Міністерство освіти і науки України
Державний університет інформаційно-комунікаційних технологій

Кваліфікаційна наукова праця
на правах рукопису

АНАНЧЕНКО ОЛЕКСІЙ ЄВГЕНОВИЧ

УДК 004.378:005.8:005.42:005.22

МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ АДАПТИВНИХ КОРПОРАТИВНИХ ОСВІТНІХ ІНФОРМАЦІЙНИХ СИСТЕМ

05.13.06 – Інформаційні технології

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело. _____ О.Є. Ананченко

Науковий керівник Бондарчук Андрій Петрович,

доктор технічних наук, професор

Київ - 2024

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.

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 в роботі поставлено та вирішено актуальне науково-практичне завдання, яке полягає в розробці методи та технології забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем. 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.

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.

У дисертаційній роботі здійснено всебічне дослідження методів і технологій для забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем, орієнтованих на підтримку стійкого та надійного функціонування навіть у динамічному та загрозливому середовищі. Основний акцент зроблено на побудові таких інформаційних систем, які б могли ефективно адаптуватися до змін у навчальному процесі, своєчасно реагувати на зовнішні виклики і кіберзагрози, а також забезпечувати високу надійність обробки даних для задоволення потреб сучасного навчального середовища.

Одним із головних наукових досягнень є розробка вдосконаленого методу метричного проксимального градієнта. Цей метод, що базується на моделі попарно-експоненціального марківського випадкового поля та методі вибору діагонального кроку, забезпечує вищу точність і швидшу збіжність алгоритму машинного навчання. Завдяки цьому стало можливим підвищити ефективність автоматизованого визначення індивідуальних освітніх траєкторій для студентів, що оптимізує процес навчання, дозволяє швидше адаптуватися до індивідуальних потреб і забезпечувати належний рівень якості освіти.

Дисертація також містить розроблену методику оцінки рівня інформаційної безпеки, яка базується на принципах адаптивності й алгоритмах машинного навчання. Ця методика дозволяє системам автоматично виявляти потенційні загрози та оцінювати рівень ризику в режимі реального часу, що є надзвичайно важливим для ефективного управління інформаційними потоками у вищих навчальних закладах. Виявлення аномалій та оцінка ризиків в режимі реального часу сприяє прийняттю обґрунтованих управлінських рішень, що дозволяє зберегти стабільність та безперервність навчального процесу, а також забезпечити захист інформаційних ресурсів.

Іншим вагомим результатом є розробка концепції центру управління інформаційною безпекою в закладах освіти, який забезпечує інтегрований підхід до кіберзахисту, включаючи моніторинг, виявлення та своєчасне реагування на потенційні загрози. Така концепція дозволяє координувати заходи з управління інформаційною безпекою на рівні всього закладу, створюючи надійні умови для захисту даних та адаптації до змін.

Для підвищення стійкості корпоративних освітніх інформаційних систем також було запропоновано та розроблено інформаційну технологію, що базується на технології блокчейн. Це дозволяє автоматизувати низку процесів, покращуючи їх прозорість і відмовостійкість. Застосування блокчейн-технології забезпечує безперервний моніторинг транзакцій та зберігання даних у захищеному вигляді, що гарантує стабільність і цілісність інформації навіть у складних умовах.

Наукова значущість роботи полягає у вдосконаленні методології забезпечення функціональної стійкості інформаційних систем у галузі освіти, що відкриває нові перспективи для розвитку адаптивних інформаційних технологій. Розроблені підходи, моделі та методи є універсальними та можуть бути адаптовані для використання в інших галузях, де існує потреба в адаптивності, кіберзахисті та надійності систем.

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.

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.

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.

Отже, практичне значення отриманих результатів полягає у можливості впровадження розроблених методик і технологій в інформаційні системи закладів вищої освіти для забезпечення безпеки й ефективності управління інформаційними ресурсами. Це сприяє оптимізації управління інформаційними потоками, підвищенню якості навчання та безперервному вдосконаленню освітніх платформ. Отримані результати дозволяють підвищити стійкість і

функціональну стабільність освітніх систем, що робить їх більш ефективними і безпечними в умовах сучасного цифрового середовища.

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).

Результати роботи мають вагоме 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.*

ANNOTATION

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

Dissertation for obtaining the scientific degree of candidate of technical sciences in the specialty 05.13.06 "Information technologies". - State University of Information and Communication Technologies. Kyiv. 2024.

The dissertation work is devoted to the development and substantiation of theoretical and methodological approaches to ensure the functional stability of adaptive corporate educational information systems of higher education institutions. The basis of the study is the problem of increasing the reliability and efficiency of the functioning of information systems in the context of growing requirements for information security and adaptability.

Currently, the methods that ensure the optimal balance between adaptability and stability of systems, as well as integration mechanisms for modular architectures, are not sufficiently developed. Issues of security and availability require new approaches that would provide a high level of protection without reducing availability for users. There is also a need to develop effective methods of updating systems to maintain their relevance over a long period of time. In addition, resilience to external influences, such as cyber threats and technical malfunctions, requires the improvement of monitoring and response technologies. All these aspects require further research and development of new technologies to ensure the functional stability of adaptive corporate educational information systems. Therefore, the work sets and solves an actual scientific and practical task, which consists in the development of methods and technologies for ensuring the functional stability of adaptive corporate educational information systems. The aim of the dissertation is to increase the functional stability of adaptive corporate educational information systems with the help of methods and technologies developed in the work and with the use of machine learning methods.

The scientific novelty of the study consists in the development of the metric proximal gradient method, which, thanks to the use of the pair-exponential Markov random field model and the diagonal step selection method, ensures faster convergence and increases the accuracy of the machine learning algorithm. This makes it possible to automate the process of determining the individual educational trajectories of students and promptly respond to changes in the educational process. A methodology for assessing the level of information security has been developed, which is based on adaptive systems of machine learning algorithms and dynamic updating of security models. This approach allows more effective detection of anomalies and assessment of risks in real time, which contributes to the adoption of informed management decisions and effective use of resources to increase system security. In addition, the information technology for ensuring functional stability has been improved using blockchain technology, which allows for automatic optimization of processes and stable operation of educational platforms even in

dynamic conditions. The practical significance of the obtained results lies in increasing the efficiency of educational processes, ensuring an adaptive approach to learning and improving the management of information flows, which in general contributes to improving the quality of educational services and continuous improvement of educational platforms.

In the dissertation, a comprehensive study of methods and technologies for ensuring the functional stability of adaptive corporate educational information systems, aimed at supporting stable and reliable functioning even in a dynamic and threatening environment, was carried out. The main emphasis is placed on the construction of such information systems that could effectively adapt to changes in the educational process, respond in a timely manner to external challenges and cyber threats, as well as ensure high reliability of data processing to meet the needs of a modern educational environment.

One of the main scientific achievements is the development of an improved metric proximal gradient method. This method, based on the pair-exponential Markov random field model and the diagonal step selection method, provides higher accuracy and faster convergence of the machine learning algorithm. Thanks to this, it became possible to increase the efficiency of automated determination of individual educational trajectories for students, which optimizes the learning process, allows for faster adaptation to individual needs and ensures the appropriate level of education quality.

The dissertation also contains a developed methodology for assessing the level of information security, which is based on the principles of adaptability and machine learning algorithms. This technique allows systems to automatically detect potential threats and assess the level of risk in real time, which is extremely important for the effective management of information flows in higher education institutions. Detection of anomalies and assessment of risks in real time facilitates the adoption of reasonable management decisions, which allows maintaining the stability and continuity of the educational process, as well as ensuring the protection of information resources.

Another important result is the development of the concept of an information security management center in educational institutions, which provides an integrated approach to cyber protection, including monitoring, detection and timely response to potential threats. This concept allows coordination of information security management measures at the level of the entire institution, creating reliable conditions for data protection and adaptation to changes.

Information technology based on blockchain technology was also proposed and developed to increase the sustainability of corporate educational information systems. This allows you to automate a number of processes, improving their transparency and fault tolerance. The use of blockchain technology ensures continuous monitoring of transactions and data storage in a secure form, which guarantees the stability and integrity of information even in difficult conditions.

The scientific significance of the work lies in the improvement of the methodology for ensuring the functional stability of information systems in the field of education, which opens new perspectives for the development of adaptive information technologies. The developed approaches, models and methods are universal and can be adapted for use in other industries where there is a need for adaptability, cyber protection and reliability of systems.

The practical value of the improved metric proximal gradient method lies in increasing the accuracy and speed of machine learning algorithms, which allows automating the process of determining individual educational trajectories of students. This ensures adaptive learning and timely response to changes in the educational process, which increases the efficiency of the educational system as a whole.

The methodology for assessing the level of information security provides tools for a comprehensive analysis of economic indicators, risks and dynamic aspects of security, which contributes to the adoption of more justified management decisions and the effective use of resources to ensure reliable security of the educational information system.

The improved technology for ensuring the functional stability of educational information systems thanks to the use of adaptive information technologies and machine learning algorithms allows you to automatically optimize processes, improve the management of information flows and respond to changes in a timely manner, ensuring the stable operation of educational platforms even in dynamic conditions.

Therefore, the practical significance of the obtained results lies in the possibility of introducing the developed methods and technologies into the information systems of higher education institutions to ensure the safety and efficiency of information resources management. This helps to optimize the management of information flows, increase the quality of education and continuous improvement of educational platforms. The obtained results make it possible to increase the stability and functional stability of educational systems, which makes them more effective and safe in the conditions of the modern digital environment.

The research results were accepted for implementation by UKR-ON LLC (implementation act dated 07.06.2024), ADELINA OUTSOURCING LLC (implementation certificate No. 1-19 dated 09.23.2024), State University of Information and Communication Technologies (implementation act dated 09/13/2024), Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine (implementation act dated 08/20/2024), Kyiv Metropolitan University named after Boris Grinchenko (implementation act dated 08/05/2024).

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.*

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

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 проведення 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. ІІІ міжнародна науково-практична конференція 8-10 листопада 2016 р. Київський національний університет ім. Т. Шевченка. С.217-218.

ЗМІСТ

ВСТУП

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., Толюпою 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., Тимощенко А.М., Герасименко В.А., Зегжда П.Д., Девянін 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., Глибовеця 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 методику 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 роботи 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.

РОЗДІЛ 1

ТЕОРЕТИКО-ПРАКТИЧНІ ОСНОВИ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ АДАПТИВНИХ КОРПОРАТИВНИХ ОСВІТНІХ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1. Інформаційна безпека вузів – основа забезпечення ефективності їх науково-педагогічної діяльності

Процес інформатизації в освіті України набирає обертів, водночас висуваючи нові вимоги до захисту даних в умовах зростаючої цифровізація країни. Одним із ключових напрямків цього процесу є побудова надійної системи захисту інформації, яка забезпечуватиме збереження даних, контроль доступу до ресурсів на серверах корпоративних мереж закладів освіти та захищену передачу інформації через канали зв'язку, що особливо важливо для дистанційного навчання.

Більш широке розуміння системи захисту інформації у вищих навчальних закладах включає в себе два важливих аспекти: захист інтелектуальної власності від зовнішніх і внутрішніх загроз, а також управління доступом і захистом інформаційного простору від потенційних ризиків. Зростання популярності та впливу Інтернету робить ці питання особливо актуальними. Під терміном "інформаційний простір" мається на увазі всі види даних, які зберігаються на серверах навчальних закладів, установ, бібліотек, електронних носіях, а також в глобальній мережі Інтернет.

Захист інформації у корпоративних мережах вищих навчальних закладів є складнішою задачею порівняно з іншими мережами, оскільки тут виникають численні та різноманітні проблеми. Зокрема, мережі часто формуються за умов обмеженого фінансування, що впливає на якість обладнання, кваліфікацію кадрів та використання ліцензованого програмного забезпечення. Крім того, у

корпоративних мережах таких закладів зазвичай бракує довгострокового планування розвитку, що призводить до орієнтації на вирішення лише поточних завдань. Це означає, що технічна архітектура та програмне забезпечення не завжди відповідають сучасним вимогам.

Особливої уваги потребує той факт, що корпоративні мережі одночасно підтримують як освітню, так і наукову діяльність, забезпечуючи при цьому управління цими процесами. Це означає, що в одній мережі функціонують різні автоматизовані системи, які працюють паралельно. Різноманітність цих систем і відсутність централізованого управління інформаційною безпекою створюють додаткові виклики. Корпоративні мережі часто відрізняються за своїм складом як у частині апаратного забезпечення, так і програмного, адже вони формувалися поступово для виконання різних завдань протягом багатьох років.

Ще однією проблемою є те, що плани з комплексного захисту інформації, якщо вони існують, часто не відповідають сучасним вимогам і не забезпечують належного рівня безпеки. Тому в умовах сучасних загроз інформаційній безпеці потрібен диференційований підхід до кожного рівня інформаційного середовища. Це включає захист інфраструктури мережі, операційних систем та програмного забезпечення, а також прикладних програм і сервісів, що використовуються кінцевими користувачами. Таким чином, забезпечення інформаційної безпеки у навчальних закладах вимагає системного підходу та врахування багатьох факторів, щоб ефективно захистити дані та інформаційний простір від різноманітних загроз.

Інформаційна безпека – важлива суспільна категорія, що становить основу функціонування та розвитку будь-якого підприємства чи організації, в тому числі й транспортного вузу. При цьому, вона охоплює різнопланові аспекти діяльності, що досліджені в працях багатьох науковців і практиків. На рисунку 1.1 представлено узагальнення найчастіше вживаних визначень терміну «інформаційна безпека університети».

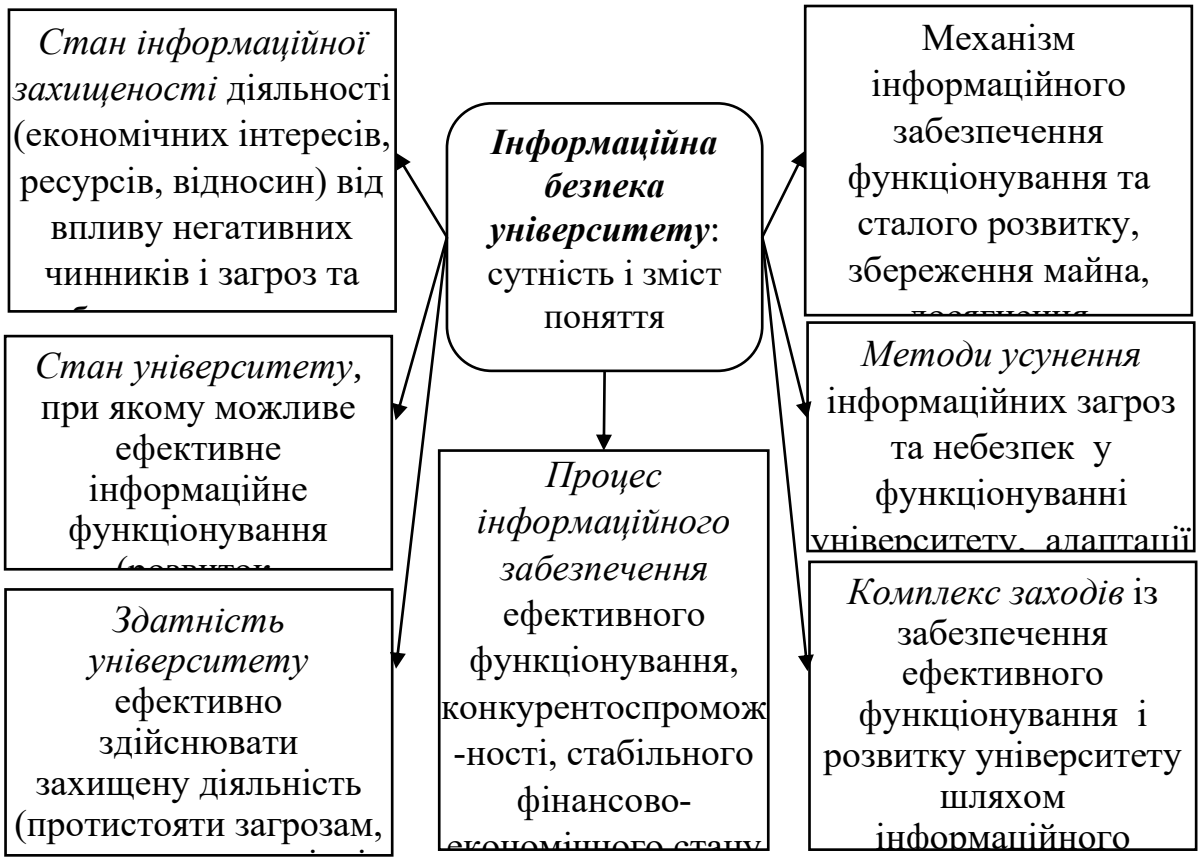

Рис 1.1. Основні аспекти визначення поняття інформаційної безпеки університету.

Інформаційна безпека університету є ключовим фактором його ефективної діяльності, адже її забезпечення сприяє досягненню поставлених наукових і дослідницьких цілей та підвищенню наукового потенціалу. Разом з тим, функціонування відомчих вищих навчальних закладів різних спеціалізацій вимагає врахування специфічних особливостей їх організаційних та технологічних процесів, а також впливу зовнішніх і внутрішніх чинників [79, 80].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» поняття «інформаційна безпека» трактується як «захист інформації та інформаційної інфраструктури від несанкціонованого доступу, знищення, модифікації та інших загроз, що можуть призвести до втрати доступності, цілісності або конфіденційності інформації» [130].

Крім того, існують визначення, що стосуються "економічної безпеки" та "науково-інформаційної безпеки", в яких наголошується на важливості збереження інформаційного потенціалу держави та його захисту від загроз, що можуть виникати у різних сферах.

Зроблено висновок, що «подальше вивчення теоретико-методологічних аспектів інформаційної безпеки, її загроз, джерел, сили та напрямів впливу, а також розробка заходів та методів для забезпечення національної інформаційної безпеки мають значний практичний інтерес». Отже, акцент варто робити на необхідності спрямування наукових досліджень у сфері інформаційної безпеки на практичне застосування отриманих результатів.

У науковій літературі зазначається, що приведення системи у відповідність до принципів природного розвитку може створити міцну основу для забезпечення її стійкості та безпеки. Науковці підкреслюють важливість орієнтації розвитку системи на актуальні потреби та виклики, що забезпечить створення надійної основи для її безпечного функціонування. Це означає, що система інформаційної безпеки повинна швидко адаптуватися до нових загроз, знижувати негативний вплив та ефективно реагувати на сучасні виклики.

У загальному розумінні безпека означає стан захищеності об'єкта чи суб'єкта від можливих загроз, а також наявність комплексу заходів та технічних засобів, які спрямовані на їх запобігання чи усунення. Відповідно, забезпечення інформаційної безпеки університетів передбачає постійний моніторинг ризиків, впровадження інноваційних рішень та адаптацію до мінливого інформаційного середовища.

Для ефективної роботи підприємств та університетів необхідно впроваджувати чіткі принципи безпечного використання ресурсів корпоративних інформаційних систем (КІС). Це має супроводжуватись розробкою офіційно затвердженого документа, в якому визначені вимоги до безпеки інформаційних ресурсів КІС та встановлено відповідальність для окремих підрозділів і посадових осіб. Такий документ може називатися «Стандартом», «Інструкцією», «Політикою» або «Планом», але в ньому

обов'язково повинні бути вказані терміни, їх визначення та скорочення, а також посилання на діючі законодавчі й нормативні акти.

Сучасна законодавча база України, що регулює діяльність інформаційних систем та телекомунікаційних мереж, включає оновлені редакції таких ключових законів, як «Про інформацію» від 2 жовтня 1992 року № 2657-XII, «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР, «Про телекомунікації» від 18 листопада 2003 року № 1280-IV та «Про захист персональних даних» від 1 червня 2010 року № 2297-VI, що визначають правові основи інформаційної діяльності, захисту інформації та персональних даних. Важливою частиною цієї бази є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, який спрямований на зміцнення кіберзахисту державних та приватних інформаційних систем, а також на протидію кіберзагрозам.

Терміни та скорочення, що використовуються в нормативних документах, можуть відрізнятися залежно від специфіки підприємства, але є загальновживані терміни, що мають уніфікований характер. Серед них: інформаційні технології (ІТ), персональний комп'ютер (ПК), інформаційна система (ІС), локальна обчислювальна мережа (ЛОМ), та інші. Користувачі, які отримали доступ до ресурсів КІС відповідно до встановленого порядку, ідентифікуються як «користувачі», тоді як для юридичних осіб, з якими укладено договірні відносини, застосовується термін «сторонні організації».

Для управління доступом до інформаційних ресурсів часто використовується «Identity Manager» (ІДМ) — централізована система для синхронізації та управління користувачами. Безпека в КІС передбачає суворий контроль доступу, і користувачі зобов'язані ознайомлюватись із нормативними документами перед отриманням доступу. Кожен користувач має персональний обліковий запис, і використання чужих облікових записів суворо заборонено.

Інформація, що обробляється в КІС, належить підприємству чи установі та підлягає захисту. Власники систем мають право контролювати діяльність користувачів, зокрема, використання корпоративної пошти та доступ до

Інтернету. Працівники зобов'язані дотримуватись конфіденційності та не розголошувати деталі щодо процедур захисту даних, що функціонують в межах корпоративних інформаційних систем.

Завдяки новим законодавчим ініціативам і посиленню систем захисту, забезпечення інформаційної безпеки набуває ще більшого значення, адаптуючись до сучасних викликів цифрової ери та технологічних загроз.

Щоб запобігти несанкціонованому доступу до ресурсів корпоративних інформаційних систем, використовуються паролі та спеціальні апаратні методи аутентифікації, що забезпечують надійне зберігання даних та мінімізують ризик їх втрати або несанкціонованого розголошення. Рекомендується оновлювати паролі кожні 90 днів, забезпечуючи значну відмінність нового пароля від попереднього. Користувачі мають дотримуватися стандартів безпеки, створюючи складні паролі та не розголошуючи їх нікому. Ідеальним є пароль, що містить щонайменше вісім символів та уникає простих комбінацій, наприклад, "123456" або "password". Він має включати різні типи символів: великі та малі літери, цифри та спеціальні знаки (наприклад, $, %, #, !).

Організації, такі як підприємства, університети та компанії, широко використовують електронну пошту та Інтернет у своїй повсякденній діяльності. Для забезпечення захисту інформації існує ряд правил: використання корпоративної пошти та мережі Інтернет повинно обмежуватися виконанням службових завдань. Забороняється надсилати електронні листи або відвідувати веб-сайти з незаконним або неприйнятним змістом, а також налаштовувати автоматичну переадресацію листів без попереднього узгодження. Не допускається самовільне розміщення інформації в Інтернеті, використання засобів для обходу мережевих фільтрів, несанкціоноване використання сервісів обміну повідомленнями та завантаження невідомого програмного забезпечення з Інтернету.

Співробітники повинні бути підготовлені до дій у випадках нестандартних або надзвичайних ситуацій. Спеціалісти, відповідальні за безпеку, мають інструктувати їх щодо правильних дій у разі виникнення таких ситуацій, як:

втрата облікових даних, крадіжка засобів аутентифікації, несанкціоновані зміни конфігурації систем, спроби отримання несанкціонованого доступу, а також втрати або крадіжки пристроїв з конфіденційними даними. У будь-яких обставинах, які можуть становити загрозу для інформаційної безпеки, необхідно вживати заходи згідно з вимогами чинного законодавства та внутрішніх політик організації.

Отже, управління інформаційною безпекою в підприємствах і університетах є окремою, самоорганізованою підсистемою загальної системи ефективного управління, яка забезпечує захист організації від негативного впливу як ззовні, так і зсередини. Це також включає в себе можливість своєчасно передбачати загрози, формувати адаптивні стратегії та гнучкість у відповіді на динамічні умови ринку. Управління інформаційною безпекою повинно бути інтегральною частиною управлінських практик сучасних організацій і охоплювати не лише реагування на загрози і ризики, але й їх прогнозування та запобігання. Усі ці аспекти складають основи інформаційної безпеки для підприємства або університету.

Сучасний розвиток інформаційного середовища України вимагає створення ефективного механізму захисту, який має враховувати:

- асортимент доступних інформаційних ресурсів та послуг;
- розвиток національних і корпоративних інформаційних мереж;
- показники зростання електронної комерції;
- рівень гармонізації українського інформаційного законодавства з європейськими стандартами;
- обсяги експорту та імпорту інформаційного капіталу;
- вдосконалення електронних систем зв’язку та Інтернету для різних галузей.

Щодо забезпечення інформаційної безпеки, важливу роль відіграє посада адміністратора безпеки. У Національному транспортному університеті було розроблено інструкцію для адміністратора безпеки (АБ), яка містить узагальнений список обов’язків і прав, а також завдання, пов’язані з підтримкою

безперебійної роботи мережі та реалізацією технічних заходів, необхідних для виконання політики інформаційної безпеки. Це включає розробку і оформлення відповідних документів, пов'язаних з інформаційною безпекою, а також складання календарних планів робіт, підготовку пропозицій щодо покращення методів і заходів захисту технологічної інформації, яка циркулює в університеті.

Для виконання своїх обов'язків АБ повинен мати знання про:

- діюче законодавство і нормативні акти, що регулюють захист інформації в автоматизованих системах;
- основні характеристики систем захисту інформації та платформ, на яких базується інформаційна система безпеки;
- методики перевірки та оновлення систем захисту інформації в університетах;
- основні методи боротьби з комп'ютерними вірусами та програмами з недокументованими функціями;
- специфікації та порядок експлуатації засобів захисту інформації.

Основні завдання адміністратора безпеки полягають у забезпеченні збереження програмно-технічних і інших цінностей, які використовуються в інформаційних системах, а також у наданні консультацій і практичної допомоги щодо захисту інформації в телекомунікаційних системах. Він організовує та пропонує керівнику відділу захисту інформації, якщо такий є, рішення для виконання вимог технічного захисту інформації, а також вживає заходів для протидії комп'ютерним вірусам і програмам з недокументованими функціями. Адміністратор є основним виконавцем заходів, пов'язаних із тестуванням, впровадженням і супроводженням засобів захисту інформації. Він також займається плануванням системи захисту у співпраці з системним адміністратором, контролюючи реалізацію заходів, що впроваджуються.

Крім того, адміністратор має контролювати відповідність актуальних конфігурацій проектній документації та відповідати за своєчасне внесення змін до проектної, експлуатаційної та робочої документації. Для досягнення ефективності в забезпеченні інформаційної безпеки важливо визначити чіткі

обов’язки та права адміністратора в різних ситуаціях. При розробці комплексної системи захисту інформації обов’язки адміністратора включають участь у проектуванні, розробці та дослідній експлуатації елементів систем захисту.

Адміністратор відповідає за розробку, оновлення та впровадження плану захисту інформації в корпоративній телекомунікаційній системі. Після затвердження актів обстеження, він, за необхідності, ініціює та контролює заходи з технічного захисту компонентів системи відповідно до чинних нормативних вимог. Адміністратор також бере участь у підготовці документів для модернізації системи захисту інформації, узагальнює пропозиції та, при потребі, долучається до розробки нормативних документів у межах університету або відділу захисту інформації.

Він також здійснює поточні заходи з обслуговування та експлуатації комплексної системи захисту інформації (КСЗІ) [74]. Адміністратор інформує керівництво університету про ефективність діючої політики інформаційної безпеки та технічних засобів, які можуть поліпшити систему захисту, включаючи їх вартість. Він підготовлює і подає пропозиції до річних і поточних планів роботи ректору або відділу захисту інформації щодо заходів із забезпечення технічного захисту інформації, забезпечуючи при цьому коректне використання доступних механізмів захисту для реалізації місцевих політик безпеки університету [74].

На завершення, адміністратор сприяє підвищенню кваліфікації співробітників відділу захисту інформації, контролює права доступу, які надає системний адміністратор, та слідкує за функціонуванням засобів технічного захисту інформації. Він визначає порядок, періодичність і строки виконання технічного обслуговування, а також контролює виконання цих заходів. Окрім того, адміністратор постійно стежить за новинами у сфері інформаційної безпеки, інформуючи про них безпосереднього керівника, технічний персонал і користувачів.

Обов'язки адміністратора безпеки в частині контролю за виконанням політики безпеки передбачають як періодичний, так і позаплановий контроль. Він повинен періодично перевіряти надійність захисту системи у співпраці зі системним адміністратором, виявляти уразливі ділянки та обладнання, чиї несправності можуть загрожувати інформаційній безпеці та призводити до матеріальних і інформаційних втрат. Адміністратор також контролює дотримання вимог щодо заборони використання програмно-апаратного забезпечення, яке не має дозволу на експлуатацію, а також проводить своєчасні перевірки журналів системних подій.

Крім того, адміністратор безпеки відповідає за антивірусний захист автоматизованих систем, сприяючи системному адміністратору у розробці процедур та інструкцій для запобігання, виявлення і видалення комп’ютерних вірусів і зловмисного програмного забезпечення. Він контролює дотримання вимог Інструкції системного адміністратора та антивірусного захисту.

У випадках нештатних ситуацій, зокрема при кібератаках, адміністратор зобов'язаний діяти швидко і ефективно. Він повинен оперативно реагувати на події, що становлять загрозу інформаційній безпеці, надавати допомогу у ліквідації загроз, визначати джерела зловмисного програмного забезпечення і зони його поширення, а також контролювати заходи щодо відновлення інформації після ушкоджень. У разі потреби він контролює дотримання встановленого порядку ремонту обладнання, а всі спроби несанкціонованого доступу фіксуються в журналі, з подальшим інформуванням ректора або начальника робочої групи про обставини і наслідки.

Всі події, які порушують функціонування інформаційної системи адміністратор записує у журналі реєстрації нештатних подій. До таких подій належать, зокрема, дії зареєстрованих користувачів, які виходять за межі їх повноважень, збої в роботі технічних засобів системи, що можуть загрожувати цілісності або доступності інформації, а також порушення правил пожежної безпеки і кліматичних умов.

Адміністратор безпеки має право періодично перевіряти рівень захищеності автоматизованих систем за погодженням із керівництвом університету, забороняти доступ користувачам, у випадку виявлення порушень політики безпеки, а також вимагати виконання заходів захисту інформації. Адміністратор вносить пропозиції та бере участь у проектуванні елементів систем захисту інформації, несе особисту відповідальність за невиконання вимог інструкції або дії, які не передбачені її положеннями під час роботи з компонентами системи. У випадку порушення правил використання обладнання проводиться службове розслідування, за підсумками якого визначається розмір завданих збитків та можливе відшкодування.

1.2. Аналіз наукових здобутків у забезпечення інформаційної безпеки адаптивних корпоративних освітніх інформаційних систем

У останні роки правове забезпечення захисту інформації в Україні, а також проблеми несанкціонованого перехоплення і доступу до інформації, інформаційна безпека комп'ютерних систем, методи розслідування злочинів у цій сфері, важливість захисту інформації в умовах рейдерства та інші аспекти інформаційної безпеки стали актуальними темами для досліджень багатьох науковців і практиків [130].

Загалом, поняття «інформація» можна умовно поділити на кілька груп. Перша група охоплює відомості про осіб, об'єкти, явища, процеси та факти. Друга група включає елементи продуктивних сил, які виникли в середині 70-х років минулого століття, або ж окремі фактори виробництва.

Інформація є відомостями про події, повідомленнями, які передаються усно або письмово, а також сукупністю свідчень, кількісних даних і знань. В. Хахановський визначає інформацію як «відображені в об'єктах матеріального світу або в психіці людини факти реальної дійсності, які можуть бути передані в просторі та часі, сприйняті органами чуттів людини (безпосередньо або з

допомогою технічних засобів), усвідомлені у момент сприйняття та використані в практичній або теоретичній діяльності» [18, С69].

Отже, інформація є безмежним ресурсом у глобальному сенсі, який активно поширюється в розвинених країнах, зокрема в Україні, завдяки високим темпам розвитку технологій і створенню різноманітних інформаційних систем. Інформаційні системи на сьогодні вимагають чіткої термінологічної ідентичності технічних понять, з якими працюють користувачі. Відповідно до ДСТУ 2874-94, дані, що офіційно документуються або публічно оприлюднюються, відносяться до поняття «інформація» [19].

Щодо терміна «інформаційна система», то серед фахівців не існує єдиного визначення. Сазонець О.М. розглядає інформаційну систему як систему, у якій організовані процеси утворення, збереження, обробки та перетворення інформації [20]. Новіков О.М. визначає інформаційну систему як організаційно-технічну систему, що реалізує технологію обробки інформації за допомогою обчислювальної техніки та програмного забезпечення [21].

Гужва В.М. описує інформаційну систему як інформаційний контур разом із технічними засобами збору, передачі, обробки і зберігання інформації, а також з персоналом, що виконує різні маніпуляції з інформацією [22].

Васильків Н.М. зазначає, що основна мета інформаційних систем полягає в генеруванні необхідної інформації для конкретної організації, що забезпечує ефективне управління її ресурсами та створення відповідного інформаційного й техніко-технологічного середовища для виконання конкретних завдань. Внутрішня управлінська інформаційна система повинна забезпечувати реалізацію різноманітних інформаційних процесів, аби задовольнити інформаційні потреби користувачів на різних рівнях прийняття рішень [24].

Бондар Н.М. підкреслює важливість спеціалізації інформаційних систем, виокремлюючи інформаційні системи менеджменту, системи для пошуку інформації, а також автоматизовані навчальні системи [25].

Трофімов В.В. розглядає інформаційну систему як взаємопов’язану сукупність інформації, засобів і методів її обробки, а також виробничого персоналу, який реалізує інформаційні процеси різними способами [26].

У дослідженні [27] пропонується визначення інформаційної системи як комп'ютеризованої системи, що дозволяє керівникам легко отримувати доступ до внутрішньої та зовнішньої інформації, граючи важливу роль у досягненні успіху. Інше визначення в роботі [28] стверджує, що інформаційна система підтримує стратегічну діяльність і хоча не є повністю комп'ютеризованою, проте функціонує як автоматизована система підтримки управлінських рівнів.

Відповідно до визначення М. Грауера, наведеного в роботі [29], управлінська інформаційна система, яка впроваджена на підприємстві, функціонує як система, що координує діяльність усіх підсистем компанії. Вона забезпечує автоматизацію всіх етапів виробництва, починаючи з проєктування й закінчуючи розподілом готової продукції, поєднуючи автоматизацію з комп'ютеризацією всіх бізнес-функцій.

Державний стандарт України (ДСТУ) пропонує таке визначення інформаційної системи: це система, що організовує накопичення та обробку інформації в певній проблемній області [30].

Інше визначення, представлене в роботі [31], говорить, що автоматизована інформаційна система представляє собою систему, яка реалізує інформаційні технології в управлінні, залучаючи персонал і технічні засоби до спільної роботи.

Дорошкевич Д.В. у своїй роботі пропонує таке визначення: інформаційна система управління – це система, що базується на зборі та аналізі інформації з використанням комп’ютерних технологій, створена для виконання управлінських функцій [32].

У праці [33] автор пропонує три різні підходи до визначення терміна "інформаційна система". З позиції бізнесу інформаційна система постає як сукупність ділової інформації, апаратно-програмного забезпечення, технологій, телекомунікацій, баз даних, методів обробки та управлінського персоналу, що забезпечує процеси збору, передачі, обробки й зберігання даних для ухвалення

обґрунтованих рішень. З технічного боку це комплекс взаємопов’язаних компонентів для збору, обробки, зберігання та розподілу інформації, який підтримує процеси ухвалення рішень та управління на рівні організації. Семантичний підхід розглядає інформаційну систему як набір взаємозалежних даних про стан об’єкта або процеси в ньому, виражених у вигляді показників та інших інформаційних наборів, оброблених за визначеними методиками та алгоритмами за допомогою технічних засобів. Враховуючи багатогранність цих підходів, автор узагальнює і пропонує сучасне визначення поняття "інформаційні системи", яке охоплює всі наведені аспекти.

В умовах сучасної економіки ринкові гравці змагаються не лише за якість продуктів і послуг, а й за здатність оперативно приймати рішення на основі інформації та швидко адаптуватися до змін. Розвиток інформаційних технологій та систем відкриває нові можливості для підвищення конкурентоспроможності. Ідеальною моделлю для суспільства є чесна та цивілізована конкуренція, проте в Україні часто зустрічається недобросовісна конкуренція, що ускладнює легальне входження в різні галузі. До проявів такої конкуренції належать агресивні дії проти конкурентів, такі як переманювання ІТ-спеціалістів, шантаж, промислове та наукове шпигунство, несанкціонований доступ до баз даних і хакерські атаки. Тому в сучасному визначенні "інформаційні системи" необхідно також враховувати функцію захисту інформації.

Інформаційна безпека охоплює захист інформаційних систем, зокрема інформаційних ресурсів, від можливих негативних впливів, які можуть завадити повному використанню інформації, а також комплекс заходів та інструментів, що забезпечують таку захищеність. Інформаційна безпека включає в себе: захист інформації, контроль за інформаційним простором та інформаційне забезпечення функціонування технічних, економічних та державних суб’єктів. Захист інформації повинен включати заходи, спрямовані на запобігання несанкціонованому доступу до даних, їх втраті, знищенню, порушенню цілісності та модифікації в інформаційних системах, а також на перехопленню інформації.

Як правило, забезпечення інформаційної безпеки здійснюється за допомогою технічних, технологічних, організаційних, економічних, адміністративних і правових заходів. Наприклад, чинне законодавство забороняє публікацію інформації, що містить державну таємницю. Внутрішні загрози включають, перш за все, нестачу необхідної інфраструктури в інформаційній сфері. Після ретельного аналізу всіх аспектів пропонується комплексне визначення терміна "інформаційна система": «інформаційна система — це організаційно-технічна система, яка за допомогою комп'ютерних та обчислювальних технологій реалізує процеси утворення, збору, обробки, перетворення, зберігання, оновлення та передачі інформації споживачу, забезпечуючи надійне використання різних уніфікованих методів і механізмів захисту інформації в рамках усіх процесів та інформаційних активів».

Дослідження теоретичних і методичних основ інформаційної безпеки як самостійного напряму кібернетичної науки були проведені багатьма дослідниками. В загальному контексті інформаційна безпека може розглядатися як складна поліструктурна наука. Можна стверджувати, що інтегрована інформаційна безпека цілісної системи формується з показників окремих взаємопов'язаних підсистем, які, в свою чергу, є складовими елементами цілісної системи.

У Національному транспортному університеті в рамках науково-дослідної роботи, за участю здобувача в якості відповідального виконавця, було розроблено план захисту інформації, який є частиною комплексної системи захисту інформації. Цей документ є результатом аналізу технології обробки інформації, оцінки ризиків, що існують для інформації, оброблюваної Єдиною інформаційною системою «Наука в університетах», а також формування політики безпеки інформації, яку планується впровадити робочою групою в цій автоматизованій системі.

1.3. Сучасні підходи до забезпечення функціональної стійкості корпоративних інформаційних систем.

Функціональна стійкість освітніх інформаційних систем – це здатність системи продовжувати виконувати свої основні функції навіть в умовах несприятливих впливів, таких як технічні збої, кіберзагрози, збільшене навантаження на ресурси або фізичні пошкодження інфраструктури. Це критичний аспект для освітніх систем, оскільки їхня безперебійна робота забезпечує безперервність навчального процесу, доступ до навчальних матеріалів і сервісів для студентів, викладачів та адміністрації.

Функціональна стійкість включає кілька ключових аспектів:

1. Надійність (reliability) – здатність системи виконувати свої функції протягом визначеного часу без збоїв. Для освітніх інформаційних систем це означає стабільне функціонування протягом навчального дня, тижня або семестру, що важливо для забезпечення доступності навчальних матеріалів та проведення онлайн-лекцій. Надійність досягається за рахунок використання якісного обладнання, надійного програмного забезпечення, а також регулярного технічного обслуговування.

2. Відновлюваність (recoverability) – здатність системи швидко відновлюватися після збоїв або аварій. В освітніх інформаційних системах це означає мінімізацію часу простою при виникненні технічних проблем, що дозволяє знизити негативний вплив на навчальний процес. Відновлюваність забезпечується за рахунок застосування методів автоматичного перезапуску сервісів, наявності планів відновлення, резервного копіювання даних.

3. Безпека (security) – здатність захищати інформацію та ресурси системи від несанкціонованого доступу, втручань та атак. Безпека є важливою складовою функціональної стійкості, оскільки кіберзагрози, такі як віруси, хакерські атаки та витоки даних, можуть впливати на стабільність роботи системи. Захист забезпечується за допомогою багаторівневої автентифікації,

шифрування даних, систем виявлення та запобігання вторгненням, а також постійного оновлення програмного забезпечення.

4. Адаптивність (adaptability) – здатність системи швидко підлаштовуватися до змін у навантаженні, умовах експлуатації та вимогах користувачів. Для освітніх інформаційних систем це означає можливість без проблем масштабувати ресурси під час пікових навантажень, таких як початок навчального року, проведення масових іспитів або організація онлайн-заходів. Адаптивність досягається завдяки використанню хмарних технологій, мікросервісної архітектури та автоматизованих систем керування навантаженням.

5. Висока доступність (high availability) – здатність забезпечувати доступність сервісів у будь-який час з мінімальним простоєм. Освітні системи потребують цілодобового доступу, особливо в умовах дистанційного або змішаного навчання, коли студенти можуть навчатися в будь-який зручний для них час. Висока доступність досягається шляхом дублювання критичних компонентів системи, використання кластерних систем, балансування навантаження та автоматичного перемикання на резервні ресурси у разі відмови основних.

6. Моніторинг та управління (monitoring and management) – постійний процес контролю за станом системи та її компонентів, що дозволяє своєчасно виявляти відхилення від нормальної роботи та реагувати на них. У контексті освітніх інформаційних систем це може включати моніторинг серверів, баз даних, мережевого трафіку, а також стану різних навчальних сервісів. Інструменти моніторингу дозволяють швидко виявляти проблеми та проводити профілактичні роботи для запобігання можливим збоям.

Сучасні підходи до забезпечення функціональної стійкості освітніх інформаційних систем мають вирішальне значення для забезпечення безперебійного доступу до навчальних ресурсів та сервісів навіть у випадку технічних збоїв чи кіберзагроз. В умовах зростання складності таких систем та

зростання вимог до безпеки й надійності, ці підходи стають основою для підтримки стабільного функціонування освітнього середовища.

Одним із ключових підходів є використання мікросервісної архітектури, яка дозволяє розбити систему на незалежні компоненти, що функціонують автономно і взаємодіють між собою через API. Це дає змогу забезпечити стійкість, оскільки навіть при виникненні збою в одному з компонентів, інші залишаються працездатними, зберігаючи доступ до освітніх ресурсів та сервісів. Оркестрація контейнерів за допомогою платформ таких як Kubernetes забезпечує автоматизоване керування життєвим циклом сервісів, що дозволяє оперативно відновлювати їх після збоїв та ефективно розподіляти навантаження між різними компонентами системи.

Для забезпечення надійного збереження та доступу до навчальних даних використовуються методи резервування та відновлення. Це включає регулярне резервне копіювання баз даних, конфігурацій та інших важливих елементів, що дозволяє швидко відновити роботу освітньої системи після аварій чи технічних проблем. Планування відновлення після аварій – важлива складова, яка передбачає детальні сценарії дій у випадку непередбачених ситуацій. Геореплікація навчальних даних у різних дата-центрах дозволяє забезпечити безперервний доступ до них навіть у разі фізичних пошкоджень основного центру обробки даних.

Для забезпечення високої доступності освітніх систем застосовуються методи моніторингу та прогнозування збоїв. Інструменти моніторингу дозволяють відстежувати продуктивність системи, своєчасно виявляти аномалії та запобігати можливим порушенням у її роботі. Особливе місце тут займають методи машинного навчання, які дозволяють на основі аналізу великих обсягів даних передбачити можливі збої та вжити заходів для їх запобігання. Завдяки розумним сповіщенням адміністратори освітніх систем отримують своєчасну інформацію про критичні події, що сприяє швидкому реагуванню та мінімізації негативного впливу на навчальний процес.

Безпека освітніх інформаційних систем є важливим аспектом їхньої стійкості. Використання систем виявлення та запобігання вторгнень дозволяє захищати систему від кіберзагроз та атак, що вплинуть на доступ до навчальних ресурсів. Сегментація мережі, VPN та шифрування даних захищають конфіденційну інформацію, забезпечуючи безпечний обмін даними між різними компонентами системи. Це дозволяє зберігати навчальні матеріали та особисті дані студентів у безпеці та мінімізувати можливі ризики, пов'язані з витоками даних.

Автоматизація процесів та впровадження DevOps-підходів також є важливими аспектами забезпечення стійкості освітніх систем. Використання автоматизованих інструментів розгортання та оновлення дозволяє швидко впроваджувати нові функціональні можливості та оновлення безпеки без переривання навчального процесу. Це забезпечує безперервний доступ до оновлених сервісів для студентів та викладачів, що є особливо важливим для підтримки актуальності навчальних матеріалів. Автоматизація інфраструктури за допомогою Infrastructure as Code (IaC) дозволяє стандартизувати управління ресурсами, знижуючи ризик людських помилок.

Забезпечення стійкості освітніх систем також включає стрес-тестування та моделювання різних сценаріїв збоїв. Це допомагає зрозуміти, як система поводитиметься під час великих навантажень, наприклад, під час масових іспитів або онлайн-занять. Використання цифрових двійників дозволяє проводити віртуальні тести, оцінюючи вплив різних факторів на функціональність системи та оптимізуючи її роботу для запобігання реальним проблемам.

Сучасні корпоративні освітні інформаційні системи повинні функціонувати навіть у разі виникнення надзвичайних ситуацій. Це досягається завдяки комплексному підходу до забезпечення функціональної стійкості, який поєднує використання новітніх технологій, управління ризиками та адаптивність системи до змін. Такий підхід забезпечує стабільний доступ до освітніх ресурсів та сприяє безперервному навчанню студентів, навіть у разі виникнення надзвичайних ситуацій.

Таблиця 1.1

Аналіз сучасних підходів до забезпечення функціональної стійкості освітніх інформаційних систем

Метод	Переваги	Недоліки
Мікросервісна архітектура	Підвищує гнучкість та масштабованість системи.	Складність управління взаємодією між мікросервісами.
	Зменшує вплив збоїв одного сервісу на всю систему.	Потребує складного налаштування оркестрації (наприклад, Kubernetes).
Резервування та відновлення	Забезпечує відновлення даних після аварій.	Може вимагати значних ресурсів для зберігання резервних копій.
	Дозволяє швидко відновити доступ до освітніх ресурсів.	Висока складність планування та впровадження процесів Disaster Recovery.
Моніторинг та прогнозування	Своєчасне виявлення та запобігання збоїв, що зменшує ризик простоїв.	Потребує налаштування систем моніторингу та аналітики, що може бути складним процесом.
	Використання машинного навчання для прогнозування збоїв дозволяє ефективніше реагувати на інциденти.	Помилкові прогнози можуть призводити до неправомірного реагування на ситуації.
Захист від кібератак	Забезпечує безпеку даних та захищає систему від несанкціонованого доступу.	Потребує регулярного оновлення політик безпеки та конфігурацій.
	Знижує ймовірність компрометації освітньої системи.	Використання складних систем безпеки може знизити продуктивність системи.
Автоматизація та DevOps-підходи	Прискорює впровадження оновлень та покращує якість розгортання.	Високі вимоги до кваліфікації персоналу та знань щодо інструментів автоматизації.
	Знижує ризик людських помилок завдяки автоматизації рутинних завдань.	Неправильна конфігурація може призвести до масових збоїв у всій системі.
Стрес-тестування та моделювання	Дозволяє виявити потенційні слабкі місця системи під навантаженням.	Може бути трудомістким та дорогим у впровадженні.
	Підвищує надійність системи шляхом підготовки до різних сценаріїв збоїв.	Не завжди можливо змоделювати всі можливі ситуації реального світу.
Методи забезпечення високої доступності	Забезпечує безперервний доступ до сервісів та навчальних матеріалів.	Висока вартість впровадження через необхідність резервного обладнання та інфраструктури.
	Знижує вплив збоїв на користувачів.	Складність управління кластерами та балансуванням навантаження.

Розподілені системи та геореплікація	Підвищує стійкість до фізичних катастроф та забезпечує доступність даних у різних регіонах.	Складність синхронізації даних між кількома вузлами.
	Зменшує затримки доступу до даних для користувачів у різних місцях.	Високі витрати на інфраструктуру для підтримки розподілених систем.
Цифрові двійники та моделювання	Дозволяє тестувати систему у віртуальному середовищі без впливу на реальні користувачі.	Потребує значних обчислювальних ресурсів для створення та обслуговування цифрових двійників.
	Знижує ризик виникнення збоїв в реальному середовищі шляхом попереднього аналізу.	Складність у налаштуванні точної моделі реальної системи.

Забезпечення функціональної стійкості освітніх інформаційних систем є критично важливим, оскільки ці системи відіграють центральну роль у забезпеченні безперервного та ефективного навчального процесу. В умовах швидких змін та зростання залежності освітніх установ від цифрових технологій, стабільність та надійність інформаційних систем стають ключовими для безперебійної роботи навчальних платформ, доступу до ресурсів і забезпечення зв'язку між викладачами та студентами.

Функціональна стійкість є необхідною для мінімізації ризику збоїв, які можуть призвести до втрати важливих навчальних матеріалів або перебоїв у проведенні занять. Вона забезпечує можливість швидкого відновлення роботи системи після технічних проблем, що зменшує негативний вплив на користувачів і зберігає довіру до цифрових інструментів навчання.

Завдяки забезпеченню функціональної стійкості освітні установи можуть ефективно адаптуватися до змін у вимогах та навантаженнях, таких як раптове збільшення кількості користувачів під час іспитів або проведення онлайн-конференцій. Це дозволяє забезпечити стабільний доступ до навчальних платформ незалежно від зовнішніх обставин, що особливо важливо в умовах дистанційного навчання або надзвичайних ситуацій, як-от пандемії чи війни.

Таким чином, функціональна стійкість є фундаментальною для підтримки безперервності навчання, зниження ризиків, а також дозволяє навчальним закладам швидко реагувати на виклики сучасного цифрового середовища, забезпечуючи надійну та безпечну інфраструктуру для здобуття знань.

1.4. Основні напрямки та завдання дисертаційних досліджень

Сучасні заклади вищої освіти дедалі більше залежать від інформаційних систем для забезпечення навчального процесу, управління ресурсами та адміністрування. Особливо актуальним це питання стало на фоні останній подій ковіду та війни, коли навчальний процес став повністю залежним від інформаційних систем, які використовую заклади . 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.

Основні напрямки та завдання дисертаційного дослідження спрямовані на створення та впровадження нових методів і технологій, які дозволяють підвищити функціональну стійкість адаптивних корпоративних освітніх інформаційних систем (АОІС) за допомогою інструментів машинного навчання. У рамках дослідження передбачається розробка інноваційних моделей аналізу та обробки освітніх даних, що враховують індивідуальні потреби студентів та викладачів, а також специфіку навчального контенту. Це дозволить створювати персоналізовані освітні траєкторії, що відповідають інтересам та здібностям кожного користувача, сприяючи кращому засвоєнню матеріалу, підвищенню якості та ефективності навчального процесу.

Метою дослідження є забезпечення здатності АОІС адаптуватися до змінних умов роботи, як внутрішніх, так і зовнішніх. Це включає здатність системи до швидкого реагування на зміни у навчальних програмах, потребах студентів та умовах зовнішнього середовища, зокрема таких як технічні збої, зміни в організаційних процесах або нові виклики у сфері інформаційної безпеки. Підвищення стійкості АОІС до таких змінних умов вимагає не лише впровадження новітніх алгоритмів і технологій, але й всебічного аналізу існуючих методів, які використовуються для оптимізації функціонування таких систем.

Особлива увага в дисертаційному дослідженні приділяється розробці алгоритмів, які дозволяють забезпечити більш ефективну обробку великих масивів освітніх даних, зокрема зниження часу обчислень і використання обчислювальних ресурсів. Це включає створення нових методів оптимізації процесів аналізу, побудови та адаптації освітніх моделей, які є більш стійкими до різних типів шуму та даних низької якості. Важливим аспектом є також дослідження можливостей зниження ресурсомісткості обчислень, що дозволить покращити продуктивність АОІС без збільшення апаратних ресурсів, що особливо актуально для середніх та малих організацій з обмеженими фінансовими можливостями.

Крім цього, завдання дослідження включають питання забезпечення безпеки даних, які обробляються та зберігаються в АОІС. Це включає розробку нових методів захисту від несанкціонованого доступу та кібератак, що дозволить знизити ризики витоку конфіденційної інформації та втрати даних. Використання криптографічних методів у поєднанні з алгоритмами машинного навчання може суттєво підвищити рівень безпеки та стійкості системи до зовнішніх загроз, що є ключовим у сучасних умовах інформаційної безпеки.

Одним з пріоритетних напрямків є впровадження технологій штучного інтелекту та машинного навчання для автоматизації та оптимізації управління освітніми процесами в АОІС. Це дозволить не лише підвищити якість освіти, але й забезпечити її гнучкість та безперервність в умовах дистанційного навчання та роботи з великими групами студентів. Розробка та впровадження таких технологій сприятимуть більш точному відслідковуванню прогресу студентів, діагностиці їхніх сильних та слабких сторін, а також своєчасному коригуванню навчального процесу відповідно до потреб конкретного користувача.

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.

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.

Таким чином, обґрунтовано основні напрямки та завдання дисертаційних досліджень, які потребують відповідних наукових вирішень.

РОЗДІЛ 2

РОЗРОБКА МОДЕЛЕЙ ТА МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ УДОСКОНАЛЕННЯ АДАПТИВНИХ КОРПОРАТИВНИХ ОСВІТНІХ ІНФОРМАЦІЙНИХ СИСТЕМ

2.1. Особливості застосування методів машинного навчання в адаптивних корпоративних освітніх інформаційних систем

В адаптивних корпоративних освітніх системах методи машинного навчання пропонують динамічні способи персоналізації та оптимізації навчального процесу. Ці системи можуть аналізувати величезні обсяги даних про окремих користувачів, такі як темп навчання, типи контенту, яким надається перевага, та області, що викликають труднощі, щоб запропонувати індивідуальні освітні траєкторії. Використовуючи алгоритми машинного навчання, ці системи можуть постійно вдосконалювати траєкторію навчання, адаптуючись у реальному часі до потреб кожного користувача, тим самим підвищуючи залученість і утримання.

Іншим важливим застосуванням машинного навчання в цих системах є предиктивна аналітика. Аналізуючи шаблони та історичні дані, система може передбачити потенційні вузькі місця в навчанні та проактивно коригувати контент або пропонувати додаткові ресурси. Ця прогностична здатність допомагає виявити учнів з групи ризику на ранній стадії, пропонуючи своєчасні втручання, щоб утримати їх на правильному шляху і знизити рівень відсіву.

Моделі машинного навчання в корпоративних освітніх системах також можуть сприяти більш ефективним методам оцінювання. Оцінюючи результати навчання і дані про поведінку користувачів, ці системи можуть запропонувати розуміння прогалин у навичках і надати рекомендації щодо цільового контенту

для їх усунення. Крім того, моделі обробки природної мови (NLP) можуть підтримувати автоматизоване виставлення оцінок і зворотний зв'язок у відкритих оцінюваннях, роблячи процес оцінювання більш ефективним і послідовним в організації.

Крім того, машинне навчання може підвищити безпеку та цілісність адаптивних освітніх систем. Алгоритми виявлення аномалій можуть відстежувати шаблони активності користувачів, відзначаючи підозрілу поведінку, яка може свідчити про несанкціонований доступ або інші загрози безпеці. Це додає додатковий рівень захисту, гарантуючи, що навчальні дані залишаються в безпеці, дозволяючи системі швидко реагувати на потенційні вразливості.

Нарешті, машинне навчання дозволяє адаптивним системам з часом ускладнюватись і розширювати свої можливості. Завдяки наявності зворотного зв'язку ці системи можуть вчитися на попередніх взаємодіях і результатах, постійно вдосконалюючи свої адаптивні функції. Це гарантує, що навчальне середовище залишається актуальним, реагує на нові корпоративні навчальні потреби та відповідає новим тенденціям в освітніх технологіях.

Для побудови індивідуальних навчальних траєкторій в адаптивних корпоративних освітніх системах методи машинного навчання можуть обробляти та аналізувати дані про учнів, щоб створювати індивідуальні освітні подорожі. Моделі машинного навчання можуть оцінювати сильні та слабкі сторони кожного учня, його вподобання та попередню успішність. Ця інформація дозволяє системі динамічно коригувати навчальну програму, представляючи контент, який відповідає поточному рівню та особистим цілям учня. Адаптивні алгоритми, такі як навчання з підкріпленням, допомагають вдосконалювати ці шляхи на основі безперервного зворотного зв'язку, гарантуючи, що матеріал залишається актуальним і цікавим у міру того, як учень просувається вперед.

Алгоритми кластеризації, такі як k-середнє або ієрархічна кластеризація, можуть групувати учнів на основі схожості стилів навчання, швидкості або

прогалин у знаннях. Така кластеризація дозволяє системі рекомендувати контент, вправи або додаткові матеріали, які відповідають унікальним потребам кожного кластера [151, 152]. Наприклад, учень, який швидко навчається, може отримати більш складний матеріал, тоді як тим, хто має труднощі з певними поняттями, можуть бути запропоновані додаткові ресурси або фундаментальні теми.

Обробка природної мови (NLP) може бути використана для аналізу взаємодії та взаємодії з різними типами контенту, такими як матеріали для читання, відео або вікторини. Визначаючи вподобання щодо певних форматів контенту, моделі NLP можуть гарантувати, що навчальні траєкторії включають типи матеріалів, які найкраще резонують з кожним користувачем, що ще більше посилює персоналізацію.

Прогностична аналітика також відіграє життєво важливу роль у підтримці індивідуальних траєкторій навчання. Вивчаючи історичні дані та закономірності прогресу учня, предиктивні моделі можуть передбачити потенційні труднощі та проактивно запропонувати альтернативні шляхи або корекційну підтримку. Ця здатність прогнозування допомагає забезпечити безперервний прогрес, спрямовуючи учнів через перешкоди та підтримуючи їхній розвиток на правильному шляху.

Крім того, алгоритми рекомендацій, подібні до тих, що використовуються в електронній комерції, можуть запропонувати контент або модулі, які відповідають кар'єрним цілям учня або сферам, що потребують вдосконалення. Це допомагає системі не лише реагувати на нагальні освітні потреби, але й підтримувати довгостроковий розвиток, забезпечуючи комплексний, індивідуалізований досвід навчання, який адаптується в міру того, як учні розвиваються і зростають у своїх ролях.

Використання машинного навчання для побудови індивідуальних освітніх траєкторій привертає увагу як міжнародних, так і українських дослідників. Такі вчені, як Райан Бейкер, Ніл Хеффернан, Шейн Доусон, а також українські дослідники, такі як Ігор Романенко, досліджували різні методи машинного

навчання для підвищення адаптивності та персоналізації освітніх систем [139]. Ці дослідження спрямовані на створення оптимізованих шляхів навчання, підвищення зацікавленості та покращення утримання учнів і результатів шляхом використання даних, отриманих на основі інсайтів.

Однією з помітних сфер досягнень є прогностична аналітика та моделювання студентів. Наприклад, Джордж Сіменс і Драган Гашевіч разом з українськими дослідниками Наталією Ковальчук та Володимиром Іваненком розробили моделі, здатні прогнозувати успішність студентів і виявляти потенційні труднощі в навчанні. Ці дослідження продемонстрували, що прогностичні моделі, інтегровані з адаптивними освітніми системами, значно знижують рівень відсіву учнів, надаючи їм індивідуальну підтримку в критичні моменти навчання.

Крім того, такі дослідники, як Каліна Яцеф, Крістіна Конаті, Іван Петров та Ольга Соколовська, зробили свій внесок, застосувавши методи кластеризації, які групують учнів на основі таких факторів, як швидкість навчання, стиль та вподобання щодо контенту.

Дослідження показали, що алгоритми кластеризації, такі як k-середнє та ієрархічна кластеризація, сприяють наданню персоналізованих рекомендацій щодо контенту, які посилюють залучення та підвищують ефективність навчання. Цей метод виявився ефективним як у корпоративному навчанні, так і в академічному середовищі, причому українські дослідники зосередилися на його застосуванні в умовах змішаного навчання.

Навчання з підкріпленням також було в центрі уваги науковців, серед яких *Худа Хан*, *Мін Чі* та український вчений *Олексій Гриценко*. Їхні роботи над моделями навчання з підкріпленням забезпечують адаптивний навчальний контент, заснований на взаємодії учнів у реальному часі. Цей метод покращує залученість учнів шляхом адаптації контенту до нагальних потреб, сприяючи створенню динамічного та гнучкого навчального середовища.

У галузі обробки природної мови (NLP) такі дослідники, як *Каролін Пенштейн Розе*, *Мішельєн Чі* та українська експертка *Марія Тимошенко*, зробили

значний внесок у розуміння взаємодії з учнями. Моделі NLP використовуються для адаптації презентації контенту та оцінки настроїв у реальному часі, що дозволяє системам регулювати рівні складності відповідно до відгуків учнів. Це дослідження уможливлює більш досконалу персоналізацію, коли адаптивні системи підлаштовують типи контенту та його подання до унікальних особливостей кожного учня.

Методика побудови освітніх траєкторій з використанням методів машинного навчання передбачає створення адаптивної системи, яка на основі збору та аналізу даних про кожного користувача автоматично формує індивідуальну траєкторію навчання. Спершу здійснюється збір даних, що включають початковий рівень знань, навички, стиль навчання, інтереси та цілі користувача, які можна отримати через анкети, тести або шляхом моніторингу активностей користувача. Наступний етап — обробка та аналіз даних, де застосовуються алгоритми кластеризації для групування користувачів зі схожими характеристиками, а також техніки зменшення розмірності для виділення ключових особливостей. Потім на основі отриманих даних розробляються моделі прогнозування, наприклад, з використанням рекурентних нейронних мереж, що дозволяють передбачити успішність користувача. Далі, з використанням методів рекомендаційних систем, система формує освітню траєкторію відповідно до інтересів, рівня знань та прогнозів моделі, використовуючи алгоритми на основі підкріплення для адаптації траєкторії в процесі навчання. Система безперервно моніторить прогрес користувача, виявляючи теми, що потребують додаткової уваги, і коригує навчальний контент у реальному часі. Після завершення навчального циклу збираються відгуки користувачів і результати тестів для оптимізації алгоритмів, що дозволяє системі постійно вдосконалювати освітні траєкторії для точнішого задоволення потреб майбутніх користувачів.

2.2. Розробка моделі попарно-експоненціального марківського випадкового поля для побудови індивідуальних освітніх траєкторій

Марківське випадкове поле (МВП) можна використовувати в поєднанні з методами машинного навчання для визначення індивідуальних освітніх траєкторій, оскільки воно добре підходить для моделювання залежностей між станами різних об’єктів, зокрема студентів у навчальному процесі. У цьому контексті МВП допомагає представити ймовірнісні зв'язки між показниками успішності студента, його поведінкою в навчальному середовищі, реакцією на навчальні матеріали, та іншими характеристиками, що можуть впливати на траєкторію навчання.

МВП дозволяє визначати комплексні залежності між різними аспектами навчання, такими як успішність у певних дисциплінах, рівень активності та потреба в додатковій підтримці. Оскільки моделі МВП здатні ефективно обробляти великі обсяги багатовимірних даних, вони є надзвичайно корисними для індивідуалізації навчання, де кожен студент може отримувати персоналізовані рекомендації на основі своїх характеристик та поведінкових факторів.

Марківські випадкові поля надають потужний математичний інструмент для побудови ефективних адаптивних освітніх систем, що дозволяє досягти більшої точності при визначенні освітніх потреб кожного студента та забезпечує стійкість системи до змін, пов'язаних із навчальним процесом.

Модель марківського випадкового поля (МВП) — це математична структура у вигляді неорієнтованого графа, яка застосовується для представлення залежностей між кількома випадковими змінними. На відміну від традиційних підходів, де змінні можуть бути розташовані незалежно одна від одної, в МВП враховуються взаємозв'язки, що дозволяє ефективніше моделювати взаємозалежні системи.

МВП складається з таких основних елементів як вузли, ребра, потенціальні функції та локальні залежності.

У контексті навчальних траєкторій вузли представляють окремі параметри студента, такі як рівень засвоєння теми, результати тестів, активність у системі, відгуки на матеріали. Кожен вузол відповідає конкретній змінній, яка може бути визначена як характеристика навчання студента.

Ребра, або зв'язки між вузлами, відображають взаємозв'язок між різними параметрами, зокрема, залежність рівня засвоєння матеріалу від активності студента або часу, витраченого на вивчення певної теми. Зв'язки можуть бути як прямими, так і опосередкованими, залежно від наявності кореляцій між показниками.

Кожне ребро має потенціальну функцію, яка визначає ймовірність певного стану вузла, враховуючи сусідні вузли. Функція визначає ймовірність високих результатів у студента, якщо він активно користується навчальними матеріалами. Ці функції базуються на історичних даних та дозволяють обчислювати ймовірності для прогнозування майбутніх результатів студента.

МВП використовує локальні ймовірності для визначення стану кожного вузла, враховуючи вплив сусідніх вузлів. Це означає, що система може більш точно моделювати залежності, уникаючи незалежного розгляду кожного елемента. Це дозволяє динамічно адаптувати навчальний шлях залежно від попередніх результатів і реакцій на певні навчальні ресурси.

Так як параметри студента, такі як рівень засвоєння теми, результати тестів, активність у системі, відгуки на матеріали є різнорідними, то доречним є використання попарно-експоненціального марківського випадкового поля.

Позначимо $\{x_1,x_2,\ldots,x_n\}$ набір даних незалежних багаторазових випробувань, причому не забуваємо, що в попарно-експоненціальному марківському випадковому полі доречно використовувати екпоненціальний розподіл, який представимо як $j(x,\theta)$, який представлений моделлю j-го вузла з параметром θ. При цьому j-ті вузли складаються з різних типів значень параметрів.

Алгоритм побудови попарно-експоненціального марківського випадкового поля (ПЕ МВП) для індивідуальної освітньої траєкторії студента буде складатися з наступних пунктів:

1. Визначення параметрів та побудова моделі у вигляді графу.

На початку алгоритму збираються вхідні дані про студента, такі як попередні результати навчання, оцінки, вподобання, темп навчання та інші параметри, що можуть вплинути на навчальну траєкторію.

Вводиться G=(V,E) – неорієнтований граф, в якому $V=\{v_1,v_2,\ldots,v_n\}$ – множина вузлів (змінних, що описують параметри студента), а $E \subset V \times V$ – множина ребер, що описують залежності між параметрами. При побудові моделі визначаються функції спостережень та параметри θ_i для кожного вузла, що описують відповідний впливовий параметр освітнього процесу (наприклад, знання або мотивація).

2. Обчислення потенціальних функцій для кожної пари вузлів.

Потенціальні функції ϕ_i – функції, що визначають силу взаємодії між вузлами на кожній ітерації, відображаючи ймовірність переходу між станами вузлів. Потенціальні функції дозволяють коригувати траєкторію навчання, забезпечуючи збереження найбільш оптимальної навчальної стратегії.

Після побудови графу для кожного ребра $(v_i,v_j) \in E$ визначається потенціальна функцію у вигляді попарно-експоненціального виразу:

$$\phi(x_i,x_j)=exp(\theta_{ij} \cdot f(x_i,x_j)), \quad (2.1)$$

де θ_{ij} – параметр взаємодії між вузлами v_i та v_j, а $f(x_i,x_j)$ – функція, що описує залежність між цими вузлами. Наприклад, для кореляції між успішністю та мотивацією можна обрати лінійну функцію, для інших – експоненційну чи логістичну.

3. Побудова функції розподілу ймовірностей.

Функція ймовірності в моделі МВП визначає, з якою ймовірністю певний набір навчальних параметрів приведе до конкретного результату, наприклад, до підвищення рівня знань.

Спільна ймовірність для всього граф знаходиться за формулою:

$$P(x) = \frac{1}{Z} \prod_{(\upsilon_i, \upsilon_j) \in E} \phi(x_i, x_j), \tag{2.2}$$

де Z – нормувальна константа (розподіл функції), яка визначається як:

$$Z = \sum_{x} \prod_{(\upsilon_i, \upsilon_j) \in E} \exp(\theta_{i,j} f(x_i, x_j)). \tag{2.3}$$

4. Визначення нормувальної константи Z (функція розбиття)

Значення Z – константа дозволяє нормувати всі ймовірності в моделі так, щоб їх сума дорівнювала одиниці. Це важливо для створення математично коректної ймовірнісної моделі, де можна обирати найбільш ймовірні стани, які визначатимуть етапи навчальної траєкторії студента.

Значення Z може бути обчислювально складним, тому для великих графів використовуються наближені методи, і значення Z знаходиться за формулою:

$$Z \approx \frac{1}{N} \sum_{k=1}^{n} \prod_{(\upsilon_i, \upsilon_j) \in E} \exp(\theta_{i,j} f(x_i^{(k)}, x_j^{(k)})), \tag{2.4}$$

де N – кількість випадкових вибірок, $x_i(k)$ – значення вузлів для k-ї вибірки.

5. Оптимізація параметрів θ за допомогою максимізації правдоподібності

Оптимізуємо параметри θ для максимізації логарифмічної правдоподібності:

$$L(\theta) = \sum_{(\upsilon_i, \upsilon_j) \in E} (\theta_{i,j} f(x_i, x_j) - \log Z. \tag{2.5}$$

Градієнт лог-правдоподібності для кожного параметра θij обчислюється як:

$$\frac{\partial L(\theta)}{\partial \theta_{ij}} = f(x_i, x_j) - \mathrm{E}_{P(x)}[f(x_i, x_j)], \tag{2.6}$$

де $E_{P(x)}[f(x_i,x_j)]$ – очікуване значення функції $f(x_i,x_j)$ відповідно до поточного розподілу $P(x)$.

6. Контроль збіжності оптимізації.

Виконуємо ітеративне оновлення параметрів θ за допомогою метричного проксимального градієнта (алгоритм методу поданий в наступному підпункті):

$$\theta_{ij}^{(t+1)} = \theta_{ij}^{(t)} + \eta \cdot \frac{\partial L(\theta)}{\partial \theta_{ij}}, \tag{2.7}$$

де η – крок навчання. Процес повторюється до збіжності θ, визначеної на основі величини градієнта або заданого порогу.

7. Прогнозування освітньої траєкторії

З оптимізованими параметрами θ оцінюємо найімовірніші стани вузлів для студента:

$$xi *= arg\max x_i P(x_i \mid x_{\setminus i}) \quad (2.8)$$

де $x_{\setminus i}$ – стани всіх вузлів, крім x_i.

8. **Адаптація освітньої траєкторії.**

Для адаптації моделі до нових даних студента повторно оптимізуємо параметри θ, враховуючи оновлені значення вузлів та ребер, при цьому зберігаючи попередньо визначену структуру графа *G*.

Порівняльна характеристика різних видів моделей, таких, як ПЕ МВП, Ізингове МВП, МВП у векторному просторі, вузлова регресія, обмежені гетерогенні розподіли наведено в таблиці 2.1.

Таблиця 2.1.

Порівняльна таблиця для методу попарно-експоненціального марківського випадкового поля (ПЕ МВП) з іншими методами

	Час навчання (с)	Складність обчислень	Точність (%)	Потреба в пам'яті (МБ)	Стійкість до гетерогенності (1-5)	Збіжність до точного рішення
ПЕ МВП	**300**	***O(n²log n)***	**92**	**200**	**5**	**Так**
Ізингове МВП	400	*O(n³)*	88	150	3	Ні
МВП у векторному просторі	500	*O(n⁴)*	85	300	4	Ні
Вузлова регресія	200	*O(n²)*	80	180	2	Ні
Обмежені гетерогенні розподіли	250	*O(n²)*	87	160	3	Ні

На основі отриманих даних використання попарно-експоненціального марківського випадкового поля (ПЕ МВП) може бути виправданим для обробки випадків з високою варіативністю локальних характеристик. ПЕ МВП дозволяє моделювати залежності між елементами за допомогою ймовірнісних функцій, що ґрунтуються на експоненційних функціях. Це забезпечує гнучкість у встановленні вагових зв'язків і дозволяє краще враховувати локальні взаємозв'язки, особливо у випадках, коли дані мають неоднорідну структуру.

ПЕ МВП також може покращити якість обробки даних, де існує необхідність у точному описі взаємодії між компонентами, наприклад, в освітніх інформаційних системах або інших адаптивних системах. За рахунок застосування експоненційних розподілів марківське випадкове поле забезпечує більш точне моделювання змін та залежностей, що сприяє швидшій та надійнішій збіжності під час оптимізації. Отже, у випадках з вираженими локальними особливостями та складними залежностями ПЕ МВП є ефективнішим підходом порівняно зі стандартними методами.

Для того, щоб покращити процес побудови індивідуальних освітніх траєкторій, доречно додати до попарно-експоненціального марківського випадкового поля метод метричного проксимального градієнта. Це поєднання дозволяє використовувати переваги обох методів: оптимізацію параметрів за допомогою проксимального градієнта та моделування ймовірнісних залежностей між параметрами через марківське випадкове поле. Ось покроковий алгоритм цього поєднання.

Використання методу метричного проксимального градієнта в комбінації з попарно-експоненційним марківським випадковим полем є перспективним підходом для побудови індивідуальних освітніх траєкторій, оскільки ці методи доповнюють один одного, забезпечуючи високий рівень адаптивності та точності в моделюванні навчальних процесів. Метод метричного проксимального градієнта ефективно оптимізує функції, що враховують різноманітні характеристики студентів, що дозволяє отримати глибше розуміння їх навчальних потреб та стилів.

Завдяки ПЕ МВП можливо моделювати складні залежності між різними ознаками, такими як попередній досвід, мотивація та результати навчання, що надає можливість враховувати як індивідуальні, так і колективні аспекти навчального процесу. Це, в свою чергу, відкриває двері для створення більш гнучких і персоналізованих освітніх траєкторій, які можуть адаптуватися до змін у навчальному середовищі та прогресу студентів.

Комбінація цих методів також покращує ефективність обробки даних, дозволяючи аналізувати великі обсяги інформації про студентів і виявляти патерни, які можуть бути неочевидними при використанні традиційних підходів. Таким чином, ця інтеграція не лише підвищує якість навчання, але й забезпечує можливість швидкої реакції на потреби студентів, формуючи динамічні і адаптивні освітні траєкторії, що ведуть до кращих результатів у навчанні.

2.3. Удосконалення методу метричного проксимального градієнта

У дослідженні представлено адаптивний підхід до вибору діагональної метрики на основі методу Барзілая-Борвейна (ББ). Цей підхід поєднує проксимальний метод Ньютона з традиційним проксимальним градієнтом, дозволяючи враховувати індивідуальні особливості студентів, їхні навчальні результати та рівень складності матеріалу. Завдяки адаптивності алгоритму досягається зниження обчислювальних витрат і точніше наближення гессіана, що сприяє вдосконаленню прогнозування освітніх траєкторій. Це є особливо корисним для великих освітніх систем, де важливо швидко та точно моделювати динамічні процеси навчання. Результати емпіричних досліджень підтвердили, що запропонований підхід значно покращує збіжність і підвищує ефективність визначення освітніх траєкторій порівняно 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:

$$\min_{m \in R^n} \quad \left\| Mc^n - y^n \right\|_2^2 + \eta \left\| M - M^{n-1} \right\|_F^2 \tag{2.9}$$

$$\left(\beta_{ББ1}^n\right)^{-1} J \le M \le \left(\beta_{ББ2}^n\right)^{-1} J$$

$$M = diag\left(m\right)$$

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:

$$\begin{aligned} \beta_{ББ1}^n &:= \left\| c^n \right\|_2^2 / \left(c^n y^n \right); \\ \beta_{ББ2}^n &:= \left(c^n, y^n \right) / \left\| y^n \right\|_2^2 \end{aligned} \tag{2.10}$$

В роботі розглядається узгоджена оптимізація, яка задається наступним чином:

$$\min_{x_1,\ldots,x_H \in R^n} \quad \sum_{i=1}^{H} f_i\left(x_i\right) + \partial_S\left(x_1,\ldots,x_H\right) \tag{2.11}$$

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

Для збереження властивостей розподіленої узгодженої оптимізації було запропоновано застосовувати блочно-діагональну структуру метрики. Використання блочно-діагонального підходу рівномірно розподіляє градієнтні кроки між вузлами, при цьому узгоджене оновлення реалізується як зважене середнє значень локальних змінних кожного вузла. Це має особливе значення

для розв'язання масштабних задач машинного навчання. У традиційних проксимальних градієнтних методах узгодження часто здійснюється шляхом простого середнього локальних змінних, що може бути не оптимальним для машинного навчання. Окремі вузли можуть обробляти значно більші обсяги даних і бути більш надійними, ніж інші, що вимагає надання їхнім оновленням більшої ваги при узгодженні. Вибір метрики з діагональною або блочною структурою дозволяє врахувати відмінності у надійності вузлів. На відміну від скалярного підходу Барзілая-Борвейна (ББ), діагональний підхід ефективніше вирішує цю задачу. У подальшій роботі запропоновано дві стратегії вибору елементів блочно-діагональної метрики, що оптимізують процес узгодження.

Основна ідея – апроксимувати локальний гессіан $\nabla^2 f_i\left(x_i^n\right)$ 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 $y_i^n = \nabla f_i\left(x_i^n\right) - \nabla f\left(x_i^{n-1}\right)$. На основі цього запропоновано наступні кроки ББ:

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

$$M_{лок.ББ}^n = blndiag\left(M_1^n, ..., M_H^n\right) \tag{2.12}$$

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

$$M_{лок.ДББ}^n = bl\,n\,diag\left(M_1^n, ..., M_H^n\right) \tag{2.13}$$

Однією з переваг запропонованого формулювання (2.9) є те, що воно має просту замкнену форму розв'язання. Для $M_n = diag\left(m_n\right)$, де $m^n = \left[m_1^n, ..., m_h^n\right] \in R^n$ розв'язання задачі (3.14) задається наступним чином:

$$m_i^n = \begin{cases} \dfrac{1}{\beta_{ББ1}^n}, & \dfrac{c_i^n y_i^n + \eta m_i^{n-1}}{\left(c_i^n\right)^2 + \eta} < \dfrac{1}{\beta_{ББ1}^n} \\ \dfrac{1}{\beta_{ББ2}^n}, & \dfrac{c_i^n y_i^n + \eta m_i^{n-1}}{\left(c_i^k\right)^2 + \eta} > \dfrac{1}{\beta_{ББ2}^n} \\ \dfrac{c_i^n y_i^n + \eta m_i^{n-1}}{\left(c_i^n\right)^2 + \eta}, & \textit{в інших випадках} \end{cases} \tag{2.14}$$

де c_i^n та y_i^n – i-й елемент c^n і y^n.

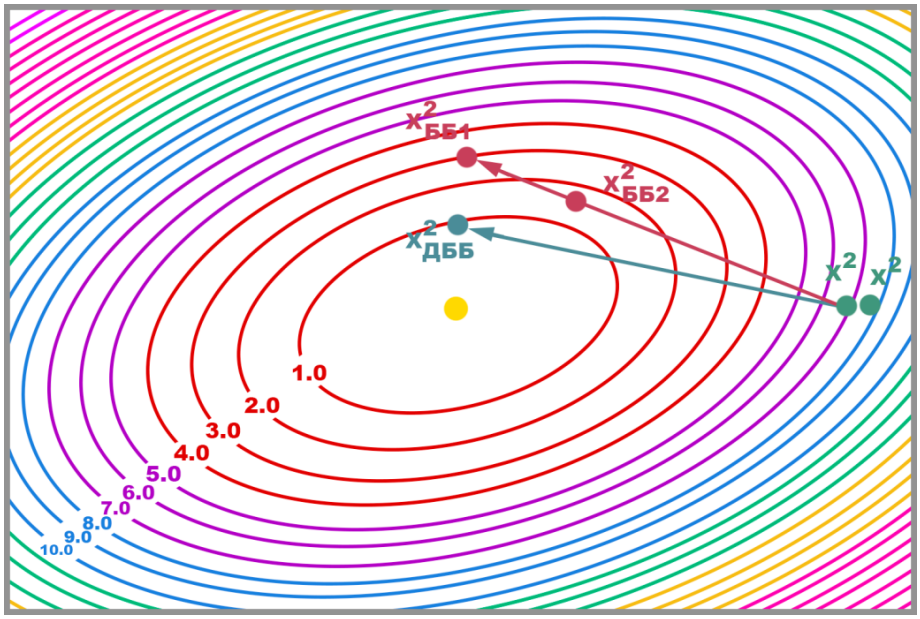

Рис. 2.1. Графічне представлення методу ББ

Хоча обидва гібридні скаляри Барзілая-Борвейна (ББ) та діагональний ББ залежать від попередньої метрики, гібридний ББ використовує обмежену інформацію: попереднє значення кроку просто повторюється для негативного початкового значення. Діагональний ББ, навпаки, повноцінніше застосовує цю додаткову інформацію за рахунок параметра μ\muμ, визначеного користувачем, що враховує баланс між кращим наближенням гессіана і числовою стабільністю. Встановлення великого значення η\etaη також прирівнюється до копіювання попереднього розміру кроку, що характерно для гібридного скаляра ББ.

Діагональна метрика діє як масштабування координат на кожній ітерації, застосовуючи подальші градієнтні та проксимальні кроки. Таким чином, алгоритм ЗМПГ із діагональною метрикою можна розглядати як процес послідовного масштабування координат, де кожен масштаб у ітерації nnn залежить від локальної кривини, тобто наближення гессіана. Це робить діагональні метрики менш чутливими до значних варіацій масштабів координат. Як і багато методів ББ, алгоритм із діагональною метрикою у (3.15) може не забезпечувати збіжність без додаткового лінійного пошуку для неквадратичних задач, тому формулу (3.15) слід розглядати як початкову метрику, а потім доповнювати її пошуком уздовж лінії.

Таким чином, запропонована діагональна метрика покращує оцінку локального гессіана з поганою обумовленістю порівняно зі стандартним скалярним кроком ББ, що забезпечує швидшу збіжність алгоритму. У поєднанні з немонотонним лінійним пошуком такий підхід гарантує загальну збіжність алгоритму. Нарешті, у низці програм машинного навчання, використовуючи як штучні, так і реальні набори даних, емпіричні результати підтверджують кращі показники збіжності запропонованої методики.

Алгоритм метричного проксимального градієнта з діагональною метрикою буде мати наступні кроки:

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

2. Обчислити $\beta^n_{BB_1}$ та $\beta^n_{BB_2}$ за формулою

$$\beta^n_{BB} := \beta_{BB}\left(c^n, y^n\right) =$$

$$= \begin{cases} \beta^n_{BB_2} & if\ \beta^n_{BB_1} < \delta\beta^n_{BB_2} \\ \beta^n_{BB_1} - \dfrac{1}{\delta}\beta^n_{BB_2} & в\ інших\ випадках \end{cases}$$

3. Ініціалізувати M^n за формулою

$$m_i^n = \begin{cases} \dfrac{1}{\beta_{BB1}^n}, & \dfrac{c_i^n y_i^n + \mu m_i^{n-1}}{\left(c_i^n\right)^2 + \mu} < \dfrac{1}{\beta_{BB1}^n} \\ \dfrac{1}{\beta_{BB2}^n}, & \dfrac{c_i^n y_i^n + \mu m_i^{n-1}}{\left(c_i^n\right)^2 + \mu} > \dfrac{1}{\beta_{BB2}^n} \\ \dfrac{c_i^n y_i^n + \eta m_i^{n-1}}{\left(c_i^n\right)^2 + \eta}, & \textit{в інших випадках} \end{cases}$$

4. Обчислити $x^{n+1} := prox_{q,M_n}\left(x^n - \left(M^n\right)^{-1}\nabla f\left(x^n\right)\right)$.

5. Повторити вирази

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

$$x^{n+1} := prox_{q,M_n}\left(x^n - \left(M^n\right)^{-1}\nabla f\left(x^n\right)\right)$$

до тих пір, поки виконується критерій

$$F\left(x^{n+1}\right) \le \widehat{F}^n - \frac{1}{2}\left\|x^{n+1} - x^n\right\|_{M^n}^2$$

$$\bar{F}^n = \max\left\{F\left(x^n\right), F\left(x^{n-1}\right), ..., F\left(x^{n-\min\left(K_{ls,n-1}\right)}\right)\right\}$$

6. Повернути метрику M^n і виконати наступну ітерацію x^{n+1}.

7. Виконувати кроки 2-6 поки критерій зупинки не буде задоволений.

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.

Метод метричного проксимального градієнта підключається в момент, коли необхідно оновити стани вузлів у марківському випадковому полі з урахуванням локальних взаємодій між вузлами. Це може відбутися в двох випадках:

1. При обчислення градієнтів функції втрат для кожного вузла. При цьому у моделі МВП обчислюється локальний градієнт для кожного вузла на основі його стану та станів сусідніх вузлів.

2. При визначенні адаптивного кроку для оновлення станів. Замість стандартного градієнтного кроку застосовується адаптивний проксимальний крок із блочною діагональною метрикою. Це дозволяє враховувати кривизну (гессіан) і структуру ПЕ МВП, забезпечуючи гнучке оновлення вузлів.

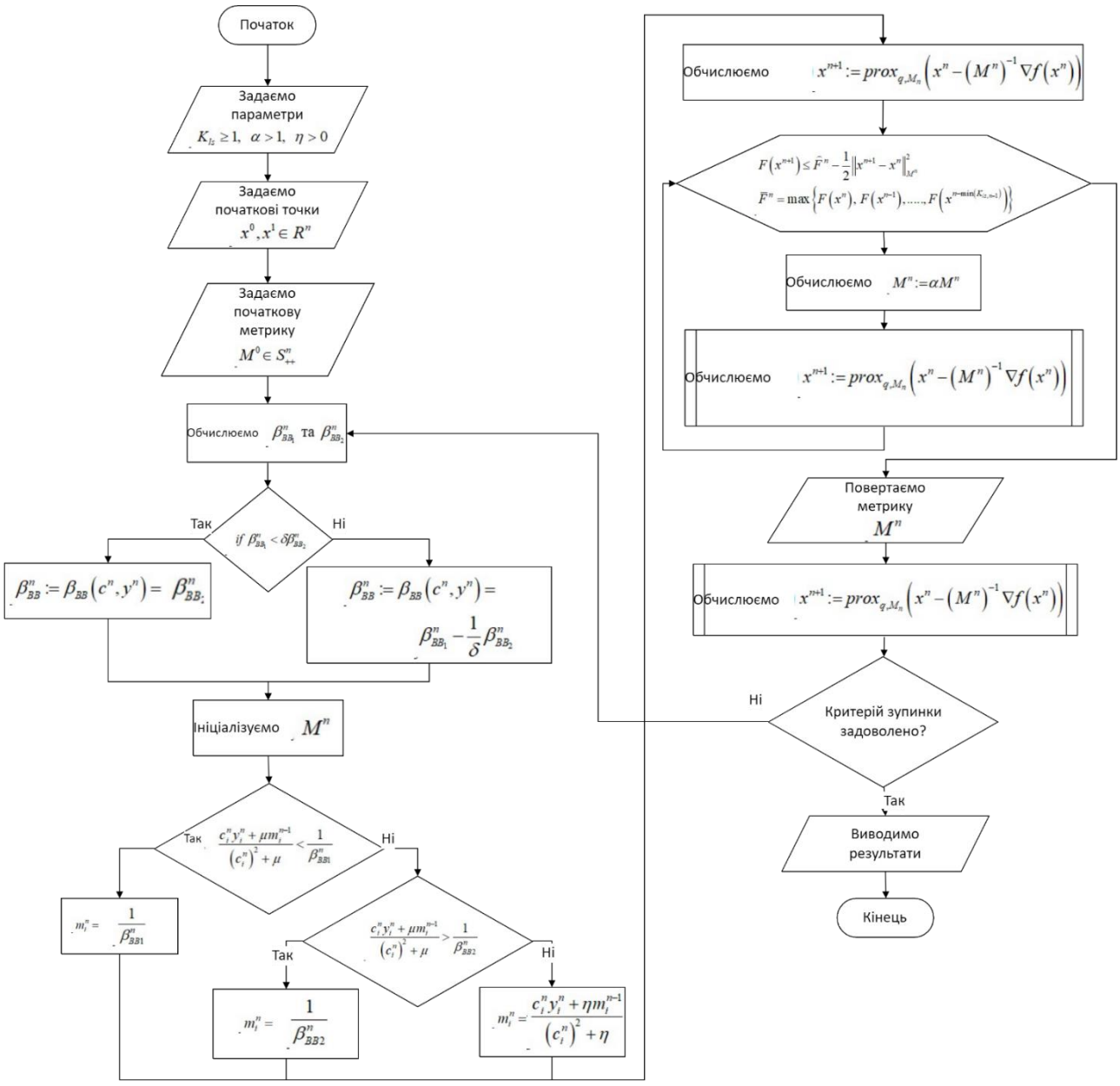

Рис. 2.2. Метод метричного проксимального градієнта з використанням діагональної метрики

Таблиця 2.2

Порівняльна характеристика методів машинного навчання

	Точність побудови траєкторії (%)	Швидкість збіжності (ітерацій)	Середньоквадратична похибка (MSE)	Час обчислення (с)
Градієнтний спуск	85	500	0.15	12
Метод Ньютона	92	120	0.08	25
Проксимальний градієнт	88	300	0.12	15
Метричний проксимальний градієнт	94	180	0.07	18
Запропонований метод (з діагональним кроком)	96	150	0.05	17

Отримані числові значення для кожного методу відображають їхню здатність вирішувати задачу побудови індивідуальних освітніх траєкторій з урахуванням ключових показників: точності побудови траєкторії, швидкості збіжності, середньоквадратичної похибки та часу обчислення. Точність побудови траєкторії (у %) показує, наскільки точно кожен метод наближається до ідеальної траєкторії, і тут запропонований метод досягає 96%, що є найвищим значенням. Швидкість збіжності, виражена в ітераціях, вказує на кількість кроків, необхідних для досягнення стабільного результату: метод з діагональним кроком показує нижчу кількість ітерацій (150), що є досить ефективним показником.

Середньоквадратична похибка (MSE), яка становить 0.05 у запропонованому методі, є найменшою серед інших, що вказує на високу точність і меншу кількість відхилень у результатах. Час обчислення для цього методу також є досить оптимальним (17 секунд), що робить його придатним для практичних задач. Отже, удосконалений в роботі метод є кращим серед представлених: він демонструє оптимальний баланс між точністю, швидкістю, стійкістю до похибок та витратами часу, що надає йому переваги для задач такого типу.

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 інформаційні системі, з метою забезпечення її функціональної стійкості.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ МЕТОДІВ ТА ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ В ОСВІТНІЙ ГАЛУЗІ

3.1. Удосконалення заходів, спрямованих на попередження та ліквідацію наслідків кібератак

Засоби забезпечення інформаційних систем, переведені в динамічний стан, перетворюються на методи – способи й прийоми реалізації дій. У цьому контексті можна виділити технічні (спостереження, контроль, ідентифікація тощо), організаційні (створення безпечних зон, встановлення режиму, проведення розслідувань, організація постів і патрулювання), інформаційні (створення характеристик працівників, аналітична обробка даних, облік конфіденційних документів), фінансові (матеріальне заохочення співробітників за успіхи у сфері безпеки, винагороди інформаторам), правові (захист прав і підтримка правоохоронних органів), кадрові (підбір, навчання та виховання персоналу для забезпечення безпеки) та інтелектуальні (сертифікація, патентування, захист бренду) методи [61, 91].

Критерії, що виступають засобом оцінки, відображають бажаний рівень інформаційної безпеки в бізнесі, тоді як показники оцінюють досягнутий стан. У зв’язку з цим підкреслюється нормативна роль критеріїв, що визначають принципи та підхід до оцінки рівня безпеки, тоді як показники є безпосередніми засобами вимірювання.

До суб’єктів, які в межах своїх повноважень виконують завдання щодо кібербезпеки, належать: підприємства, освітні заклади та громадські організації, які здійснюють діяльність або надають послуги, пов’язані з національними інформаційними ресурсами, електронними послугами, проведенням електронних правочинів, електронними комунікаціями, захистом інформації та кібербезпекою, а також організації, що відносяться до критичної

інфраструктури [78].

У рамках своєї компетенції, ці суб’єкти забезпечують низку заходів для запобігання використанню кіберпростору в незаконних цілях, включно з військовими, розвідувальними та терористичними активностями. Це передбачає як попередження, так і ефективне реагування на можливі загрози, щоб мінімізувати ризики протиправного втручання.

Важливим напрямом їхньої діяльності є виявлення кіберінцидентів та кібератак, а також своєчасна й дієва реакція на них. Вони не тільки ліквідовують наслідки таких загроз, але й реалізують стратегії, що дозволяють знижувати ймовірність їх повторення.

Інформаційний обмін стосовно виявлених та потенційних кіберзагроз — ще одна важлива функція, яка дозволяє оперативно реагувати на нові виклики та попереджати інші зацікавлені сторони про можливі ризики.

Значну увагу приділяють профілактичним, організаційним та освітнім заходам, спрямованим на підвищення кібербезпеки та кібероборони. Ці заходи охоплюють навчання персоналу, створення умов для безпеки інфраструктури та підвищення загальної обізнаності щодо захисту даних.

Проведення аудиту інформаційної безпеки на підконтрольних об’єктах є важливим аспектом, що сприяє виявленню вразливих місць у системах і вчасному усуненню ризиків. Водночас, вони здійснюють додаткові заходи для забезпечення захисту кіберпростору від хакерських дій

Критерії та порядок визначення об’єктів, які належать до критичної інфраструктури, а також перелік таких об’єктів, загальні вимоги до їх кіберзахисту, застосування індикаторів кіберзагроз і вимоги щодо проведення незалежного аудиту інформаційної безпеки встановлюються компетентними урядовими органами [].

Ефективність національної системи кібербезпеки забезпечується завдяки цілісній системі заходів, спрямованих на вдосконалення методів та засобів захисту інформаційних систем. Це включає розробку та оперативне оновлення політики кібербезпеки, яка підтримує розвиток кіберпростору та відповідає

міжнародним стандартам. Важливим завданням є вдосконалення законодавчої бази, узгодження нормативних актів у сферах електронних комунікацій, захисту інформації та кібербезпеки згідно з міжнародними нормами. Крім того, для об'єктів критичної інфраструктури впроваджуються обов'язкові стандарти інформаційної безпеки, що охоплюють етапи створення, експлуатації та модернізації, з урахуванням міжнародних стандартів і галузевої специфіки.

Створення конкурентного середовища для постачальників послуг у сфері електронних комунікацій, інформаційної безпеки та кіберзахисту також є ключовим елементом. До розробки концептуальних документів у сфері кібербезпеки залучаються експерти з наукових установ, професійних і громадських організацій. Проводяться регулярні тренінги для персоналу з відпрацювання дій у разі кіберінцидентів і надзвичайних ситуацій у кіберпросторі. Крім того, активно впроваджується система аудиту інформаційної безпеки з використанням найкращих світових практик і міжнародних стандартів, розвивається мережа команд реагування на комп'ютерні надзвичайні ситуації, а також вдосконалюються технічні та криптографічні засоби захисту інформації.

Значна увага приділяється дотриманню вимог щодо захисту державних інформаційних ресурсів, створенню та підтримці функціонування Національної телекомунікаційної мережі, а також обміну інформацією про кіберінциденти між учасниками системи кібербезпеки. Створюється єдина система індикаторів кіберзагроз, яка відповідає міжнародним стандартам, а також розширюється підготовка бакалаврів і магістрів з кібербезпеки відповідно до потреб державного сектору.

Крім того, запроваджується організаційно-технічна модель національної системи кібербезпеки, що дозволяє оперативно реагувати на кібератаки. Також встановлюються правила для безпечного використання Інтернету та надання державними органами електронних послуг. Співпраця державного і приватного секторів відіграє важливу роль у запобіганні кіберзагрозам для критичної інфраструктури, а періодичний огляд стану національної системи кібербезпеки та розробка індикаторів її ефективності сприяють підтриманню високого рівня

захисту.

Стратегічне планування і підтримка програм розвитку електронних комунікацій та інформаційних технологій доповнюються розвитком міжнародної співпраці у сфері кібербезпеки, яка відповідає національним інтересам України. При цьому обмежується участь підприємств, підконтрольних державі-агресору, у заходах з забезпечення інформаційної безпеки. Для своєчасного виявлення загроз національній безпеці в кіберпросторі також розвивається система контррозвідувального забезпечення, а заходи протидії кіберзагрозам регулярно посилюються для надійного захисту державних інтересів.

Державний центр кіберзахисту здійснює впровадження організаційно-технічної моделі національної системи кібербезпеки. На нього покладено обов’язки щодо створення та підтримки елементів захищеного доступу державних органів, включаючи освітні установи, до Інтернету. Крім цього, центр займається організацією антивірусного захисту національних інформаційних ресурсів, проводить аудити інформаційної безпеки, оцінює стан кіберзахисту об'єктів критичної інфраструктури. Він також відповідає за виявлення вразливостей, реагування на кіберінциденти, координацію діяльності команд реагування на комп’ютерні надзвичайні ситуації та розробку сценаріїв реагування і нейтралізації кіберзагроз. Центр впроваджує програми та методології для кібернавчань, сприяючи загальному підвищенню рівня захисту [76].

CERT-UA, урядова команда реагування на комп’ютерні надзвичайні ситуації, створена з метою збору та аналізу даних про кіберінциденти. Її діяльність включає ведення державного реєстру кіберінцидентів і надання практичної допомоги власникам об’єктів кіберзахисту в питаннях запобігання, виявлення та ліквідації наслідків кіберінцидентів [92].

У сучасному світі технологічна інформація набуває важливої стратегічної ролі. Вона охоплює документовані дані про склад, властивості та параметри технологічних процесів, які застосовуються для керування об’єктами в різних

галузях протягом усього їхнього життєвого циклу, а також інформацію з автоматизованих систем керування цими об’єктами [135]. Особливу увагу зосереджено на захисті технологічної інформації, що стосується критичної транспортної, інформаційної та телекомунікаційної інфраструктури, а також об’єктів підвищеної небезпеки, адже їхні збої можуть призвести до аварій чи надзвичайних ситуацій, створюючи загрозу національній безпеці, здоров'ю громадян і стабільності суспільства. Окремі дані, що стосуються певних об’єктів або їх груп, можуть бути класифіковані як інформація з обмеженим доступом.

Системний адміністратор відіграє важливу роль у забезпеченні захисту від кібератак та усуненні їхніх наслідків. Його діяльність повинна бути чітко регламентована, з визначенням обов’язків, прав та особистої відповідальності, що сприятиме підвищенню ефективності кібербезпеки в організації [125].

Основним завданням адміністратора безпеки є забезпечення безперебійної роботи мережі та реалізація технічних заходів, необхідних для впровадження політики інформаційної безпеки, а саме: забезпечення працездатності серверів і основного обладнання системи, виконання робіт відповідно до календарних планів на підставі доручень адміністратора безпеки, підготовка пропозицій щодо покращення методів і заходів для забезпечення безпеки технологічної інформації, що обробляється в системі, а також виконання модернізації системи.

Для виконання своїх обов'язків адміністратор безпеки (АБ) повинен мати знання про діючі державні та відомчі нормативні акти, що регулюють захист інформації в автоматизованих системах. Він також має бути ознайомлений з основними характеристиками систем захисту інформації та апаратно-програмних платформ, на основі яких формується Система. Важливими є також методики перевірки та оновлення систем захисту інформації в межах Системи, основні способи протидії комп'ютерним вірусам і програмам з недокументованими можливостями, а також характеристики та порядок експлуатації технічних засобів захисту інформації.

Системний адміністратор несе безпосередню відповідальність за забезпечення безперебійної роботи інформаційної мережі та її апаратно-

програмного комплексу. Йому потрібно підтримувати працездатність підсистеми КСЗІ та гарантувати безперешкодний доступ зареєстрованих користувачів до Системи відповідно до політики безпеки. Системний адміністратор також організовує створення атрибутів доступу для нових користувачів і електронних поштових скриньок, а також відповідає за виконання антивірусного та антиспамового захисту для електронної пошти користувачів. Важливо, щоб він проводив встановлення та оновлення антивірусного програмного забезпечення в мережі користувачів інформаційно-телекомунікаційної системи.

Крім того, системний адміністратор повинен знати функціональну схему організації інформаційної мережі, алгоритм перевірки працездатності інформаційної мережі, а також порядок технічного обслуговування серверного та мережевого обладнання. Він має бути ознайомлений з оперативно-технічними даними підсистем, таких як обладнання та канали зв'язку, і повинен забезпечити працездатність Системи під час аварійних ситуацій. Системний адміністратор також зобов'язаний знати основні профілактичні заходи, що проводяться в Системі, та можливі тимчасові порушення функціонування каналів зв'язку.

До ключових обов'язків системного адміністратора входить організація розподілу та оновлення програмних засобів протидії комп'ютерним вірусам і недокументованим програмам. Він надає консультативну та практичну допомогу співробітникам і користувачам Системи у встановленні та налаштуванні антивірусного програмного забезпечення. Адміністратор повинен забезпечити функціонування інформаційної мережі відповідно до рекомендованих норм і надавати користувачам послуги щомісячно та в повному обсязі. Він зобов'язаний повідомляти керівнику Системи про неполадки в об'єктах, системах, лініях зв'язку та про втрату зв'язку з підсистемами, а також інформувати адміністратора безпеки про раптові зміни у зв'язку, які можуть вплинути на обмін інформацією.

Системний адміністратор має право вносити пропозиції та брати участь у проєктуванні, створенні й випробуванні елементів і систем Системи. Він може призупиняти доступ до мережі Системи для користувачів під час проведення

профілактичних робіт. У разі виявлення порушень цієї Інструкції та "Інструкції користувачу Системи" адміністратор повинен доповідати про них керівнику Системи для визначення необхідних заходів.

При цьому системний адміністратор несе персональну відповідальність за недотримання вимог цієї інструкції, а також за всі дії, що не регламентуються інструкцією, виконані ним під час роботи з елементами системи. У разі порушення системним адміністратором встановлених правил експлуатації обладнання Системи проводиться службове розслідування, на основі якого приймається рішення щодо визначення розміру збитків і їх компенсації відповідно до чинного законодавства. В окремих випадках може розглядатися можливість притягнення його до адміністративної або кримінальної відповідальності [138].

Обґрунтовано та сформульовано основні принципи та концептуальні положення забезпечення інформаційної безпеки в освітній сфері. Наведено удосконалену термінологічну базу у сфері кібербезпеки. Встановлено, що діяльність системного адміністратора може відігравати важливу роль у реалізації удосконалених заходів, спрямованих на попередження та ліквідацію наслідків кібератак.

3.2. Особливості оцінки загроз інформаційної безпеки

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. Зокрема, важливим є збільшення прибутку вузу від НДДКР за рахунок комерціалізації розробок та залучення додаткових обсягів коштів для якісного виконання проектів.

Таким чином, сукупність розглянутих передумов спрямована на актуалізацію інформаційної безпеки. Одночасно необхідно відзначити фундаментальну роль саме економічних передумов, які повинні виступати тією

рушійною силою для розвитку освітньої галузі, яка сприятиме активізації наукової діяльності. В той же час, найбільш залежними від стану інших передумов гарантування інформаційної безпеки є економічні передумови, які формують основи фінансового забезпечення даного сектору вищої освіти.

Водночас, необхідно зазначити, що дослідження передумов інформаційної безпеки, підкреслюючи об'єктивну необхідність її гарантування, як важливого підґрунтя розвитку освітньої галузі підтверджує доцільність дослідження умов і чинників інформаційної безпеки проведення НДДКР у вузах на базі врахування їх економічних інтересів (як форми прояву наукових потреб) та гармонізації економічних відносин у відповідності з логікою далі викладеного дослідження.(рис 3.1)

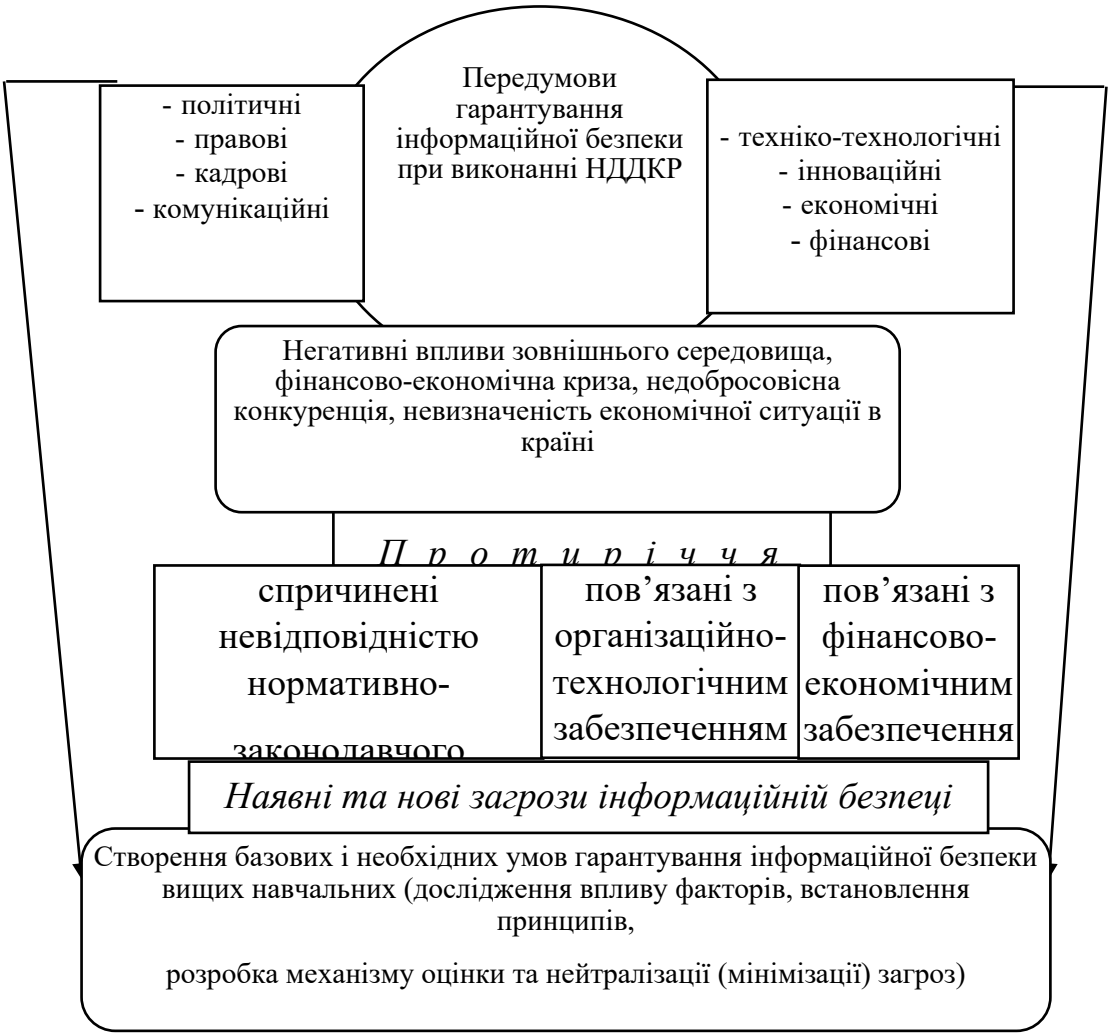

Рис. 3.1. Послідовність дослідження інформаційної безпеки у вузах

Оцінка загроз інформаційній безпеці вищих навчальних закладів (ВНЗ) має свої специфічні риси, які відрізняють її від загальноприйнятих підходів у інших сферах. Варто зазначити, що існує відсутність єдиної методології комплексної оцінки інформаційної безпеки в освітньому секторі. Інформаційна безпека різних університетів в системі освіти повинна базуватися на організаційно-технічних умовах, що забезпечують стабільне функціонування системи за обмежених ресурсів, своєчасному виявленні загроз технічного, інформаційного та економічного характеру, а також на розробці комплексу заходів, що сприяють нейтралізації або мінімізації їх впливу. Крім того, оцінка загроз інформаційній безпеці ВНЗ має враховувати особливості організації їх науково-педагогічної діяльності. Ця оцінка повинна надати відповіді на питання щодо можливого впливу загроз та доцільності впровадження засобів і заходів, спрямованих на їх нейтралізацію. На мою думку, іноземні методики не завжди можуть бути адекватно застосовані в умовах України, а також існує проблема невизначеності в складі критеріїв оцінки інформаційної безпеки, їх градації та інтерпретації.

Сучасні економічні умови, у яких функціонують вітчизняні університети, вимагають активного пошуку нових джерел фінансування, інноваційних підходів до управління та нових рольових функцій для учасників освітньої діяльності. Комерціалізація наукових досягнень змушує по-новому оцінювати університетські процеси, які вже охоплюють не лише освітні та наукові завдання, але й організаційні, технологічні, фінансові та комерційні аспекти. У сучасному контексті комерціалізація результатів наукових досліджень є не просто потребою, а ключовим елементом успішного розвитку університету.

Сфера освіти у більшості університетів має необхідну інфраструктуру та кадровий потенціал для реалізації науково-дослідних проєктів і трансформації їхніх результатів у комерційні продукти, які можуть бути успішно представлені на ринку науково-технічної продукції. Процес комерціалізації науково-технічних розробок полягає у перетворенні актуальних результатів науково-дослідних і дослідно-конструкторських робіт (НДДКР) на ринкові продукти та послуги з метою отримання доходу шляхом їх продажу, ліцензування або

самостійного використання [127]. Цей процес охоплює пошук та оцінку інновацій, відбір перспективних ідей для фінансування, залучення необхідних ресурсів, юридичне закріплення прав на інтелектуальну власність, впровадження інновацій у виробництво та подальшу модифікацію й підтримку інтелектуального продукту.

Для ефективного просування наукових розробок університетів на ринок ключовим фактором є інвестиції. Оскільки університети зазвичай не мають достатніх фінансових ресурсів, важливо налагодити взаємодію з потенційними споживачами наукової продукції. Закріплення прав на інтелектуальну власність забезпечує захист від несанкціонованого копіювання або використання сторонніми дослідниками. У зв’язку з цим особливу увагу слід приділити впровадженню методів та технологій забезпечення інформаційної безпеки для адаптивних корпоративних освітніх інформаційних систем. Рекомендується детально розглянути складові інформаційної безпеки, інтегрувати їх та узагальнити показники ефективності в єдину оцінку їх дієвості [128].

Логіка даного дослідження полягає в переході від вказаних передумов, як об'єктивної необхідності забезпечення інформаційної безпеки, через розв'язання протиріч у розвитку різних університетів, до формування сприятливих умов для реалізації механізму безпеки. Ці умови включають не лише сукупність факторів і обставин, що впливають на рівень інформаційної безпеки, але й тенденції та вимоги – принципи, згідно з якими відбуватиметься використання НДДКР різними ВНЗ. Процедура проведення оцінки інформаційної безпеки, що охоплює основні елементи алгоритму забезпечення інформаційної безпеки наукових розробок, представлена на рисунку 3.2.

Рис. 3.2. Процедура гарантування інформаційної безпеки ВНЗ при науково-дослідних розробках

Оцінка проводиться на основі розрахунку сукупного критерію (інтегрального показника), який отримується шляхом визначення та підсумування окремих складових і функціональних критеріїв інформаційної безпеки. Ці функціональні критерії розраховуються шляхом порівняння потенційних збитків із витратами на реалізацію заходів, спрямованих на їх запобігання [57]. Після виконання цих етапів визначається сукупний критерій безпеки (Кіб):

$$К_{іб} = \sum_{i=1}^{n} K_i D_i \qquad (3.1)$$

де $К_i = \frac{СЗi}{Зi}$ - величина окремого критерію за і–ю функціональною складовою; Di – питома вага значущості і–ої функціональної складової, іноді визначається експертами (метод експертних оцінок); n – число функціональних складових інформаційної безпеки; СЗі – сукупні збитки за і–ю функціональною складовою інформаційної безпеки, грошові одиниці; Зі – сумарні витрати на реалізацію заходів щодо попередження збитку за і–ю складовою інформаційної безпеки, грошові одиниці [57].

У нашому випадку функціональними компонентами інформаційної безпеки можуть бути фінансова, інтелектуальна, кадрова, техніко-технологічна, політико-правова, інформаційна, екологічна та силова складові. Формула для розрахунку сукупного критерію інформаційної безпеки може потребувати певних уточнень: до чисельного значення загальних витрат «$З_i$» додаються суми відповідних збитків «$З_{зі}$», які вдалося уникнути завдяки реалізованим заходам щодо запобігання шкоди за і-ю складовою інформаційної безпеки. Таким чином, розрахунок $К_i$ матиме наступний вигляд [130]:

$$К_i = \frac{СЗ_i}{(З_i + З_{Зi})} \tag{3.2}$$

Крім того, важливо оцінити рівень інформаційної безпеки $К_{iб}$ у порівнянні з аналогічними показниками інших університетів, що підпорядковуються Міністерству освіти і науки України. Для комплексної оцінки рівня інформаційної безпеки доцільно використовувати співвідношення між обсягом брутто-інвестицій ВНЗ та розміром інвестиційних ресурсів, які забезпечують конфіденційні умови, необхідні для інформаційної безпеки наукових розробок. Розрахунок проводиться за такою формулою:

$$Р_{iб} = \frac{БІ_t}{It_{iб}} \tag{3.3}$$

де $БІ_t$ – брутто – інвестиції вузу в році t, грошові одиниці; $It_{іб}$ – інвестиції університету в році t, що необхідні для забезпечення його інформаційної безпеки, грошових одиниці.

Брутто-інвестиції складаються з бюджетних коштів, які направляються на проекти, реінвестованих прибутків поточного та майбутніх періодів, накопичень минулих років, а також амортизаційних відрахувань, якщо такі є. Обсяг інвестицій, необхідних для забезпечення інформаційної безпеки, також включає кошти для реалізації запланованих заходів, закупівлі необхідних технічних засобів, впровадження нововведень, зменшення витрат на дослідження та розширення і диверсифікацію джерел фінансування науково-дослідних процесів тощо. Числове значення $P_{іб}$ може коливатися від «0» до «1», де «0» вказує на найнижчий рівень інформаційної безпеки, а наближення до «1» свідчить про високий рівень.

Підвищення рівня інформаційної безпеки досягається завдяки техніко-технологічним нововведенням та документації політики інформаційної безпеки, при цьому важливо враховувати витрати на окремі проекти. Оцінюючи складові вищезгаданої формули, вважаю доцільним наголосити, що рівень інформаційної безпеки Ріб слід визначати на основі результатів наукової діяльності за рік. Цей показник дозволяє більш точно оцінити стан інформаційної безпеки з огляду на вплив тривалих загроз (протягом року чи кількох років) і проаналізувати загальний обсяг фінансових витрат за цей період.

Суть методу полягає в оцінці рівня інформаційної безпеки за її складовими з подальшим узагальненням для отримання інтегрального показника безпеки ВНЗ. До складових інформаційної безпеки, як правило, відносять: фінансову, ринкову, інтерфейсну, інтелектуальну та інші.

При цьому здійснюється розрахунок оціночних показників інформаційної безпеки, які можуть бути віднесені до п’яти зон: абсолютної безпеки, нормального чи нестабільного рівня, критичного або кризового рівня безпеки. З певними застереженнями цей методичний підхід може бути використаний для

оцінки інформаційної безпеки й інших університетів у процесі виконання ними реальних замовлень на наукові розробки.

3.3. Розробка методики оцінки рівня інформаційної безпеки освітньої інформаційної системи

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.

Розглянемо математичні моделі, які дозволяють здійснювати кількісну оцінку рівня інформаційної безпеки закладів вищої освіти [53]:

1. Модель багатокритеріального аналізу (AHP) - дозволяє визначити вагу різних критеріїв, що впливають на інформаційну безпеку, та використовує їх для інтегрованої оцінки рівня безпеки.

Модель складається з структурування проблеми, порівняння критеріїв, розрахунок ваг за допомогою матриці парних порівнянь (3.4).

$$A = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ \frac{1}{a_{12}} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_{1n}} & \frac{1}{a_{2n}} & \cdots & 1 \end{bmatrix}, \quad (3.4)$$

де a_{ij} - відносна важливість критерію і порівняно з критерієм j.

Власні вектори і значення розраховуються за формулою:

$$Aw = \lambda_{\max} w, \quad (3.5)$$

де λ_{max} - найбільше власне значення матриці порівнянь, w - власний вектор, що представляє ваги критеріїв.

Ваги визначаються за формулою:

$$w_i = \frac{a_i}{\sum_{i=1}^{n} a_i}, \quad (3.6)$$

де w_i – вага критерію і, a_i – елемент власного вектора.

Обчислення узагальненої оцінки:

$$S_j = \sum_{i=1}^{n} w_i \cdot s_{ij}, \quad (3.7)$$

де S_j - узагальнена оцінка альтернативи j, s_{ij} - оцінка альтернативи j за критерієм i.

2. Модель економічної оцінки (CBA) - оцінює економічну доцільність заходів інформаційної безпеки, використовуючи методику розрахунку чистої теперішньої вартості (NPV). Визначається модель за допомогою ідентифікації витрат і вигод, дисконтування, яке знаходиться за формулою

$$PV = \frac{FV}{(1+r)^t}, \tag{3.8}$$

де PV – теперішня вартість, FV – майбутня вартість, r – ставка дисконтування, t– кількість років.

3. **Розрахунок чистої теперішньої вартості (NPV):**

$$NPV = \sum_{t=1}^{T} \frac{B_t - C_t}{(1+r)^t}, \tag{3.9}$$

де B_t – вигоди в році t, C_t – витрати в році t, r – ставка дисконтування, T – період оцінки.

3. Модель аналізу ризиків - допомагає ідентифікувати і оцінити ймовірності і впливи потенційних загроз, що дозволяє ефективно управляти ризиками.

Модель складається з ідентифікації загроз та оцінка ймовірностей і впливів. Рівень ризику розраховується за формулою:

$$R = P \times I, \tag{3.10}$$

де R – рівень ризику, P – ймовірність виникнення загрози, I – вплив загрози.

4. Модель системної динаміки – описує динамічні процеси в системі інформаційної безпеки, дозволяючи прогнозувати зміни та розробляти стратегії управління.

Основні етапи моделі визначення компонентів системи, побудова діаграм причинно-наслідкових зв'язків, розробка диференціальних рівнянь, кількість інцидентів:

$$\frac{dI}{dt} = -aI + bC, \tag{3.11}$$

де I – кількість інцидентів, a – коефіцієнт зниження інцидентів, b – коефіцієнт впливу витрат на зниження інцидентів, C – витрати на безпеку.

Рівень навчання персоналу визначається за формулою:

$$\frac{dL}{dt} = -cL + dT, \tag{3.12}$$

де L – рівень навчання персоналу, c – коефіцієнт зниження рівня навчання, d – коефіцієнт впливу технічного захисту на навчання, T – рівень технічного захисту.

Технічний захист визначається формулою:

$$\frac{dT}{dt} = -eT + f, \tag{3.13}$$

де T – рівень технічного захисту, e – коефіцієнт зниження технічного захисту, f– постійний рівень підвищення технічного захисту.

Витрати на безпеку обчислюється за формулою:

$$\frac{dC}{dt} = g - hC, \tag{3.14}$$

де C – витрати на безпеку, g – постійний рівень витрат на безпеку, h – коефіцієнт зниження витрат.

Ці математичні моделі забезпечують комплексний підхід до оцінки рівня інформаційної безпеки, враховуючи різні аспекти і дозволяючи приймати обґрунтовані рішення для підвищення захищеності інформаційних систем у закладах вищої освіти [53].

Для досягнення найбільш комплексної та точної оцінки рівня інформаційної безпеки закладів вищої освіти, доцільно використовувати

комбінований підхід, який об'єднує декілька математичних моделей. Запропонована комбінація включає:

Опис алгоритму

1. **Визначення критеріїв та побудова ієрархії (AHP)**
   - визначення основних критеріїв безпеки;
   - побудова ієрархії критеріїв та альтернатив;
   - визначення ваг кожного критерію за допомогою парних порівнянь.
2. **Збір даних та оцінка альтернатив (WSM, AHP)**
   - збір даних про різні альтернативи заходів безпеки;
   - оцінка альтернатив за кожним критерієм;
   - застосування методу зважених сум для обчислення інтегрального показника.
3. **Економічний аналіз (CBA)**
   - визначення витрат та вигод для кожної альтернативи;
   - обчислення чистої поточної вартості (NPV) та співвідношення вигод та витрат (BCR);
   - інтеграція результатів CBA у метод зважених сум.
4. **Аналіз ризиків**
   - оцінка ймовірності та впливу різних загроз;
   - коригування оцінок альтернатив з урахуванням результатів аналізу ризиків.
5. **Системна динаміка**
   - моделювання взаємодії компонентів системи безпеки з плином часу;
   - прогнозування довгострокових наслідків впровадження заходів безпеки.
6. **Прийняття рішення на основі об'єднаних результатів**
   - Інтеграція результатів всіх моделей;
   - прийняття рішення щодо вибору найбільш ефективних заходів інформаційної безпеки.

Комбінована методика, хоча й потребує більше ресурсів і часу, забезпечує найвищі результати за комплексністю, точністю, об'єктивністю та

гнучкістю. Це робить її найкращим вибором для закладів вищої освіти, які можуть дозволити собі її впровадження. Інші методи можуть бути використані як альтернатива у випадках обмежених ресурсів або часу.

Таблиця 3.1

Таблиця порівняння методів з числовими даними

Метрика	Метод порівняльного аналізу	Метод KPI	Метод експертних оцінок	Метод аналізу статистичних даних	Комбінована методика
Комплексність	4	5	6	5	9
Точність	±15%	±10%	±5%	±7%	±3%
Об'єктивність	70%	80%	50%	90%	95%
Гнучкість	5	6	7	5	9
Вартість	10,000 грн	50,000 грн	100,000 грн	50,000 грн	150,000 грн
Час виконання	1 місяць	3 місяці	6 місяців	6 місяців	4 місяці
Простота використання	8	7	5	6	6

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 $D=\{d_1,d_2,...,d_n\}$, де кожен елемент d_i вважається валідним, якщо виконується умова d_i є валідним $\Leftrightarrow$ (d_i

не дублікат)∧(d_i актуальний). Це забезпечує використання тільки актуальних і релевантних даних для подальшого аналізу.

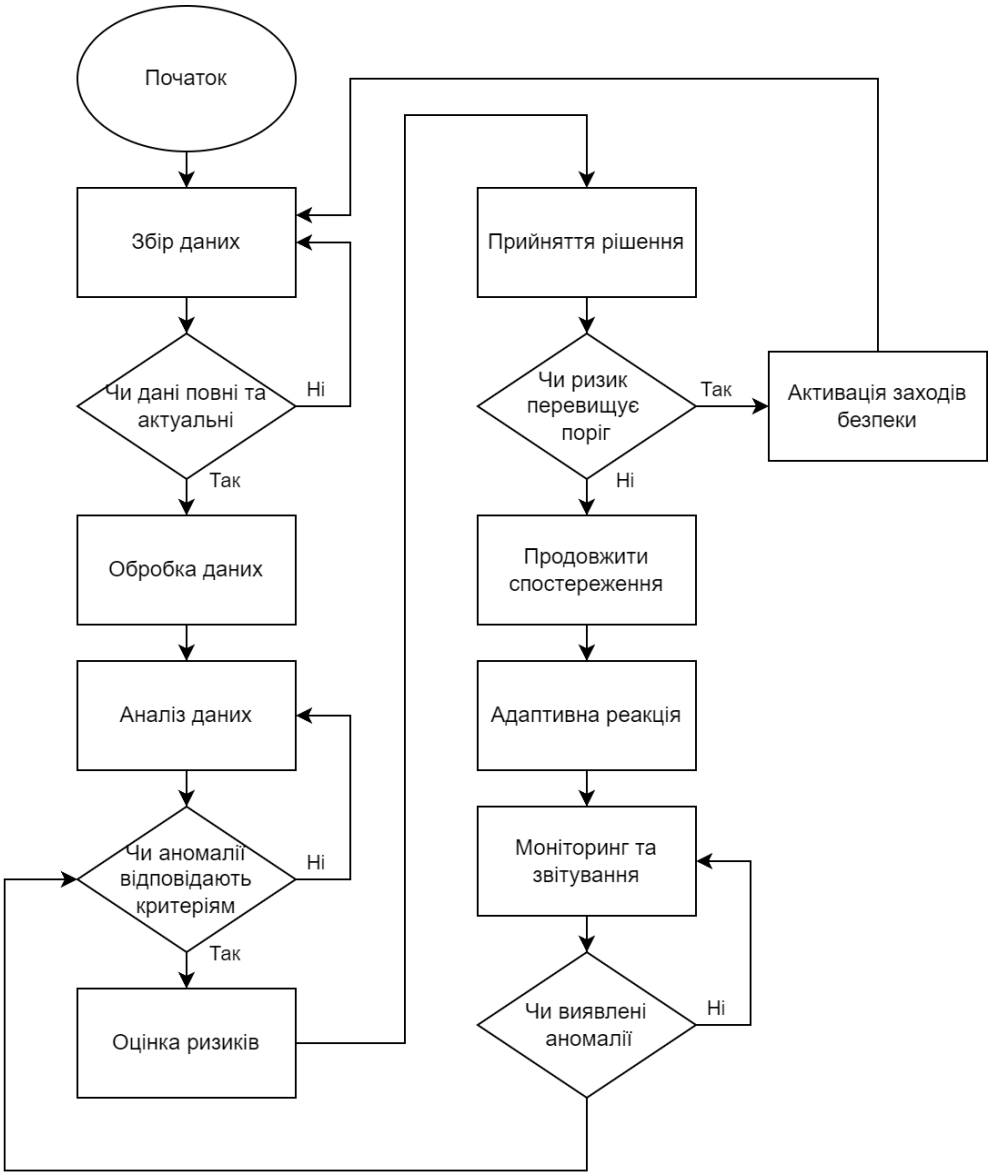

Рис. 3.3. Блок-схема алгоритму оцінки рівня інформаційної безпеки для інформаційної системи

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 є 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 $A=\{a_1,a_2,...,a_m\}$, де a_i є аномалією ⇔ (a_i перевищує поріг).

Таблиця 3.2

Методики оцінки рівня інформаційної безпеки освітньої інформаційної системи

Крок	**Що виконує**	**Умови перевірки**	**Обрахунки**	**Результат**
Вхідні дані	Збір вхідних даних: логи, дані моніторингу, внутрішні та зовнішні джерела загроз.	Всі зібрані дані мають бути доступними для обробки.	Підготовка вхідних даних для аналізу.	Вхідний набір даних Dinput
1. Збір даних	Збір даних з різних джерел (логи, системи моніторингу, джерела загроз).	Дані мають бути повними та актуальними: $d_i \neq$ дублікат$\wedge d_i$ актуальний.	Перевірка на актуальність та унікальність даних.	Набір валідних даних $D=\{d_1,d_2,...,d_n\}$
2. Попередня обробка даних	Очищення даних: видалення дублікатів та некоректних записів.	Якщо d_i є дублікатом або некоректним, він не враховується.	Фільтрація та очищення даних.	Очищені дані для подальшого аналізу D_{clean}
3. Аналіз даних	***Виявлення аномалій за допомогою машинного навчання (кластеризація, класифікація).***	***Аномалії відповідають критеріям: a_i>поріг***	***Кластеризація даних для виявлення аномалій.***	***Набір аномалій $A=\{a_1,a_2,...,a_m\}$***
4. Оцінка ризиків	***Оцінка ризиків на основі ймовірності та впливу.***	***Якщо ризик перевищує поріг: R_i>T***	***Обрахунок ризику для кожного інциденту.***	***Класифікація ризиків (низький, середній, високий).***
5. Прийняття рішень	Прийняття рішення щодо заходів безпеки.	Якщо R_i>T, активуються протоколи безпеки. Інакше: спостереження.	Визначення дій на основі оціненого ризику.	Активація протоколів безпеки або продовження моніторингу.
6. Адаптивна реакція	***Адаптація системи до нових загроз на основі нових даних.***	***Нові дані D_{new}, оновлення моделі M_{new}.***	***Оновлення моделей на основі нових даних.***	***Оновлена система, адаптована до нових загроз.***
7. Моніторинг та звітування	***Постійний моніторинг за станом інформаційної безпеки.***	***Якщо аномалії A виявлені: вжити заходів, інакше продовжити моніторинг.***	***Виявлення нових аномалій та відповідні дії.***	***Постійний контроль та оновлення заходів безпеки.***

Вихідний результат	Загальний результат після застосування всіх кроків алгоритму.	Система повністю адаптована до поточних та нових загроз.	Аналіз і адаптація системи до загроз.	Адаптивна, надійна система безпеки.

Кроки 3,4,6 та 7 методики мають нововведення, а саме:

1. В кроці 3 при аналізі даних активне використання машинного навчання для автоматичного виявлення загроз.

2. В кроці 4 при оцінці ризиків об'єднання аналізу ймовірності та впливу для точнішого визначення ризику.

3. В кроці 6 нововведенням є адаптація системи – система автоматично адаптується до нових загроз через динамічне оновлення моделі.

4. В кроці 7 вводиться постійний моніторинг з автоматичним коригуванням моделей безпеки.

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

$$R_i = P_i \cdot I_i, \tag{8}$$

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 3.3.

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.
Запропонована модель	*Адаптивна, заснована на аналізі даних та машинному навчанні.*	*Автоматизоване прийняття рішень, постійне навчання, адаптивність до нових загроз.*	*Потребує належного налаштування та наявності даних для навчання.*

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 [59].

Таблиця 3.4

Порівняльна характеристика моделей за відповідними метриками

Модель	Ефективність моделі (E)	Час реакції (TR)	Складність впровадження (CI)	Адаптивність (A)	Кількість помилкових 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

Запропонована модель	*90%*	*Швидкий*	*Низька*	*Висока*	*2%*	*Низька*

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.

3.4. Напрямки організаційно-технічного забезпечення системи управління інформаційної безпеки у вищих закладах освіти

В наш час сучасних інформаційних та телекомунікаційних технологій соціальні мережі є одним з необхідних інструментів надання оперативної інформації щодо змін в освітньому процесі, пов’язаних з реформою вищої освіти. Інформування у соціальних мережах про нові закони, рішення Уряду, накази Міносвіти та інші нормативно-правові акти у сфері вищої освіти допомагає як професорсько-викладацькому складу, так і студентам своєчасно дізнатись про усі зміни галузі та відповідно реагувати на них. Це стосується зокрема стандартів вищої освіти: 120 нових стандартів для бакалаврів, 80 – для магістрів і 50 – для докторів філософії. Затвердження стандартів є важливим кроком до виконання декількох завдань вищої освіти: наближення до європейських стандартів. Зокрема одною із цілей є реальна академічна автономія вищих учбових закладів, яка надасть їм можливість самим розробляти освітні та особливо науково-дослідні та дослідно-конструкторські програми. Адже не секрет, що в провідних країнах Європейського Союзу та США превалююча частина науково-дослідних пропозицій виконується науковим потенціалом тамтешніх університетів. Тому на мій погляд саме стандарти вищої освіти мають стати для вищих навчальних

закладів орієнтиром того, що конкретно державі, ринку та бізнесу необхідно від їх науково-дослідної діяльності. Все це підтверджує необхідність повсюдної комерціалізації наукових розробок. Нагальною проблемою у вузах стають напрацювання методичної бази в створенні та функціонуванні системи внутрішнього забезпечення якості як навчання, так і наукових розробок. В першу чергу необхідна дійова система виявлення плагіату в наукових роботах як студентів-магістрів, так і в здобувачів вчених ступенів.

В цьому напрямі велике значення має ефективне функціонування Національного репозиторію академічних текстів. На мій погляд він повинен, в першу чергу, систематизувати тексти всіх дисертацій, що були написані та захищені в Україні, Росії, Білорусі мінімум за останні п’ять десятиліть. Об’єктивно можна передбачити, що доступ до його сайтів буде мати декілька режимів. Один – це відкритий для всіх. Інший – це з певними обмеженнями для користувачів інформаційної системи. Адже саме тут накопичуються матеріали і бази даних, що мають на своїх розробках гриф «Таємно», «Для службового користування», «Для обмеженого користування», захищені авторськими правами, відомості конфіденційного характеру тощо. Зрозуміло, що і у різних вищих навчальних закладах в тій чи інший мірі ці дані присутні і стосуються певної категорії співробітників. Зважаючи на вищевикладене об’єктивно виникає необхідність визначити основні напрямки оптимізації організаційно-технічного забезпечення управління інформаційною безпекою в освітній галузі. Узагальнено управління захистом можна визначити як контроль над розподілом інформації в інформаційних системах. Це передбачає забезпечення роботи засобів і механізмів захисту, реєстрацію виконуваних функцій і стану цих механізмів, а також фіксацію подій, пов’язаних із порушеннями захисту. Звичайно не всі співробітники, а тим більше студенти можуть мати допуск до баз обмеженого користування. Проте знати про існування системи інформаційного забезпечення безпеки ІС мають знати всі.

Коли користувач працює окремо, вирішуючи лише власні завдання і обробляючи лише свої дані, можна надійно захистити інформацію за допомогою

індивідуальних засобів захисту та ізоляції. Проте на практиці така ситуація трапляється рідко: зазвичай існує потреба у спільному вирішенні завдань, обміні даними або їх колективному аналізі. Це створює інформаційні ресурси, доступні декільком користувачам, що викликає проблему довіри: якщо доступ до файлу чи набору даних мають декілька користувачів, виникає питання відповідальності у разі інциденту.

Наявність спільно використовуваних ресурсів, особливо тих, що доступні для змін, може порушувати політику безпеки. Завдання захисту, налаштування системи захисту та контролю за її функціонуванням стають частиною загальної реалізації політики інформаційної безпеки в освітній сфері. Ефективне управління захисними засобами сприяє успішному функціонуванню системи загалом. При цьому крайнощі – відсутність захисту або повний контроль – рідко призводять до оптимальної роботи.

Налаштування засобів захисту необхідне для приведення їх у відповідність до плану безпеки, з особливою увагою до їх сумісності з використовуваними програмами. Управління системою захисту включає періодичне оновлення бази даних користувачів, які мають доступ до різних об’єктів системи.

Особливу увагу при управлінні системою захисту слід звернути на:

- документування всіх змін у базі даних, бажано через систему заявок від посадових осіб, відповідальних за надання доступу до ресурсів системи;

- регулярне резервне копіювання бази даних для уникнення втрати актуальної версії в разі збою.

Контроль за функціонуванням ІС охоплює моніторинг небезпечних подій, аналіз причин їх виникнення та усунення наслідків. Управління і контроль зазвичай здійснює адміністративна група, до складу якої входять адміністратор безпеки, менеджер безпеки та оператори. Під час виконання досліджень дані в системі слід організувати так, щоб мінімізувати ризик несанкціонованого доступу. Інформацію необхідно структуровано розміщувати для зручності уповноважених користувачів та недоступності для тих, кому доступ не дозволено.

Кожен користувач повинен мати настільки мало привілеїв, наскільки це можливо без шкоди для працездатності системи. Ці принципи - ключові при визначення повноважень користувачів та організації захисту наборів даних.

Кожен повинен нести персональну відповідальність за свої дії, при цьому захист слід організувати так, щоб дії користувачів були якомога більш незалежними. У тих випадках, коли це неможливо і виникає проблема взаємної підозри, слід використовувати засоби контролю.

Щоб запобігти загрозам безпеці або усунути їх наслідки, в університетах важливо чітко розуміти всі можливі загрози інформаційних систем. Більшість таких загроз, що здатні частково або повністю порушити цілісність інформації чи працездатність системи, є актуальними не лише для навчальних закладів, а й для підприємств. До них належать: перехоплення даних із комунікаційних ліній, крадіжка паролів, спроби несанкціонованого доступу до системи, створення чи модифікація записів у базі даних захисту, незаконне отримання і використання привілеїв, доступ до обмежених даних, запуск неперевірених виконуваних файлів або командних скриптів, які можуть містити шкідливий код, а також накопичення зайвої інформації на дисках чи в оперативній пам’яті. Також існує ризик використання мережевих вузлів як точок доступу для проникнення в інші частини комп’ютерної мережі.

У кожному з цих випадків повинні вживатися негайних заходів для запобігання порушення працездатності ІС та збереження даних.

При цьому необхідно зупинитися на такому небезпечному порушенні, як несанкціонований доступ (НСД). Справа в тому, що поняття "несанкціонований" досить важко визначити.

Найчастіше під НСД розуміють проникнення користувача до інформації, яка йому не повинна бути доступна. Це можливо у двох випадках:

1. У программноаппаратних засобах підтримки політики безпеки є помилки, що призводять до можливості дій, що дозволяють їх обхід. У цьому випадку єдиний вихід - зміна засобів захисту (внести виправлення в робочому порядку зазвичай не представляється можливим).

2. Коли НСД виявився можливий в результаті некоректно сформульованої або реалізованої політики безпеки для даної конфігурації технічних і програмних засобів інформаційної системи.

Для виключення випадків НСД слід переглянути політику безпеки або способи її реалізації, перевірити повноту і однозначність сформульованих вимог. Це питання більше відноситься до проектування і реалізації засобів захисту або політики безпеки, але ніяк не до управління захистом.

Усі засоби захисту та управління мають бути об'єднані в так звану достовірну обчислювальну базу (ДОБ). ДОБ – це концептуальне поняття, що позначає повністю захищений механізм обчислювальної системи, включаючи апаратні та програмні компоненти, призначений для підтримки реалізації політики безпеки у вищих навчальних закладах [90].

У різних засобах захисту ДОБ може реалізуватися по-різному, а її здатність до безперебійної роботи залежить від її структури та належного управління. Надійність ДОБ є ключовим фактором у забезпеченні політики безпеки захищеної інформаційної системи. Таким чином, ДОБ виконує подвійну функцію — підтримує реалізацію політики безпеки та гарантує цілісність захисних механізмів, тобто самої себе. ДОБ доступна всім користувачам системи, проте її модифікація дозволена лише спеціально уповноваженим особам, таким як адміністратори системи та привілейовані співробітники закладу [63].

Процес, який виконується від імені ДОБ, вважається достовірним, оскільки система захисту повністю довіряє йому, а всі його дії відповідають політиці безпеки. Тому основним завданням захисту ДОБ є збереження її цілісності, забезпечуючи надійний захист програм та даних ДОБ від несанкціонованих змін. Щоб підтримувати політику безпеки та власний захист, ДОБ має забезпечити захист суб’єктів (процесів) та об’єктів системи як в оперативній пам’яті, так і на зовнішніх носіях [130].

Захист ДОБ зазвичай базується на концепції ієрархічної декомпозиції інформаційної системи.

Концепція ієрархічної декомпозиції передбачає, що кожен компонент виконує певну функцію, яку, за необхідності, можна розділити на підфункції, кожна з яких реалізується й захищається окремо. Цей процес може проходити в кілька етапів, де основний акцент захисту зосереджується на міжрівневому інтерфейсі, що об'єднує підфункції в єдину систему, мінімізуючи горизонтальні зв'язки. Окрім захисту самої себе, ДОБ забезпечує безпеку користувачів, у тому числі захист від дій інших користувачів. Для цього використовуються аналогічні механізми захисту, спрямовані на збереження суб’єктів та об’єктів як у пам’яті, так і на зовнішніх носіях. Доступ до інформації на зовнішніх носіях здійснюється через підсистему вводу/виводу, яка входить до нижніх і середніх рівнів ДОБ. При зверненні до файлу чи запису в першу чергу перевіряються права користувача на доступ до даних, що визначається інформацією з бази даних захисту, яка є частиною ДОБ та також підлягає контролю доступу [63].

Однією з умов ефективної роботи ДОБ є наявність багаторежимного процесора, який підтримує привілейований і звичайний режими роботи, а також має апаратну підтримку механізмів перемикання режимів і віртуальної пам’яті. ДОБ складається з низки захисних механізмів, які сприяють реалізації політики безпеки. Основним елементом ДОБ є ядро безпеки, що включає апаратні та програмні компоненти, захищені від модифікацій і перевірені на коректність. Ядро реалізує концепцію монітора посилань, що є абстрактним механізмом захисту, який контролює всі спроби доступу суб’єктів до об’єктів.

Окрім ядра безпеки, ДОБ включає механізми, що забезпечують функціонування системи, такі як планувальники процесів, диспетчери пам’яті, програми для обробки переривань, примітиви вводу/виводу, а також інші апаратні й програмні засоби та системні набори даних. Монітор посилань представляє концепцію контролю доступу, де керування здійснюється над взаємодією суб'єктів з об'єктами у віртуальному середовищі. База даних захисту містить інформацію про права доступу, основу якої складає матриця доступу (МД) або її інше подання, що забезпечує основу для виборчої політики безпеки. Операційні системи, що підтримують виборче керування доступом,

використовують МД для полегшення контролю за використанням і передачею привілеїв [124].

Монітор посилань виконує перевірку прав доступу кожного суб’єкта до об’єктів на основі даних із бази захисту й політики безпеки (виборчої чи повноважної) та може реєструвати факти доступу у системному журналі. Реалізація моніторингу посилань покладена на ядро безпеки, яке повинне відповідати низці вимог, а саме: контролювати всі спроби доступу суб’єктів, бути захищеним від модифікацій та підробок, проходити тестування для забезпечення надійності й мати компактну структуру [90].

Для забезпечення автентичності суб’єкта та підтвердження його прав необхідні процеси ідентифікації, аутентифікації та авторизації. Ідентифікація визначає елемент системи за допомогою унікального ідентифікатора або іншої заздалегідь відомої інформації, забезпечуючи однозначне розпізнавання суб'єктів і об’єктів. Аутентифікація підтверджує ідентифікацію користувача, процесу або іншого компонента системи та перевіряє цілісність даних, щоб запобігти несанкціонованим змінам. Авторизація надає суб'єкту відповідні права для доступу до певного об'єкта.

При вході в систему і введенні імені користувача здійснюється ідентифікація, при введенні пароля – аутентифікація, і якщо користувач з даними ім'ям і паролем за реєстрований в інформаційній системі вузу, йому дозволяється доступ до певних об'єктів і ресурсів (авторизація) [134].

Як показує практика, вхід користувача в систему - одне з найбільш вразливих місць захисту; відомо безліч випадків злому пароля, входу без пароля, його перехвату і т.д. Тому при виконанні входу і користувач, і система повинна бути впевнена, що вони працюють безпосередньо один з одним, між ними немає інших програм і вводиться істинна [56].

Достовірний маршрут реалізується привілейованими процедурами ядра безпеки, робота якого забезпечується механізмами ДОБ, а також деякими іншими механізмами, які виконують допоміжні функції.

Реєстрація та протоколювання забезпечують отримання і аналіз інформації про стан ресурсів системи за допомогою спеціальних засобів контролю, а також реєстрацію дій, визнаних потенційно небезпечними для інформаційної системи.

Такими засобами можуть бути різні системні утиліти або прикладні програми, що виводять інформацію безпосередньо на системну консоль або інший, визначений для цієї мети пристрій, а також системний журнал. Крім того, майже всі ці засоби контролю можуть не тільки виявити будь-яку подію, але й фіксувати його.

Більшість систем містять інструменти для ведення обліку сеансів роботи окремих користувачів, охоплюючи як повні сеанси, так і окремі параметри. Системи безпеки зазвичай мають засоби управління системним журналом (audit trail), які є важливими для контролю та допомагають адміністраторам запобігати правопорушенням завдяки можливості швидко фіксувати події, що відбуваються в системі, виявляти методи та заздалегідь відому інформацію, які можуть використовувати зловмисники, а також оцінювати ступінь порушення і надавати рекомендації щодо їх розслідування та виправлення ситуації. Зміст системного журналу та інших наборів даних, які зберігають інформацію про результати контролю, повинен періодично перевірятися і аналізуватися для підтвердження дотримання політики безпеки. Після завершення роботи програми оброблювана інформація не завжди повністю видаляється з пам'яті: частини даних можуть залишатися в оперативній пам'яті, на дисках, стрічках та інших носіях, зберігаючись до перезапису або знищення. Внаслідок цього на звільненому просторі диска можуть залишатися їхні фрагменти. Хоча зміна заголовка файлу ускладнює доступ до цих залишків, використання спеціалізованих програм та обладнання може зробити це можливим. Цей процес відомий як "збірка сміття" (disk scavenging) і може призвести до витоку конфіденційної інформації, тому для його запобігання використовуються спеціальні інструменти, які можуть бути інтегровані в ядро безпеки операційної системи або встановлюватися додатково [130].

Контроль цілісності забезпечується процедурами ядра безпеки, контролюючими механізмами підтримки ДОБ. Основну роль відіграють такі механізми, як підтримка віртуальної пам'яті (для створення області даного процесу) і режим виконання процесу (визначає його можливості в рамках даної галузі і поза нею).

Область виконання процесу може містити або вкладатися в інші підобласті, які становлять єдину ієрархічну структуру інформаційної системи. Процес може змінювати області, що називається перемиканням області процесу (process switching). Воно завжди пов'язане з переходом центрального процесора в привілейований режим роботи.

Під контролем доступу розуміється обмеження можливостей використання ресурсів інформаційної системи програмами, процесами або іншими системами (для мережі) у відповідності з політикою безпеки [56]. Під доступом розуміється виконання деякої операції над об'єктом з безлічі дозволених для даного типу. Приклади таких операцій - читання, відкриття, запис набору даних, звернення до пристрою і т.д.

Контроль повинен здійснюватися при доступі до:

- оперативної пам'яті;
- пристроям прямого доступу;
- пристроям послідовного доступу;
- програм і підпрограм;
- наборам даних.

Основним фокусом засобів контролю доступу є спільно використовувані набори даних та ресурси інформаційної системи. Спільне використання об'єктів викликає ситуацію "взаємної недовіри", де різні користувачі одного й того ж об'єкта не можуть повністю довіряти одне одному. У випадку, якщо з цим об'єктом відбудеться якась непередбачена ситуація, всі учасники стають підозрюваними. Існує чотири основні способи організації доступу до спільно використовуваних об'єктів [87]. Перший – фізичний, коли суб'єкти звертаються до різних фізичних об'єктів, таких як однотипні пристрої чи набори даних на

різних носіях. Другий — тимчасовий, при якому суб'єкти з різними правами доступу до одного й того ж об'єкта отримують до нього доступ у різний час. Третій спосіб – логічний, коли суб'єкти мають доступ до спільно використовуваного об'єкта в межах одного операційного середовища, проте цей доступ контролюється засобами розмежування, що моделюють віртуальне середовище, де один суб'єкт має доступ до всіх об'єктів. Четвертий спосіб — криптографічний, що передбачає зберігання всіх об'єктів у зашифрованому вигляді, а права доступу визначаються на основі наявності ключа для розшифрування об'єкта.

3.5. Розробка концепції центру управління інформаційною безпекою у вищому навчальному закладі.

Швидкий розвиток інформаційних технологій підвищує актуальність створення надійної багатофункціональної системи захисту, яка забезпечить високий рівень безпеки освітніх установ від внутрішніх і зовнішніх загроз. Великі університети мають численний професорсько-викладацький склад, аспірантів і студентів, які в тій чи іншій мірі користуються інформаційно-телекомунікаційними мережами. З точки зору інформаційної безпеки, інсайдером є співробітник закладу, який має доступ до конфіденційних даних в комп'ютерній мережі університету. Інсайдерська атака може проявлятися у вигляді шахрайства, саботажу або крадіжки інтелектуальної власності. Канали витоку інформації можуть бути зовнішніми, такими як CD, DVD і флеш-накопичувачі, а також внутрішніми, наприклад, електронна пошта, блоги або соціальні мережі. Внутрішні порушники діляться на кілька категорій, зокрема лояльних інсайдерів (недбалі та маніпульовані), скривджених, нелояльних інсайдерів, які мотивовані зовнішніми факторами (фінансові мотиви, впровадження) та інших порушників, захист від яких неможливо забезпечити технічними засобами. Протидія інсайдерським загрозам здійснюється на трьох рівнях: на етапі прийому на роботу проводиться комплексна перевірка

працівника, включаючи психологічні тести та інформацію з баз даних попереднього місця роботи; в процесі роботи використовуються організаційно-технічні засоби, системи фізичного та інформаційного захисту, психологічна, юридична та технологічна протидія, а також моніторинг дій користувачів і аудит вразливих місць організації; при звільненні проводиться комплексний аналіз доступної інформації і перерозподіл прав доступу. Основні напрямки захисту від інсайдерів охоплюють захист документів, контроль каналів витоку інформації та моніторинг дій користувачів. Основний принцип системи захищеного документообігу полягає в тому, щоб забезпечити захист документа з моменту його створення до моменту знищення [53].

Університети, що проводять значні обсяги наукових досліджень та дослідно-конструкторських робіт, а також мають або можуть мати бази даних з обмеженим або таємним характером, повинні розглянути можливість створення центру управління інформаційною безпекою. Security Operation Center (SOC) – це методологія, яка формує загальний підхід до консолідації та централізації функцій управління всім комплексом гетерогенних систем інформаційної безпеки, спрямована на підвищення ефективності системи менеджменту інформаційної безпеки. Зазвичай вона включає такі складові, як система управління інформаційною безпекою та подіями (SIEM), система управління безпекою та вразливостями, а також система управління відповідністю. SIEM є засобом автоматизації, що дозволяє збирати, агрегувати та корелювати велику кількість подій безпеки з різних джерел, таких як операційні системи, системи управління базами даних, мережеві елементи, системи виявлення та запобігання вторгненням (IDS/IPS) та мережеве обладнання [54]. Система управління безпекою та вразливостями забезпечує виявлення та ідентифікацію вразливостей в операційних системах, системах управління базами даних, мережевих службах, протоколах та програмах, а також надає механізми для управління життєвим циклом виявлених вразливостей в інформаційній мережі університету. Система управління відповідністю автоматизує процеси оцінки відповідності IT-інфраструктури вимогам корпоративних політик інформаційної безпеки та

міжнародних стандартів. Центр оперативного управління інформаційною безпекою (ЦОУІБ) – це централізований підрозділ університету, який займається питаннями безпеки на організаційному та технічному рівнях, його мета полягає у виявленні інцидентів та мінімізації втрат від них під час виконання науково-дослідних і дослідно-конструкторських робіт [51].

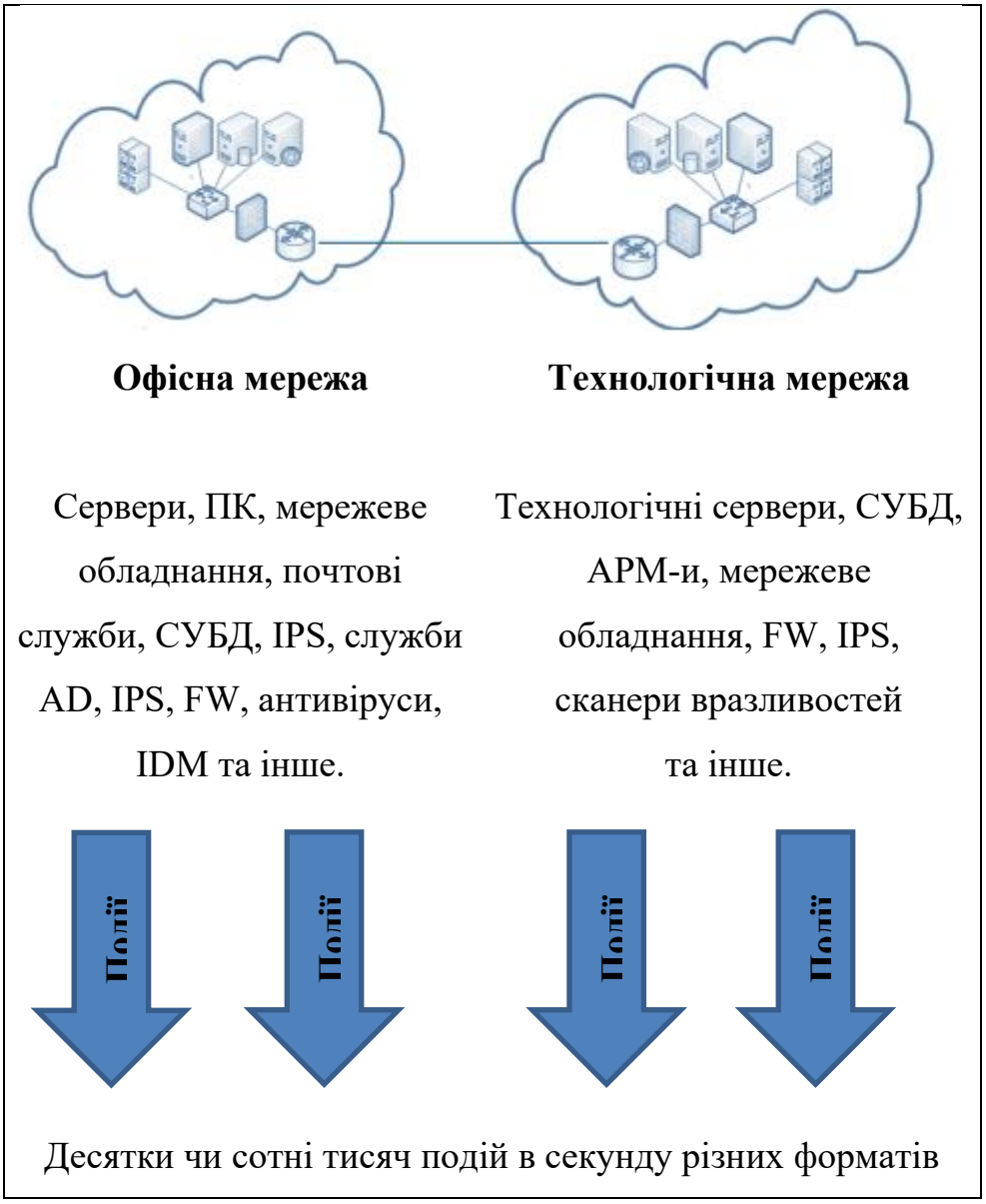

Рис. 3.4.Проблемні аспекти мережі в університетах

Інцидентом є подія або потенційна можливість її виникнення, яка може призвести до порушення вимог інформаційної безпеки, конфіденційності,

цілісності або доступності інформаційних ресурсів. Це також може бути будь-яка нестандартна ситуація, що веде до зниження якості науково-дослідної роботи або переривання доступу до інформаційної системи для користувачів. Управління інцидентами охоплює дії, спрямовані на відновлення нормального функціонування з мінімальними затримками та впливом на бізнес-операції, зосереджуючи увагу на короткостроковому відновленні сервісу. Це передбачає виявлення та реєстрацію інцидентів, їх класифікацію та первинну підтримку, дослідження і діагностику, вирішення проблем та відновлення, а також закриття інцидентів. Додатково передбачено володіння ситуацією, моніторинг, відстеження та забезпечення зв'язку в процесі управління інцидентами [58].

Інциденти можуть призвести до ряду негативних наслідків, зокрема до шкоди іміджу та репутації університету, втрати ключових клієнтів, які замовляють науково-дослідні та дослідно-конструкторські роботи, дезорганізації науково-дослідної діяльності та зниження рейтингу наукового персоналу. Серед актуальних проблем у сфері інформаційної безпеки для більшості університетів є запізніле виявлення інцидентів та відсутність актуальної інформації про стан інформаційної безпеки. В університетах, як правило, відсутні можливості для своєчасного виявлення інцидентів, і ще важче виявляти проблеми до того, як вони призведуть до інциденту. У освітньому секторі спостерігається значний витратний процес виявлення, обробки та розслідування інцидентів, особливо в умовах нестачі кадрів [60]. Процеси реагування на інциденти інформаційної безпеки не мають чітких регламентів, а фахівці не отримали належного навчання і не мають ефективних інструментів для їх вирішення. Для оцінки рівня зрілості Центрів управління інформаційною безпекою (SOC) в університетах використовують чотири напрямки, детально наведені в таблиці 3.4.

Процесний підхід – це підхід до організації та аналізу ВНЗ, заснований на виділенні і розгляді її наукових-процесів, кожен з яких протікає у взаємозв'язку з іншими процесами університету або зовнішнім середовищем. Важливе значення має захист персональних даних провідних науковців [53].

Таблиця 3.4

Напрями оцінки зрілості SOC

ВНЗ	Науковий потенціал	Процеси	Технології
Місія ЦОУІБ	Базові метрики	Базові метрики	Архітектура
Прозорість і вимірність	Навчання	Експлуатація ЦОУІБ	Збір даних
Фінансування	Сертифікація	Аналітика і розслідування загроз	Моніторинг і аналіз
Звітність	Досвід	ІТ-процеси ЦОУІБ	Кореляція подій
Взаємозв’язок з замовником НДДКР	Атестація	Взаємодія з замовниками НДДКР	Обслуговування системи

Інженери інформаційної сфери або іншої сфери, які є співробітниками університету, що надає послуги замовнику, змінюються, що призводить до відсутності повної картини стану інфраструктури клієнта. Це може серйозно впливати на рівень інформаційної безпеки, ефективності життєдіяльності наукового колективу. Відсутність, як правило, в компанії-замовника директора з інформаційних технологій та політик існування інфраструктури, її планування, планування бюджету може мати не дуже гарні наслідки. В окремих випадках спостерігається психологічний вплив на науковців, що обслуговують НДДКР — із остраху втратити замовника, виконуються «забаганки», які негативно впливають на стан ІБ системи, що, як правило, пов'язане з недоліками в інформаційній освіті замовника та небажанням витрачати потрібні кошти на підтримку інформаційної інфраструктури, інші чинники [53].

Виходячи з реалій сьогодення та об’єктивно оцінюючи обсяги наукових розробок в університетах в ЦОУІБ головними мають стати IDS / IPS - Системи виявлення й запобігання вторгнень. В загальному вигляді система виявлення вторгнень (IDS) - програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп'ютерну систему або мережу в освітній галузі.

IDS все частіше стають необхідним доповненням інфраструктури мережевої безпеки. В доповнення до міжмережевих екранів (firewall), робота яких відбувається на основі політики безпеки, IDS служать механізмами моніторингу та спостереження підозрілої активності. Вони можуть виявити атакуючих, які обійшли Firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить подальші кроки щодо запобігання атаки. Технології виявлення проникнень не роблять систему абсолютно безпечною. Проте практична користь від IDS існує [53].

Використання систем виявлення вторгнень (IDS) сприяє досягненню кількох важливих цілей. По-перше, вони дозволяють виявити вторгнення або мережеві атаки. По-друге, IDS можуть прогнозувати потенційні майбутні атаки і виявляти вразливості, що допомагає запобігти їх подальшому розвитку, оскільки зловмисник зазвичай виконує низку попередніх дій, таких як мережеве зондування чи тестування для виявлення слабких місць цільової системи. Крім того, системи IDS документують існуючі загрози, забезпечують контроль якості адміністрування з точки зору безпеки, що особливо важливо в великих і складних мережах вищих навчальних закладів. IDS також надають корисну інформацію про вже відбулися вторгнення, що дозволяє відновити і скоригувати фактори, які призвели до цих подій, а також визначити місце походження атаки щодо локальної мережі, що має значення для прийняття рішень щодо розміщення ресурсів.

Система IDS складається з кількох елементів: сенсорної підсистеми, яка відповідає за збір подій, пов'язаних із безпекою захищеної мережі або системи; підсистеми аналізу, призначеної для виявлення мережевих атак і підозрілих дій;

сховища, де накопичуються первинні події та результати аналізу; а також консолі управління, яка дозволяє налаштовувати IDS, спостерігати за станом захищеної системи і самої IDS, а також переглядати виявлені інциденти. Далі на рисунку 4.2 представлена структура університетських систем запобігання вторгненням під час проведення науково-дослідних і дослідно-конструкторських робіт [54].

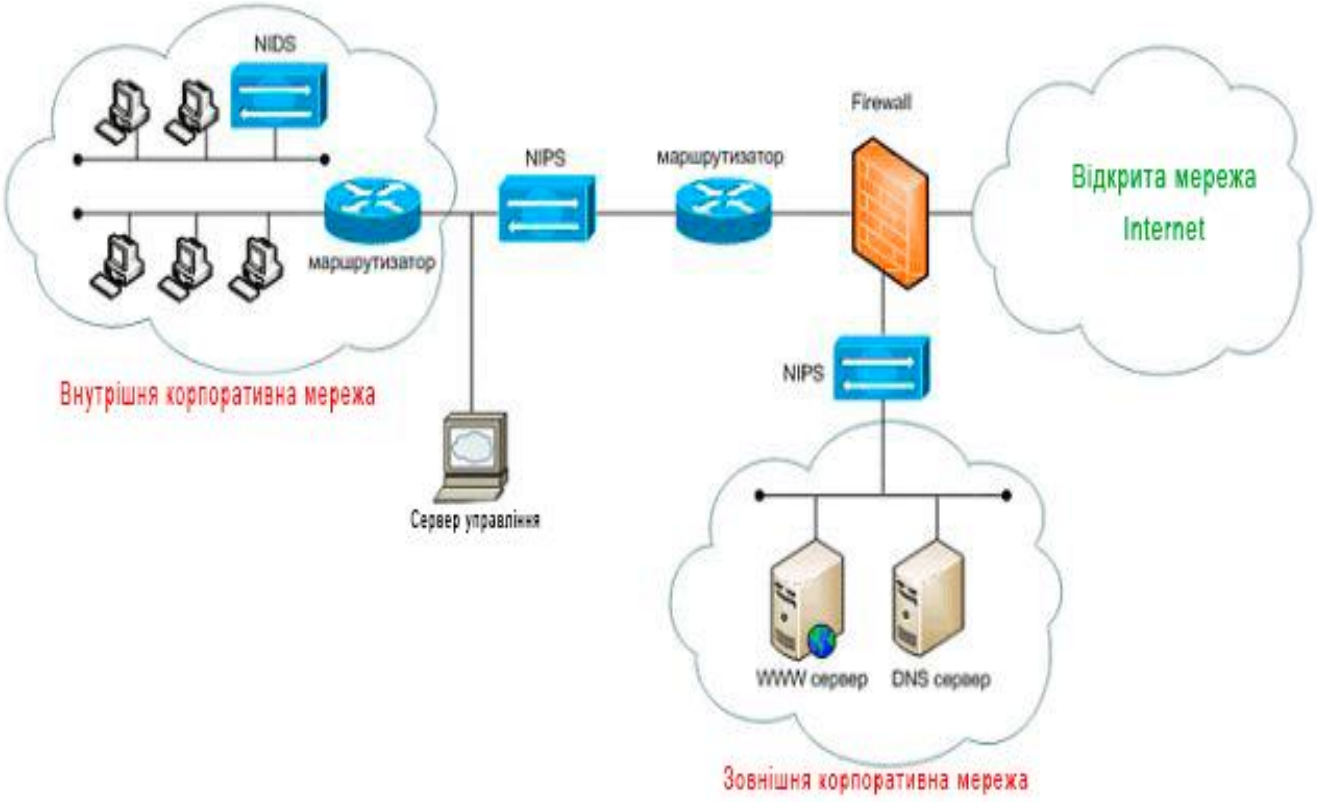

Рис. 3.5. Система запобігання вторгнення (IPS)

Система запобігання вторгненням (IPS) — це програмний або апаратний засіб, який проводить моніторинг мережі або комп'ютерної системи в реальному часі з метою виявлення, запобігання або блокування шкідливої активності. Загалом IPS має подібності з IDS у класифікації та функціях, але головна відмінність полягає в її здатності діяти в реальному часі та автоматично блокувати мережеві атаки. Кожна IPS містить модуль IDS.

РОЗДІЛ 4

РОЗРОБКА АДАПТИВНОЇ КОРПОРАТИВНОЇ ОСВІТНЬОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

4.1. Математична модель забезпечення функціональної стійкості адаптивної корпоративної освітньої системи

Математична модель забезпечення функціональної стійкості адаптивної корпоративної освітньої системи 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.

$$Maximize\ F(T,S,R,A) = \alpha_1 T + \alpha_2 S - \alpha_3 R + \alpha_4 A \tag{4.1}$$

$$T_i = f(X_1, X_2, \ldots, X_n) \tag{4.2}$$

$$R = \sum_{i=1}^{m} P_i \cdot I_i \le R_{\max} \tag{4.3}$$

$$S = A \cdot (q - R) \ge S_{\min} \tag{4.4}$$

$$A \ge A_{min} \tag{4.5}$$

$$C_T + C_S + C_R \le C_{total} \tag{4.6}$$

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.

Формула (4.2) визначає, що функціональність системи T залежить від здатності підлаштовуватись під індивідуальні показники студента та пропонувати оптимальні навчальні траєкторії.

Формула (4.3) визначає сукупний рівень ризику, що є зваженою сумою ймовірностей та впливів усіх можливих загроз. Загальний ризик не повинен перевищувати встановлену верхню межу R_{max}, щоб підтримувати безпеку системи на прийнятному рівні.

Формула (4.4) вимагає, щоб рівень безпеки системи S був не меншим за встановлене мінімальне значення S_{min}. Безпека системи знижується зі збільшенням ризику, тому R має підтримуватися на достатньо низькому рівні.

Формула (4.5) гарантує, що система має достатній рівень адаптивності для підлаштування освітніх траєкторій та безпекових механізмів під мінливі умови та потреби користувачів.

Формула (4.6) гарантує, що сумарні витрати на підтримку функціональності, безпеки та мінімізацію ризиків не перевищуватимуть доступний бюджет.

Тобто цільова функція $F(T,S,R,A)$ максимізує функціональну стійкість системи, одночасно забезпечуючи ефективну навчальну траєкторію, необхідний рівень безпеки та адаптивність. Обмеження встановлюють допустимі межі для ризику, безпеки, адаптивності та витрат, що дозволяє системі функціонувати стійко та з максимальною продуктивністю.

Розроблена модель відноситься до класу задач нелінійного програмування. Розв’язати таку систему можна за допомогою методів метод Ньютона, градієнтних методів, а також з використанням методу Лагранжа. Проте слід наголосити, що в більшості випадків використовують спеціалізовані пакети (як-

от MATLAB або програмні засоби на основі Python), які мають вбудовані алгоритми для нелінійного програмування.

Таблиця 4.1

Опис змінних математичної моделі функціонально стійкої системи

Змінна	Опис	Одиниці виміру	Коефіцієнт/Параметр
T	Функціональність системи	Кількість сервісів	α_1 – вага функціональності
S	Рівень безпеки	Відсотки (%) або бали	α_2 – вага безпеки
R	Рівень ризику	Очікувані збитки (гроші)	α_3 – вага ризику
A	Адаптивність системи	Кількість адаптацій/оновлень	α_4 – вага адаптивності
P_i	Ймовірність ризику	Ймовірність (0 до 1)	Параметр
I_i	Ступінь впливу ризику	Відсотки або гроші	Параметр
C_T	Витрати на функціональність	Гроші	Параметр
C_S	Витрати на безпеку	Гроші	Параметр
C_R	Витрати на управління ризиками	Гроші	Параметр
C_{total}	Загальні допустимі витрати	Гроші	Параметр
T_{total}	Загальний допустимий ресурс	Час або кількість операцій	Параметр
S_{min}	Мінімальний рівень безпеки	Відсотки (%) або бали	Параметр

Запропонована математична модель відображає забезпечення функціональної стійкості адаптивної корпоративної освітньої системи та є основою для побудови інформаційної технології.

4.2. Розробка інформаційної технології забезпечення функціональної стійкості

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 [61].

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.

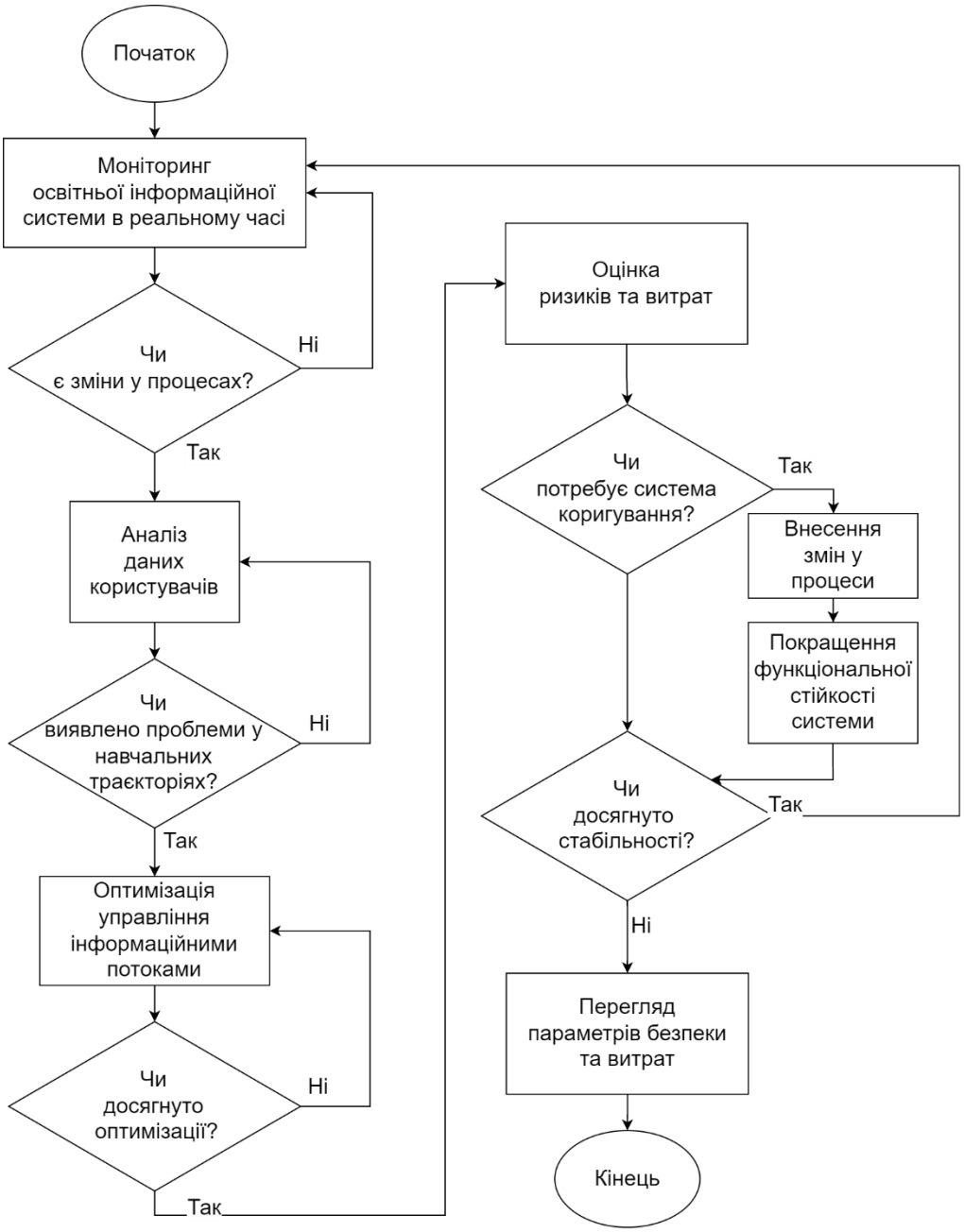

Рис. 4.1. Блок-схема інформаційної технології забезпечення функціональної стійкості освітньої інформаційної системи

Кожен блок алгоритму має свій математичний апарат, який використовується для проведення обрахунків. Для моніторингу змін у реальному часі використовуються статистичні метрики, такі як середнє значення та стандартне відхилення для набору даних X_t у часі t:

$$\mu_t = \frac{1}{n}\sum_{i=1}^{n} X_{i,t}\,, \tag{4.7}$$

$$\sigma_t = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(X_{i,t} - \mu_t)^2}\,, \tag{4.8}$$

де μ_t — середнє значення, а σ_t — стандартне відхилення. Якщо поточне значення виходить за межі $\mu_t \pm 3\sigma_t$, це може вважатися аномалією.

Крім того на даному кроці працює методика оцінки рівня інформаційної безпеки освітньої інформаційної системи, запропонована в розділі 3, яка дозволяє визначити ризики, атаки та забезпечує безпеку розробленої системи.

Для виявлення значущих змін у процесах використовуємо дисперсійний аналіз:

$$F = \frac{MSB}{MSW} = \frac{\frac{1}{k-1}\sum_{i=1}^{k} n_i(\overline{X}_i - \overline{X})^2}{\frac{1}{N-k}\sum_{i=1}^{k}\sum_{j=1}^{n_i}(X_{ij} - \overline{X}_i)^2}\,, \tag{4.9}$$

де MSB – міжгрупова дисперсія, MSW – внутрішньогрупова дисперсія, n_i – кількість спостережень в групі, $\overline{X}i$— середнє значення в групі, $\overline{X}$ – загальне середнє.

Лінійна регресія використовується для прогнозування поведінки користувачів:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_n X_n + e\,, \tag{4.10}$$

де Y – прогнозований результат (наприклад, ефективність навчання), $X_1, X_2, \ldots, X_n$ – вхідні фактори (дані користувачів), $\beta_0, \beta_1, \ldots, \beta_n$ – коефіцієнти моделі, e – випадкова похибка.

Для побудови та коригування освітніх траєкторій використовується метод метричного проксимального градієнта з діагональним кроком на основі моделі попарно-експоненціального марківського випадкового поля, описаний в розділі 2.

При коригуванні освітніх траєкторій моделі для визначення ваг критеріїв використовується матриця парних порівнянь A:

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} \\ \frac{1}{a_{12}} & 1 & a_{23} \\ \frac{1}{a_{13}} & \frac{1}{a_{23}} & 1 \end{pmatrix}, \tag{4.11}$$

Для кожного критерію необхідно обчислити власні числа матриці та нормалізувати їх, щоб визначити ваги. Оптимізація з використанням методу зважених сум (WSM) відбувається за формулою:

$$Z = \sum_{i=1}^{n} \omega_i X_i , \tag{4.12}$$

де w_i – ваги критеріїв, а X_i – значення показників.

Модель лінійного програмування для мінімізації витрат або часу при оптимізації інформаційного потоку має вигляд

$$\min Z = c_1 x_1 + c_2 x_2 + \ldots + c_n x_n , \tag{4.13}$$

$$a_{11} x_1 + a_{12} x_2 + \ldots + a_{1n} x_n \le b_1 , \tag{4.14}$$

де c_i – витрати на одиницю потоку, x_i – обсяг ресурсу.

Для визначення максимального потоку в мережі використовується теорія графів (алгоритм Форда-Фалкерсона):

$$f_{\max} = \max \sum_{u \in V} f(u, \upsilon) , \tag{4.15}$$

де *f(u,v)* – потік з вузла *u* до вузла *v*.

При оцінці ризиків та витрат використовується формула аналізу витрат та вигод:

$$NPV = \sum_{t=0}^{t} \frac{B_t - C_t}{(1+r)^t}, \quad (4.16)$$

де B_t – вигоди у періоді t, C_t – витрати у періоді t, r – ставка дисконту, T — період аналізу.

При цьому ризик визначається за формулою

$$R = PL, \quad (4.17)$$

де R – ризик, P – ймовірність події, L – збитки від події.

Для визначення функціональної стійкості застосовується модель системної динаміки для оцінки стійкості системи в часі, а також модель стійкості системи до впливів:

$$\frac{dX(t)}{dt} = f(X(t), t), \quad (4.18)$$

$$S = \frac{R_{до}}{R_{після}} \cdot 100\%, \quad (4.19)$$

де $X(t)$ – змінні системи, а $f(X(t),t)$ – функція залежності змінних від часу, $R_{до}$ – рівень стійкості до впровадження змін, а $R_{після}$ – після впровадження.

Ці всі кроки інформаційної технології дозволяють забезпечити функціональну стійкість освітньої інформаційної системи.

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.

4.3. Розробка адаптивної корпоративної освітньої інформаційної системи

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.

Інформаційна система буде включати в себе декілька сервісів різного рівня захисту. Також система має включати в себе і сторону студента та інтеграцію з іншими системами управління (бухгалтерські або дистанційного навчання)

Рівень перший

“Авторизація” – відсутня.

“Користувачу доступні”: розклад, електронний журнал відвідуваності, робочі плани, блок де можуть бути розміщені корисні посилання та інструкції для абітурієнтів.

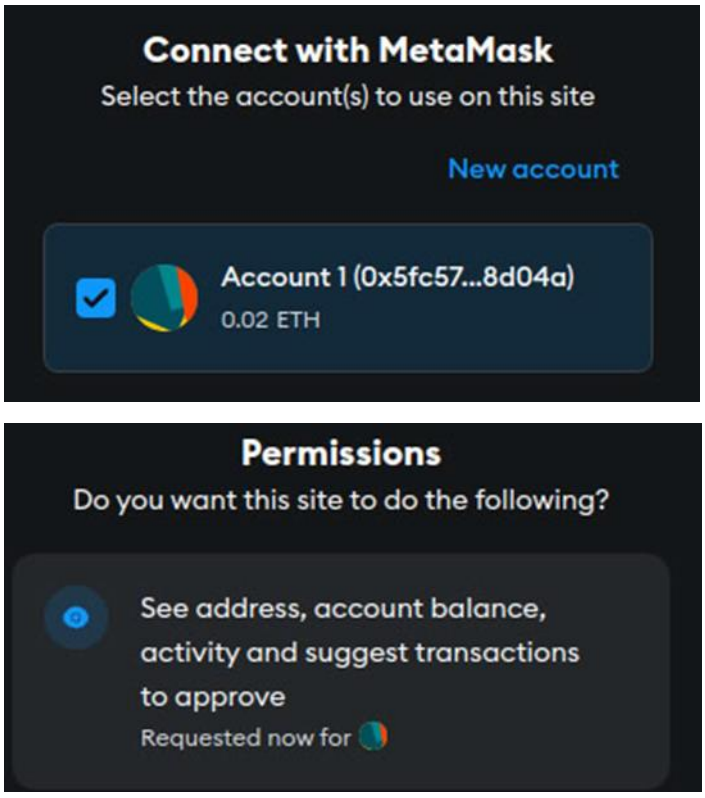

Рис. 4.2. Авторизація в інформаційній систему

Рівень другий

“Авторизація” – криптогаманець викладача.

“Користувачу доступні”: редагування електронного журналу відвідування та оцінок, бронювання вільних аудиторій, запит на зміну розкладу, система управління задачами (як в Jira або Trello), опитування, а також попередні розділи.

Рис. 4.3. Авторизація в корпоративній освітньо інформаційній системі

Рівень третій

“Авторизація” – криптогаманець викладача, а також окреме введення гугл аутентифікатора.

“Користувачу доступні”: документообіг, категорії з НДР, бухгалтерські дані, особистий кабінет викладача, а також попередні розділи.

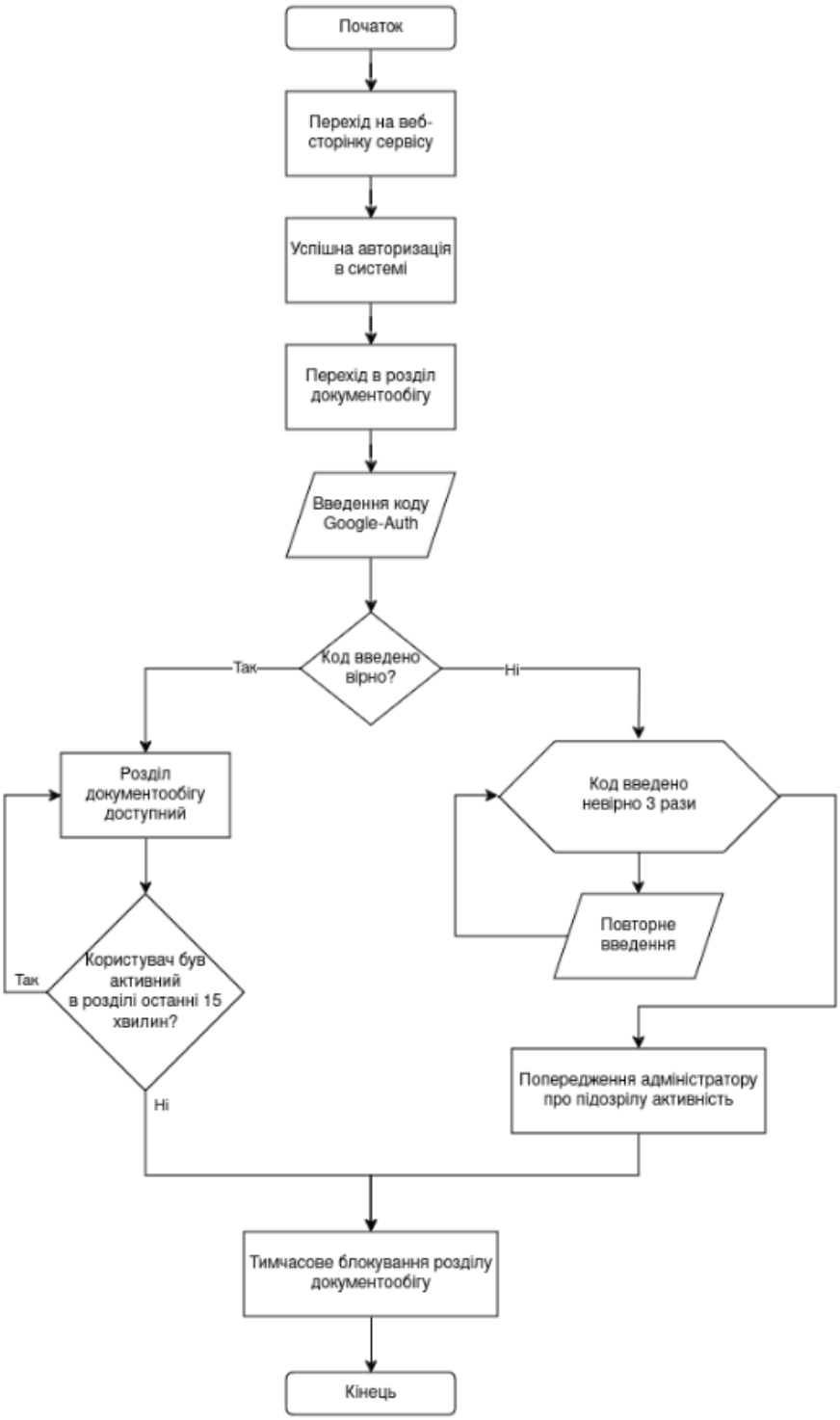

Рис. 4.4. Авторизація в підрозділі НДР

Рівень АДМІНІСТРАТОР

“Авторизація” – криптогаманець викладача, а також окреме введення гугл аутентифікатора. (доступна лише з локальної мережі або через VPN).

“Користувачу доступні”: робота з системою доступу викладачів, логування, моніторинг підозрілих подій, а також попередні розділи.

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 (AI)

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

Технічна частина

Розміщення серверів

Для системи потрібно два серверних масива.

Перший (основний) буде розміщено на території університету в захищеному приміщенні з обмеженим доступом. Він буде виконувати всі обчислювальні процеси і зберігати дані.

Другий (бекапний або запасний) буде зберігати копії бази даних, буде виконувати задачі моніторингу системи, а також слугувати запасним майданчиком для розгортання у випадку необхідності. (так досягається значна економія ресурсів у порівнянні з тим, щоб тримати одразу два увімкнених сервери)

Система

Має бути побудована на ізольованих контейнерах Docker. Це додасть ще один рівень безпеки, а також дозволить швидко перенести сервіс у хмару. Мати систему зовнішнього моніторингу, яка буде перевіряти доступність всіх сервісів

системи за різними метриками (ping, link downs, CPU/Memory utilization). Роутери, які мають вихід в інтернет повинні мати посилений Firewall.

Моніторинг підозрілих подій

Буде використовувати заздалегідь визначені правила та сигнатури для виявлення відомих атак і загроз (SQL- ін'єкції, атак типу DDoS та інші). Завдяки машинному навчанню, система буде вчитися на звичайних поведінкових паттернах користувачів і систем, створюючи модель нормальної поведінки. Після виявлення підозрілої події система може автоматично реагувати на загрозу і приймати рішення відповідно до правил безпеки. На основі даних логування подій може буде проводити детальний аналіз з використанням методів машинного навчання, щоб виявити причини виникнення і допоможе адміністратору обрати запобіжні заходи на майбутнє.

Інтелектуальний наставник студента

Задача даного елемента системи полягає в зборі та аналізі всіх даних, які пов’язані зі студентом. На основі зібраних даних AI буде генерувати рекомендації для студента щодо того, на яких аспектах навчання варто зосередитися. Це можуть бути додаткові матеріали для вивчення, поради щодо розподілу часу або рекомендації щодо відвідування додаткових занять. Система буде взаємодіяти зі студентом через інтерфейс, пропонуючи йому регулярно надавати зворотний зв'язок про навчання і потім на основі цих даних втручатися та коригувати освітню траєкторію для досягнення кращих результатів.

Відмовостійкість

Фізичний сервер має бути забезпечений безперебійним живленням та окремим генератором для постійного електроживлення.

Сервер повинен мати доступ в інтернет через різних провайдерів. Важливо, щоб проміжні вузли між всесвітньою мережею і сервером мали різні шляхи для кожного провайдера. Також варто додати, що провайдери мають послугу з

виділення декількох айпі адрес. Бажано придбати декілька IP адрес, для можливості перемикання між ними у разі довгострокових кібератак.

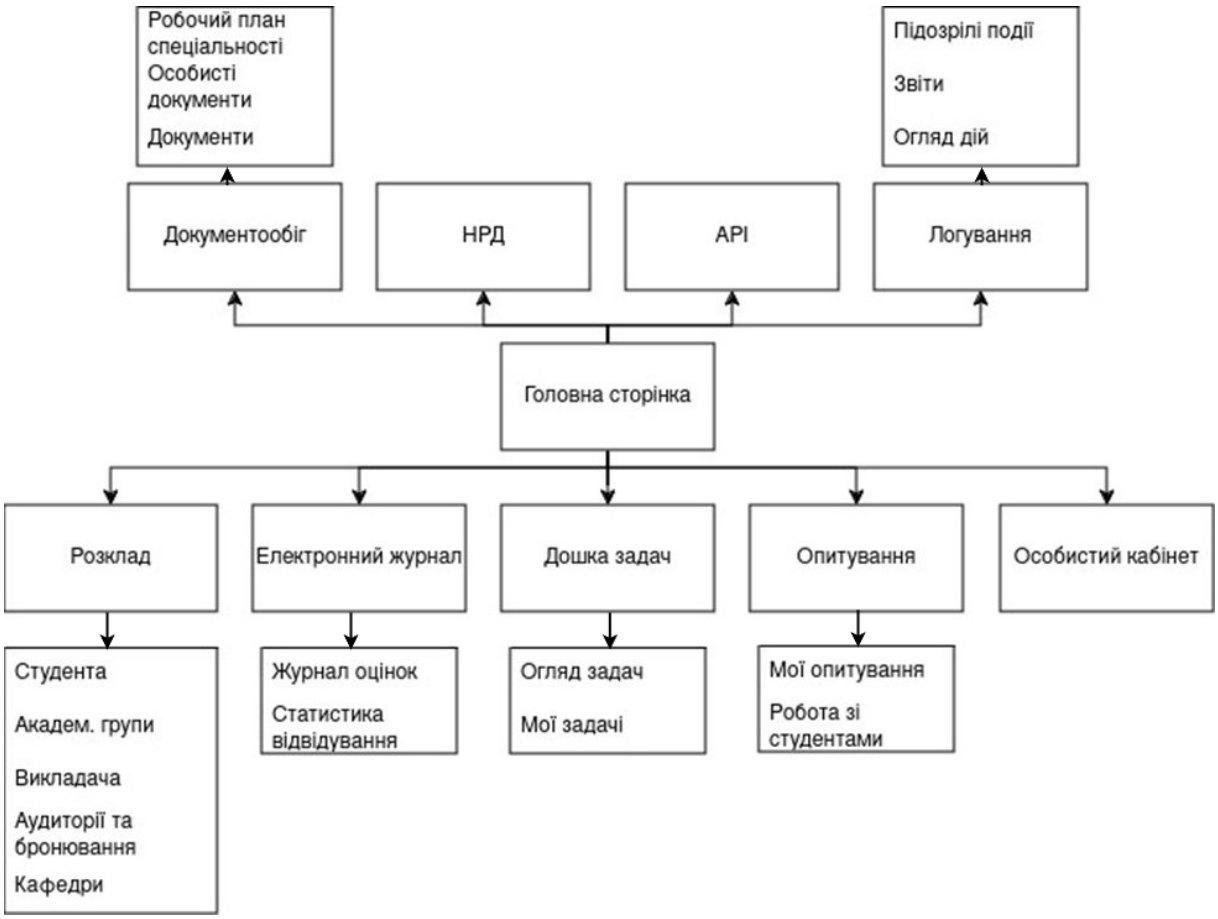

Рис. 4.5. Функціонал інформаційної системи

Таким чином, в дисертаційній роботі реалізовано третій науковий результат, який полягає в розроблені корпоративної освітньої інформаційної системи з використанням запропонованих методик, наукова новизна якої полягає у забезпечені стійкості адаптивних корпоративних освітніх інформаційних систем закладів вищої освіти. Використання запропонованої методики дозволить оптимізувати роботу закладів вищої освіти та оцифровувати документообіг закладів [61].

Дизайн

Для кольорової схеми були обрані відтінки білого та світло-сірого для фону та помаранчевий для виділення важливих елементів, таких як кнопки,

індикатори прогресу та активні пункти меню. Текст чорний або сірий, що забезпечує хороший контраст із світлим фоном.

Макет в себе включає бічну панель з опціями навігації, активний пункт меню виділений помаранчевим кольором. Також у верхній частині розташована горизонтальна панель із пошуковим рядком, іконкою сповіщень та випадаючим меню профілю користувача у правому верхньому куті. Використано прості та монохромні іконки, що добре вписуються у загальний мінімалістичний дизайн.

Dashboard

Головна сторінка порталу для авторизованого користувача (рис.4.6) виконує одразу декілька ключових функцій:

- швидкий доступ до інформації – дашборд надає користувачам миттєвий огляд найважливіших даних, таких як поточний прогрес у курсах, завдання, ресурси та майбутні події. Це допомагає швидко орієнтуватися в системі без необхідності переходити в різні розділи;
- централізація управління – об’єднує всі основні функції системи в одному місці, дозволяючи користувачам легко керувати завданнями, переглядати розклад, слідкувати за результатами та отримувати доступ до ресурсів. Це значно спрощує робочий процес;
- мотивація та контроль – за допомогою дашборду користувачі можуть бачити свої досягнення та оцінки, що допомагає їм контролювати свій прогрес і мотивує до подальшого навчання;
- оперативність – важливі сповіщення та нагадування про дедлайни або майбутні події відображаються безпосередньо на дашборді, допомагаючи користувачам не пропустити важливі дати або події.

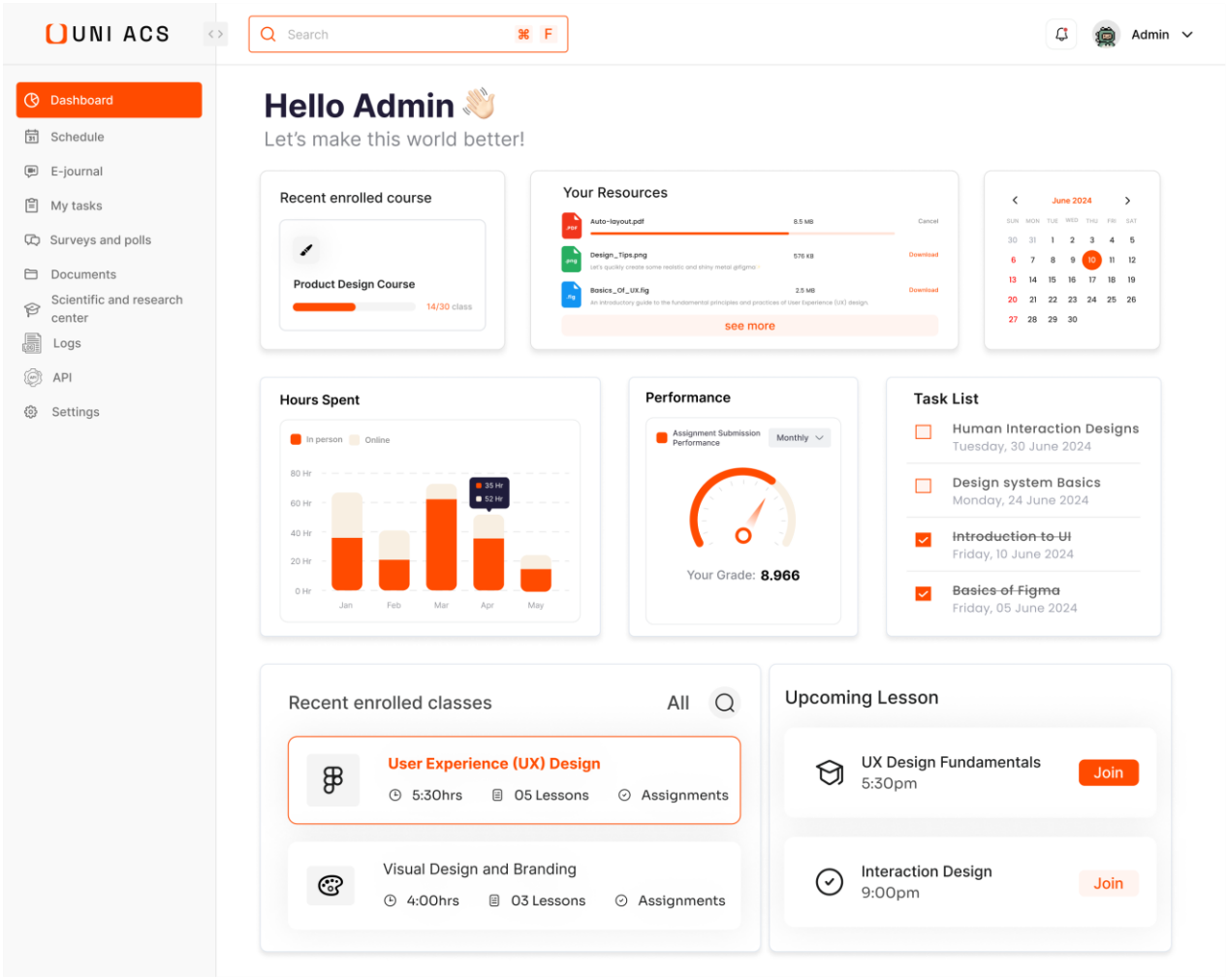

Рис. 4.6. Головна сторінка порталу

На рис. 4.6 зображені такі віджети:

- нещодавно зареєстрований курс – відображає інформацію про останній оновлений курс, включаючи назву курсу та прогрес (наприклад, 14/30 занять);
- ваші ресурси – перелік ресурсів для завантаження, таких як PDF чи зображення, з індикаторами прогресу завантаження (для розділу з науковими роботами);
- календар – міні-календар на поточний місяць з виділеними важливими датами або дедлайнами;
- витрачений час – стовпчаста діаграма, що показує час, витрачений на задачі, з розрізненням між «Очна» та «Онлайн» форми навчання;

- результативність – віджет у вигляді шкали, що показує оцінку або показник результативності користувача, який вираховується на основі кількості виконаних задач та витраченого часу за певний проміжок бізнес-часу;
- список завдань – перелік майбутніх завдань або дедлайнів із чекбоксами для виконаних завдань;
- нещодавно зареєстровані класи – список нещодавно зареєстрованих класів з деталями, такими як витрачений час, кількість уроків та наявність завдань.
- майбутні заняття – розділ з переліком майбутніх уроків із кнопкою «Join» для швидкого доступу.

Варто зазначити, що це версія адміністратора, в якій доступні всі розділи та віджети для дашборда. Для гостя порталу головна сторінка буде мати поле пошуку, кнопку авторизації та доступ до розкладу занять (рис. 4.7)

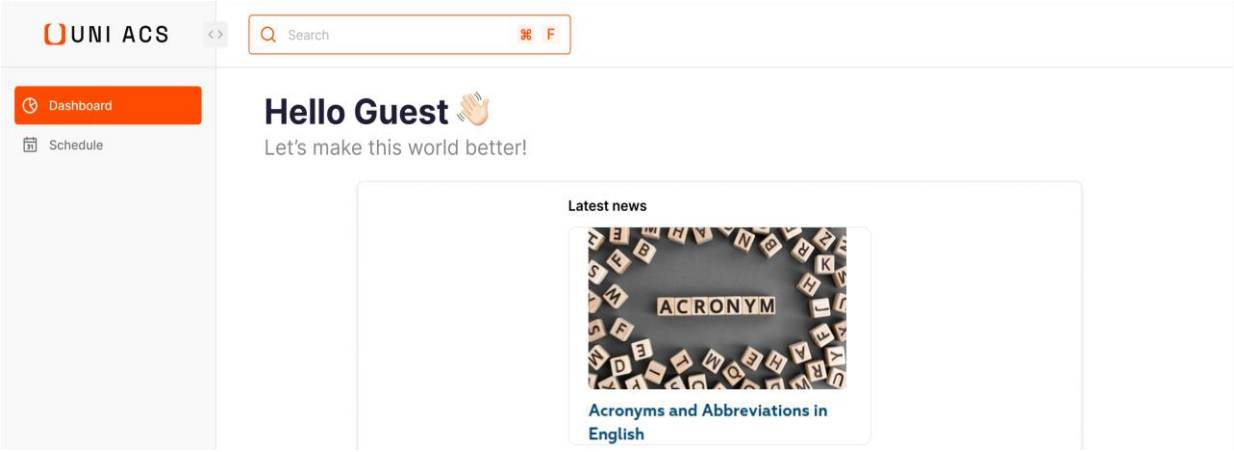

Рис. 4.7. Головна сторінка порталу для неавторизованого користувача

Додаткові рішення.

Для ефективнішого використання ресурсів система не включає в себе корпоративний чат. Використання готових рішень дозволить приступити до роботи швидше та ефективніше. В порівнянні зі звичайними месенджерами корпоративні пропонують наступні переваги:

- вищий рівень безпеки завдяки шифруванню та контролю доступу;

- можливість адміністрування доступу та налаштування прав;
- організацію командної роботи через канали та групи;
- архівування розмов для майбутнього використання або відповідності вимогам законодавства;
- спеціалізовану технічну підтримку.

Також пропонується розгорнути корпоративну систему контроля версій для ізоляції розробок на підконтрольних серверах навчального закладу.

Таблиця 4.2

Порівняння інформаційних систем

Параметр	Moodle	Описана система
Час завантаження сторінки (мс)	700 мс	450 мс
Час налаштування системи (години)	8 годин	9 годин
Час відновлення після збою (години)	3 години	0.75 години
Кількість підтримуваних користувачів	7,000	20,000
Захищеність від атак (кількість загроз)	70 загроз/рік	70 загроз/рік
Пропускна здатність системи (запити/сек)	150 запитів/сек	400 запитів/сек
Рівень персоналізації (відсоток)	60%	95%

Якщо порівнювати за відповідними метриками розроблену інформаційну систему і для прикладу одну з найбільш популярних систем, яка використовується в вузах Moodle, то можна побачити перевагу запропонованої системи та доцільність до впровадження.

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 ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Adams T., Brown J. Development of Information Security Models in Education. // Educational Cybersecurity. 2022. Vol. 18, No. 4, pp. 90-97.

2. Ali F., Bukhari S.A. Applications of Machine Learning in Education: A Review. // International Journal of Emerging Technologies in Learning. 2023. Vol. 18, No. 3. P. 57-69.

3. Anderson J., White K. Gradient-Based Methods in Machine Learning Security. // Journal of Computational Intelligence. 2023. Vol. 11, No. 7, pp. 320-328.

4. Baker, R.S., Heffernan, N.T. Early Detection of Student Struggles in Online Learning Environments // Journal of Educational Data Mining, Vol. 8, No. 2 (2021), pp. 12-25.

5. Blackwell R., Connors L. Machine Learning Models for Cyber Risk Assessment. // Cyber Risk Analysis Journal. 2023. Vol. 10, No. 6, pp. 205-212.

6. Blake A., Thompson R. Cybersecurity in Adaptive Learning Systems. // Journal of Adaptive Learning. 2022. Vol. 5, No. 2, pp. 120-128.

7. Chen P., Zhao Y. An Overview of Adaptive Learning Techniques: Challenges and Future Directions. // Journal of Educational Technology & Society. 2023. Vol. 26, No. 1. P. 50-62.

8. Chen X., Zhu Y. Advances in Proximal Gradient Methods for Machine Learning. // Journal of Machine Learning Research. 2022. Vol. 23, No. 1. P. 1-30.

9. Choi Y., Choi E. A Markov Random Field Approach to Spatial Data Analysis. // Journal of Spatial Statistics. 2023. Vol. 53. P. 101-118.

10. Fernández J., Romero C. Data Mining and Learning Analytics in Education: A Review. // IEEE Transactions on Learning Technologies. 2023. Vol. 16, No. 1. P. 1-16.

11. Grushevska O., Piskunov M. Machine Learning Approaches for Adaptive Learning Systems. // Journal of Educational Technology and Online Learning. 2023. Vol. 2. No. 1. P. 20-35.

12. Hwang G.J., Chen C.H. Adaptive Learning: Current Trends and Future Directions. // Educational Technology & Society. 2022. Vol. 25, No. 3. P. 5-15.

13. Johnson M., Taylor G. Threat Prevention and Response in Cybersecurity. // Information Systems Security. 2023. Vol. 20, No. 3, pp. 85-92.

14. Jovanović J., Gašević D. Learning Analytics in Higher Education: A Systematic Review. // Computers in Human Behavior. 2022. Vol. 121. P. 106-117.

15. Khan, H., Chi, M. Reinforcement Learning Approaches in Adaptive Learning Environments // Computers & Education, Vol. 158 (2020), pp. 104-116.

16. Kim H., Park S. Strategies for Cyber Attack Prevention in Corporate Systems. // Journal of Security Studies. 2023. Vol. 9, No. 5, pp. 200-207.

17. Kim J., Lee S. Cybersecurity Assessment Models for Educational Systems. // International Journal of Information Security. 2023. Vol. 12, No. 1, pp. 145-153.

18. Kim K., Kim J. Advances in Adaptive Learning Technology: A Systematic Review. // Educational Research Review. 2022. Vol. 20. P. 1-16.

19. Kulikowski K. The Role of Machine Learning in Education: A Review. // Journal of Education and Information Technologies. 2022. Vol. 27, No. 4. P. 249-267.

20. Lee J., Kim J. Optimization with Proximal Methods: Theory and Applications. // Mathematical Programming. 2023. Vol. 191, No. 1. P. 1-27.

21. Li Z., Chen Y. Proximal Gradient Methods in Machine Learning Applications. // Machine Learning Journal. 2023. Vol. 16, No. 2, pp. 233-240.

22. Liao W.K., Tseng Y.H. Application of Markov Random Field in Educational Technology. // Educational Technology & Society. 2022. Vol. 25, No. 2. P. 40-51.

23. Liu Y., Zhao L. Metric Proximal Gradient Method for High-Dimensional Data. // Journal of Machine Learning Research. 2023. Vol. 24, No. 1. P. 1-26.

24. Ma Y., Li J. Pairwise Exponential Models for Statistical Learning. // Journal of Statistical Theory and Practice. 2023. Vol. 17, No. 3. P. 150-167.

25. Miao Z., Wang H. Adaptive Learning Strategies Based on Machine Learning Algorithms. // Journal of Computer Assisted Learning. 2022. Vol. 38, No. 2. P. 204-217.

26. Milani F., Bazzanella M. Advances in Adaptive Learning Systems through Machine Learning Techniques. // Computers & Education. 2022. Vol. 180. P. 104-121.

27. Morales P., Vega M. Machine Learning in Security Platforms: A Review. // International Journal of Security Studies. 2022. Vol. 6, No. 3, pp. 158-166.

28. Pal S., Dasgupta A. Machine Learning and Adaptive Learning: Recent Developments and Future Directions. // Journal of Computer Science and Technology. 2023. Vol. 38, No. 4. P. 753-769.

29. Patel S., Kumar A. Proximal Gradient Optimization in Security Applications. // Journal of Optimization and Security. 2022. Vol. 7, No. 8, pp. 89-97.

30. Ramos A., Kotsiantis S. Machine Learning for Education: A Survey. // Education and Information Technologies. 2023. Vol. 28, No. 4. P. 1345-1360.

31. Rosé, C.P., Chi, M.T.H. Natural Language Processing for Adaptive Education Systems // Annual Review of Applied Linguistics, Vol. 41 (2021), pp. 112-128.

32. Sanchez F., Rodriguez C. Cybersecurity Threat Detection Using Proximal Gradient Methods. // Journal of Cybersecurity Research. 2022. Vol. 8, No. 4, pp. 310-318.

33. Siemens, G., Gašević, D. Learning Analytics in Education: Enhancing Student Success through Data // Journal of Learning Analytics, Vol. 7, No. 1 (2020), pp. 54-67.

34. Taylor P., Green E. Advances in Information Security for Educational Institutions. // International Journal of Educational Technology. 2023. Vol. 7, No. 3, pp. 52-60.

35. Torres F., Martinez R. Resilient Machine Learning Models for Cybersecurity. // Cybersecurity & Intelligence. 2023. Vol. 19, No. 7, pp. 135-143.

36. Valsan V., Pochiraju K. An Efficient Proximal Gradient Algorithm for Large-Scale Problems. // Numerical Linear Algebra with Applications. 2023. Vol. 30, No. 3. P. e2351.

37. Vasiliev A., Alimov A. Deep Learning in Educational Technology: An Overview. // Educational Technology Research and Development. 2023. Vol. 71, No. 3. P. 431-448.

38. Wang X., Zhou H. Advanced Machine Learning Techniques for Cyber Defense. // Journal of Artificial Intelligence Research. 2023. Vol. 27, No. 5, pp. 410-418.

39. Wu J., Chen S. A Comparative Study of Proximal Gradient and Stochastic Gradient Descent Methods. // Journal of Optimization Theory and Applications. 2023. Vol. 189, No. 2. P. 123-143.

40. Xu Z., Gao Y. Individual Learning Pathways in Smart Learning Environments. // Journal of Educational Computing Research. 2023. Vol. 61, No. 1. P. 73-92.

41. Yacef, K., Conati, C. Clustering Techniques for Personalized Learning in Educational Systems // International Journal of Artificial Intelligence in Education, Vol. 29, No. 3 (2019), pp. 203-215.

42. Yang Y., Liu Z. The Evolution of Adaptive Learning Systems: A Review. // International Journal of Educational Technology in Higher Education. 2023. Vol. 20, No. 5. P. 1-12.

43. Yang Y., Wu Y. Proximal Gradient Methods for Non-Convex Optimization. // SIAM Journal on Optimization. 2023. Vol. 33, No. 2. P. 992-1017.

44. Zeng Y., Wang Y. Intelligent Education and Adaptive Learning: Trends and Challenges. // Educational Sciences: Theory and Practice. 2023. Vol. 23, No. 1. P. 45-58.

45. Zhang J., Wu Z. Pairwise Exponential Markov Random Fields for Image Segmentation. // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2022. Vol. 44, No. 12. P. 6935-6949.

46. Zhang Y., Chen H. Exploring the Individual Learning Pathways in Adaptive Learning Systems. // International Journal of Information and Education Technology. 2022. Vol. 12, No. 6. P. 453-460.

47. Zhao Y., Xu L. Risk Assessment Models for Cybersecurity in Digital Platforms. // Journal of Digital Security. 2023. Vol. 10, No. 6, pp. 67-74.

48. Zhou F., Lee M. Proximal Gradient Optimization in Cybersecurity Systems. // Computational Security. 2023. Vol. 15, No. 2, pp. 100-107.

49. Zhou L., Xie Y. Applications of Markov Models in E-learning. // International Journal of E-Learning & Distance Education. 2022. Vol. 37, No. 1. P. 55-67.

50. Zhou Y., Wang X. Learning with Markov Random Fields: Algorithms and Applications. // Pattern Recognition. 2023. Vol. 122. P. 108-123.

51. Ананченко О.Є. Важливість інформаційної складової при проведення 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.

52. 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.

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

54. 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.

55. 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.

56. 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.

57. 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.

58. 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.

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

60. 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.

61. 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.

62. 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.

63. 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.

64. Бойко О.І. Математичні моделі для оцінки стійкості освітніх систем. // Науковий вісник НТУ "ХПІ". 2023. Вип. 2. С. 40-47.

65. Бондар В.Ю. Системи підтримки прийняття рішень в адаптивних освітніх системах. // Вісник НТУУ "КПІ". 2023. Вип. 3. С. 37-44.

66. Бондаренко В.Ю. Розробка адаптивних систем управління навчанням. // Журнал інформаційних технологій. 2023. Вип. 5. С. 77-85.

67. Бондаренко Н.І. Організаційні аспекти функціонування центру управління інформаційною безпекою у вищих навчальних закладах. // Вісник Сумського державного університету. 2023. Вип. 10. С. 18-25.

68. Бондаренко О.В. Моделі попарно-експоненціального марківського випадкового поля в задачах комп'ютерного зору. // Вісник Сумського державного університету. 2023. Вип. 6. С. 89-95.

69. Бондаренко О.О. Напрями розвитку інформаційних технологій в освіті. // Науковий вісник ХНУ. 2023. Вип. 5. С. 15-22.

70. Василенко О.М., Іванченко С.П. Використання машинного навчання для розпізнавання атак. // Інформаційна безпека. 2022. Вип. 3. С. 65-73.

71. Величко І.П. Використання методів машинного навчання для адаптації освітніх траєкторій. // Науковий вісник Миколаївського національного університету імені В.О. Сухомлинського. 2023. Вип. 2. С. 71-78.

72. Власенко М.В. Технології адаптивного навчання в інформаційних системах. // Науковий вісник Київського національного університету імені Тараса Шевченка. 2023. Вип. 10. С. 24-30.

73. Власенко О.А. Оцінка інформаційної безпеки: підходи та методики. // Науковий журнал "Технології в освіті". 2023. Вип. 6. С. 55-63.

74. Вороненко Т.Ф. Нові технології захисту інформації в освітніх установах. // Вісник Сумського державного університету. 2023. Вип. 7. С. 44-51.

75. Воронін А.І. Використання машинного навчання в адаптивних освітніх системах. // Науковий вісник ХНУ. 2023. Вип. 9. С. 22-29.

76. Воронін С.М., Щербак М.В. Розробка інформаційних платформ з високим рівнем кібербезпеки. // Журнал системної інженерії. 2023. Вип. 9. С. 19-26.

77. Ганущак Т.П. Адаптивні методи оптимізації на основі проксимального градієнта. // Вісник Національного технічного університету України "КПІ". 2023. Вип. 9. С. 37-43.

78. Герасименко Д.Ю. Методи машинного навчання для виявлення загроз у кіберпросторі. // Кібербезпека та інформаційні системи. 2023. Вип. 6. С. 55-62.

79. Головін С.П. Технології для покращення інформаційної безпеки в освітньому процесі. // Науковий вісник ДДТУ. 2023. Вип. 3. С. 33-39.

80. Гонтар В.М. Розробка критеріїв оцінки інформаційної безпеки в освіті. // Збірник наукових праць. 2023. Вип. 2. С. 87-95.

81. Гончаренко Л.В. Методологія розробки адаптивних систем в освіті. // Науковий вісник НТУ "ХПІ". 2023. Вип. 6. С. 14-21.

82. Гордієнко С.І. Центр управління інформаційною безпекою в системі вищої освіти: концептуальні засади. // Науковий вісник Черкаського національного університету. 2023. Вип. 7. С. 22-30.

83. Гребінь С.В. Моделі та методи навчання на основі аналізу даних в освітніх системах. // Вісник Черкаського університету. 2023. Вип. 5. С. 30-37.

84. Гречко Ю.І. Використання машинного навчання для аналізу освітніх даних. // Науковий вісник Сумського державного університету. 2023. Вип. 2. С. 42-49.

85. Григор'єва І.В. Розробка адаптивних навчальних систем: досвід та перспективи. // Науковий журнал "Педагогіка та психологія". 2023. Вип. 2. С. 49-56.

86. Григорович Р.П. Система управління інформаційною безпекою в закладах вищої освіти. // Науковий вісник ХНУ. 2023. Вип. 5. С. 28-35.

87. Гринько А.В. Методи визначення рівня захищеності інформаційних систем. // Вісник НТУ "ХПІ". 2023. Вип. 10. С. 55-61.

88. Гриценко О.В. Застосування підходів з підкріпленням для адаптації навчального контенту в корпоративних системах // Український журнал "Технології в освіті", Том 4 № 18 (2023), ст. 133-140.

89. Грищенко Т.В. Моделювання функціональної стійкості в інформаційних системах освіти. // Вісник КНУ імені Тараса Шевченка. 2023. Вип. 9. С. 33-40.

90. Захаренко І.В. Ефективні стратегії кіберзахисту для університетів. // Вісник університету. 2023. Вип. 12. С. 88-94.

91. Захаренко Т.Ю. Розробка адаптивної корпоративної інформаційної системи в освіті. // Журнал інформаційних технологій. 2023. Вип. 1. С. 52-60.

92. Захаров П.О. Адаптивні платформи для забезпечення кібербезпеки в освіті. // Науковий вісник НУ "ЛП". 2023. Вип. 5. С. 66-73.

93. Зеленський В.Ю. Попередження та ліквідація наслідків кібератак. // Вісник Національного технічного університету. 2023. Вип. 8. С. 12-19.

94. Іваненко В.П. Застосування машинного навчання для забезпечення інформаційної безпеки. // Інформаційні системи та технології. 2023. Вип. 7. С. 45-52.

95. Кобзєва О.І. Адаптивні інформаційні технології в освіті: теорія та практика. // Науковий журнал "Технології в освіті". 2023. Вип. 6. С. 11-18.

96. Коваленко В.І. Методи машинного навчання для оптимізації процесів в освітніх інформаційних системах. // Науковий вісник НПУ імені М.П. Драгоманова. Серія 1, 2023, Вип. 2, С. 45-53.

97. Коваленко В.О. Адаптивна освітня інформаційна система: теорія та практика. // Науковий журнал "Технології в освіті". 2023. Вип. 3. С. 49-56.

98. Коваленко О.В. Організаційно-технічні аспекти інформаційної безпеки в університетах. // Вісник Сумського державного університету. 2023. Вип. 3. С. 15-23.

99. Коваленко С.П. Розробка математичної моделі для оцінки стійкості освітніх інформаційних систем. // Науковий журнал "Технології в освіті". 2023. Вип. 4. С. 18-25.

100. Ковальчук В.О. Оцінка вразливостей інформаційних систем у вищій освіті. // Вісник Сумського державного університету. 2023. Вип. 2. С. 12-19.

101. Ковальчук Н.В., Іваненко В.М. Використання предиктивних моделей для побудови індивідуальних освітніх траєкторій у корпоративних системах // Журнал "Інформаційні технології в освіті", Том 5 № 12 (2022), ст. 89-95.

102. Корнійчук А.І. Інформаційні технології для адаптації освітніх систем. // Вісник Сумського державного університету. 2023. Вип. 8. С. 12-20.

103. Костенко Н.І. Адаптивні системи в освіті: концепції та реалізація. // Науковий вісник ДДТУ. 2023. Вип. 3. С. 39-46.

104. Костюк О.В. Концепція центру управління інформаційною безпекою в університеті. // Науковий вісник НТУУ "КПІ". 2023. Вип. 4. С. 8-16.

105. Костюк О.В. Попарно-експоненціальні моделі в статистичному навчанні. // Науковий вісник Миколаївського національного університету імені В.О. Сухомлинського. 2023. Вип. 3. С. 66-72.

106. Кочеткова Н.І. Адаптивні технології навчання на основі штучного інтелекту. // Науковий вісник Хмельницького національного університету. 2023. Вип. 1. С. 50-58.

107. Кравченко О.О. Застосування методу метричного проксимального градієнта в адаптивних системах навчання. // Науковий журнал "Проблеми освіти". 2023. Вип. 4. С. 23-30.

108. Кравчук Н.В. Моделі управління інформаційною безпекою в освіті. // Журнал інформаційних технологій. 2023. Вип. 6. С. 39-46.

109. Кривенко Р.С. Оптимізація з використанням попарно-експоненціальних марківських випадкових полів. // Науковий журнал "Інформаційні технології і комп'ютерна інженерія". 2023. Вип. 2. С. 73-80.

110. Кудрявцев О.В. Системи підтримки прийняття рішень у навчальних закладах: сучасні тенденції. // Науковий вісник Ужгородського університету. 2023. Вип. 2. С. 112-119.

111. Кузнецова Т.Є. Методи запобігання та реагування на кібератаки в освітніх закладах. // Інформаційні технології в освіті. 2023. Вип. 5. С. 15-22.

112. Кузьменко Л.М. Розробка інформаційних систем для управління навчальним процесом. // Вісник Одеського національного університету. 2023. Вип. 6. С. 18-25.

113. Лаптєв М.О. Інноваційні технології в забезпеченні інформаційної безпеки в освіті. // Збірник наукових праць. 2023. Вип. 1. С. 100-107.

114. Левченко І.В. Розробка моделі оцінки рівня інформаційної безпеки освітніх інформаційних систем. // Науковий вісник НТУУ "КПІ". 2023. Вип. 2. С. 22-29.

115. Левченко С.П. Розробка адаптивних освітніх технологій: сучасні тенденції. // Вісник НТУ "ХПІ". 2023. Вип. 8. С. 33-40.

116. Лисенко А.М. Аналіз математичних моделей для забезпечення функціональної стійкості. // Вісник Одеського національного університету. 2023. Вип. 1. С. 55-62.

117. Литвиненко А.М. Створення центру управління інформаційною безпекою у вищому навчальному закладі. // Вісник університету. 2023. Вип. 11. С. 45-52.

118. Мельник І.В. Інформаційні технології для забезпечення функціональної стійкості в освіті. // Науковий вісник НТУУ "КПІ". 2023. Вип. 5. С. 50-58.

119. Мельник Л.С. Оцінка ризиків інформаційної безпеки в корпоративних системах. // Вісник НТУУ "КПІ". 2022. Вип. 9. С. 44-52.

120. Мельник О.І. Організація реагування на кібератаки в навчальних закладах. // Науковий вісник Ужгородського університету. 2023. Вип. 1. С. 44-50.

121. Мельничук І.І. Попарно-експоненціальне марківське випадкове поле: теорія та застосування. // Науковий вісник Державного університету інформаційних технологій та штучного інтелекту. 2023. Вип. 4. С. 36-42.

122. Михайлюк О.С. Напрями організаційно-технічного забезпечення інформаційної безпеки. // Науковий вісник ДДТУ. 2023. Вип. 1. С. 12-19.

123. Михайлюк Р.Л. Адаптивні інформаційні системи: переваги та виклики. // Вісник Сумського державного університету. 2023. Вип. 10. С. 25-32.

124. Мороз Т.А., Соловей О.П. Аналіз рівня кіберзахисту для інформаційних платформ. // Український журнал кібербезпеки. 2023. Вип. 2. С. 18-25.

125. Навак Л.С., Попович І.А. Забезпечення кібербезпеки у корпоративних інформаційних системах. // Вісник КНУ. 2022. Вип. 3. С. 45-52.

126. Назаренко М.С., Бойко І.В. Розробка інформаційних платформ для навчальних цілей з використанням машинного навчання. // Інформаційні технології та безпека. 2023. Вип. 6. С. 37-45.

127. Нестеренко О.В. Нові підходи до формування індивідуальних освітніх траєкторій. // Вісник Національної академії педагогічних наук України. 2023. Вип. 8. С. 88-96.

128. Носенко Л.Є. Сучасні технології в управлінні освітніми процесами. // Вісник НТУУ "КПІ". 2023. Вип. 3. С. 66-73.

129. Олійник Ю.О. Методика оцінки інформаційної безпеки освітніх інформаційних систем. // Вісник Національного технічного університету "ХПІ". 2023. Вип. 9. С. 45-53.

130. Островська Л.П. Інформаційна безпека в освітніх установах: проблеми та рішення. // Науковий журнал "Технології в освіті". 2023. Вип. 5

131. Островська Т.В. Використання даних для адаптації освітніх процесів. // Науковий вісник Черкаського національного університету. 2023. Вип. 2. С. 11-18.

132. Папуша С.Ф. Інноваційні технології в управлінні освітніми системами. // Науковий вісник Львівського національного університету імені Івана Франка. 2023. Вип. 4. С. 34-41.

133. Петренко С.В., Мельник А.В. Інтелектуальні системи підтримки прийняття рішень в освіті. // Вісник Національного технічного університету України “Київський політехнічний інститут”. 2023. № 4. С. 12-19.

134. Петров В.Ф. Метричний проксимальний градієнт для оптимізації складних функцій. // Вісник Київського національного університету імені Тараса Шевченка. 2023. Вип. 5. С. 14-21.

135. Петров Д.О., Коваленко О.С. Моделі прогнозування загроз у кібербезпеці. // Журнал кібербезпеки. 2022. Вип. 1. С. 11-19.

136. Петрова А.С. Розробка адаптивної освітньої інформаційної системи на основі методів машинного навчання. // Вісник наукових досліджень. 2023. Вип. 4. С. 18-25.

137. Писаренко О.І. Алгоритми оптимізації на основі методу метричного проксимального градієнта в задачах машинного навчання. // Збірник наукових праць "Технології в освіті". 2023. Вип. 3. С. 45-52.

138. Пономаренко М.І. Оцінка ризиків інформаційної безпеки в закладах вищої освіти. // Науковий вісник Миколаївського національного університету. 2023. Вип. 8. С. 66-72.

139. Романенко І.М. Кластеризація даних у системах індивідуалізованого навчання: сучасні підходи та алгоритми // Науковий вісник "Освітні технології та системи", Том 10 № 27 (2023), ст. 210-217.

140. Ромашенко В.Ю. Застосування технологій блокчейн для захисту освітніх систем. // Журнал інформаційних технологій. 2023. Вип. 3. С. 76-84.

141. Руденко О.М. Підходи до адаптивного навчання на основі даних. // Науковий вісник Державного університету інформаційних технологій та штучного інтелекту. 2023. Вип. 5. С. 40-47.

142. Савченко Т.В. Особливості оцінки загроз інформаційній безпеці в навчальних закладах. // Науковий журнал "Технології в освіті". 2023. Вип. 4. С. 28-35.

143. Савчук Т.Ф. Розробка стратегії інформаційної безпеки для вищих навчальних закладів. // Збірник наукових праць. 2023. Вип. 3. С. 66-72.

144. Сидоренко А.Ю. Кіберзахист освітніх установ: сучасні виклики та рішення. // Вісник Національної академії педагогічних наук України. 2023. Вип. 9. С. 102-110.

145. Сидоренко А.Ю. Оцінка ризиків інформаційної безпеки в освітній галузі. // Науковий вісник НТУУ "КПІ". 2023. Вип. 7. С. 30-38.

146. Сидоренко В.Ю. Методи виявлення загроз інформаційним платформам. // Науковий вісник ХНУ. 2023. Вип. 11. С. 33-40.

147. Сидоренко М.П. Розробка технології забезпечення стійкості освітніх інформаційних систем. // Журнал інформаційних технологій. 2023. Вип. 6. С. 44-52.

148. Сидоренко О.Є. Технології адаптивного навчання в корпоративних інформаційних системах. // Проблеми та перспективи розвитку освіти в Україні: Збірник наукових праць. 2022. Вип. 3. С. 87-92.

149. Сисоєва Т.А., Чабан В.І. Моделі навчання на основі даних в освітніх системах. // Науковий журнал "Проблеми освіти". 2023. Вип. 3. С. 77-84.

150. Ставніцер О.Л. Сучасні методи оптимізації: метричний проксимальний градієнт і його застосування. // Науковий вісник Національного університету "Львівська політехніка". 2023. Вип. 5. С. 55-63.

151. Степаненко О.Ф. Машинне навчання для адаптивних освітніх систем. // Вісник КНУ імені Тараса Шевченка. 2023. Вип. 12. С. 40-47.

152. Степаненко Т.І., Яременко М.В. Методологія створення адаптивних освітніх систем на базі машинного навчання. // Збірник наукових праць «Технології в освіті». 2023. Вип. 5. С. 56-63.

153. Стеценко В.Ю. Вдосконалення навчальних алгоритмів з використанням попарно-експоненціальних марківських полів. // Науковий вісник Ужгородського університету. 2023. Вип. 1. С. 29-36.

154. Терещенко Л.І. Моделі оцінки загроз для інформаційних систем в освіті. // Журнал інформаційних технологій. 2023. Вип. 2. С. 44-50.

155. Тимошенко М.О. Методи обробки природної мови для адаптивних освітніх систем // Вісник Київського національного університету ім. Т. Шевченка. Серія "Інформаційні технології", Том 3 № 15 (2023), ст. 56-64.

156. Тищенко Т.І. Організація інформаційної безпеки у вищих навчальних закладах. // Вісник Національного університету "Львівська політехніка". 2023. Вип. 8. С. 22-29.

157. Ткаченко Д.В. Адаптивні інформаційні технології для освітніх систем. // Науковий журнал "Технології в освіті". 2023. Вип. 7. С. 30-37.

158. Ткаченко С.А. Адаптивні навчальні платформи: сучасні розробки та перспективи. // Науковий вісник ХНУ. 2023. Вип. 10. С. 57-64.

159. Федоренко В.Ю. Математичні підходи до забезпечення стійкості освітніх систем. // Науковий вісник ЛНУ. 2023. Вип. 3. С. 20-27.

160. Федоренко Н.С. Методика оцінки рівня інформаційної безпеки освітніх систем. // Науковий вісник Черкаського національного університету. 2023. Вип. 4. С. 12-20.

161. Червоненко О.Ю. Інформаційні технології для забезпечення функціональної стійкості в навчальних закладах. // Науковий вісник ХНУ. 2023. Вип. 11. С. 66-74.

162. Черненко А.І. Системи захисту від атак на інформаційні платформи. // Журнал інформаційних технологій. 2023. Вип. 1. С. 78-86.

163. Чорненький В.Ф. Штучний інтелект у освіті: можливості та виклики. // Вісник Запорізького національного університету. 2023. Вип. 6. С. 90-97.

164. Чубенко А.Ю. Системи адаптивного навчання на основі методів штучного інтелекту. // Науковий журнал «Інформаційні технології і комп'ютерна інженерія». 2023. Вип. 4. С. 22-29.

165. Шевченко Д.О. Інноваційні підходи до адаптивних освітніх систем. // Науковий вісник НТУУ "КПІ". 2023. Вип. 4. С. 38-45.

166. Шевченко Р.В. Тенденції розвитку інформаційної безпеки в освіті. // Вісник наукових досліджень. 2023. Вип. 3. С. 55-61.

167. Яковенко Т.А., Кошель А.О. Методи оцінки якості навчання в адаптивних системах. // Інформаційні технології в освіті. 2023. Вип. 1. С. 11-18.

ДОДАТОК А

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 проведення 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. ІІІ міжнародна науково-практична конференція 8-10 листопада 2016 р. Київський національний університет ім. Т. Шевченка. С.217-218.

ДОДАТОК Б

ЗАТВЕРДЖУЮ

Перший проректор
Державного університету інформаційно-
комунікаційних технологій
доктор технічних наук, професор

_____ Корченко О.Г.
"13" 03 2024 р.

АКТ
про реалізацію результатів наукових досліджень
Ананченко Олексія Євгеновича

Комісія у складі: голови – Жебки Вікторії Вікторівни, завідувача кафедри Технологій цифрового розвитку, д.т.н., проф., та членів комісії – Зінченко Ольги Валеріївни, завідувача кафедри Штучного інтелекту, д.т.н., доц., Лащевської Наталії Олександрівни, завідувача кафедри Комп'ютерної інженерії, к.т.н., доц. встановила, що наукові положення та результати, розроблені особисто Ананченко О.Є., а саме:

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.
є важливим вкладом в удосконалення сучасних корпоративних освітніх систем та дозволять покращити процес навчання студентів як в дистанційному, так і в змішаному форматі.

Результати дисертаційної роботи отримані та використовуються в рамках науково-дослідних робіт Державного університету інформаційно-комунікаційних технологій, а саме «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).

На основі аналізу представлених матеріалів комісія встановила, що отримані наукові результати дисертаційної роботи та опубліковані наукові роботи здобувача Ананченка О.Є. використовуються в навчальному процесі Державного університету інформаційно-комунікаційних технологій при дипломному та курсовому проектуванні, а також при викладанні навчальних дисциплін: «Безпека систем баз даних», «Методології організації та проведення наукових досліджень», «Штучний інтелект», «Основи технологій цифрового розвитку» та ін.

Голова комісії:
доктор технічних наук, професор Вікторія ЖЕБКА

Члени комісії:

доктор технічних наук, доцент Ольга ЗІНЧЕНКО

кандидат технічних наук, доцент Наталія ЛАЩЕВСЬКА

ЗАТВЕРДЖУЮ

Директор Інституту тедекомунікацій і глобального інформаційного простору НАН України, чл.-кор НАНУ Трофимчук О. М.

«20» серпня 2024 року

АКТ
про впровадження результатів дисертаційної роботи
Ананченко Олексія Євгеновича

Комісія Інституту телекомунікацій і глобального інформаційного простору НАНУ у складі: голови комісії Триснюка В.М., та членів комісії – Яковлєва Є.О., Охарєва В.О. засвідчує окремі наукові результати дисертаційного дослідження, отримані особисто Ананченко О.Є., впроваджено при підготовці звітних матеріалів за темою НДР «Розробка засобів інформаційно-аналітичної підтримки завдань забезпечення стійкості об'єктів критичної інфраструктури в регіональній соціоекосистемі за умов зростання природних, техногенних і соціальних загроз» (№ ДР 0121U109216),

Актуальність теми дослідження полягає в необхідності підвищення стійкості корпоративних освітніх інформаційних систем в умовах зростаючих кіберзагроз та змін в освітньому середовищі. Це науково-практичне завдання є важливим через потребу у покращенні функціональності та безпеки сучасних освітніх платформ.

Зокрема Ананченко О.Є. удосконалений метод метричного проксимального градієнта, методику оцінки рівня інформаційної безпеки на основі алгоритмів машинного навчання, технологію забезпечення функціональної стійкості інформаційної системи.

Розроблені Ананченко О.Є.методики забезпечують підвищення функціональної стійкості інформаційної системи за допомогою удосконаленого методу машинного навчання, що дозволяє автоматично коригувати індивідуальні освітні траєкторії студентів та своєчасно реагувати на загрози. Крім того, впроваджена технологія блокчейн забезпечує контроль за інформаційними потоками та підвищує ефективність управління безпекою даних.

Рекомендуємо Ананченко О.Є. продовжити дослідження в даному напрямку.

Економічний ефект від впровадження не розраховувався, у зв'язку з науковими призначенням результатів.

Акт складено для представлення в спеціалізовану вчену раду та не є основою для виплати винагороди за впровадження та інших авторських винагород.

Голова комісії
Завідувач відділу досліджень
навколишнього середовища д.т.н, проф Триснюк В.М.
Члени комісії
Головний науковий співробітник
д.т.н., с.н.с. Яковлєв Є.О.
Старший науковий співробітник
к.т.н.,с.н.с. Охарєв В.О.

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА

ФАКУЛЬТЕТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ТА МАТЕМАТИКИ
вул. Левка Лук'яненка, 13-Б, м. Київ, Україна, 04207
Тел.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

BORYS GRINCHENKO
KYIV METROPOLITAN UNIVERSITY

FACULTY
OF INFORMATION TECHNOLOGIES
AND MATHEMATICS
13-B Levka Lukianenka St, Kyiv, Ukraine, 04207
Tel.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

АКТ
про впровадження результатів дисертаційного дослідження
Ананченка Олексія Євгеновича
на тему «Методи та технології забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем», поданої на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.06 – інформаційні технології

Цим Актом, ґрунтуючись на рішенні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка, засвідчуємо, що нижчеперелічені наукові положення, а саме:

1) удосконалений метод метричного проксимального градієнта;
2) методика оцінки рівня інформаційної безпеки на основі алгоритмів машинного навчання;
3) технологія забезпечення функціональної стійкості інформаційної системи

розроблені особисто Ананченком Олексієм Євгеновичем у ході проведення ним дисертаційних досліджень та отримали високу оцінку при обговоренні на засіданнях кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Впровадження матеріалів дисертації в освітній процес здійснюється з урахуванням особливостей інфраструктури закладу освіти. Основна увага приділяється адаптації корпоративної освітньої інформаційної системи під існуючі технічні ресурси Київського столичного університету імені Бориса

Грінченка та інтеграції з поточними інформаційними системами. Особливості впровадження полягають у використанні розроблених методів машинного навчання для автоматизації управління освітнім процесом, а також у впровадженні методів інформаційної безпеки для захисту даних студентів та викладачів.

Розроблені методики забезпечують підвищення функціональної стійкості інформаційної системи за допомогою удосконаленого методу машинного навчання, що дозволяє автоматично коригувати індивідуальні освітні траєкторії студентів та своєчасно реагувати на загрози. Окрім того, впровадження технології блокчейн забезпечить контроль за інформаційними потоками та підвищить ефективність управління безпекою даних.

Зазначені наукові результати:

по-перше, впроваджені в освітній процес кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка, що відображено у програмах навчальних дисциплін спеціальності 125 Кібербезпека за захист інформації першого (бакалаврського), другого (магістерського) та третього (освітньо-наукового) рівнів вищої освіти;

по-друге, впроваджені в програмно-апаратне забезпечення лабораторій безпеки інформаційних активів, антивірусного захисту інформації, систем технічного та криптографічного захисту інформації.

Дослідження Ананченка Олексія Євгеновича відповідає всім вимогам до організації наукового пошуку та дає позитивний результат у практичному застосуванні.

Декан
Факультету інформаційних технологій та математики
кандидат фізико-математичних наук,
старший науковий співробітник Оксана ЛИТВИН

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА ЄДРПОУ 45307814 ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА МАТЕМАТИКИ УКРАЇНА

ТОВ «УКР-ОН»
м. Київ. вул. Харківське шосе, буд. 158, оф.86
ЕДРПОУ 41329131

ДОВІДКА
про впровадження результатів дисертаційної роботи
Ананченко Олексія Євгеновича

Актуальність впровадження наукових розробок обумовлена зростаючими вимогами до надійності та функціональної стійкості інформаційних систем в умовах динамічного розвитку технологій та підвищення загроз інформаційної безпеки. З урахуванням цих викликів, сучасні компанії потребують інтеграції передових рішень, що дозволять забезпечити стійкість систем до змін, підвищити їх продуктивність і захистити від загроз безпеці.

Наукові результати, що впроваджуються, були розроблені в рамках дослідження на тему "Методи та технології забезпечення функціональної стійкості адаптивних корпоративних інформаційних систем". Основною метою є підвищення стійкості корпоративних інформаційних систем за допомогою удосконалених методів машинного навчання, що дозволять оптимізувати процеси управління, обробки даних та безпеки.

Компанія бере на впровадження **розроблений науковий підхід по використанню технології блокчейн для забезпечення функціональної стійкості інформаційної системи**. Вона дозволяє використовувати децентралізовані механізми для моніторингу та оптимізації інформаційних процесів. Впровадження блокчейн допоможе компанії забезпечити більшу прозорість і контроль за транзакціями, покращити інтеграцію системи з іншими бізнес-процесами та забезпечити її стійкість до зовнішніх і внутрішніх загроз. Алгоритми машинного навчання, інтегровані у цю технологію, дадуть змогу автоматично аналізувати потоки даних, що призведе до оптимізації роботи системи в цілому.

Цінність цього дослідження полягає в можливості підвищення ефективності та стійкості інформаційної системи компанії, зокрема за рахунок прискорення обробки даних, автоматизації процесів управління ризиками та безпекою, а також впровадження інноваційних рішень на основі технології блокчейн. В результаті, компанія отримає інформаційну систему, здатну адаптуватися до сучасних викликів і забезпечити стабільне функціонування у будь-яких умовах.

Директор
ТОВ “УКР-ОН” _____ Гашко А.О

ADELINA
Call Center & BPO

№1-19 від 23.09.2024 р.

До спеціалізованої вченої ради Д 26.861.05 при
Державному університеті інформаційно-комунікаційних технологій

ДОВІДКА
про впровадження результатів дисертаційної роботи
Ананченка Олексія Євгеновича
на тему «Методи та технології забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем»

Цією довідкою засвідчується, що результати, отримані в дисертаційному дослідженні здобувача Державного університету інформаційно-комунікаційних технологій Ананченко Олексія Євгеновича на тему «Методи та технології забезпечення функціональної стійкості адаптивних корпоративних освітніх інформаційних систем», використані при реалізації проектів корпоративних інформаційних систем та впроваджені в ТОВ «АДЕЛІНА АУТСОРСИНГ».

Перелік наукових результатів, їх практичне значення для впровадження в ТОВ «АДЕЛІНА АУТСОРСИНГ»:
1. Методика оцінки рівня інформаційної безпеки, яка 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.
2. Удосконалена методика забезпечення функціональної стійкості інформаційних систем завдяки використанню адаптивних інформаційних технологій і алгоритмів машинного навчання, що дозволяє оптимізувати процеси, покращувати управління інформаційними потоками та своєчасно реагувати на зміни, забезпечуючи стабільну роботу інформаційних систем навіть у динамічних умовах.

Adelina Call Center & BPO — найбільший контакт-центр України, один з провідних регіональних гравців з офісами в Україні, Казахстані, Туреччині та Польщі. Загальний штат компанії нараховує понад 4000 співробітників. За 20 років діяльності компанія реалізувала більше 300 проектів для 192 замовників з 29 країн на 24 різних мовах.

Успішна робота компанії в сучасних умовах не можлива без постійного впровадження таких новітніх технологій, як штучний інтелект, великі дані, хмарні обчислення, забезпечення стійкого функціонування та розвитку інформаційних систем компанії. Такі рішення потребують впровадження нових методів забезпечення функціональної стійкості інформаційних систем та автоматизації процесів підготовки та постійного розвитку персоналу.

Ананченко О.Є. залучався до обговорення та впровадження методики оцінки рівня інформаційної безпеки, алгоритмів машинного навчання. Таким чином, наукові та практичні результати дослідження можуть знайти подальше практичне застосування в процесі побудови та удосконалення існуючих адаптивних корпоративних інформаційних систем.

Довідку надано до спеціалізованої вченої ради Д 26.861.05 при Державному університеті інформаційно-комунікаційних технологій.

Директор
ТОВ «АДЕЛІНА АУТСОРСИНГ» **О. І. Чорнобривцев**

ТОВ «АДЕЛІНА АУТСОРСИНГ»
ЄДРПОУ 40186059, ІПН 401860526550
Адреса: 03124 м. Київ, бул. Вацлава Гавела, буд. 4, Діамант Центр, 2-й поверх
IBAN UA583005280000026000455017639 в АТ «ОТП Банк» м. Київ, МФО 300528
| www.adelina.com.ua | sales@adelina.com.ua | +380 44 369-56-78