

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ

АНАНЧЕНКО ОЛЕКСІЙ ЄВГЕНОВИЧ

УДК 004.378:005.8:005.42:005.22

МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ
СТІЙКОСТІ АДАПТИВНИХ КОРПОРАТИВНИХ ОСВІТНІХ
ІНФОРМАЦІЙНИХ СИСТЕМ

Спеціальність 05.13.06 – інформаційні технології

Реферат
Дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2024

Дисертацією є рукопис

Робота виконана на кафедрі технологій цифрового розвитку Державного університету інформаційно-комунікаційних технологій Міністерства освіти і науки України, м. Київ

Науковий керівник: доктор технічних наук, професор **Бондарчук Андрій Петрович**, директор Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій

Офіційні опоненти доктор технічних наук, професор **Корнага Ярослав Ігорович**, декан факультету інформатики та обчислюваної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

доктор технічних наук, професор **Триснюк Василь Миколайович**, завідувач відділу досліджень навколишнього середовища Інституту телекомунікацій і глобального інформаційного простору.

Захист відбудеться «12» листопада 2024 року о 14.00 годині на засіданні спеціалізованої вченої ради Д 26.861.05 при Державному університеті інформаційно-комунікаційних технологій за адресою: 03110, м. Київ, вул. Солом'янська 7, конференц-зал

Автореферат розісланий «11» жовтня 2024 р.

Вчений секретар
спеціалізованої вченої ради
кандидат педагогічних наук, доцент

В.О. Корецька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Залежність освітніх установ від інформаційних систем постійно зростає, адже ці системи відіграють ключову роль в управлінні навчальними процесами, адмініструванні та зберіганні даних. Це ставить високу вимогу до їх надійності та безперервної роботи.

В умовах швидких змін в освітніх методологіях та розвитку технологій виникає потреба в адаптивності інформаційних систем, які повинні не лише забезпечувати стабільну роботу, але й гнучко реагувати на зміни та оновлення без значних перерв. Водночас корпоративні освітні системи стикаються з численними загрозами, такими як кібератаки, технічні збої та людські помилки, що підвищує важливість забезпечення їхньої функціональної стійкості для мінімізації ризиків і забезпечення безперервності освітнього процесу.

Впровадження новітніх технологій, таких як штучний інтелект, великі дані, хмарні обчислення та блокчейн, вимагає розробки нових методів забезпечення функціональної стійкості, що охоплюють як технічні аспекти, так і організаційні підходи. Крім того, у конкурентному середовищі надійність та стійкість інформаційних систем є важливими чинниками для збереження репутації освітніх установ та їхньої привабливості для студентів і викладачів. Також зростають регуляторні вимоги щодо захисту персональних даних та забезпечення конфіденційності інформації, що підкреслює необхідність розробки та впровадження надійних технологій для забезпечення відповідності законодавчим нормам.

Проблеми функціональної стійкості інформаційних систем досліджувались в роботах Машкова О.А., Барабаша О.В., Вишнівського В.В., Обідіна Д.М., Кравченка Ю.В., Кононова О.А. Питання відмовостійкості систем досліджувались в роботах Авіжиєніса А.А., Ільїна О.Ю., Коростіля Ю.М. та інших. Питання стійкості систем щодо зовнішніх впливів досліджувалась Хорошком В.О., Субачем І.Ю., Журавським Ю.В., Рубаном І.В., Оксіюком О.Г., Толуюпою С.В. та іншими вченими.

Теоретичній розробці питань, пов'язаних з підтримкою достатнього рівня інформаційної безпеки, багато уваги приділяли вчені Оксіюк О.Г., Данчук В.Д., Рудницький В.М., Павленко П.М., Новіков О.М., Радіонов А.Н., Тимошенко А.М., Герасименко В.А., Зегжда П.Д., Дев'янін П.М., Прушо А.А., Хоффман П.Д., Домарєв В.В., Брягін О.В., Шевченко В.Л., Тесля Ю.М. та багато інших.

Проблема теоретичного та методологічного розвитку інформаційних систем та технологій, аналізу та оцінки їх захисту присвячені праці вітчизняних і зарубіжних учених, таких як: Іванова С.М., Йеттера В.М., Мишеніна А.І., Смирнова Г.М., Маккорміка Дж., Глибовця М.М., Голуба С.В., Тейлора Ф., Харві Р., Файна С. та багато інших.

Хоча багато вчених внесли значний вклад у дослідження функціональної стійкості інформаційних систем, залишається ряд невирішених проблем. Наразі недостатньо розроблені методи, що забезпечують оптимальний баланс

між адаптивністю та стабільністю систем, а також інтеграційні механізми для модульних архітектур. Питання безпеки і доступності потребують нових підходів, які б забезпечували високий рівень захисту без зниження доступності для користувачів. Також існує необхідність у розробці ефективних методів оновлення систем для підтримки їх актуальності протягом тривалого часу. Крім того, стійкість до зовнішніх впливів, таких як кіберзагрози і технічні несправності, потребує вдосконалення технологій моніторингу і реагування. Усі ці аспекти вимагають подальшого дослідження і розробки нових технологій для забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем. Тому є актуальним **науково-практичним завданням** розробити методи та технології забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи і отримані результати безпосередньо відповідають пріоритетності розвитку інформаційних та комунікаційних технологій в Україні, що сформульовано в Законі України «Про пріоритетні напрями розвитку науки і техніки» від 11.07.2001 р. № 2623-III.

Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій і є частиною досліджень в рамках науково-дослідних робіт:

- «Підвищення ефективності процесу управління 3D принтером з використанням методів машинного навчання» (Державний реєстраційний номер 0124U001849, ДУІКТ, м. Київ),
- «Розробка моделі оптимізації транспортної мережі за допомогою нейромережевого аналізу» (Державний реєстраційний номер 0124U001868, ДУІКТ, м. Київ).

Особисто автором в вищеназваних НДР запропоновано: удосконалений метод машинного навчання, що дозволяє забезпечити швидшу збіжність алгоритму машинного навчання; методика оцінки ефективності забезпечення інформаційної безпеки, яка на відміну від існуючих, полягає у поєднанні безпосередньо розрахунку ефективності засобів інформаційної безпеки та ефективності механізму їх впровадження; а також запропоновано методіку забезпечення функціональної стійкості інформаційної системи.

Мета і задача дослідження. Метою дисертації є підвищення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем за допомогою розроблених в роботі методів та технологій та з використанням методів машинного навчання.

У відповідності до поставленої мети, для вирішення науково-практичного завдання, в роботі сформульовані такі завдання:

1. Проаналізувати стан адаптивних корпоративних освітніх інформаційних систем, включаючи їхню архітектуру та основні показники стійкості.

2. Сформувати систему показників та критеріїв оцінки функціональної стійкості корпоративних освітніх інформаційних систем в умовах зовнішніх та внутрішніх загроз.

3. Удосконалити метод машинного навчання, що дозволить оптимізувати процес управління адаптивних корпоративних освітніх інформаційних систем.

4. Розробити методику оцінки рівня інформаційної безпеки.

5. Розробити корпоративну освітню інформаційну систему на основі запропонованих в роботі методу та методики.

6. Удосконалити інформаційну технологію забезпечення функціональної стійкості освітньої інформаційної системи.

7. Запропонувати напрями подальшого розвитку засобів забезпечення інформаційної безпеки в освітній галузі.

Об'єкт дослідження – процес забезпечення функціональної стійкості адаптивних освітніх корпоративних інформаційних систем.

Предмет дослідження – методи та засоби забезпечення стійкого функціонування освітніх корпоративних інформаційних систем.

Методи дослідження. Для вирішення поставлених завдань, щодо досягнення задач і мети дисертаційної роботи використані різні методи, зокрема системний аналіз, узагальнення та наукової абстракції, методи математичної статистики при дослідженні достовірності запропонованих методів захисту інформації, методи моделювання та програмування при розробленні інформаційної технології кібербезпеки, методи адаптивного управління структурою процесів навчання та виконання науково-дослідних робіт, методи загальнонаукового передбачення та прогнозу.

Методологічну основу досліджень дисертації та вихідну інформаційну базу для дослідження становлять вітчизняні та зарубіжні наукові публікації, офіційна статистична звітність освітніх закладів та суб'єктів господарювання України.

Наукова новизна одержаних результатів полягає в наступному:

1. Набув подальшого розвитку метод метричного проксимального градієнта, який відрізняється від існуючих використанням моделі попарно-експоненціального марківського випадкового поля та методу вибору діагонального кроку, що дозволяє забезпечити швидшу збіжність та підвищити точність алгоритму машинного навчання. Це дозволяє покращувати процес навчання студентів за рахунок автоматичного визначення індивідуальної освітньої траєкторії та вчасно реагувати на будь-які зміни в адаптивних корпоративних освітніх інформаційних системах.

2. Розроблено методику оцінки рівня інформаційної безпеки освітньої інформаційної системи, наукова новизна якої визначається використанням адаптивних систем алгоритмів машинного навчання та динамічного оновлення моделей безпеки, що дозволяє підвищити ефективність автоматичного виявлення аномалій та оцінювати ризики в реальному часі.

3. Удосконалено інформаційну технологію забезпечення функціональної стійкості освітньої інформаційної системи з використанням технології блокчейн, яка відрізняється від існуючих впровадженням адаптивних інформаційних технологій для моніторингу та оптимізації процесів у реальному часі, що дозволяє підвищити ефективність навчальних процесів та забезпечити безперервне вдосконалення освітньої платформи.

Практичне значення одержаних результатів:

1. Практичне значення удосконаленого методу метричного проксимального градієнта полягає в підвищенні точності та швидкості алгоритмів машинного навчання, що дозволяє автоматизувати процес визначення індивідуальних освітніх траєкторій студентів. Це забезпечує адаптивне навчання та вчасне реагування на зміни в навчальному процесі, що підвищує ефективність освітньої системи в цілому.

2. Методика оцінки рівня інформаційної безпеки надає інструменти для комплексного аналізу економічних показників, ризиків та динамічних аспектів безпеки, що сприяє прийняттю більш обґрунтованих управлінських рішень та ефективному використанню ресурсів для забезпечення надійної захищеності освітньої інформаційної системи.

3. Удосконалена технологія забезпечення функціональної стійкості освітніх інформаційних систем завдяки використанню адаптивних інформаційних технологій і алгоритмів машинного навчання дозволяє автоматично оптимізувати процеси, покращувати управління інформаційними потоками та своєчасно реагувати на зміни, забезпечуючи стабільну роботу освітніх платформ навіть у динамічних умовах.

Таким чином, порівняно з існуючими підходами запропонована в роботі методика та розроблена на основі неї інформаційна технологія дозволяє автоматизувати процес управління, істотно підвищити точність і забезпечити стабільну роботу освітньої платформи в будь-якій ситуації.

Результати досліджень прийняті до впровадження ТОВ «УКР-ОН» (акт впровадження від 07.06.2024), ТОВ «АДЕЛІНА АУТСОРСИНГ» (довідка про впровадження №1-19 від 23.09.2024 р.), Державний університет інформаційно-комунікаційних технологій (акт впровадження від 13.09.2024), Інститут телекомунікацій і глобального інформаційного простору НАН України (акт впровадження від 20.08.2024), Київський столичний університет імені Бориса Грінченка (акт впровадження від 5.08.2024).

Особистий внесок здобувача. Всі положення, які виносяться на захист, належать особисто автору. В роботах, які опубліковані в співавторстві, особисто здобувачу належать: в [3] виділено методи, що забезпечують інформаційну безпеку телемереж; в [5] систематизовано інформацію щодо можливих загроз втручання в КІС, виконано класифікацію загроз інформаційної безпеки підприємств, розроблено блок-схему організації виконання вимог до засобів попередження загроз; в [5] проаналізовано наслідки рішення РНБО від 2.09.2015р. про введення санкцій для підприємств ІТ-технологій, зокрема використання антивірусів «Лабораторія Касперського», «Доктор Веб».

Апробація результатів дисертації. Основні положення роботи й висновки дисертації пройшли апробацію та були висвітлені у доповідях та тезах на науково-практичних заходах:

Науково-технічної конференції «Інформаційна безпека України» Київського національного університету ім. Т. Шевченка. – 12-13 березня 2015р., - Київ, Міжнародної науково-практичної конференції викладачів, аспірантів і студентів Волинського національного університету ім. Л. Українки «Перспективи розвитку економіки України». – 24-25 травня 2011р., – Луцьк, науково-технічної конференції «Інформаційна безпека України» Київського національного університету ім. Т. Шевченка. – 10-11 березня 2016р., – Київ, VIII міжнародної науково-практичної конференції «Проблеми економіки і управління на залізничному транспорті». – 10-11 жовтня 2013р., м. Судак АР Крим, III міжнародної науково-практичної конференції. – 8-10 листопада 2016р., Київський національний університет ім. Т. Шевченка, LXXIV наукової конференції професорсько-викладацького складу, аспірантів, студентів та співробітників відокремлених структурних підрозділів університету. – 16-18 травня 2018р., – Київ.

Публікації. Результати досліджень опубліковані в 13 працях, з яких 7 статей надруковані в наукових фахових виданнях. Авторський внесок у роботах, написаних у співавторстві, здобувачем розкрито у списку опублікованих праць за темою дисертації.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків.

Повний обсяг роботи 153 сторінок, у тому числі 115 сторінок основного тексту.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертації, сформульовано головну мету і задачі дослідження, визначено об'єкт, предмет, теоретичні та методологічні основи дослідження, розкрито наукову новизну і практичне значення дисертації, наведено інформацію про публікації, апробацію і впровадження результатів дослідження.

У першому розділі **«Теоретико-практичні основи функціональної стійкості адаптивних корпоративних освітніх інформаційних систем»** розглядаються основні концептуальні підходи до забезпечення надійного та безперервного функціонування інформаційних систем у закладах вищої освіти. Функціональна стійкість розуміється як здатність системи зберігати працездатність та ефективно виконувати свої функції в умовах змінних зовнішніх і внутрішніх факторів. Актуальність цієї проблеми зумовлена необхідністю забезпечення високого рівня надійності та безпеки інформаційних ресурсів, які є основою сучасних освітніх процесів.

У цьому контексті розглядаються сучасні підходи до забезпечення функціональної стійкості інформаційних систем, включаючи методи управління ризиками, резервування даних та захисту від кібератак. Особлива увага приділяється адаптивним підходам, які дозволяють системам реагувати

на зміни в навколишньому середовищі або в самій системі, зменшуючи ймовірність збоїв та підвищуючи їх стійкість. Адаптивність стає ключовим чинником для забезпечення функціональної стійкості, оскільки освітні установи стикаються з постійними змінами у вимогах до інформаційних систем, технологіях та кібербезпеці.

Особливе місце в дослідженні займають методи та моделі оцінки функціональної стійкості. Важливим елементом є інтеграція інформаційної безпеки в загальну архітектуру адаптивної системи, що дозволяє забезпечити захист від різних загроз, таких як атаки на мережеву інфраструктуру або втрати даних. Розглядаються моделі ризиків, механізми прогнозування збоїв та методи оцінки надійності інформаційних систем, які забезпечують більш точне визначення можливих ризиків і сценаріїв відновлення системи.

Сучасні заклади вищої освіти дедалі більше залежать від інформаційних систем для забезпечення навчального процесу, адміністрування та управління ресурсами. В умовах швидкого розвитку технологій та підвищених вимог до безпеки і надійності інформаційних систем виникає необхідність у забезпеченні їхньої функціональної стійкості. Системи повинні працювати безперервно навіть в умовах непередбачуваних зовнішніх впливів, технічних збоїв або кібератак, адже порушення їхньої роботи може спричинити серйозні наслідки для навчального процесу та безпеки даних.

Адаптивність стає ключовою характеристикою освітніх інформаційних систем, оскільки вона дозволяє системам підлаштовуватися до змін, реагувати на нові загрози та ризики, а також оптимізувати свою роботу відповідно до мінливих умов. Водночас актуальною є проблема інтеграції інформаційної безпеки у ці системи, адже це є важливою складовою їхньої загальної стійкості. Існуючі методи забезпечення стійкості не завжди достатньо ефективні в умовах постійної еволюції загроз і вимог до систем, тому необхідне впровадження нових підходів.

З огляду на це, завдання розробити методи та технології забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем набуває особливої актуальності. Це дозволить не лише забезпечити безперервність роботи систем, а й підвищити їхню надійність, безпеку та ефективність, що є критично важливим для сучасних освітніх установ.

Другий розділ дисертації **«Розробка моделей та методів машинного навчання для удосконалення адаптивних корпоративних освітніх інформаційних систем»** присвячено удосконаленню моделей та методів машинного навчання для підвищення ефективності та безпеки у функціонуванні адаптивних корпоративних освітніх інформаційних систем.

Машинне навчання дозволяє створювати персоналізовані освітні траєкторії, автоматично аналізувати успішність та потреби співробітників, а також прогнозувати та запобігати потенційним проблемам у навчанні. Крім того, важливим аспектом використання методів машинного навчання є забезпечення безпеки адаптивних корпоративних освітніх інформаційних систем, перешкоджанню злому системи та виявлення протиправних дій всередині системи. Це сприяє оптимізації навчальних ресурсів, підвищенню

кваліфікації працівників і, як наслідок, загальної продуктивності організації, що є критично важливим у сучасному конкурентному бізнес-середовищі.

Отже, в другому розділі запропоновано використання попарно-експоненціального марковського випадкового поля, що розкриває марківську структуру за різнорідними змінними; сформульовано наближену задачу максимальної правдоподібності, ввівши верхню границю логарифмічної статистичної функції; розроблено масштабований алгоритм ADMM з відновленнями в закритій формі; доведено, що запропонована оцінка є розрідженою; запропонована методика на основі введеної моделі та алгоритму.

Попарно-експоненціальне марківське випадкове поле, що належить до класу багатовимірних експоненціальних розподілів, виступає важливим інструментом для моделювання складних взаємодій у корпоративних освітніх інформаційних системах (КОІС). Воно дозволяє ефективно представляти спільний розподіл різнорідних змінних, що значно прискорює аналіз структурної організації вузлів із невідомими параметрами. Такий підхід може бути корисним у визначенні індивідуальних освітніх траєкторій студентів, оскільки допомагає моделювати їхні навчальні потреби та поведінкові закономірності на основі експоненціальних розподілів.

Алгоритм змінного метричного проксимального градієнта, який використовує модифікацію проксимального градієнта, забезпечує гнучкість у виборі кроків і підлаштовується під особливості навчальної системи. Наприклад, у контексті освітніх траєкторій, швидка збіжність алгоритму дозволяє швидко коригувати рекомендації щодо навчальних матеріалів і стратегії навчання для кожного студента. На основі дослідження вибору кроку алгоритму, було встановлено, що використання діагонального кроку є ефективнішим порівняно зі скалярним. Однак, наукова література ще не пропонує універсальних правил для оптимізації діагональних кроків в умовах випуклої оптимізації.

У роботі запропоновано адаптивний підхід до вибору діагональної метрики на основі методу Барзілая-Борвейна (ББ). Цей підхід інтегрує проксимальний метод Ньютона з класичним проксимальним градієнтом, дозволяючи враховувати індивідуальні параметри студентів, їхні навчальні досягнення та складність матеріалу. Адаптивність алгоритму сприяє зменшенню обчислювальних витрат і більш точному наближенню гессіана, що дозволяє покращити прогнозування освітніх траєкторій. Це особливо важливо для великих освітніх систем, де необхідно швидко та точно моделювати динамічні процеси, що відбуваються під час навчання. Емпіричні дослідження показали, що запропонований підхід значно покращує збіжність і підвищує ефективність визначення освітніх траєкторій у порівнянні зі скалярними методами.

Така модель дозволяє адаптивним КОІС не лише надавати індивідуальні рекомендації студентам, але й постійно вдосконалювати навчальні стратегії з урахуванням змін у поведінкових закономірностях і потребах студентів.

Для відображення гессіанської геометрії f введено діагональну метрику M^n , яка на кожній ітерації n обчислюється наступним чином:

$$\begin{aligned} \min_{m \in \mathbb{R}^n} \quad & \|Mc^n - y^n\|_2^2 + \eta \|M - M^{n-1}\|_F^2 \\ & (\beta_{BB1}^n)^{-1} J \leq M \leq (\beta_{BB2}^n)^{-1} J \\ & M = \text{diag}(m) \end{aligned} \quad (1)$$

де гіперпараметр $\eta > 0$ управляє компромісом між задоволенням січної стану $M^n c^n \approx y^n$ та узгодженістю з попередньою метрикою M^{n-1} . Якщо Гессіан змінюється швидко, то необхідно обрати значення μ достатньо малим. В такому випадку цей параметр буде грати роль числового захисту. Якщо ж Гессіан при ітераціях не сильно змінюється, то обираємо велике значення μ . Діагональні елементи обмежені, тобто гарантовані кроком ББ:

$$\begin{aligned} \beta_{BB1}^n &:= \|c^n\|_2^2 / (c^n y^n); \\ \beta_{BB2}^n &:= (c^n, y^n) / \|y^n\|_2^2 \end{aligned} \quad (2)$$

Запропонований алгоритм з діагональною метрикою буде мати наступні кроки:

1. Задаємо параметри $K_{ls} \geq 1$, $\alpha > 1$, $\eta > 0$, початкові точки $x^0, x^1 \in \mathbb{R}^n$ та початкову метрику $M^0 \in S_{++}^n$

2. Обчислюємо β_{BB1}^n та β_{BB2}^n за формулою

$$\begin{aligned} \beta_{BB}^n &:= \beta_{BB}(c^n, y^n) = \\ &= \begin{cases} \beta_{BB2}^n, & \text{якщо } \beta_{BB1}^n < \delta \beta_{BB2}^n \\ \beta_{BB1}^n - \frac{1}{\delta} \beta_{BB2}^n, & \text{в інших випадках} \end{cases} \end{aligned} \quad (3)$$

3. Ініціалізуємо M^n за формулою

$$m_i^n = \begin{cases} \frac{1}{\beta_{BB1}^n}, & \frac{c_i^n y_i^n + \mu m_i^{n-1}}{(c_i^n)^2 + \mu} < \frac{1}{\beta_{BB1}^n} \\ \frac{1}{\beta_{BB2}^n}, & \frac{c_i^n y_i^n + \mu m_i^{n-1}}{(c_i^n)^2 + \mu} > \frac{1}{\beta_{BB2}^n} \\ \frac{c_i^n y_i^n + \eta m_i^{n-1}}{(c_i^n)^2 + \eta}, & \text{в інших випадках} \end{cases} \quad (4)$$

4. Обчислюємо $x^{n+1} := \text{prox}_{q, M^n} \left(x^n - (M^n)^{-1} \nabla f(x^n) \right)$.

5. Повторюємо вирази

$$M^n := \alpha M^n$$

В роботі розглядається узгоджена оптимізація, яка задається наступним чином:

$$\min_{x_1, \dots, x_H \in R^n} \sum_{i=1}^H f_i(x_i) + \partial_S(x_1, \dots, x_H) \quad (5)$$

де H – це кількість розподілених вузлів графічної моделі. Для кожного вузла $i \in \{1 \dots H\}$, $f_i: R^n \rightarrow R$ – це опуклі та диференційовані функції з даними D_i , $x_i \in R^n$ – локальні копії спільної змінної, обмежені узгодженим набором $C = \{(x_1, \dots, x_H) \mid x_1 = \dots = x_H\}$, ∂_S – індикаторна функція на S .

Щоб зберегти властивість розподіленої узгодженої оптимізації (16), було запропоновано використання блочно-діагональної структури для метрики. При будь-якому блочно-діагональному підході кроки градієнта рівномірно розподіляються між вузлами, а наступне узгоджене оновлення стає зваженим середнім для локальних змінних кожного вузла. Це особливо важливо для вирішення масштабних завдань машинного навчання. У стандартних методах проксимального градієнта крок узгодження зазвичай базується на простому середньому значенні локальних змінних, що не завжди є оптимальним для алгоритмів машинного навчання. Зокрема, деякі вузли можуть обробляти значно більші обсяги даних і бути більш надійними, ніж інші, тому їхнім оновленням слід надавати більшу вагу під час узгодження.

Ця задача вирішується шляхом вибору метрики з діагональною або блочною структурою, яка дозволяє врахувати різницю в надійності вузлів. На відміну від скалярного методу Барзілая-Борвейна (ББ), діагональний підхід ефективніше справляється з такою ситуацією. У подальшій роботі було запропоновано дві стратегії для вибору елементів блочно-діагональної метрики, що дозволяють оптимізувати процес узгодження. Основна ідея – апроксимувати локальний гессіан $\nabla^2 f_i(x_i^n)$ в кожному вузлі i лише на основі локальної інформації, тобто локальний крок $c_i^n = x_i^n - x_i^{n-1}$ та локальну зміну градієнта $y_i^n = \nabla f_i(x_i^n) - \nabla f(x_i^{n-1})$. На основі цього запропоновано наступні кроки ББ:

1. Локальний ББ крок. Кожен вузол оцінює $M_i^n = \beta_{\text{ББ}}(c_i^n, y_i^n)J$ з (14) на основі локальних змінних c_i^n та y_i^n . В такому випадку метрика задається наступним чином:

$$M_{\text{лок.ББ}}^n = \text{blndiag}(M_1^n, \dots, M_H^n) \quad (6)$$

2. Локальний діагональний крок ББ. Кожен вузол оцінює $M_i^n := M_{\text{ДББ}}(c_i^n, y_i^n)$ за (15). Потім задається метрика наступним чином:

$$M_{\text{лок.ДББ}}^n = \text{blndiag}(M_1^n, \dots, M_H^n) \quad (7)$$

Отже, запропонована діагональна метрика забезпечує кращу оцінку погано обумовленого локального гессіана порівняно зі стандартним

скалярним кроком ББ, що призводить до швидшої збіжності алгоритму. У поєднанні з немонотонним лінійним пошуком загальний алгоритм гарантовано є збіжним. Нарешті, для декількох програм машинного навчання із штучними та реальними наборами даних, емпіричні результати демонструють кращу поведінку збіжності для запропонованої методології.

Інтеграція машинного навчання в освітні системи дозволяє автоматизувати процеси персоналізації навчання, покращити аналіз даних про успішність та потреби учнів, а також забезпечити адаптивність навчальних матеріалів відповідно до індивідуальних вимог. Це не лише підвищує ефективність навчання, але й сприяє розвитку інноваційного потенціалу організації, роблячи її більш гнучкою та конкурентоспроможною на ринку.

Таким чином, в дисертаційній роботі реалізовано перший науковий результат, який полягає в тому, що набув подальшого розвитку метод метричного проксимального градієнта, який відрізняється від існуючих використанням моделі попарно-експоненціального марківського випадкового поля та методу вибору діагонального кроку, що дозволяє забезпечити швидшу збіжність та підвищити точність алгоритму машинного навчання. Це дозволяє покращувати процес навчання за рахунок автоматичного визначення індивідуальної освітньої траєкторії студента та вчасно реагувати на будь-які зміни в інформаційній системі.

У третьому розділі **«Удосконалення методів та технологій забезпечення кіберзахисту в освітній галузі»** розглянуто особливості оцінки загроз інформаційній безпеці.

Вирішення проблемних питань інформаційної безпеки потребує комплексного обґрунтування підходів, при цьому повинні бути досліджені всі можливі фактори, показники, індикатори та інтегрально оцінений їх вплив на фінансово-економічний стан вузу.

Оцінка загроз інформаційній безпеці вищих навчальних закладів (ВНЗ) має свої особливості та відмінності від загальноприйнятих положень для інших галузей. Варто зауважити, що в освітній галузі наразі відсутня загальноприйнята методика для комплексної оцінки інформаційної безпеки. Інформаційна безпека різних вузів у системі освітньої галузі має ґрунтуватися на організаційно-технічних умовах стабільного функціонування системи при виділенні обмежених ресурсів, своєчасному виявленні загроз техніко-технологічного, інформаційного та економічного характеру, а також розробці системи заходів, що забезпечать нейтралізацію або мінімізацію їх впливу. При цьому оцінка загроз інформаційній безпеці вузів має враховувати особливості організації їх науково-педагогічної діяльності. Оцінка інформаційної безпеки повинна надати відповідь щодо можливого впливу загроз та доцільності застосування засобів і заходів, спрямованих на їх нейтралізацію.

Алгоритм оцінки рівня інформаційної безпеки для інформаційної системи (рис. 1) розпочинається зі збору даних із різних джерел, таких як логи системи (журнали доступу, події безпеки), дані із систем моніторингу (вразливості, попередження), а також внутрішніх і зовнішніх джерел загроз. На цьому етапі дані повинні бути перевірені на повноту та актуальність. Якщо

дані містять дублікати або застарілу інформацію, вони виключаються. Формально, зібрані дані можуть бути представлені у вигляді множини $D=\{d_1, d_2, \dots, d_n\}$, де кожен елемент d_i вважається валідним, якщо виконується умова $d_i \in \text{валідним} \Leftrightarrow (d_i \text{ не дублікат}) \wedge (d_i \text{ актуальний})$. Це забезпечує використання тільки актуальних і релевантних даних для подальшого аналізу.

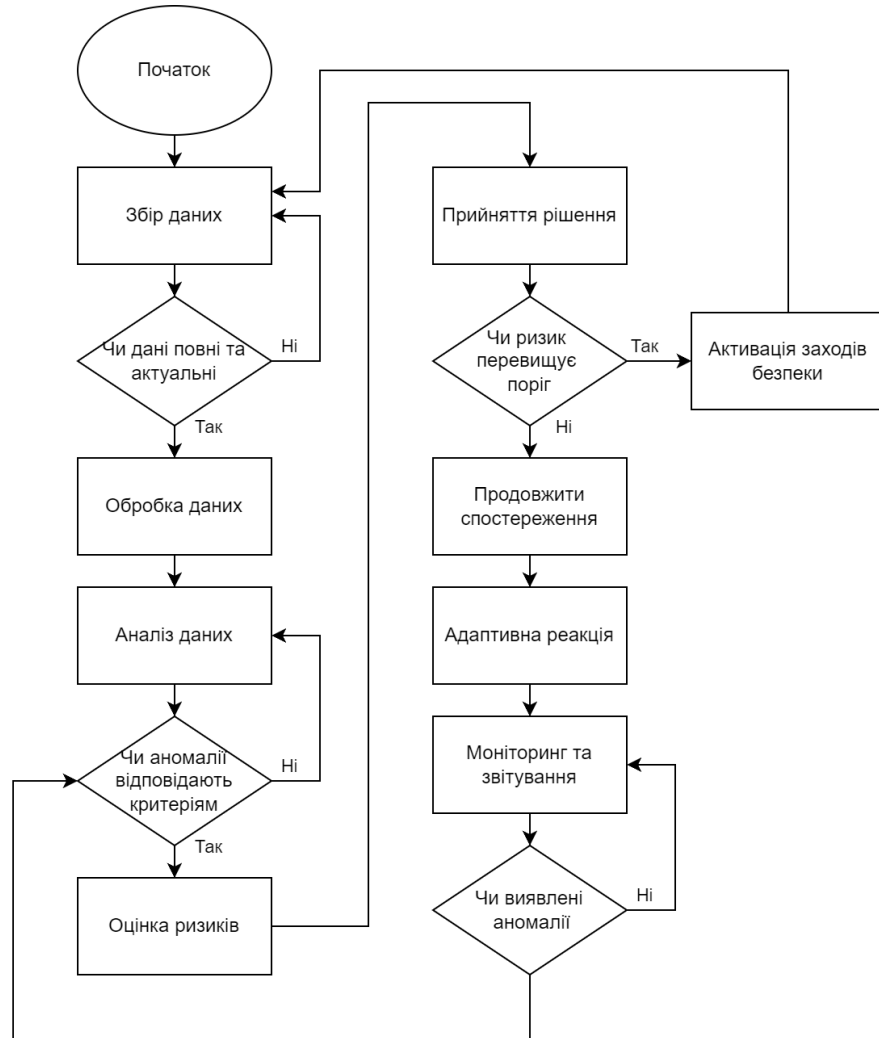


Рис. 1. Блок-схема алгоритму оцінки рівня інформаційної безпеки для інформаційної системи

На етапі попередньої обробки дані очищуються від дублікатів і некоректних записів, що підвищує точність подальшого аналізу. Дані, які не відповідають вимогам, виключаються з подальшої обробки. Умова виключення виглядає так: якщо $d_i \in \text{дублікатом або некоректним}$, то d_i не враховується. Після цього система переходить до аналізу даних за допомогою алгоритмів машинного навчання для виявлення аномалій. Тут застосовуються алгоритми класифікації або кластеризації, що дозволяє системі ідентифікувати аномалії на основі заданого порогу. Множина аномалій визначається як $A=\{a_1, a_2, \dots, a_m\}$, де $a_i \in \text{аномалією} \Leftrightarrow (a_i \text{ перевищує поріг})$.

Оцінка ризиків проводиться на основі ймовірності виникнення загрози та її потенційного впливу. Ризик кожної загрози розраховується за формулою

$$R_i = P_i \cdot I_i, \quad (8)$$

де P_i — ймовірність загрози, а I_i — вплив загрози. Якщо ризик R_i перевищує встановлений поріг T , то система активує протоколи безпеки: $R_i > T \Rightarrow$ Активація заходів безпеки. Таким чином, на основі оціненого рівня ризику система самостійно приймає рішення щодо активації відповідних заходів.

Фінальним кроком є моніторинг системи та адаптація до нових загроз. Якщо з'являються нові дані D_{new} , система оновлює свої моделі: $M_{new} = f(M_{old}, D_{new})$, де M_{new} — нова модель, а M_{old} — попередня модель. Це дозволяє системі адаптуватися до нових загроз у режимі реального часу, забезпечуючи її функціональну стійкість і здатність до швидкої реакції на зміни в середовищі загроз.

Запропонована модель оцінки рівня інформаційної безпеки демонструє значні переваги порівняно з існуючими моделями завдяки автоматизації, адаптивності та використанню сучасних технологій, що робить її більш ефективною у боротьбі з новими загрозами.

Таблиця 1

Порівняльна характеристика моделей

Модель	Особливості застосування	Переваги	Недоліки
Модель OCTAVE	Використовується для оцінки організаційних ризиків.	Фокус на управлінні ризиками, розгляд всіх аспектів безпеки.	Висока складність, потребує значних ресурсів.
Модель FAIR	Оцінка ризиків та їх фінансового впливу.	Визначення економічної цінності ризиків, простота.	Не враховує технічні аспекти, зосереджена на фінансах.
Модель NIST SP 800-30	Оцінка ризиків у відповідності до стандартів NIST.	Стандартизований підхід, підтримка різних галузей.	Може бути складним для невеликих організацій.
Модель ISO/IEC 27001	Стандарт для управління інформаційною безпекою.	Всебічне управління безпекою, міжнародна визнаність.	Високі вимоги до документації, потреба у сертифікації.
<i>Запропонована модель</i>	<i>Адаптивна, заснована на аналізі даних та машинному навчанні.</i>	<i>Автоматизоване прийняття рішень, постійне навчання, адаптивність до нових загроз.</i>	<i>Потребує належного налаштування та наявності даних для навчання.</i>

Запропонована модель має найвищу ефективність (90%) та найшвидший час реакції, а також показує високу адаптивність до нових загроз. Вона також характеризується низькою складністю впровадження і мінімальною кількістю помилкових спрацьовувань, що робить її економічно вигідним рішенням для

організацій (табл. 2). Ці метрики підкреслюють переваги нової моделі у порівнянні з традиційними методами, які можуть вимагати більше ресурсів і часу для впровадження та адаптації.

Таблиця 2
Порівняльна характеристика моделей за відповідними метриками

Модель	Ефективність моделі (E)	Час реакції (TR)	Складність впровадження (CI)	Адаптивність (A)	Кількість помилок спрацьовувань (FP)	Вартість (C)
Модель OCTAVE	70%	Середній	Висока	Низька	15%	Середня
Модель FAIR	63%	Довгий	Середня	Низька	20%	Висока
Модель NIST SP 800-30	70%	Середній	Висока	Низька	10%	Середня
Модель ISO/IEC 27001	85%	Середній	Висока	Низька	5%	Висока
<i>Запропонована модель</i>	90%	<i>Швидкий</i>	<i>Низька</i>	<i>Висока</i>	2%	<i>Низька</i>

Таким чином в дисертаційній роботі реалізовано другий науковий результат, який полягає в розробці методики оцінки рівня інформаційної безпеки освітньої інформаційної системи, наукова новизна якої визначається використанням адаптивних систем алгоритмів машинного навчання та динамічного оновлення моделей безпеки, що дозволяє підвищити ефективність автоматичного виявлення аномалій та оцінювати ризики в реальному часі.

Четвертий розділ дисертації «**Розробка адаптивної корпоративної освітньої інформаційної системи з використанням методів машинного навчання**» присвячено розробці методики та інформаційної технології забезпечення функціональної стійкості корпоративної освітньої інформаційної системи.

В роботі представлено математичну модель забезпечення функціональної стійкості адаптивної корпоративної освітньої системи. Вона складається з декількох ключових компонентів: функціональність системи, безпека, рівень ризиків і адаптивність навчальних траєкторій. Ці змінні дозволяють оцінити ефективність функціонування системи в умовах різних загроз і змінних вимог, а також як вона підлаштовується під індивідуальні потреби користувачів.

Цільова функція описує максимізацію ефективності навчального процесу за умови мінімізації ризиків та забезпечення безпеки доступу. Ця модель повинна враховувати адаптивність освітніх траєкторій і контроль ризиків, а також збереження безперервності роботи системи

$$\text{Maximize } F(T, S, R, A) = \alpha_1 T + \alpha_2 S - \alpha_3 R + \alpha_4 A$$

$$T_i = f(X_1, X_2, \dots, X_n)$$

$$R = \sum_{i=1}^m P_i \cdot I_i \leq R_{\max} \quad (9)$$

$$S = A \cdot (q - R) \geq S_{\min}$$

$$A \geq A_{\min}$$

$$C_T + C_S + C_R \leq C_{\text{total}}$$

де T – функціональність системи, S – рівень безпеки, R – рівень ризику, A – адаптивність системи, P_i – ймовірність ризику, I_i – ступінь впливу ризику, C_T – витрати на функціональність, C_S – витрати на безпеку, C_R – витрати на управління ризиками, C_{total} – загальні допустимі витрати, T_{total} – загальний допустимий ресурс, S_{\min} – мінімальний рівень безпеки.

На основі математичної моделі функціональної стійкості адаптивної корпоративної освітньої системи розроблена інформаційна технологія забезпечення функціональної стійкості. Блок-схема інформаційної технології забезпечення функціональної стійкості освітньої інформаційної системи представлена на рис. 2. Вона передбачає використання сучасних інформаційних технологій для моніторингу та адаптації освітнього процесу в реальному часі. Основою технології є інтеграція алгоритмів машинного навчання, які аналізують поведінку користувачів, виявляють аномалії та прогнозують зміни в системі. Це дозволяє автоматично коригувати навчальні траєкторії студентів, підвищуючи ефективність навчальних процесів та забезпечуючи індивідуалізацію освітніх шляхів. Завдяки постійному моніторингу та аналізу даних, можна своєчасно реагувати на зміни, забезпечуючи надійну роботу системи навіть в умовах зростаючих навантажень або зовнішніх загроз.

Інформаційна технологія також включає механізми оптимізації інформаційних потоків і ресурсів за допомогою лінійного програмування та теорії графів, що дозволяє підвищити продуктивність системи. Крім того, вона застосовує аналіз ризиків і витрат для оцінки ефективності заходів безпеки, а також системну динаміку для прогнозування довгострокових наслідків змін у платформі. Цей комбінований підхід дозволяє створити освітню платформу, яка є гнучкою, стійкою до зовнішніх загроз і здатною адаптуватися до індивідуальних потреб користувачів, забезпечуючи безперервне вдосконалення навчальних процесів.

Таким чином, в дисертаційній роботі реалізовано третій науковий результат, який полягає в удосконаленні інформаційної технології забезпечення функціональної стійкості освітньої інформаційної системи з використанням технології блокчейн, яка відрізняється від існуючих впровадженням адаптивних інформаційних технологій для моніторингу та оптимізації процесів у реальному часі, що дозволяє підвищити ефективність навчальних процесів та забезпечити безперервне вдосконалення освітньої платформи.

Інформаційна система, що побудована на основі запропонованих в роботі методів, методики та інформаційної технології буде включати в себе декілька сервісів різного рівня захисту. Також система має включати в себе і сторону студента та інтеграцію з іншими системами управління.

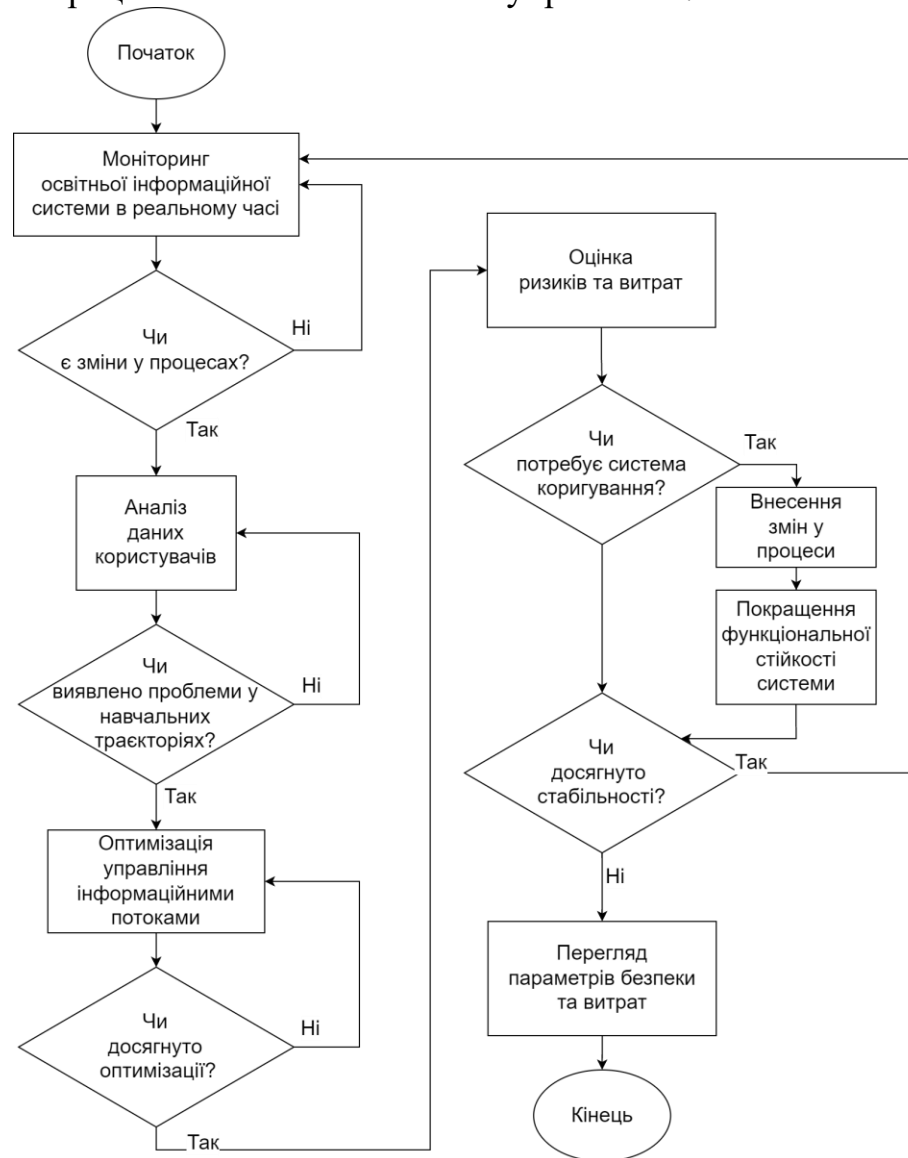


Рис. 2. Блок-схема інформаційної технології забезпечення функціональної стійкості освітньої інформаційної системи

Функціонал інформаційної системи:

1. Розклад, електронний журнал відвідуваності, робочі плани, силабуси дисциплін.

2. Редагування електронного журналу відвідування та оцінок, бронювання вільних аудиторій, запит на зміну розкладу, система управління задачами (аналог Jira або Trello), опитування.

3. Документообіг, категорії з НДР, бухгалтерські дані, особистий кабінет викладача.

4. Робота з системою доступу викладачів, логування, моніторинг підозрілих подій з використанням методів машинного навчання.

5. Для студента використовується штучний інтелект для покращення навчання та побудови індивідуальної освітньої траєкторії.

Технічна частина проекту передбачає використання двох серверних масивів: основного для обчислювальних процесів і зберігання даних, та бекапного для зберігання резервних копій і моніторингу системи. Основна система будується на Docker-контейнерах для підвищення безпеки та можливості швидкого перенесення в хмару. Також застосовуються посилені мережеві заходи, зокрема, налаштування Firewall і моніторинг підозрілих подій із використанням машинного навчання, що дозволяє реагувати на загрози в режимі реального часу.

Інтелектуальна частина проекту включає розробку інтелектуального наставника для студентів, який на основі аналізу їхніх даних створює рекомендації щодо навчального процесу. Завдяки збору даних і взаємодії зі студентом, система допомагає йому коригувати навчальні стратегії для досягнення кращих результатів. Така система включає функції зворотного зв'язку та адаптації під конкретні потреби студентів.

Дизайн та інтерфейс системи побудовані на мінімалістичному підході з використанням простих кольорів і монохромних іконок. Головна сторінка (Dashboard) надає користувачам швидкий доступ до основної інформації, як-от прогрес у навчанні, майбутні події та завдання. Для адміністраторів доступні додаткові функції моніторингу і управління, а також корпоративні інструменти для безпечної командної роботи і контролю версій систем.

ВИСНОВКИ

В результаті дисертаційних досліджень вирішено важливе науково-практичне завдання розробки методів та технології забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем. Це завдання має суттєве значення для забезпечення стабільної та безперервної роботи адаптивних корпоративних освітніх інформаційних систем, оскільки воно спрямоване на підвищення їхньої стійкості до внутрішніх і зовнішніх загроз, що є критичним для підтримки безпеки даних та ефективного навчального процесу в сучасних умовах.

В дисертації одержані наступні основні результати:

1. Проведено детальний аналіз сучасного стану адаптивних корпоративних освітніх інформаційних систем, включаючи їхню архітектуру та основні показники стійкості. Виявлено ключові проблеми та виклики, що

стосуються забезпечення їхньої стабільної роботи в умовах зовнішніх та внутрішніх загроз.

2. Сформовано систему показників та критеріїв для оцінки функціональної стійкості корпоративних освітніх інформаційних систем. Запропонована система дозволяє враховувати як зовнішні, так і внутрішні загрози, що сприяє покращенню контролю та управління стійкістю систем.

3. Запропоновано вдосконалений метод машинного навчання, який дозволяє оптимізувати процес управління адаптивними корпоративними освітніми інформаційними системами. Це забезпечило підвищення ефективності прийняття рішень щодо управління стійкістю системи у динамічних умовах.

4. Розроблено методику оцінки рівня інформаційної безпеки, що враховує адаптивні можливості системи та використовує алгоритми машинного навчання для виявлення аномалій та оцінки ризиків в реальному часі.

5. Удосконалено інформаційну технологію забезпечення функціональної стійкості корпоративної освітньої інформаційної системи, що дозволило підвищити її здатність адаптуватися до зовнішніх впливів та загроз без втрати ефективності.

6. На основі запропонованих методів та методики створено корпоративну освітню інформаційну систему, яка забезпечує високу функціональну стійкість та інформаційну безпеку в умовах постійних загроз.

7. Результати досліджень прийняті до впровадження ТОВ «УКР-ОН» (акт впровадження від 07.06.2024), ТОВ «АДЕЛІНА АУТСОРСИНГ» (довідка про впровадження №1-19 від 23.09.2024 р.), Державний університет інформаційно-комунікаційних технологій (акт впровадження від 13.09.2024), Інститут телекомунікацій і глобального інформаційного простору НАН України (акт впровадження від 20.08.2024), Київський столичний університет імені Бориса Грінченка (акт впровадження від 5.08.2024).

8. Мета досліджень підвищення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем за допомогою розроблених в роботі методів та технологій та з використанням методів машинного навчання досягнута.

9. Подальший напрямок наукових досліджень може бути зосереджений на розробці нових алгоритмів для аналізу великих обсягів даних у реальному часі, а також удосконалення методів підвищення функціональної стійкості корпоративних освітніх систем через інтеграцію з хмарними технологіями та їх масштабування для великих навчальних закладів.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Ананченко О.Є. Розробка корпоративної освітньої інформаційної системи за допомогою методів машинного навчання та методик забезпечення інформаційної безпеки / Том 2 № 22 (2023): Кібербезпека: освіта, наука, техніка, С. 264-271.

2. Ананченко О.Є. Методика оцінки ефективності забезпечення інформаційної безпеки освітньої інформаційної системи / Том 1 № 21 (2023): Кібербезпека: освіта, наука, техніка, С. 297-305.

3. Ананченко О.Є. Комплексне застосування підприємствами методів забезпечення економіко-інформаційної безпеки телекомунікаційних мереж загального користування / В.Д. Данчук, В.М. Гурнак, О.Є. Ананченко, В.Є. Ананченко // Збірник наукових праць Державного економіко-технологічного університету транспорту. – 2015. – Вип.31. – К.: ДЕТУТ, - С. 196-203.

4. Ананченко О.Є. Питання формування організаційної структури системи управління інформаційною безпекою підприємства / О.Є. Ананченко // Науково-технічний журнал «Сучасний захист інформації». №1. – 2016. – К.: ДУТ. – С. 79-83.

5. Ананченко О.Є. Організація виконання вимог до засобів забезпечення інформаційної безпеки на підприємствах / В.Д. Данчук, О.Є. Ананченко // Науковий журнал «Управління проектами, системний аналіз і логістика» - ч.1 – Вип. 46. – 2015. – К.: НТУ – С. 40-47.

6. Ананченко О.Є. Питання безпеки при використанні ресурсів корпоративних інформаційних систем / Ананченко О.Є. // Збірник наукових праць Державного економіко-технологічного університету транспорту – 2016 – Вип.35 – К.: ДЕТУТ. – С. 154-159.

7. Ананченко О.Є. Необхідність врахування економічних наслідків при прийнятті макрополітичних рішень / В.М. Гурнак, А.В. Петунін, О.Є. Ананченко // Управління проектами, системний аналіз і логістика. – К.: НТУ. – 2015. Вип.16 – С. 40-47.

8. Ананченко О.Є. Удосконалення методів забезпечення інформаційної безпеки корпоративних інформаційних систем / В.Д. Данчук, О.Є. Ананченко, В.Є. Ананченко // Збірник наукових доповідей та тез науково-технічної конференції «Інформаційна безпека України» Київського національного університету ім. Т. Шевченка. – 12-13 березня 2015р. – м. Київ. – С. 96-97.

9. Ананченко О.Є. Важливість інформаційної складової при проведенні міжнародних заходів / О. Ананченко, В. Ананченко // Збірник тез XVI міжнародної науково-практичної конференції викладачів, аспірантів і студентів Волинського національного університету ім. Л. Українки «Перспективи розвитку економіки України» – 24-25 травня 2011р. – м. Луцьк. – С. 257-259.

10. Ананченко О.Є. Основні методи забезпечення інформаційної безпеки при використанні ресурсів корпоративних інформаційних систем / О.Є. Ананченко // Збірник наукових доповідей та тез науково-технічної конференції «Інформаційна безпека України» Київського національного університету ім. Т. Шевченка. – 10-11 березня 2016р. – м. Київ. – С. 14-15.

11. Ананченко О.Є. Стан і проблеми міжнародних транзитних перевезень / В.М. Гурнак, М.В. Гурнак, О.Є. Ананченко // Матеріали VIII міжнародної науково-практичної конференції «Проблеми економіки і управління на залізничному транспорті». –10-11 жовтня 2013р. – м. Судак. АР Крим. С. 93-95.

12. Ананченко О.Є. Необхідність впровадження організаційних заходів та технологічних методів захисту електронних інформаційних ресурсів / В.Д.

Данчук, О.Є. Ананченко, / LXXIV наукова конференція професорсько-викладацького складу, аспірантів, студентів та співробітників відокремлених структурних підрозділів університету. – К.: НТУ, 2018. – С. 517.

13. Ананченко О.Є. Питання комплексного підходу при впровадженні заходів інформаційної безпеки / В.Д. Данчук, О.Є. Ананченко// Інформаційні технології та взаємодії. III міжнародна науково-практична конференція 8-10 листопада 2016 р. Київський національний університет ім. Т. Шевченка. С.217-218.

АНОТАЦІЯ

Ананченко О.Є. Методи та технології забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 «Інформаційні технології». – Державний університет інформаційно-комунікаційних технологій. Київ. 2024.

Дисертаційна робота присвячена розробці та обґрунтуванню теоретичних та методичних підходів щодо забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем закладів вищої освіти. В основу дослідження покладено проблему підвищення надійності та ефективності функціонування інформаційних систем у контексті зростаючих вимог до інформаційної безпеки та адаптивності.

Наукова новизна дослідження полягає у розвитку методу метричного проксимального градієнта, який завдяки використанню моделі попарно-експоненціального марківського випадкового поля та методу вибору діагонального кроку забезпечує швидшу збіжність і підвищує точність алгоритму машинного навчання. Це дозволяє автоматизувати процес визначення індивідуальних освітніх траєкторій студентів і оперативно реагувати на зміни в навчальному процесі. Розроблено методику оцінки рівня інформаційної безпеки, яка базується на адаптивних системах алгоритмів машинного навчання та динамічному оновленні моделей безпеки. Такий підхід дозволяє ефективніше виявляти аномалії та оцінювати ризики в реальному часі, що сприяє прийняттю обґрунтованих управлінських рішень та ефективному використанню ресурсів для підвищення захищеності системи. Крім того, удосконалено інформаційну технологію забезпечення функціональної стійкості за допомогою технології блокчейн, що дозволяє автоматично оптимізувати процеси та забезпечити стабільну роботу освітніх платформ навіть у динамічних умовах. Практична значущість отриманих результатів полягає у підвищенні ефективності навчальних процесів, забезпеченні адаптивного підходу до навчання та покращенні управління інформаційними потоками, що в цілому сприяє підвищенню якості освітніх послуг та безперервному вдосконаленню освітніх платформ.

Результати роботи мають вагомe значення для підвищення надійності, безпеки та ефективності функціонування корпоративних освітніх інформаційних систем, що сприятиме розвитку освітніх закладів у цифрову епоху.

Ключові слова: функціональна стійкість, методи захисту інформаційних технологій, автоматизована система, освітня інформаційна система, машинне навчання, блокчейн, NFT.

SUMMARY

Ananchenko O.E. Methods and technologies for ensuring the functional stability of adaptive corporate educational information systems.

Dissertation for the degree of Candidate of Technical Sciences in the speciality 05.13.06 'Information Technologies.' - State University of Information and Communication Technologies. Kyiv. 2024.

The dissertation is devoted to the development and substantiation of theoretical and methodological approaches to ensuring the functional sustainability of adaptive corporate educational information systems of higher education institutions. The research is based on the problem of increasing the reliability and efficiency of information systems in the context of growing requirements for information security and adaptability.

The scientific novelty lies in the development of a metric proximal gradient method, incorporating a pairwise-exponential Markov random field model and a diagonal step selection method. This approach enables faster convergence and improved accuracy of machine learning algorithms, automating the identification of individual learning paths for students and ensuring timely responses to changes in the educational process. Additionally, a methodology for assessing the information security of educational information systems has been developed. This method uses adaptive machine learning systems and dynamic model updates, allowing for more effective anomaly detection and real-time risk assessment. It supports better decision-making and resource optimization for enhanced system security, ensuring that vulnerabilities are quickly addressed. The study also enhances information technology for maintaining the stability of educational systems through blockchain. This integration of adaptive technologies enables real-time monitoring and process optimization, ensuring stable operation even under dynamic conditions.

The practical significance of the results is evident in several areas. The improved metric proximal gradient method increases the speed and accuracy of machine learning, automating the determination of individual learning trajectories. This ensures adaptive learning and enhances overall educational efficiency. The proposed security assessment methodology enables comprehensive analysis of risks and security, supporting informed management decisions. Lastly, the enhanced stability technology ensures automatic optimization and effective management of information flows, guaranteeing consistent and resilient operation of educational platforms.

The results of the work are of great importance for increasing the reliability, security and efficiency of the functioning of corporate educational information systems, which will contribute to the development of educational institutions in the digital era.

Keywords: functional stability, information technology protection methods, automated system, educational information system, machine learning, blockchain, NFT.