Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерних наук_____
(повна назва)

Кафедра _____Інформаційних управляючих систем_____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____
_____Дослідження методів управління безпекою ІТ-проєктів_____
_____державного навчального закладу_____
(тема)

Виконав:
здобувач ___2___ року навчання,
групи ___УПГІТм-23-1_____
_____Анна РАДОУЦЬКА_____
(власне ім'я, прізвище)

Спеціальність ___122 Комп'ютерні науки____
(код і повна назва спеціальності)
Тип програми _____освітньо-наукова_____
(освітньо-професійна або освітньо-наукова)
Освітня програма __Управління проектами в галузі інформаційних технологій_____
(повна назва освітньої програми)

Керівник проф. каф. ІУС, Ірина ПАНФЬОРОВА
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри _____ Костянтин_ПЕТРОВ__
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафеда Інформаційних управляючих систем

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління проектами в галузі інформаційних технологій
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
" 21 " квітня 20 25 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Радоуцькій Анні Костянтинівні
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження методів управління безпекою ІТ проєктів державного навчального закладу

затверджена наказом по університету від " 28 " березня 2025 р. № 235Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії " 02 " червня 2025 р.

3. Вихідні дані до роботи науково-технічні публікації; джерела інтернету; науково-технічна література, що стосуються теми кваліфікаційної роботи; результати апробації дослідження на прикладі реального ІТ-проєкту державного навчального закладу щодо впровадження системи електронного документообігу.

4. Перелік питань, що потрібно опрацювати у роботі аналіз загроз інформаційній безпеці ІТ-проєктів державних закладів; аналіз існуючих методів забезпечення інформаційної безпеки; обґрунтування мети кваліфікаційної роботи та постановка задачі; аналіз методу оптимізації за Парето в управлінні ІТ-проєктами; розробка комбінованого методу вибору методів забезпечення ІБ ІТ-проєктів державних навчальних закладів.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз загроз інформаційній безпеці ІТ-проєктів державних навчальних закладів	21.04.2025 – 22.04.2025	Виконано
2	Аналіз існуючих методів забезпечення інформаційної безпеки	23.04.2025 – 24.04.2025	Виконано
3	Обґрунтування мети кваліфікаційної роботи та постановка задачі	24.04.2025 – 25.04.2025	Виконано
4	Аналіз методу оптимізації за Парето в управлінні ІТ-проєктами	26.04.2025 – 29.04.2025	Виконано
5	Розробка комбінованого методу вибору методів забезпечення ІБ ІТ-проєктів державних навчальних закладів	30.04.2025 – 17.05.2025	Виконано
6	Оформлення пояснювальної записки та графічного матеріалу	18.05.2025 – 27.05.2025	Виконано
7	Підготовка презентації	28.05.2025	Виконано
8	Попередній захист роботи	02.06.2025	
9	Захист кваліфікаційної роботи	06.06.2025	

Дата видачі завдання 21 __квітня__2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ _проф. каф ІУС Ірина ПАНФЬОРОВА_
(підпис) (посада, власне ім’я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 69 с., 26 табл., 1 дод., 26 джерел.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАКЛАДИ ОСВІТИ, КОМБІНОВАНИЙ МЕТОД, ОПТИМІЗАЦІЯ ЗА ПАРЕТО, ФУНКЦІЯ ВИГОДИ.

Кваліфікаційна робота присвячена дослідженню методів забезпечення інформаційної безпеки в ІТ-проєктах державних навчальних закладів з урахуванням обмежених ресурсів та високих вимог до захисту даних.

Об’єктом дослідження є методи забезпечення інформаційної безпеки в ІТ-проєктах освітніх установ.

Предметом дослідження виступає задача вибору оптимального набору методів забезпечення інформаційної безпеки з урахуванням обмежень.

Метою даної роботи є аналіз основних загроз інформаційній безпеці ІТ-проєктів у державних навчальних закладах, вивчення існуючих методів захисту та розробка комбінованого методу вибору методів забезпечення інформаційної безпеки ІТ-проєктів державних навчальних закладів.

У роботі було виконано дослідження загроз інформаційній безпеці ІТ-проєктів та методів захисту, сформульовано обмеження методу оптимізації за Парето та запропоновано комбінований метод вибору методів забезпечення інформаційної безпеки, проведено експериментальне застосування методу на ІТ-проєкті системи електронного документообігу в державному навчальному закладі.

Отримані результати можуть бути використані для прийняття рішень щодо інформаційної безпеки у ІТ-проєктах державних навчальних закладів та адаптації до інших типів ІТ-проєктів.

ABSTRACT

Explanatory note of the qualification work: 69 pages, 26 tables, 1 appendices, 26 sources.

BENEFIT FUNCTION, COMBINED METHOD, EDUCATIONAL INSTITUTIONS, INFORMATION SECURITY, PARETO OPTIMIZATION

The qualification work is devoted to the study of methods for ensuring information security in IT projects of state educational institutions, considering limited resources and high data protection requirements.

The object of the study is the methods used to protect information security in IT projects within educational institutions.

The subject of the study is the task of selecting the optimal set of methods for ensuring information security, taking into account the limitations.

The purpose of this work is to analyze the main threats to the information security of IT projects in state educational institutions, study existing protection methods, and develop a combined method for choosing methods for ensuring information security in IT projects of state educational institutions.

This work includes a study of threats to the information security of IT projects and protection methods, the formulation of the limitations of the Pareto optimization method and proposal of a combined method for choosing methods for ensuring information security, and the experimental application of this method to an electronic document management system in a state educational institution.

The results obtained can be used to support decision-making related to information security in IT projects of public educational institutions and can be adapted to other types of IT projects.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ІБ – інформаційна безпека

ПЗ – програмне забезпечення

2FA – Two-factor authentication

CIA – Confidentiality, Integrity, Availability

DDoS – Distributed Denial of Service

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

MitM – Man-in-the-Middle

SIEM – Security Event and Incident Management

ВСТУП

Сучасні ІТ-проєкти дедалі більше інтегруються в інфраструктуру державних установ, зокрема у сфері освіти, де активно впроваджуються електронні сервіси, системи документообігу та платформи для навчання. Разом із зростанням цифровізації зростає і кількість інформаційних загроз, які можуть порушити конфіденційність, цілісність і доступність інформаційних систем.

Інформаційна безпека (ІБ) стала однією з ключових проблем у процесі планування, розробки та впровадження ІТ-продуктів. Особливо актуальною вона є для державних навчальних закладів, де обмежені ресурси ускладнюють використання складних та дорогих систем захисту. Водночас освітні ІТ-системи обробляють персональні дані здобувачів освіти, викладачів і співробітників, що робить їх привабливою ціллю для кібератак.

Наявні методи забезпечення ІБ відрізняються за вартістю, цільовими загрозами, від яких вони захищають, та складністю впровадження, тому важливо мати формалізований підхід до їх вибору з урахуванням специфіки конкретного ІТ-проєкту. Наразі більшість підходів до вибору засобів захисту ґрунтуються на суб’єктивних експертних оцінках або не враховують реальні обмеження, такі як бюджет чи терміни реалізації.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ

1.1 Аналіз загроз безпеці ІТ-проєктів державних навчальних закладів

1.1.1 Дослідження управління ризиками ІТ-проєктів

Управління ризиками в ІТ-проєктах – це частина життєвого циклу ІТ-проєкту, що допомагає мінімізувати негативні наслідки непередбачених подій та підвищити ймовірність успішного завершення проєкту.

Ризик – це невизначена подія або умова, яка, якщо вона відбудеться, може мати позитивний або негативний вплив на одну або більше цілей ІТ-проєкту, при цьому виявлені ризики можуть реалізуватись або реалзіуватись. Команди ІТ-проєкту намагаються визначити та оцінити відомі та нові ризики, як внутрішні, так і зовнішні щодо проєкту, протягом усього життєвого циклу [1]. Ризики можуть виникати як при виконанні проєкту, так і при експлуатації розробленого в результаті проєкту ІТ-продукту, тому необхідно визначити різницю між ІТ-проєктом та ІТ-продуктом.

ІТ-проєкт – це тимчасова діяльність, спрямована на створення унікального ІТ-продукту, послуги або результату в сфері інформаційних технологій. У ІТ-проєкту є визначений початок і кінець, конкретні цілі та обмеження щодо ресурсів і часу, наприклад, розробка нового програмного забезпечення або впровадження інформаційної системи є ІТ-проєктами [2].

ІТ-продукт – це результат ІТ-проєкту, який призначений для задоволення конкретних та визначених потреб користувачів або ринку. Як ІТ-проєкт ІТ-продукт має власний життєвий цикл, який включає етапи розробки, впровадження, підтримки та подальшого покращення. ІТ-продукт може існувати тривалий час після завершення ІТ-проєкту під час якого продукт було створено, і може потребувати постійного оновлення та вдосконалення відповідно до змін на ринку та вимог користувачів [2].

Існуючі ризики при експлуатації можна розділити на 4 типи.

Технічні ризики – це ризики, що напряму пов’язані з технологіями такими як програмне та апаратне забезпечення. В цей тип ризиків входить все, що стосується мережевої безпеки, різноманітних цифрових активів, системної безпеки та відповідності новим регулятивним вимогам. Наприклад, такими ризиками є збої програмного та апаратного забезпечення, витік даних, несумісність платформ.

Зовнішні ризики – це ризики, що виникають поза межами організації та часто є неконтрольованими. До цього типу ризиків відносять політичні, економічні, кліматичні або регуляторні зміни. Наприклад, в цю категорію можна віднести зміни у законодавстві, погодні умови, постачальники, ринок, вплив зацікавлених сторін, пандемії.

Організаційні ризики – це ризики, які є зумовленими внутрішніми процесами, ресурсами, культурою компанії та взаємодією між системами. Цей тип ризиків включає такі ризики як нестача ресурсів, зміни у пріоритетах, фінансування, взаємодія між системами, якість роботи.

Ризики управління проєктом пов’язані з процесами управління ІТ-проєктом, такими як планування, оцінка, комунікація та розробка контрактів. Цей тип ризиків напряму викликаний помилками в плануванні проєкту, наприклад, неточним оцінювання ресурсів або проблеми у комунікації між членами команди [3].

Управління ризиками включає не лише їх оцінку, а й наступне прийняття рішень про те, які ризики є можливість мінімізувати, уникнути або прийняти. Такий підхід вимагає постійного моніторингу та перегляду раніше визначених ризиків, так як зміни протягом життєвого циклу ІТ-проєкту та життєвого циклу ІТ-продукту можуть створювати нові ризики.

1.1.2 Дослідження інформаційної безпеки ІТ-проєкту та ІТ-продукту

Одним з критичних видів ризиків в ІТ-проєктах є ризики, пов’язані з ІБ. У сучасному технологічному середовищі, коли загрози постійно еволюціонують і набувають нових форм, до питання захисту інформації потрібно підходити комплексно і враховувати етап управління ІБ як необхідну складову виконання ІТ-проєкту та подальшого впровадження та використання ІТ-продукту.

ІБ – це стан захищеності ІТ-проєкту від інформаційних загроз, який визначається рівнем шкоди, що може бути заподіяна існуванню, функціонуванню чи діяльності проєкту в разі реалізації загроз [4].

Необхідно визначити, що хоч ІБ та кібербезпека є тісно пов’язаними, але все ж таки вони мають відмінності. ІБ охоплює всі аспекти захисту інформації, і є незалежною від носія чи середовища її зберігання та обробки. Кібербезпека, у свою чергу, є частиною ІБ, яка зосереджена саме на захисті інформації у цифровому просторі. Кібербезпека спрямована на запобігання загрозам, що виникають у кіберсередовищі, зокрема кібератакам, хакерським зломам, зловмисному програмному забезпеченню та іншим видам цифрових загроз.

Для визначення дій, які необхідно провести на етапі управління ІБ ІТ-проєкту, потрібно розрізняти поняття ІБ ІТ-проєкту і ІБ ІТ-продукту.

ІБ ІТ-проєкту фокусується на захисті даних, інформаційних систем і процесів під час реалізації та виконання ІТ-проєкту. Поняття забезпечення ІБ включає забезпечення конфіденційності, цілісності та доступності даних, а також мінімізацію ризиків, пов’язаних з інформаційними загрозами на всіх етапах виконання. Цей аспект безпеки охоплює управління ризиками, планування безпеки та застосування відповідних заходів для забезпечення безпеки даних і процесів у межах ІТ-проєкту [5].

ІБ ІТ-продукту зосереджена на захисті ІТ-продукту після завершення розробки ІТ-продукту та його впровадження. Цей тип безпеки включає в себе заходи, спрямовані на забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється ІТ-продуктом, після того як ІТ-продукт введено в експлуатацію і охоплює як захист даних у ІТ-продукті так і забезпечення безпеки користувачів і їх взаємодії з ІТ-продуктом [6].

Отже, хоча обидва типи безпеки мають на меті захист від загроз, безпека ІТ-проєкту охоплює весь процес його реалізації, а безпека ІТ-продукту – саме готовий ІТ-продукт після його розробки та впровадження.

Управління ІБ – це процес, спрямований на забезпечення захисту інформаційних систем, даних та інфраструктури від можливих загроз, атак, несанкціонованого доступу та інших ризиків, що можуть негативно вплинути на їхню функціональність, конфіденційність, цілісність та доступність. Управління ІБ включає в себе не тільки технічні засоби захисту, але й управлінські, організаційні та юридичні заходи, спрямовані на запобігання, виявлення та реагування на інциденти безпеки. Управління ІБ є невід'ємною частиною загального управління ризиками в ІТ-проєкті, оскільки дозволяє мінімізувати можливі загрози і знижувати негативний вплив на бізнес-процеси [1, 6].

Управління ІБ при експлуатації ІТ-проєкту фокусується на впровадженні заходів безпеки вже на етапі розробки ІТ-проєкту. Це включає в себе інтеграцію методів забезпечення безпеки в процесі розробки ІТ-проєкту.

Після того, як ІТ-продукт введено в експлуатацію, потрібно регулярно перевіряти та моніторити систему на наявність нових загроз і вразливостей. Це включає в себе постійну перевірку відповідності ІТ-продукту вимогам безпеки, оновлення програмного забезпечення та впровадження виправлень безпеки для усунення нововиявлених вразливостей та адаптації до нових загроз.

Отже, впровадження методів забезпечення ІБ ІТ-продукту відбувається протягом життєвого циклу ІТ-проєкту, але використання цих методів, їх оновлення та підтримка відбуваються в процесі експлуатації ІТ-продукту, отриманого в результаті виконання ІТ-проєкту.

1.1.3 Дослідження ризиків інформаційної безпеки ІТ-продукту

Загалом, ризики ІБ ІТ-проєкту стосуються небезпек, що з’являються під час самого процесу розробки, планування та впровадження проєкту. Вони можуть бути як організаційними, так і технічними, і можуть призвести до витоку, втрати або ушкодження інформації ще до запуску ІТ-продукту. Натомість ризики ІБ ІТ-продукту виникають після того, як продукт вже створено і можливо навіть введено в експлуатацію. Такі ризики пов’язані з реальним застосуванням системи, взаємодією з користувачами, зовнішніми серверами, мережами та іншими компонентами.

Отже, ризики ІБ ІТ-продукту – це можливі події або дії, які можуть призвести до порушення конфіденційності, цілісності та доступності даних та систем, що входять до складу ІТ-продукту [7]. Ці ризики можуть виникати в результаті зовнішніх чи внутрішніх загроз, а також технічних чи організаційних недоліків, що впливають на ІБ ІТ-продукту протягом його життєвого циклу.

Основні ризики ІБ для ІТ-продукту можна розділити на три наступні категорії.

Випадкові ризики – це ризики, що виникають через збіг обставин і можуть мати негативні наслідки, і є складнопрогнозованими. До типових прикладів такого типу ризиків належать вихід з ладу технічного обладнання,

надзвичайні ситуації, перебої в електропостачанні, пошкодження каналів зв’язку, поломка пристроїв блокування, що обмежують доступ до інформації.

Суб’єктивні ризики – ризики, що виникають через помилки або неналежні дії співробітників під час обробки чи зберігання даних. Сюди належить нехтування внутрішніми правилами та вимогами безпеки, розголошення конфіденційної інформації, несанкціонований доступ до даних, порушення правил передачі інформації, використання незахищених каналів зв’язку.

Об’єктивні ризики – це ті ризики, що виникають внаслідок проникнення в систему шкідливого програмного забезпечення, встановлення шпигунських пристроїв, тощо. Такий тип ризиків неможливо повністю усунути через постійне вдосконалення методів зловмисників і недосконаліть захисних систем, але можливо розробити різносторонню систему захисту від атак, яка допоможе мінімізувати наслідки у разі реалізації цього ризику.

Таким чином, розуміння ризиків ІБ та їх класифікація дозволяє сформувати уявлення про типові загрози ІБ. Проте протидія цим ризикам не буде повноцінною без завчасного впровадження відповідних заходів ще на етапі проєктування та реалізації ІТ-проєкту. Саме тому важливою частиною є дослідження процесу забезпечення ІБ в межах ІТ-проєкту, що містить планування, втілення та підтримку потрібних методів захисту протягом усього життєвого циклу ІТ-проєкту.

1.1.4 Дослідження процесу забезпечення інформаційної безпеки ІТ-проєкту

Визначення ризиків ІБ ІТ-продукту є необхідним етапом для забезпечення ІБ ІТ-продукту в майбутньому в експлуатації, проте цей крок не

гарантує повного усунення загроз. Для правильного управління ІБ необхідно планувати забезпечення ІБ методами, які забезпечують постійний контроль та реагування на можливі інциденти, ще на етапі виконання ІТ-проєкту.

Для забезпечення ІБ ІТ-проєкту на кожному етапі його життєвого циклу важливо здійснювати низку заходів, спрямованих на виявлення, оцінку та управління ризиками:

а) ініціювання;

1) з'ясування вимог до захисту даних та інформації, врахування юридичних та бізнес аспектів, включаючі вимоги до конфіденційності, цілісності та доступності даних;

2) ідентифікація можливих загроз, тобто первинний аналіз безпеки для виявлення можливих загроз, таких як внутрішні або зовнішні атаки, фізичні загрози чи недоліки в технологічній інфраструктурі;

б) планування;

1) оцінювання можливих загроз та вразливостей, які можуть виникнути під час реалізації проєкту, проведення аналізу ризиків, визначення їх ймовірності та серйозності, а також оцінку потенційного впливу на проєкт;

2) формування стратегії для мінімізації ризиків, вибір заходів контролю, зокрема для захисту даних та інформаційних систем;

в) виконання;

1) впровадження різних методів забезпечення ІБ таких як шифрування, контроль доступу, моніторинг мережі тощо;

2) оперативне виявлення та реагування на загрози, а також усунення виявлених вразливостей, отже постійний моніторинг проєкту дозволяє вчасно виявити порушення безпеки та швидко реагувати на них;

г) моніторинг і контроль;

1) моніторинг і перевірка того, наскільки добре реалізовані заходи безпеки, а також виявлення нових загроз або ризиків, що з'явились під час виконання проєкту;

2) коригування заходів безпеки, адаптація плану безпеки, додавання нових методів контролю або зміна існуючих стратегій для покращення рівня безпеки;

д) закриття;

1) оцінка результатів безпеки, тобто підсумковий огляд забезпечення ІБ в рамках ІТ-проєкту, перевірка коректності виконання всіх вимог щодо захисту інформації;

2) завершення процесів безпеки, передача прав доступу, якщо необхідно, а також відключення або захист будь-яких тимчасових систем, використаних у ІТ-проєкті.

1.1.5 Дослідження методів забезпечення інформаційної безпеки ІТ-проєктів державних навчальних закладів

Процес забезпечення ІБ ІТ-проєкту може відрізнятись в залежності від галузі, в якій він реалізується. Об’єктом дослідження кваліфікаційної роботи є державні навчальні заклади.

Державний навчальний заклад – це навчальний заклад, який надає освітні послуги на рівні вищої освіти, тобто готує фахівців за різними напрямами навчання та спеціальностями. Такі заклади здійснюють підготовку бакалаврів, магістрів та аспірантів у різних галузях знань і можуть бути як державними, так і приватними. Державні навчальні заклади зазвичай фінансуються з державного бюджету і підпорядковуються органам управління освіти.

Управління ІБ в державних навчальні заклади – це процес, який включає в себе розробку, впровадження та підтримку стратегій, політик, процедур і заходів, що забезпечують захист інформації та інформаційних систем в таких закладах. Це передбачає заходи з охорони конфіденційності, цілісності та доступності даних, що зберігаються, обробляються та передаються в цих установах. Управління ІБ в державних навчальних закладах є критично важливим для захисту персональних даних здобувачів вищої освіти, викладачів і адміністративного персоналу, а також для забезпечення безпеки наукових, навчальних і фінансових даних. Однак, реалізація цього процесу стикається з низкою специфічних загроз, характерних саме для ІТ-проєктів у сфері освіти, які відрізняються від особливостей загроз у комерційних або інших державних сферах.

По-перше, освітні ІТ-системи зберігають та обробляють конфіденційні дані, включаючи персональну інформацію здобувачів освіти, викладачів та адміністративного персоналу. Це робить їх привабливою мішенню для кіберзлочинців, які можуть намагатися викрасти, продати або використати ці дані для подальшого шахрайства.

По-друге, такі системи повинні гарантувати безперебійний доступ до освітніх ресурсів, електронних бібліотек, навчальних платформ та адміністративних сервісів. Будь-яка загроза, що впливає на доступність системи, може серйозно порушити навчальний процес та дискредитувати роботу закладу.

По-третє, через відкритість освітнього середовища та широку аудиторію користувачів (здобувачі освіти, викладачі, адміністрація) забезпечення ІБ стає складнішим. Велика кількість підключених пристроїв, відсутність суворого контролю доступу та різний рівень цифрової грамотності серед користувачів підвищують ризики фішингових атак, зараження вірусами та несанкціонованого доступу до системи.

По-четверте, обмежені бюджети державних навчальних закладів часто не дозволяють впроваджувати передові системи захисту, оновлювати програмне забезпечення або навчати персонал основам ІБ, що не дає можливості імплементувати високовартісні методи захисту на всі випадки, створює додаткові вразливості та ускладнює швидке реагування на нові загрози.

Управління ІБ ІТ-проєкту державного навчального закладу включає наступні етапи:

– оцінка ризиків – визначення можливих загроз та вразливостей, які можуть вплинути на інформаційні ресурси державного навчального закладу;

– розробка політик безпеки – створення чітких правил і процедур для забезпечення захисту інформації;

– захист інформаційних систем – забезпечення безпеки програмного та апаратного забезпечення, що використовуються для зберігання і обробки даних;

– навчання персоналу – підготовка співробітників навчального закладу до роботи з інформаційними системами;

– моніторинг та реагування на інциденти – стеження за станом безпеки та швидке реагування на інциденти, які можуть порушити інформаційну безпеку;

– оновлення та вдосконалення систем безпеки – постійне вдосконалення методів і технологій для підтримки високого рівня захисту інформаційних ресурсів.

1.2 Аналіз основних аспектів безпеки ІТ-проєктів

Сучасна ІБ ІТ-проєктів базується на фундаментальних принципах, які визначають ефективність захисту даних і систем від потенційних загроз. Однією з найважливіших концепцій у сфері ІБ є модель CIA (Confidentiality, Integrity, Availability), яка включає три ключові принципи [8]:

– конфіденційність – принцип спрямований на захист конфіденційної інформації від несанкціонованого доступу та розголошення, який гарантує, що лише авторизовані користувачі можуть і включає методи, які використовуються для збереження конфіденційності (шифрування, захист паролем, аутентифікація користувачів контроль доступу, впровадження суворої політики конфіденційності) [9];

– цілісність – принцип який гарантує, що інформація залишається точною, повною та узгодженою протягом усього життєвого циклу, що не дає неавторизованим користувачам змінювати, підробляти або видаляти дані, і методами, що забезпечують принцип цілісності є цифрові підписи, контроль версій, суворий контроль доступу і тп;

– доступність – принцип забезпечує доступ до інформації та систем авторизованим користувачам у разі потреби, має вирішальне значення для підтримки функціональності інформаційних систем, мінімізації часу простою та забезпечення доступу авторизованих користувачів до потрібних їм даних, так як системи, що забезпечують принцип доступності включають системи резервування, системи резервного копіювання, системи планування аварійного відновлення та системи для балансування мережевого навантаження.

Разом ці принципи утворюють комплексну структуру, яка допомагає ефективно організувати процеси забезпечення ІБ в проєкті. У контексті ІТ-проєктів державних навчальних закладів ці принципи набувають

особливого значення, оскільки такі проєкти обробляють великий обсяг конфіденційної інформації, забезпечують стабільність навчального процесу та потребують захисту від внутрішніх і зовнішніх загроз.

У випадку державних навчальних закладів принцип конфіденційності є одним з головних, так як системи державних навчальних закладів працюють з персональними даними здобувачів освіти, викладачів і співробітників. Захист цих даних є обов’язковим не лише з погляду етичних норм, а й через законодавчі вимоги, такі як Закон України «Про захист персональних даних».

Цілісність необхідна для забезпечення достовірності академічної інформації. Будь-які зміни в оцінках, дипломах або базах даних здобувачів освіти можуть призвести до компрометації репутації державного навчального закладу. Також забезпечення цілісності навчальних матеріалів у системах дистанційного навчання гарантує, що здобувачі освіти отримують правильну та актуальну інформацію.

Доступність є критично важливою для ІТ-проєктів державних навчальних закладів, оскільки навчальний процес залежить від безперебійного доступу до електронних бібліотек, систем управління навчанням, онлайн-курсів та адміністративних сервісів. Атаки на ІТ-інфраструктуру або технічні збої можуть паралізувати роботу державного навчального закладу, що буде мати негативний вплив на освітній процес.

1.3 Аналіз існуючих загроз та методів забезпечення безпеки в ІТ-проєктах державних навчальних закладів

1.3.1 Дослідження існуючих загроз

Протидія загрозам починається в першу чергу з їх ідентифікації, отже, потрібно розглянути найпоширеніші види загроз для ІТ-проєктів державних

навчальних закладів. Ці загрози можуть завдати значної шкоди як користувачам системи, так і самій інфраструктурі закладу. Вони реалізуються через вразливості в програмному забезпеченні, слабкі механізми аутентифікації, соціальну інженерію та інші методи атак. З метою ефективного управління ризиками необхідно дослідити основні технологічні загрози.

Шкідливе програмне забезпечення (ПЗ) (Malware) – це ПЗ, створене для несанкціонованого проникнення, пошкодження або порушення роботи інформаційних систем. Воно включає віруси, черв'яки, трояни, програми-вимагачі (ransomware) та шпигунське ПЗ (spyware) [10]. Основні цілі таких атак – крадіжка конфіденційної інформації, виведення системи з ладу або отримання нелегітимного доступу до ресурсів.

Атаки з використанням вразливостей нульового дня (Zero-Day Exploits) представляють собою атаки на невідомі раніше вразливості програмного і апаратного забезпечення, що не мають відповідних виправлень, через неоновлене програмне забезпечення [11].

Атаки на паролі – це атаки, в результаті яких злочинці отримують несанкціонований доступ до облікових записів шляхом перебору паролів (brute force), атак за словником (dictionary attacks) або реєстрації натискань клавіш (keylogging).

Атаки «Людина посередині» (Man-in-the-Middle, MitM) – це вид атак, які передбачають перехоплення комунікацій між двома сторонами з метою викрадення, підміни або маніпуляції переданою інформацією [12, 13]. Це може включати перехоплення мережевого трафіку, підробку сертифікатів безпеки та експлуатацію нешифрованих каналів зв'язку.

Розподілені атаки на відмову в обслуговуванні (Distributed Denial of Service, DDoS) – це вид атак, які виконуються шляхом масового перевантаження мережевих або серверних ресурсів та призводять до відмови у доступі для легітимних користувачів. Такі атаки – це зловмисна спроба

заблокувати доступ до сервісу, який надається через мережу. DDoS атаки можуть бути спрямовані як проти веб серверів так і проти мереж, а збитки від таких атак можуть вар’юватися від легких незручностей користувачів веб-сайту до серйозних фінансових втрат, або ж слугувати відволікаючим маневром для інших атак [14].

1.3.2 Дослідження методів забезпечення інформаційної безпеки ІТ-проєкту

Для забезпечення належного рівня захисту ІТ-проєктів, що будуть використовуватись у державних навчальних закладах, існує набір технічних та організаційних методів.

Технічні методи – це методи, які мають бути реалізовані в проєкті, починаючи від першої фази його життєвого циклу, та є спрямованими на захист мереж, серверів, баз даних та користувачів від загроз з боку зловмисників.

До технічних методів забезпечення ІБ ІТ-проєкту можна віднести:

– антивірусні та антишкідливі програми – це ПЗ, яке допомагає виявляти та знищувати віруси, троянські програми, шкідливі програми та інші види шкідливого ПЗ (malware), що може потрапити на комп'ютери та сервери. Антишпигунські програми забезпечують захист від шпигунського ПЗ, яке збирає персональні дані без відома користувача;

– фаєрволи – це системи (апаратні, програмні або комбіновані), що регулюють та контролюють трафік в інформаційних мережах, виконують функції фільтрації трафіку на основі попередньо встановлених правил і є першим бар'єром між внутрішніми системами і зовнішніми загрозами [15];

– шифрування – це метод, що захищає дані, які передаються через Інтернет, шляхом застосування алгоритму, який робить ці дані нечитабельними [16];

– системи виявлення вторгнень (Intrusion Detection System, IDS) – це системи, що моніторять мережу та аналізують трафік на наявність будь-якої підозрілої або незвичної активності, і при виявленні аномальних активностей сигналізують про це [17];

– системи запобігання вторгненням (Intrusion Prevention System, IPS) – це системи, що також можуть виявляти загрози, але вони також автоматично реагують на можливі виявлені атаки, блокуючи їх [18, 19];

– багатофакторна аутентифікація – це метод, що впроваджує кількарівневу аутентифікацію, маючи декілька рівнів перевірки таких, як комбінація пароля, код від мобільного додатку або смс, біометричні дані (відбитки пальців, розпізнавання обличчя тощо);

– бекапи та відновлення даних – це регулярне створення резервних копій даних захищає від втрати інформації в разі кібератак, збоїв обладнання або інших непередбачених ситуацій, і у випадку аварії бекапи дозволяють швидко відновити критично важливі дані та функціональність систем [20];

– мережевий моніторинг – це метод, що дозволяє виявляти аномалії або небажану активність у мережах (великі об'єми трафіку, підозрілі з'єднання);

– системи управління ІБ (Security Event and Incident Management, SIEM) – це системи, що збирають, зберігають і аналізують величезні обсяги інформації про події в мережі та системах для виявлення загроз, порушень безпеки або аномальних дій, зазвичай мають різноманітні надбудови для аналізу в основному безпекових даних [21].

ІТ-продукт у державних освітніх установах є кінцевим результатом розробки та впровадження ІТ-проєкту, що містить програмні, апаратні та організаційні компоненти. Проєктування ІТ-продукту передбачає аналіз вимог, вибір технологій, розробку, тестування та впровадження. На цьому

етапі потрібно закласти стратегію безпеки, оскільки на початкових стадіях вже можна запобігти деяким вразливостям, що можуть створювати загрози для даних та систем у майбутньому. Планування безпеки ІТ-продукту має відбуватися ще на етапі проєктування.

Також державні навчальні заклади мають відповідати вимогам законодавства у сфері захисту інформації, таких як закони України про кібербезпеку та захист персональних даних. Відповідність міжнародним стандартам забезпечує належний рівень захисту інформаційних систем та дозволяє запровадити кращі практики управління безпекою. Тільки комплексний підхід дозволяє створити надійну систему захисту, яка забезпечує безпеку даних, безперебійну роботу освітніх платформ державних навчальних закладів та зменшення ризиків несанкціонованого втручання. Надійний ІТ-продукт є комбінацією різноманітних методів забезпечення ІБ.

1.4 Постановка задачі дослідження

Після проведення аналізу загроз ІБ ІТ-проєктів у державних навчальних закладах виділено низку ключових аспектів, які необхідно врахувати. По-перше, основною проблемою є об’єктивні загрози ІБ, що виникають через зовнішні та внутрішні фактори, які не залежать від людських помилок. До таких загроз відносяться інформаційні атаки на освітні установи, уразливості у ПЗ, відсутність належного рівня захисту даних, збої у роботі інформаційних систем.

Додатковою проблемою є складність у забезпеченні належного рівня ІБ через недостатнє фінансування, застарілі технології та обмежені ресурси для впровадження сучасних методів захисту. Це може призвести до витоку конфіденційної інформації, втрати доступу до критично важливих даних,

компрометації навчального процесу та репутаційних втрат для освітніх установ.

Основними проблемами, що виникають під час управління безпекою ІТ-проєктів у державних освітніх установах, є:

– нечіткість вимог до безпеки – відсутність єдиних стандартів щодо захисту освітніх ІТ-систем;

– обмеженість ресурсів – державні навчальні заклади часто мають обмежене фінансування та неможливість впровадити всі можливі методи забезпечення ІБ;

– динамічність загроз – постійний розвиток технологій створює нові виклики для безпеки інформації, що ускладнює підтримку актуальності захисних заходів.

Проблеми, описані вище, дають змогу визначити предмет, об'єкт та мету даного дослідження.

Предметом дослідження в рамках кваліфікаційної роботи є процес вибору методів забезпечення ІБ в ІТ-проєктах державних освітніх закладів.

Об'єктом дослідження виступають методи захисту від загроз ІБ ІТ-проєкту державних навчальних закладів.

Метою даної роботи є аналіз основних загроз ІБ ІТ-проєктів у державних навчальних закладах, вивчення існуючих методів захисту та розробка комбінованого методу вибору методів забезпечення ІБ ІТ-проєктів державних навчальних закладів в умовах бюджетних обмежень.

Для досягнення мети кваліфікаційної роботи необхідно вирішити наступні задачі дослідження:

– проаналізувати існуючі методи забезпечення ІБ ІТ-проєктів;

– розробити класифікацію загроз ІБ ІТ-проєктів державних навчальних закладів та методи захисту від визначених загроз;

– розробити комбінований метод вибору методів забезпечення ІБ з урахуванням специфіки ІТ-проєктів державних навчальних закладів;

– експериментально перевірити отримані результати вирішення задачі вибору методів забезпечення ІБ ІТ-проєктів державних навчальних закладів.

2 РОЗРОБКА КОМБІНОВАНОГО МЕТОДУ ВИБОРУ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІТ-ПРОЄКТІВ ДЕРЖАВНИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

2.1 Аналіз методу оптимізації за Парето для вибору методів забезпечення інформаційної безпеки в ІТ-проєктах

Забезпечення ІБ сучасних ІТ-проєктів є складною багатофакторною задачею, особливо коли мова йде про проєкти в державному секторі, де ресурси є обмеженими, а вимоги до безпеки постійно зростають. Через це для вирішення багатофакторної задачі доцільним є використання методів багатокритеріальної оптимізації, що дозволяють приймати рішення з урахуванням кількох критеріїв одночасно.

Багатокритеріальна оптимізація – це розділ математичної оптимізації, яка займається задачами, в яких необхідно одночасно оптимізувати дві або більше цільових функції. У такому випадку покращення однієї з цільових функцій можливо лише за рахунок погіршення принаймні однієї іншої.

Оптимізація за Парето – це пошук таких комбінацій або рішень, при яких неможливо покращити будь-який аспект без погіршення іншого. Метою оптимізації за Парето є пошук оптимальних (домінуючих) точок. Оптимальними точками є значення, що не покращуються – точки, краще яких не можна підібрати за всіма критеріями.

Для формування Парето-фронту (множини Парето-оптимальних рішень) використовується алгоритм повного перебору комбінацій для створення потенційних рішень [22].

Застосування методу оптимізації за Парето для управління ІБ ІТ-проєктів має ряд вагомих переваг. По-перше, метод дозволяє комплексно враховувати різноманітні аспекти методів захисту без необхідності зведення їх до єдиного узагальненого критерію, що особливо важливо коли критерії

мають різну природу та одиниці вимірювання [23]. По-друге, метод забезпечує об'єктивність, оскільки не вимагає суб'єктивного визначення вагових коефіцієнтів для різних критеріїв на етапі формування множини оптимальних рішень. По-третє, такий метод оптимізації гарантує глобальну оптимальність вибраних рішень, тобто їхню недомінованість за всіма наявними критеріями.

В управління безпекою ІТ-проєктів державних навчальних закладів можливо виділити два основних критерії, що напряму впливають на визначення кінцевого набору методів захисту.

По-перше, здатність методу запобігати, виявляти або нейтралізувати різні категорії загроз. Цей критерій може вимірюватись як через кількість типів загроз, від яких захищає оцінюваний метод, так і через якісну оцінку експертів, щодо рівня захисту для кожного типу загроз.

Другим критерієм, що має вплив на кінцевий набір методів і є найбільш підходящими для оцінюваного проєкту, є вартість впровадження. Цей критерій включає всі прямі фінансові витрати на придбання, впровадження та підтримку методу захисту, адже вартість є одним з найбільш обмежуючих факторів, особливо для державних навчальних закладів з чітко визначеними бюджетами. Оцінювання витрат на впровадження кожного з методів має бути проведено безпосередньо перед початком вибору підходящого набору методів. Приблизне оцінювання проводиться проєктним менеджером або бізнес-аналітиком ІТ-проєкту задля отримання актуальної вартості впровадження та подальшого використання кожного методу.

Для вирішення поставленої задачі вибору методів забезпечення ІБ пропонується комбінований метод, результатом якого є сформована множина методів управління ІБ.

Множина методів захисту – це всі методи забезпечення ІБ, які є доступними для імплементації в ІТ-проєкті. Множину методів захисту можна представити формулою:

$$M = \{m_1, m_2, ..., m_k\}, \quad (2.1)$$

де M – множина методів захисту, що використовуються для усунення загроз;

m_j – j-ий метод захисту.

Метод m_j протидіє множині загроз $Z(m_j)$ з формулами:

$$Z = \{z_1, z_2, ..., z_n\}, \quad (2.2)$$

$$z_i \subseteq Z, \quad (2.3)$$

де Z – множина всіх загроз;

z_i – i-а загроза, $i \in \{1, 2, ..., n\}$.

Метод m_l домінує над методом m_t, за формулами:

$$|Z(m_l)| \geq |Z(m_t)|, \quad (2.4)$$

$$c_l \leq c_t, \quad (2.5)$$

де $Z(m_j)$ – множина загроз, які усуває метод m_j;

c_j – вартість впровадження методу m_j.

При цьому має виконуватись хоча б одна сувора нерівність принаймні за одним критерієм.

2.2 Проблеми використання методу оптимізації за Парето для управління безпекою ІТ-проєктів державних навчальних закладів

Метод оптимізації за Парето є методом, який дозволяє вирішити поставлену задачу багатокритеріальної оптимізації вибору методів забезпечення ІБ в ІТ-проєктах державних навчальних закладів, але однак цей метод також має недоліки.

Державні навчальні заклади України функціонують у специфічних умовах, що створює унікальні виклики для управління безпекою їхніх ІТ-проєктів. Незважаючи на теоретичну потужність методу оптимізації за Парето, його пряме застосування в цьому контексті стикається з рядом суттєвих обмежень та проблем.

У специфіці державних навчальних закладів прямий вплив на вибір методів забезпечення ІБ мають, в першу чергу, жорсткі бюджетні обмеження. Фінансування ІТ-проєктів та заходів з забезпечення ІБ здійснюється в межах обмеженого державного бюджету з чіткими процедурами контролю витрат, отже вартість впровадження методів захисту стає критичним фактором при прийнятті рішень.

У контексті цих особливостей класичний метод оптимізації за Парето демонструє ряд суттєвих обмежень таких, як проблема вибору кінцевого рішення, відсутність гарантії повного покриття загроз, складність оцінки та порівняння методів захисту.

Перше обмеження зумовлено тим, що метод оптимізації за Парето формує множину недомінованих рішень, але не дає однозначної відповіді, яке з них слід вибрати. При застосуванні оригінального методу оптимізації за Парето виникають труднощі з балансуванням між рівнем захисту та вартістю. Наприклад, для типового набору вхідних даних метод оптимізації може дати

кілька десятків Парето-оптимальних комбінацій методів захисту, що значно ускладнює процес вибору без залучення висококваліфікованих фахівців з ІБ.

Наступним обмеженням є відсутність гарантії повного покриття загроз, адже класичний метод оптимізації за Парето зосереджується на пошуку недомінованих рішень за обраними критеріями, але не гарантує, що ці рішення забезпечать захист від усіх критичних загроз, актуальних для державного навчального закладу.

При виборі методів вирішення задачі багатокритеріальної оптимізації необхідно враховувати, що рівень захисту як критерій має комплексний характер і складно піддається кількісній оцінці, особливо коли йдеться про різні типи загроз. Класичний метод оптимізації за Парето вимагає чітких кількісних оцінок, що створює труднощі при порівнянні методів.

Таким чином, хоча метод оптимізації за Парето теоретично є потужним інструментом для вирішення багатокритеріальної оптимізації, але його практичне застосування для управління ІБ ІТ-проєктів у державних навчальних закладах стикається зі значними обмеженнями, що вимагає розробки комбінованого методу, адаптованого до специфіки цієї предметної області.

2.3 Розробка комбінованого методу для вибору методів забезпечення інформаційної безпеки ІТ-проєктів державних навчальних закладів

Для подолання виявлених в попередньому розділі обмежень методу оптимізації за Парето для вибору методів управління ІБ ІТ-проєктів державних навчальних закладів пропонується комбінований метод, що забезпечує процес вибору методів з урахуванням трьох ключових критеріїв:

здатність методу запобігати, виявляти або нейтралізувати різні категорії загроз та вартість впровадження.

Запропонований комбінований метод базується на пріоритеті повного покриття загроз, бінарній моделі покриття загроз, жадібному алгоритмі вибору методів та явному врахуванні бюджетних обмежень.

На відміну від класичного підходу, який розглядає здатність методу запобігати, виявляти або нейтралізувати різні категорії загроз як один з багатьох рівнозначних критеріїв, у комбінованому методі обов’язковою умовою є повне покриття всіх критичних загроз та мінімізація вартості.

Для спрощення оцінки здатність методу запобігати, виявляти або нейтралізувати різні категорії загроз пропонується використовувати бінарну модель, де для кожної пари «метод-загроза» є два варіанти значення. У випадку, якщо метод захищає від конкретної загрози, то він має значення 1, тобто забезпечує. У випадку, якщо він не забезпечує захист від конкретного виду загроз, то він має значення 0.

Замість повного перебору всіх можливих комбінацій методів пропонується використовувати жадібний алгоритм, який послідовно додає методи з найкращим співвідношенням «нові покриті загрози/вартість». Жадібний алгоритм дає можливість поступово побудувати набір методів, при цьому обираючи найкращий з існуючих на кожній ітерації.

Комбінований метод безпосередньо враховує бюджетні та часові обмеження, які є характерними для державних навчальних закладів, і за рахунок раніше описаних концептів, що покращують результат, отриманий за допомогою методу оптимізації за Парето, формуючи набір методів у межах існуючих обмежень.

Отже, комбінований метод включає кілька ітерацій. Треба враховувати, що для його застосування мають бути попередньо визначені вхідні дані. Ці вхідні дані містять інформацію про існуючі загрози, від яких потрібно

захистити готовий ІТ-продукт, наявні методи захисту, вартість впровадження кожного з методів захисту та бюджетні обмеження реалізуємого ІТ-проєкту.

Використовуючи надані вхідні дані, потрібно розробити таблицю «Здатність методу усувати загрозу» (таблиця 2.1). На даному етапі необхідно залучити експертів, щоб отримати їхню оцінку, що має два можливі варіанти: 0, якщо метод не здатний усунути загрозу, 1, якщо здатний усунути.

Таблиця 2.1 – Бінарне представлення здатності методу усувати загрозу

	z_1	z_2	z_3	z_4	z_5
m_1 (Брандмауери)	1	0	0	0	0
m_2(Антивірусний захист)	0	1	0	0	0
m_3 (Багатофакторна аутентифікація)	0	0	1	0	0
m_4 (Шифрування даних)	0	0	0	1	0
m_5 (Системи резервного копіювання)	0	0	0	0	1
m_6(SIEM-система)	1	1	1	1	0
m_7 (Системи захисту від фішингу)	0	1	1	0	0
m_8 (Захищений доступ до мережі – VPN)	1	0	0	1	0

Після отримання від експертів оцінки здатності методів забезпечувати захист від кожного з видів загроз розпочинається перша ітерація. В першу чергу підраховується кількість покритих загроз для кожного методу і

розраховується співвідношення кількості загроз, від яких захищає метод, до його вартості, що була попередньо надана у вхідних даних.

Отримане значення показує, наскільки вартісним є метод відносно кількості загроз, від яких він забезпечує захист. За принципом жадібного алгоритму потрібно обрати метод з найвищим отриманим значенням. Обраний метод захисту додається до кінцевого набору методів, які будуть найбільш підходящими для забезпечення ІБ у визначених часових та бюджетних обмеженнях, і після цього розпочинається друга ітерація.

У другій ітерації необхідно оновити існуючу таблицю «Здатність методу запобігати, виявляти або нейтралізувати загрозу», заповнюючи її нулями у стовпцях загроз, від яких захищає метод, що було обрано у попередній ітерації, адже тепер ці загрози більше не є актуальними. Знову підраховується кількість покритих загроз для кожного методу і розраховуємо співвідношення кількості загроз, від яких захищає метод, до його вартості. За тим самим принципом жадібного алгоритму обирається метод з найбільшим значенням та додається в набір обраних методів. Процес ітерування має продовжуватись до моменту, поки всі можливі загрози не будуть усунуті обраним набором методів. Паралельно з розрахунком та вибором методів необхідно слідкувати за бюджетними та часовими обмеженнями. Якщо на якійсь з ітерацій вартість методу забезпечення ІБ буде перевищувати наявні ресурси, то необхідно прибрати його з таблиці «Здатність методу усувати загрозу».

Результатом використання комбінованого методу при умові, що часові та бюджетні обмеження є реалістичними, є набір методів, що будуть перекривати всі загрози ІБ ІТ-проєкта.

3 ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ РЕАЛІЗАЦІЇ КОМБІНОВАНОГО МЕТОДУ ПРИ ВИБОРІ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Розробка функції вигоди методу забезпечення інформаційної безпеки

Базуючись на результатах другого розділу пропонується комбінований метод для забезпечення ІБ з урахуванням специфіки державних ІТ-проєктів. Одним з основним елементів методу є функція вигоди, яка дозволяє порівняти методи за співвідношенням між кількістю загроз, що вони покривають, та вартістю їх впровадження.

Функція вигоди $U(m_j)$ для методу m_j визначається за формулою:

$$U(m_j) = \frac{|Z(m_j)|}{c(m_j)}, \quad (3.1)$$

де m_j – j-ий метод захисту;

$Z(m_j)$ – множина всіх загроз, від яких захищає метод m_j;

$c(m_j)$ – вартість впровадження методу m_j.

На кожній ітерації розробленого комбінованого методу обирається метод із максимальною функцією вигоди $U(m_j)$ серед усіх доступних методів, які не перевищують наявні бюджетні ресурси. Після вибору методу множина покритих загроз оновлюється, а підмножина $Z(m_j)$ для інших методів оновлюється через виключення загроз, яким протидіє вже обраний метод.

3.2 Схема застосування комбінованого методу

На першому кроці відбувається формування вхідних даних. На цьому етапі визначаються множина загроз та множина методів за формулою, що протидіять загрозам ІБ, що використовуються в подальших етапах. Множину загроз захисту можна представити формулою:

$$Z = \{z_1, z_2, ..., z_n\}, \tag{3.2}$$

де Z – множина всіх загроз;

z_i – i-а загроза, $i \in \{1, 2,..., n\}$.

Множину методів захисту можна представити формулою:

$$M = \{m_1, m_2, ..., m_k\}, \tag{3.3}$$

де M – множина методів захисту, що використовуються для усунення загроз;

m_j – j-ий метод захисту, $j \in \{1, 2,..., k\}$.

На другому кроці відбувається Парето-фільтрація, яка дозволяє прибрати методи, які точно мають гірші вхідні характеристики, ніж інші наявні.

Методи захисту оцінюються за двома критеріями, де перший – $|Z(m_j)|$, тобто кількість загроз, які усуває метод, і цей показник має максимізуватися, а другий –$c(m_j)$, тобто вартість впровадження методу, має мінімізуватися.

У Парето-фільтрації методів використовується концепція домінування.

Метод m_l домінує над методом m_t, якщо задовольняються задані нерівності:

$$\left|Z(m_l)\right| \geq \left|Z(m_t)\right|, \tag{3.4}$$

$$c(m_l) \leq c(m_t) \ , \tag{3.5}$$

де $Z(m_j)$ – множина загроз, які усуває метод m_j;

$c(m_j)$ – вартість впровадження методу m_j.

При цьому хоча б одна з цих нерівностей є строгою. Методи, які є меньш вигідними, виключаються з розгляду на цій ітерації.

На третьому кроці відбувається обчислення функції вигоди. Для кожного методу, що залишився після Парето-фільтрації, обчислюється функція вигоди за формулою (3.1).

Функція вигоди дозволяє оцінити метод захисту з урахуванням його здатності усувати загрози та його вартості впровадження.

Четвертий крок передбачає використання жадібного підходу для подальшого вибору методів. Для цього обирається метод із найбільшим значенням функції вигоди $U(m_j)$, його вартість має не перевищувати залишковий бюджет, цей метод додається до фінального набору методів захисту і загрози, що були усунуті обраним методом, більше не враховуються $Z(m_j)$.

Процес повторюється до повного покриття всіх загроз або вичерпання бюджету. Якщо бюджет вичерпано, вибір припиняється, а отриманий на цей момент набір методів забезпечення ІБ є найбільш вигідним у рамках встановленого бюджету.

4 ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА РОЗРОБЛЕНОГО КОМБІНОВАНОГО МЕТОДУ ВИБОРУ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1 Загальний опис ІТ-проєкту електронного документообігу у державному навчальному закладі

Для перевірки запропонованого комбінованого методу забезпечення ІБ проведено його застосування у ІТ-проєкті електронного документообігу в державному навчальному закладі.

Метою ІТ-проєкту є розробка та впровадження системи електронного документообігу із застосуванням методів забезпечення ІБ у державному навчальному закладі. Розроблена система дозволяє автоматизувати процес зберігання, підписання та обміну внутрішніми документами, забезпечити конфіденційність та цілісність збережених даних.

Функціонал системи включає функції створення користувачем документів, підписання документів, зберігання документів в електронному архів та сповіщення про будь-які зміни в статусі чи складі документа.

Забезпечення ІБ починається з визначення типів загроз. Для ІТ-проєкту електронного документообігу у державному навчальному закладі актуальними будуть загрози представлені в таблиці 4.1.

Таблиця 4.1 – Загрози для ІТ-проєкту електронного документообігу

Код загрози	Назва
z_1	Несанкціонований доступ до документів
z_2	Фішинг та крадіжка облікових даних
z_3	Вірусні атаки та шкідливе ПЗ

Кінець таблиці 4.1

Код загрози	Назва
z_4	Компрометація внутрішньої переписки
z_5	Втрата або пошкодження даних

Далі необхідно визначити множину, що включає методи забезпечення ІБ (таблиця 4.2), які можуть бути використані для захисту від виявлених загроз, та їх вартості.

Таблиця 4.2 – Методи забезпечення ІБ

Код заходу	Назва заходу	Вартість, грн
m_1	Антивірусне ПЗ	2000
m_2	VPN-доступ	4000
m_3	Аудит доступів	1000
m_4	Двофакторна аутентифікація (2FA)	5000
m_5	Шифрування бази даних	3000
m_6	Моніторинг внутрішнього листування	2000

Перед початком порівняння стандартного інтуїтивного методу та розробленого комбінованого методу необхідно описати здатності методу запобігати, виявляти або нейтралізувати загрози. Результати надано в таблиці 4.3, де 1 – це здатність методу m_j протидіяти загрозі z_i, а 0 – не здатність.

Таблиця 4.3 – Здатність методу усувати загрозу

	z_1	z_2	z_3	z_4	z_5	z_6
m_1	0	0	1	0	0	0
m_2	0	1	0	1	0	0
m_3	1	0	0	0	0	0
m_4	1	1	0	0	0	0
m_5	0	1	0	0	1	0
m_6	0	0	0	1	0	0

4.2 Порівняння розробленого комбінованого методу на ІТ-проєкті державного державного навчального закладу з класичним підходом

4.2.1 Аналіз вхідних даних на етапі вибору методів для ІТ-проєкту в державних навчальних закладах

Для порівняння звичайного методу вибору методів захисту з залученням експертів і розробленого комбінованого методу практично необхідно застосувати їх на тестових даних на двох альтернативах:

– альтернатива А, що включає експертне інтуїтивне прийняття рішення (традиційний підхід);

– альтернатива В, що демонструє використання комбінованого методу з попередньою Парето-фільтрацією, жадібним вибором та функцією вигоди.

Вхідними даними перед початком експерименту на етапі вибору методів є список загроз, методи забезпечення ІБ, а також їх вартість, що описано в таблиці 4.4. Ці дані будуть незмінні при тестуванні обох підходів.

Таблиця 4.4 – Вхідні дані ІТ-проєкту

Вхідні дані	Значення
Бюджет	10 000 грн

4.2.2 Аналіз результатів ефективності альтернативи А

В рамках альтернативи А рішення приймалися на основі попереднього досвіду окремих фахівців проєктної команди та типових підходів, які зазвичай застосовуються у схожих ІТ-проєктах державного сектору. Вибір відбувався швидко, без чіткої прив’язки до конкретних загроз чи багатокритеріального аналізу. Основною метою було вкластися в бюджет, використавши перевірені засоби захисту.

У підсумку команда обрала наступні методи:

– двофакторна аутентифікація (m_4) як основний інструмент захисту облікових записів, вартість методу склала 5000 грн;

– антивірусне ПЗ (m_1) як стандартний захист від шкідливого ПЗ, вартість методу склала 2000 грн;

– VPN-доступ (m_2) для безпечного з’єднання з системою поза межами мережі закладу, вартість методу склала 4000 грн.

Ці три методи разом покривали частину актуальних загроз, а їх сумарна вартість складала 11 000 грн, що перевищувало встановлений бюджет (10 000 грн). У зв’язку з цим було прийнято компромісне рішення виключити

VPN-доступ (m_2), що дозволило зменшити витрати до 7000 грн, однак водночас залишило деякі загрози без покриття.

Оскільки система вже була розроблена і впроваджена, а бюджет ІТ-проєкту було використано, то додаткові заходи не було дозволено впроваджувати. Через це частина загроз залишилась не усунутими. Як результат, хоча підхід до вибору методів забезпечення ІБ був швидким та зручним з точки зору планування, але відсутність системного підбору методів призвела до того, що не для всіх загроз було впроваджено протидію. Згодом це може призвести до репутаційних та правових наслідків у випадку реалізації якоїсь з загроз.

4.2.3 Аналіз результатів ефективності альтернативи В

В альтернативі В з такими ж вхідними даними було застосовано комбінований метод. Після аналізу таблиці «Здатність методу запобігати, виявляти або нейтралізувати загрозу» стало очевидно, що жоден метод не є домінованим, тобто всі методи $m_1 - m_6$ залишаються в Парето-фронті.

Наступним кроком було послідовне застосування жадібного алгоритму. Для кожного методу, що залишився, за формулою обчислюється функція вигоди:

$$U(m_j) = \frac{|Z(m_j)|}{c(m_j)}, \quad (4.1)$$

де m_j – j-ий метод захисту;

$Z(m_j)$ – множина всіх загроз, від яких захищає метод m_j;

$c(m_j)$ – вартість впровадження методу m_j.

Таблиця 4.5 – Ітерація 1 застосування жадібного алгоритму

Метод	Загрози	$\left\|Z(m_j)\right\|$	$c(m_j)$	$U(m_j)$
m_1	z_3	1	2000	0.00050
m_2	z_2, z_4	2	4000	0.00050
m_3	z_1	1	1000	0.00100
m_4	z_1, z_2	2	5000	0.00040
m_5	z_2, z_5	2	3000	0.00067
m_6	z_4	1	2000	0.00050

Обирається m_3, бо цей метод усуває z_1. Залишок бюджету складає 9000 грн.

Після ітерації 1 загрози z_2, z_3, z_4, z_5 не були усунуті обраними методами, тому потрібно перейти до наступної ітерації (таблиця 4.6).

Таблиця 4.6 – Ітерація 2 застосування жадібного алгоритму

Метод	Загрози	$\left\|Z(m_j)\right\|$	$c(m_j)$	$U(m_j)$
m_1	z_3	1	2000	0.00050
m_2	z_2, z_4	2	4000	0.00050
m_4	z_2	1	5000	0.00020

Кінець таблиці 4.6

Метод	Загрози	$\left\|Z(m_j)\right\|$	$c(m_j)$	$U(m_j)$
m_4	z_2	1	5000	0.00020
m_5	z_2, z_5	2	3000	0.00067
m_6	z_4	1	2000	0.00050

Обирається m_5 , бо цей метод усуває z_1. Залишок бюджету складає 6000 грн. На ітерації 2 загрози z_3, z_4 залишились не усунутими, тому потрібно перейти до наступної ітерації (таблиця 4.7).

Таблиця 4.7 – Ітерація 3 застосування жадібного алгоритму

Метод	Загрози	$\left\|Z(m_j)\right\|$	$c(m_j)$	$U(m_j)$
m_1	z_3	1	2000	0.00050
m_2	z_4	1	4000	0.00025
m_4		0	5000	0
m_6	z_4	1	2000	0.00050

Обирається m_6, бо цей метод усуває z_4 і є дешевшим у впровадженні за m_2. Залишок бюджету складає 6000 грн. На ітерації 3 загроза z_3 залишились не усунутою, тому потрібно перейти до наступної ітерації (таблиця 4.8).

Таблиця 4.8 – Ітерація 4 застосування жадібного алгоритму

Метод	Загрози	$\left\|Z(m_j)\right\|$	$c(m_j)$	$U(m_j)$
m_1	z_3	1	2000	0.00050

Обирається m_1, який усуває z_3, і залишок бюджету складає 2000 грн.

В результаті застосування розробленого комбінованого методу вибору заходів забезпечення ІБ було сформовано набір методів (таблиця 4.9), який забезпечує усунення всіх ідентифікованих загроз для ІТ-проєкту. На відміну від традиційного підходу, в якому рішення було прийнято суб’єктивно, використання розробленого комбінованого методу дозволило більш об’єктивно оцінити кожен метод за співвідношенням користі для виділеного набору загроз та вартості впровадження.

Таблиця 4.9 – Набір обраних методів

Код заходу	Назва заходу	Вартість, грн
m_1	Антивірусне ПЗ	2000
m_3	Аудит доступів	1000
m_5	Шифрування бази даних	3000
m_6	Моніторинг внутрішнього листування	2000

В розробленому комбінованому методі методи забезпечення ІБ спочатку фільтруються, а після цього використовується жадібний алгоритм до значень, отриманих в результаті розрахунків за функцією вигоди. Ця особливість дозволяє більш об’єктивно підбирати методи забезпечення ІБ. Жадібний алгоритм, що працює на основі залишкових загроз, поступово формує фінальний набір рішень, які створюють найкращій набір методів забезпечення ІБ у межах заданого бюджету.

У результаті сформований набір заходів дозволив не лише покрити всі загрози з першої спроби, але й уникнути повторних витрат, перевищення термінів реалізації та необхідності в екстрених доопрацюваннях через неперекриті загрози. Отриманий результат підтверджує доцільність застосування розробленого комбінованого методу для реальних ІТ-проєктів у сфері державної цифровізації, коли ресурси є обмеженими, а вимоги до безпеки – високими.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було проведено аналіз сучасних загроз для ІТ-проєктів державних навчальних закладів та методів забезпечення ІБ. Цей аналіз дозволив виявити недоліки методу вибору методів забезпечення ІБ з залученням експертів.

У межах дослідження було обґрунтовано актуальність проблеми вибору методів забезпечення ІБ в умовах обмежених ресурсів ІТ-проєктів, проаналізовано класифікацію загроз ІБ, досліджено існуючі технічні та організаційні методи захисту, а також розглянуто можливості їх застосування у ІТ-проєкті державного навчального закладу. Також у роботі було обґрунтовано необхідність формалізації підходу до прийняття рішень під час вибору методів захисту.

Для виконання завдання поставленого у роботі було проаналізовано існуючі методи забезпечення ІБ ІТ-проєктів, розроблено класифікацію загроз та методів усунення визначених загроз. Як результат було розроблено комбінований метод вибору методів забезпечення ІБ, що використовує функцію вигоди та жадібний алгоритм. Розроблений метод було протестовано на ІТ-проєкті державного навчального закладу, що включає розробку електронної системи документообігу. Результати застосування розробленого комбінованого методу на проєкті було порівняно з застосуванням традиційного підходу з залученням експертів.

Запропонований комбінований метод був апробований на прикладі реального ІТ-проєкту державного навчального закладу щодо впровадження системи електронного документообігу. В результаті експериментального дослідження було продемонстровано ефективність комбінованого підходу, який забезпечив повне покриття загроз при оптимальному використанні ресурсів.

Кваліфікаційна робота виконана відповідно до вимог методичних вказівок [25] та оформлена згідно зі стандартами [26].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. PMBOK. Encyclopedia of Education and Information Technologies. Cham, 2020. С. 1258. URL: https://doi.org/10.1007/978-3-030-10576-1_300500 (дата звернення: 18.05.2025).

2. Близнюкова І. О., Данченко О.Б., Тесленко П. О. Аналіз сучасних визначень ІТ-проектів "Управління проектами в умовах пандемії COVID-19": тези доповідей XVIII Міжнародної конференції (м. Київ, 15 травня 2021 р.)/ відпов. за випуск С.Д. Бушуєв. Київ: КНУБА, 2021. С. 100-103.

3. Risk Types in Project Management - Project Management Academy Resources. Project Management Academy Resources. URL: https://projectmanagementacademy.net/resources/blog/risk-types-in-project-management/ (дата звернення: 25.04.2025).

4. Архипов О.Є., Архипова Є.О. Особливості розуміння понять «інформаційна безпека» та «безпека інформації» / О.Є. Архипов, Є.О. Архипова // Информационные технологии и безопасность: основы обеспечения информационной безопасности (ИТБ-2014): Материалы XIV международной научнопрактической конференции. К.: ИПРИ НАН Украины, 2014. С.18-30.

5. ISO/IEC 27001:2013. Information Security Risk Management for ISO/IEC. На заміну ISO/IEC 27001:2005 ; чинний від 2013-10-01. Вид. офіц. 2013. 37 с.

6. Anderson R., Anderson R. J. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020. 1232 с.

7. Поліщук Д. В. Модель оцінки ризиків інформаційної системи / Д. В. Поліщук, М. В. Захарова, М. В. Люта // Сучасні електромеханічні та інформаційні системи : монографія / за заг. ред. І. В. Панасюка. Київ : КНУТД, 2021. С. 102-106.

8. Nweke L. O. Using the CIA and AAA models to explain cybersecurity activities. PM World Journal. 2017. Т. 6, № 12.

9. Гончарова І.П. Кібербезпека в цифровому освітньому середовищі закладів професійної освіти: електронний навчальний курс / І.П. Гончарова, Біла Церква, БІНПО ДЗВО «УМО» НАПН УКРАЇНИ, 2022. 80 с.

10. A. P. Namanya, A. Cullen, I. U. Awan and J. P. Disso, "The World of Malware: An Overview," 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, Spain, 2018, pp. 420-427, doi: 10.1109/FiCloud.2018.00067.

11. Waheed, A.; Seegolam, B.; Jowaheer, M. F.; Sze, C. L. X.; Hua, E. T. F.; Sindiramutty, S. R. Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure. 2024,. https://doi.org/10.20944/preprints202407.2338.v1

12. Mallik A. MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. Cyberspace: Jurnal Pendidikan Teknologi Informasi. 2019. Т. 2, № 2. С. 109. URL: https://doi.org/10.22373/cj.v2i2.3453 (дата звернення: 29.04.2025).

13. Raikar, M.M., Odeyar, P., Gupta, A., Priyanka, S.H., Tandur, A. Secure Communication in Vehicle-to-Grid Networks: A Study on Man in the Middle Attack Mitigation, Emerging Electronics and Automation, Singapore, 2025.

14. DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments / M. K. Hasan та ін. Energy Reports. 2023. Т. 9. С. 1318–1326. URL: https://doi.org/10.1016/j.egyr.2023.05.184 (дата звернення: 30.04.2025).

15. Використання фаєрволів як важливих компонентів системи безпеки вебсайтів та додатків / С. ЯЦЮК та ін. Herald of Khmelnytskyi National University. Technical sciences. 2025. Т. 349, № 2. С. 500–504. URL: https://doi.org/10.31891/2307-5732-2025-349-73 (дата звернення: 07.05.2025).

16. Increasing the level of security of internet things network systems due to encryption of data on devices with limited computer systems / R. Chernenko та ін.

Cybersecurity: Education, Science, Technique. 2021. Т. 3, № 11. С. 124–135. URL: https://doi.org/10.28925/2663-4023.2021.11.124135 (дата звернення: 10.05.2025).

17. Mohammad Aljanabi, Mohd Arfian Ismail Intrusion Detection: A Review. Mesopotamian Journal of Cyber Security. 2021. С. 1–4. URL: https://doi.org/10.58496/mjcs/2021/001 (дата звернення: 29.05.2025).

18. Safana Hyder Abbas, Wedad Abdul Khuder Naser, Amal Abbas Kadhim. Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Global Journal of Engineering and Technology Advances. 2023. Т. 14, № 2. С. 155–158

19. Радоуцька А. К., Панфьорова І.Ю. Дослідження методів виявлення аномалій у трафіку комп'ютерних мереж освітніх закладів. Радіоелектроніка та молодь у XXI столітті: матеріали міжнар. молодіжного форуму. м. Харків. 16 – 18 квітня 2025 р. Харків. 2025. С. 192–194.

20. Data Backup Strategies in Disaster Recovery: Ensuring Minimal Downtime. https://www.researchgate.net/publication/383276577_Data_Backup_Strategies_in_Disaster_Recovery_Ensuring_Minimal_Downtime. URL: https://www.researchgate.net/publication/383276577_Data_Backup_Strategies_in_Disaster_Recovery_Ensuring_Minimal_Downtime (дата звернення: 16.05.2025).

21. ДОСЛІДЖЕННЯ СУЧАСНОГО СТАНУ SIEM-СИСТЕМ / Т. Смірнова та ін. Кібербезпека: освіта, наука, техніка, 2024. Т. 1, № 25. С. 6–18. URL: https://doi.org/10.28925/2663-4023.2024.25.618

22. Любченко В. В., Берлізов Є. В. Алгоритм знаходження парето-оптимального рішення задачі наступного релізу. Электротехничні и компьютерні системи. 2015. № 19. С. 165–168.

23. I. B. Sirodgea, A. Ya. Kuzomin, M. V. Shtukin. Багатокритериальна оптимізація в інтелектуальних системах підтримки прийняття рішень. Реєстрація, зберігання і обробка даних. 2012. Т. 14, № 2. С. 106–115. URL:

https://doi.org/10.35681/1560-9189.2012.14.2.105057 (дата звернення: 16.05.2025).

24. Методичні вказівки щодо розробки та оформлення кваліфікаційної роботи другого (магістерського) рівня вищої освіти за освітньо-науковою програмою «Управління проектами в галузі інформаційних технологій» / Упоряд.: Петров К.Е., Левикін В.М., Чалий С.Ф., Євланов М.В., Міхнов Д.К., Міхнова А.В., Чала О.В. Харків: ХНУРЕ, 2025. 24 с.

25. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура і правила оформлювання. Чинний від 22.06.2015. Київ: ДП «УкрНДНЦ», 2016. 31 с.

26. ДСТУ 8302:2015. Інформація та документація. Бібліографічні посилання. Загальні положення та правила складаня. – Чинний від 04.03.2016. Київ: ДП «УкрНДНЦ», 2016. 20 с.