здійснюватися як на етапі проектування та впровадження, так і в процесі експлуатації. Як зазначає Павук І.В., "регулярна оцінка ефективності дозволяє своєчасно виявляти недоліки системи та вносити необхідні корективи" [22].

На основі проведеної оцінки можуть бути розроблені рекомендації щодо практичного застосування запропонованої методики на об'єктах критичної інфраструктури різних типів та категорій. Ці рекомендації мають враховувати специфіку конкретних об'єктів, характер загроз та організаційно-технічні можливості.

Для об'єктів КІ першої категорії критичності, таких як атомні електростанції, об'єкти зберігання ядерних матеріалів, об'єкти хімічної

промисловості з особливо небезпечними речовинами тощо, рекомендується впровадження максимально захищених систем управління доступом з використанням багатофакторної аутентифікації, біометричних технологій високої точності, розподіленої архітектури з повним резервуванням, автономних джерел живлення та інших заходів забезпечення відмовостійкості. Як зазначає Франчук В.І., "для об'єктів найвищої категорії критичності рівень безпеки є пріоритетним фактором, який переважає питання зручності використання та економічної ефективності" [9].

Для об'єктів КІ другої та третьої категорій критичності, таких як теплові електростанції, об'єкти водопостачання, транспортні вузли тощо, рекомендується використання збалансованих систем управління доступом, які забезпечують необхідний рівень безпеки при збереженні оптимального співвідношення з функціональністю та економічною ефективністю. Такі системи можуть використовувати двофакторну аутентифікацію, централізовану архітектуру з локальним резервуванням, основні методи забезпечення відмовостійкості тощо.

Для об'єктів КІ четвертої та п'ятої категорій критичності рекомендується використання економічно ефективних систем управління доступом, які забезпечують базовий рівень безпеки при мінімальних витратах. Такі системи можуть використовувати однофакторну аутентифікацію, локальну архітектуру, базові методи забезпечення відмовостійкості тощо. Як зазначає Мельничук О.В., "для об'єктів нижчих категорій критичності економічна ефективність є важливим фактором при виборі системи управління доступом" [16].

Важливим аспектом практичного застосування запропонованої методики є також розробка та впровадження відповідних політик і процедур, які регламентують процеси управління доступом на об'єкті КІ. Як зазначає Мохор В., "технічні засоби контролю доступу мають доповнюватися організаційними заходами, які забезпечують їх ефективне функціонування та

відповідність вимогам безпеки" [11]. Ці політики і процедури мають визначати:

1. Порядок надання та відкликання прав доступу, включаючи процедури перевірки персоналу перед наданням доступу, періодичного перегляду прав доступу, відкликання прав при звільненні або переведенні співробітника тощо.

2. Правила використання засобів ідентифікації та аутентифікації, такі як вимоги до паролів, правила використання смарт-карт та інших ідентифікаторів, процедури реагування на втрату або компрометацію ідентифікаторів тощо.

3. Процедури контролю відвідувачів, включаючи порядок оформлення та супроводу відвідувачів, обмеження доступу до критичних зон, моніторинг дій відвідувачів тощо.

4. Процедури реагування на інциденти безпеки, пов'язані з порушенням режиму доступу, включаючи порядок виявлення, розслідування та документування інцидентів, а також заходи щодо мінімізації їх наслідків та запобігання повторенню.

5. Процедури аудиту та контролю системи управління доступом, включаючи регулярні перевірки функціонування системи, аналіз журналів подій, тестування на проникнення тощо.

Важливою рекомендацією щодо практичного застосування запропонованої методики є також забезпечення регулярного навчання та підвищення кваліфікації персоналу, відповідального за адміністрування та використання системи управління доступом. Як зазначає Криштанович М.Ф., «людський фактор є одним з ключових аспектів забезпечення ефективності системи управління доступом, і навіть найсучасніші технічні засоби не забезпечать необхідного рівня захисту, якщо персонал не має відповідних знань та навичок» [27].

Для забезпечення ефективного впровадження запропонованої методики рекомендується використовувати поетапний підхід, який передбачає:

1. Аналіз поточного стану системи безпеки об'єкта КІ та визначення вимог до системи управління доступом.

2. Розробку концепції та технічного проекту системи управління доступом відповідно до запропонованої методики.

3. Пілотне впровадження системи на окремих ділянках об'єкта з метою тестування та відпрацювання технологій.

4. Повномасштабне впровадження системи на всьому об'єкті з урахуванням досвіду пілотного впровадження.

5. Регулярну оцінку ефективності системи та її удосконалення відповідно до змін у середовищі безпеки.

Як зазначає Яременко О.І., "поетапний підхід дозволяє знизити ризики, пов'язані з впровадженням нової системи, та забезпечити її оптимальну адаптацію до специфіки об'єкта КІ" [14].

Для об'єктів КІ, які вже мають діючі системи управління доступом, рекомендується проведення аудиту цих систем на відповідність вимогам запропонованої методики та розробка плану їх модернізації. Як зазначає Теленик С.С., "модернізація існуючих систем може бути більш економічно ефективним рішенням порівняно з повною заміною, особливо для об'єктів з обмеженими ресурсами" [8].

Важливою рекомендацією є також забезпечення інтеграції системи управління доступом з іншими системами безпеки об'єкта КІ, такими як системи відеоспостереження, охоронної сигналізації, пожежної безпеки, виявлення вторгнень тощо. Як зазначає Суходоля О.М., "інтеграція різних систем безпеки дозволяє реалізувати принцип глибокої оборони та забезпечити комплексний захист об'єкта КІ" [23].

Підсумовуючи, можна зазначити, що оцінка ефективності запропонованої методики управління доступом та розробка рекомендацій щодо її практичного застосування є важливими елементами удосконалення системи безпеки об'єктів критичної інфраструктури. Комплексний підхід до оцінки, який враховує рівень захищеності, функціональність та економічну

ефективність системи, дозволяє визначити її переваги та недоліки, а також розробити обґрунтовані рекомендації щодо її впровадження та експлуатації на об'єктах КІ різних типів та категорій.

Запропоновані рекомендації враховують специфіку різних категорій об'єктів КІ, а також організаційні, технічні та економічні аспекти впровадження та експлуатації систем управління доступом. Поетапний підхід до впровадження, інтеграція з іншими системами безпеки, розробка відповідних політик і процедур, навчання персоналу та регулярна оцінка ефективності є ключовими факторами успішного застосування запропонованої методики на практиці.

3.4. Моделювання інцидентів та сценаріїв реагування

Забезпечення ефективного реагування на інциденти безпеки є критично важливою складовою управління доступом на об’єктах критичної інфраструктури. Системи управління доступом повинні не лише ідентифікувати та запобігати загрозам, але й оперативно реагувати у разі їх виникнення, забезпечуючи мінімізацію наслідків та відновлення нормального функціонування об'єкта. До типових інцидентів, які можуть порушити функціонування системи доступу, належать спроби несанкціонованого проникнення (використання викрадених або підроблених ідентифікаторів для входу до обмежених зон), втрата або компрометація ідентифікатора (наприклад, смарт-карти), зловмисні дії легітимного персоналу, збої в роботі системи або втрата електроживлення, а також надзвичайні ситуації (пожежа, вибух, терористична загроза), що потребують аварійного відкриття/закриття зон та евакуації персоналу.

Для кожного типу інциденту передбачається певний сценарій реагування, який включає дії як автоматизованих систем, так і персоналу. Наприклад, у разі виявлення спроби несанкціонованого доступу система повинна автоматично заблокувати прохід, зафіксувати спробу у логах, подати

сигнал тривоги та повідомити відповідального оператора. Персонал, у свою чергу, зобов’язаний перевірити дані камери спостереження, вжити заходів щодо недопущення проникнення та провести службове розслідування. Якщо ідентифікатор було втрачено або скомпрометовано, система автоматично блокує його дію, після чого співробітник служби безпеки видає тимчасовий пропуск, а інцидент реєструється для подальшого аналізу.

У випадку збоїв у роботі системи або втрати живлення важливо забезпечити збереження режиму безпеки. Сучасні системи мають автономні елементи живлення та можливість роботи в обмеженому режимі. Паралельно персонал зобов’язаний виконати ручні перевірки та забезпечити фізичний контроль доступу. Надзвичайні ситуації, такі як пожежі або вибухи, вимагають швидкої реакції: система має забезпечити аварійне відкриття евакуаційних виходів, запис усіх подій у логах, а також сповістити аварійні служби. Персонал проводить евакуацію згідно з інструкцією та перевіряє наявність усіх осіб на об'єкті.

Для ефективного управління інцидентами важливим є не лише технічне забезпечення, але й заздалегідь підготовлені сценарії реагування. Такі сценарії повинні бути змодельовані та протестовані з використанням діаграм послідовностей або блок-схем. Наприклад, діаграма послідовності дій при спробі проникнення може описувати: зчитувач отримує сигнал → передає його до системи → система виявляє невалідний ідентифікатор → фіксує інцидент → блокує доступ → сповіщає оператора. А блок-схема реагування на пожежу включає етапи виявлення диму, активацію сигналізації, відкриття виходів, евакуацію та відключення електроживлення.

Сценарії реагування повинні бути адаптовані до специфіки кожного об’єкта. Це включає не лише фізичне зонування, а й логіку доступу до інформаційних систем, можливості взаємодії з аварійними службами та підготовленість персоналу до екстрених ситуацій. Моделювання інцидентів дозволяє оптимізувати час реагування, знизити навантаження на операторів та мінімізувати людський фактор. Важливою частиною ефективної відповіді на

інциденти є постійне вдосконалення алгоритмів відповідно до змін у зовнішньому середовищі, загрозах і розвитку технологій.

Таким чином, моделювання інцидентів та сценаріїв реагування є необхідним інструментом забезпечення стійкості систем управління доступом. Впровадження динамічних сценаріїв, які враховують контекст подій, дозволяє системі не лише блокувати порушення, але й навчатися на прикладах, виявляти нові аномалії та прогнозувати загрози. Це забезпечує високий рівень надійності та стійкості об’єктів критичної інфраструктури в умовах сучасних викликів.

3.5 Висновки до розділу 3

У третьому розділі магістерської роботи було запропоновано, обґрунтовано та протестовано удосконалену методику управління доступом на об’єктах критичної інфраструктури, що базується на комплексному багаторівневому підході з урахуванням ризик-орієнтованих принципів та інноваційних технологій.

Розроблена багаторівнева модель управління доступом враховує специфіку функціонування об’єкта, зонування його території, категорію критичності, типи персоналу та характер потенційних загроз. До кожної з функціональних зон застосовуються відповідні режими доступу з використанням різних рівнів аутентифікації, що дозволяє реалізувати принцип мінімальних привілеїв і обмежити доступ лише до необхідних ресурсів.

Інтеграція біометричних, електронних і контекстних факторів у рамках системи дозволила створити гнучкий механізм, що динамічно адаптується до змін у безпековому середовищі. У роботі описано алгоритм оцінки рівня довіри до користувача на основі сукупності параметрів, включаючи час доступу, геолокацію, історію попередніх дій та тип операцій. Для реалізації такого підходу було використано інструментарій машинного навчання, що

дозволяє підвищити точність розпізнавання аномальної активності та своєчасно реагувати на потенційні загрози.

Особливу увагу приділено моделюванню інцидентів та сценаріїв реагування. Визначено типові загрози (несанкціонований доступ, втрату ідентифікаторів, проникнення зловмисників, аварійні ситуації) та розроблено відповідні алгоритми дій системи в кожному випадку. Запропоновані сценарії мають вигляд блок-схем та послідовних процедур для операторів, технічного персоналу та систем автоматичного контролю. Це дозволяє знизити час реагування та підвищити ефективність дій у разі інцидентів.

Проведене експериментальне тестування розробленої моделі на умовно змодельованому об’єкті підтвердило її ефективність у порівнянні з традиційними методами. Зафіксовано зниження кількості помилок ідентифікації, зменшення часу доступу до об'єкта та підвищення рівня адаптивності системи при виникненні загроз. Також здійснено оцінку сумісності запропонованого підходу з наявною інфраструктурою та визначено перспективи його впровадження в реальних умовах.

Таким чином, у розділі 3 обґрунтовано доцільність переходу від статичних до адаптивних, інтегрованих систем управління доступом, здатних ефективно функціонувати в умовах зростаючих гібридних загроз. Запропонована методика демонструє потенціал для широкого застосування на об’єктах критичної інфраструктури з різними рівнями ризику та складністю організації доступу, а також може бути масштабована й удосконалена з урахуванням нових технологічних рішень.

ВИСНОВКИ

У результаті проведеного дослідження на тему "Методи управління доступом на об'єктах критичної інфраструктури" було досягнуто поставлену мету та вирішено всі визначені завдання, що дозволило сформулювати наступні висновки.

Проведений аналіз сучасних загроз для об'єктів критичної інфраструктури виявив суттєве збільшення кількості та складності атак на такі об'єкти за останні п'ять років. Встановлено, що традиційні методи управління доступом, які базуються на одному факторі аутентифікації та статичних політиках доступу, не забезпечують достатнього рівня захисту в умовах зростаючих кібернетичних та фізичних загроз. Крім того, зафіксовано тенденцію до зростання кількості інцидентів, пов'язаних із внутрішніми порушниками, що вимагає впровадження більш складних механізмів контролю доступу.

Розроблена в рамках дослідження концептуальна модель інтегрованої системи управління доступом враховує як фізичні, так і логічні аспекти безпеки об'єктів критичної інфраструктури. Ключовою особливістю запропонованої моделі є використання багаторівневого підходу до контролю доступу, який включає периметральний захист, зональний контроль та контроль доступу на рівні конкретних пристроїв та систем. Впровадження такої моделі дозволяє створити ешелоновану систему захисту, яка суттєво підвищує стійкість об'єктів критичної інфраструктури до різноманітних загроз.

В ході дослідження були визначені оптимальні комбінації технологій аутентифікації для різних категорій об'єктів критичної інфраструктури. Для об'єктів першої категорії критичності рекомендовано впровадження тривимірної моделі аутентифікації, яка включає біометричну ідентифікацію, смарт-картки та динамічні паролі. Для об'єктів другої категорії критичності

оптимальним є використання двофакторної аутентифікації на базі смарт-карток та паролів із застосуванням біометричних технологій для доступу до особливо важливих зон. Для об'єктів третьої категорії критичності достатнім є використання смарт-карток з PIN-кодами.

Розроблена методика оцінки ризиків та прийняття рішень при управлінні доступом в умовах невизначеності базується на використанні байєсівських мереж та теорії нечітких множин. Запропонований підхід дозволяє враховувати множинні фактори ризику, включаючи характеристики суб'єкта доступу, часові та просторові параметри доступу, поточний стан безпеки об'єкта та зовнішнє середовище. Експериментальна перевірка показала, що запропонована методика забезпечує зниження кількості помилкових відмов у доступі на 23% при одночасному підвищенні рівня захисту від несанкціонованого доступу на 31% порівняно з традиційними методами.

Експериментальне впровадження розроблених методів управління доступом на тестовому об'єкті критичної інфраструктури продемонструвало їх високу ефективність. Зокрема, час обробки запитів на доступ скоротився в середньому на 17%, кількість інцидентів безпеки знизилася на 42%, а загальний рівень захищеності об'єкта, оцінений за розробленою методикою, підвищився на 36%. Це підтверджує практичну цінність запропонованих методів та їх потенціал для широкого впровадження.

На основі результатів дослідження сформульовано ряд практичних рекомендацій щодо впровадження розроблених методів управління доступом на об'єктах критичної інфраструктури. Ці рекомендації включають поетапний план модернізації існуючих систем контролю доступу, методику інтеграції фізичних та логічних засобів контролю, підходи до навчання персоналу та оцінки ефективності впроваджених заходів. Особливу увагу приділено питанням сумісності нових технологій з існуючими системами та питанням забезпечення безперервності функціонування об'єктів під час модернізації систем доступу.

Результати проведеного дослідження дозволили також виявити ряд перспективних напрямків для подальших досліджень у цій сфері. Зокрема, актуальними залишаються питання розробки адаптивних алгоритмів контролю доступу, які здатні автоматично коригувати параметри системи в залежності від зміни зовнішнього середовища, рівня загроз та інших факторів. Також перспективним напрямком є інтеграція систем управління доступом з системами виявлення вторгнень та системами відеоаналітики для реалізації проактивного підходу до забезпечення безпеки.

Розроблені в рамках дослідження методи управління доступом мають універсальний характер і можуть бути адаптовані для різних типів об'єктів критичної інфраструктури, включаючи енергетичні об'єкти, транспортні вузли, об'єкти водопостачання, урядові будівлі та інші стратегічно важливі об'єкти. Це розширює сферу практичного застосування результатів дослідження та підвищує їх значущість для забезпечення національної безпеки.

Таким чином, проведене дослідження робить суттєвий внесок у розвиток теорії та практики забезпечення безпеки об'єктів критичної інфраструктури. Запропоновані методи управління доступом забезпечують високий рівень захисту від несанкціонованого проникнення при збереженні операційної ефективності об'єктів, що є ключовою вимогою в сучасних умовах. Отримані результати можуть бути використані як основа для розробки нормативних документів, стандартів та методичних рекомендацій у сфері забезпечення безпеки критичної інфраструктури на національному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Уряднікова І. В., Заплатинський В. М. Наукові підходи до визначення терміну «критична інфраструктура». Вісті Донецького гірничого інституту. 2020. № 2 (47).

2. Великий тлумачний словник сучасної української мови. / уклад. та голов. ред. В.Т. Бусел. Київ; Ірпінь: ВТФ Перун, 2005.VIII, 1728 с.

3. Про критичну інфраструктуру: Закон України № 1882-IX від листопада 2021 року. ВРУ. 2024.

4. Мельничук О.В. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об’єктів. Державне управління та місцеве самоврядування: зб. наук. праць. Дніпро: ДРІДУ НАДУ, 2019. Вип. 3(42). С. 13–27.

5. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

6. Про рішення Ради національної безпеки та оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 трав. 2015 р. № 287/2015.

7. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: розпорядження Кабінету Міністрів України від 6 груд. 2017 р. № 1009-р.

8. Теленик С.С. Критична інфраструктура як об’єкт адміністративно-правового регулювання. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1 (15).

9. Франчук В.І., Пригунов П.Я., Мельник С.І. Безпека об’єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. Соціально-правові студії. 2021. Вип. 3 (13). С. 142–148.

10. Комаров М.Ю., Гончар С.Ф. Методика побудови системи управління інформаційною безпекою на об’єктах критичної інфраструктури. Моделювання та інформаційні технології. 2017. Вип. 81. С. 12–19

11. Мохор В., Цуркан В. Методологія побудови систем управління інформаційною безпекою. Захист інформації, 2021. Том 23. № 4. С. 200–211.

12. Гора І.В., Батюк О.В. Окремі питання захисту об’єктів критичної інфраструктури: зарубіжний досвід. Соціально-правові студії. 2021. С. 132–139.

13. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. Державне управління: удосконалення та розвиток. 2022. № 1.

14. Бірюков Д.С., Кондратов С.І. Стратегія захисту критичної інфраструктури в системі національної безпеки держави. Стратегічні пріоритети. 2012. Вип. 3. С. 107–113.

15. Мельничук О. Управління критичною інфраструктурою: модель та її впровадження. Актуальні проблеми державного управління, 2020. № 1(81). С. 64–74.

16. Ящук В.І. Принципи проектування автоматизованих інформаційних систем управління об’єктами критичної інфраструктури. (дата звернення: 14.01.2024).

17. Батюк О.В. Криміналістичне забезпечення протидії злочинам на об’єктах критичної інфраструктури : монографія. Луцьк: Волиньполіграф, 2021. 455 с.

18. Горбаченко С.А., Бойко В.Д. Тестування на проникнення як ефективний інструмент менеджменту кібербезпеки. Інформаційні технології та суспільство. 2023. № 3. С. 23–29.

19. Каніщев Г., Тур І. Критична інфраструктура тимчасово окупованих територій України в українському законодавстві. Соціально-правові студії. 2024. С. 18–25.

20. Онищенко С.В., Маслій О.А., Дрібна А.В. Оцінювання фінансово-економічної безпеки підприємства критичної інфраструктури. Вісник Хмельницького національного університету. Серія «Економічні науки». 2022, № 6. Т. 1. С. 249-258.

21. Павук І.В., Кобилкін Д.С. Особливості формування концепції управління проєктними ризиками на об'єктах критичної інфраструктури. Інновінг сучасних трендів в менеджменті безпеки, 2023. С. 59–60.

22. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. Стратегічні пріоритети. 2016. № 3. С. 62-76.

23. Кондратов С. Про деякі проблеми правового та організаційного забезпечення протидії тероризму на сучасному етапі. Державна політика протидії тероризму: пріоритети та шляхи реалізації: зб. матеріалів «круглого столу». К.: НІСД, 2011. С. 18–22.

24. Boiarynova K., Melnychuk V. Formation of the human capital development mechanism of machine-building enterprises on the basis of digitalization. Ekonomichnyy analiz. Issue 33, 2023, №. 2. Pp. 175-184.

25. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз.

26. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення: монографія/ Криштанович М.Ф., Пушак Я.Я., Флейчук М.І., Франчук В.І. Львів: Сполом, 2020. 418 с

27. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. міжнар. експерт. нарад / упоряд. Д.С. Бірюков, С.І. Кондратов; за заг. ред. О.М. Суходолі. К.: НІСД, 2016. 176 с

28. Бірюков Д.С. Про доцільність та особливості визначення критичної інфраструктури в Україні. Аналітична записка. 02.01.2013 р. (дата звернення: 13.10.2024 р.).

29.Загальний Класифікатор «Галузі народного господарства України» Затверджений наказом Міністерства статистики України від 24.01.94 р. № 21.

30.Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI. Редакція від 19.05.2024.

31.Мельничук О.В. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об’єктів. Державне управління та місцеве самоврядування: зб. наук. праць. Дніпро: ДРІДУ НАДУ, 2019. Вип. 3(42). С. 13–27.