



DOI 10.28925/2663-4023.2026.35.1453

УДК 004.056:519.85

Стадник Марія Андріївна

кандидат технічних наук, доцент

доцент кафедри кібербезпеки

Тернопільський національний технічний університет імені Івана Пулюя, м. Тернопіль, Україна

ORCID: 0000-0002-0287-2254

stadnyk_m@tntu.edu.ua

Тимошук Дмитро Іванович

доктор філософії

старший викладач кафедри кібербезпеки

Тернопільський національний технічний університет імені Івана Пулюя, м. Тернопіль, Україна

ORCID: 0000-0003-0246-2236

dmytro.tymoshchuk@tntu.edu.ua

Деркач Марина Володимирівна

кандидат технічних наук, доцент

доцент кафедри кібербезпеки

Тернопільський національний технічний університет імені Івана Пулюя, м. Тернопіль, Україна

ORCID: 0000-0001-8977-2776

m_derkach@tntu.edu.ua

МАТЕМАТИЧНА МОДЕЛЬ ПРІОРИТЕЗАЦІЇ ВІДНОВЛЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ПІСЛЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОЦЕСАХ ЗАБЕЗПЕЧЕННЯ НЕПЕРЕРВНОСТІ БІЗНЕСУ

Анотація. У статті досліджено та формалізовано задачу оптимального планування робіт із відновлення інформаційних систем і пов'язаних безпекових перевірок після інцидентів інформаційної безпеки в межах процесів забезпечення неперервності бізнесу з урахуванням технологічних залежностей, обмеженості ресурсів і цільових показників часу відновлення (RTO). Обґрунтовано доцільність застосування математичних методів оптимізації для визначення пріоритетів відновлення з урахуванням бізнес-критичності систем, часових характеристик і вимог інформаційної безпеки. Проаналізовано наявні підходи до планування відновлення та визначено необхідність комплексного врахування ресурсних обмежень, технологічних залежностей і безпекових перевірок. Запропоновано математичну модель на основі змішаночислового лінійного програмування, спрямовану на мінімізацію зваженої тривалості простою інформаційних систем і штрафів за перевищення RTO. Особливістю моделі є розмежування технічного відновлення та безпекової перевірки як взаємопов'язаних операцій з їх спільною оптимізацією, що дозволяє визначати момент безпечного повернення систем до експлуатації. Розроблено алгоритм формування оптимального плану з урахуванням доступності ресурсів і технологічних залежностей. Проведено обчислювальний експеримент на прикладі шести взаємозалежних інформаційних систем. Встановлено зменшення значення цільової функції на 1,14 % порівняно з евристичними стратегіями RTO-first та Criticality-first. Абляційний експеримент показав зниження значення цільової функції на 42,89 % порівняно з реалізованим двоетапним підходом та скорочення кількості систем із порушеним RTO з чотирьох до однієї. Аналіз чутливості підтвердив суттєвий вплив доступності ресурсів і тривалості безпекових перевірок на характеристики відновлення. Практичне значення результатів полягає в можливості використання моделі для обґрунтування пріоритетів відновлення інформаційних систем, раціонального розподілу обмежених ресурсів і підтримки управлінських рішень у процесах забезпечення неперервності бізнесу.

Ключові слова: інформаційна безпека, інциденти інформаційної безпеки, неперервність бізнесу, відновлення інформаційних систем, управління IT-проектами, календарне планування проектів, пріоритезація відновлення, математична оптимізація, змішаночислове лінійне програмування, RTO, ресурсні обмеження, безпекові перевірки



ВСТУП

Сучасний розвиток цифрових технологій супроводжується зростанням залежності організацій від інформаційних систем, хмарних сервісів та інтегрованої інформаційно-комунікаційної інфраструктури. Порушення їх функціонування внаслідок інцидентів інформаційної безпеки може спричиняти переривання критичних бізнес-процесів, фінансові втрати та зниження операційної стійкості організацій. Дослідження [1, 2] підтверджують важливість урахування впливу IT-інцидентів на діяльність організацій та впровадження механізмів забезпечення неперервності бізнесу.

Управління неперервністю бізнесу (Business Continuity Management, BCM) спрямоване на підтримання критичних функцій організації та відновлення її діяльності після виникнення несприятливих подій. Ефективність зазначених процесів значною мірою залежить від їх узгодження з вимогами інформаційної безпеки, оскільки відновлення доступності інформаційних ресурсів повинно супроводжуватися забезпеченням їхньої цілісності та захищеності. Взаємозв'язок управління неперервністю бізнесу та інформаційної безпеки досліджено в роботі [3], тоді як багаторівневі механізми забезпечення неперервності та аварійного відновлення розглянуто в [4].

Особливої складності набуває відновлення інформаційних систем після кіберінцидентів, зокрема атак програм-вимагачів, компрометації облікових записів та несанкціонованої модифікації даних. На відміну від традиційних технічних відмов, такі інциденти потребують не лише відновлення працездатності систем, але й локалізації загроз, перевірки цілісності інформаційних ресурсів та підтвердження безпечності їх повернення до продуктивного середовища. Дослідження кіберстійкості [5, 6] підкреслюють важливість комплексного реагування на кіберзагрози, а роботи [7, 8] розглядають підходи до відновлення функціонування систем після кібератак.

Додатковими чинниками, що ускладнюють процес відновлення, є технологічні залежності між інформаційними системами та обмеженість доступних ресурсів. Функціонування критичних бізнес-сервісів може залежати від доступності баз даних, мережевої інфраструктури, служб автентифікації та інтеграційних компонентів. Необхідність урахування взаємозалежностей під час планування відновлення обґрунтовано в дослідженнях [9, 10]. Питання оптимізації відновлення за умов часткової втрати функціональності та різних сценаріїв прийняття рішень розглянуто в [11, 12]. Водночас математичні методи координації відновлювальних операцій і розподілу ресурсів досліджуються в роботах [13, 14], а спільна оптимізація планування та використання відновлювальних ресурсів представлена в [15].

Таким чином, ефективне відновлення інформаційних систем після інцидентів інформаційної безпеки потребує комплексного підходу, що поєднує управління інцидентами, забезпечення інформаційної безпеки та управління неперервністю бізнесу. Застосування математичного моделювання дозволяє формалізувати процес визначення послідовності відновлювальних операцій з урахуванням бізнес-критичності, технологічних залежностей, часових і ресурсних обмежень та вимог безпечного повернення систем до експлуатації.

Наукова новизна дослідження полягає в удосконаленні математичної моделі плану відновлення взаємозалежних інформаційних систем після інцидентів інформаційної безпеки шляхом інтеграції операцій технічного відновлення та перевірки безпекової готовності в єдину задачу змішаночислової лінійної оптимізації. Особливістю запропонованого підходу є формалізація безпекової перевірки як окремої операції з визначеними часовими характеристиками, ресурсними потребами та умовами виконання, а також використання моменту її завершення для оцінювання фактичного часу повернення інформаційної системи до експлуатації та дотримання встановленого RTO. Такий підхід забезпечує формування ресурсно допустимого розкладу відновлення з урахуванням технологічних залежностей, бізнес-критичності інформаційних систем і вимог інформаційної безпеки.

Постановка проблеми. У практиці управління неперервністю бізнесу одним із ключових показників є RTO, який визначає допустимий часовий орієнтир відновлення відповідної діяльності або сервісу. Водночас визначення черговості відновлення виключно на основі RTO чи критичності окремих інформаційних систем не гарантує ефективного використання ресурсів і мінімізації сукупних втрат від простою. Зокрема, система з найвищою бізнес-критичністю може залежати від функціонування інших компонентів, відновлення яких потребує додаткового часу та залучення обмежених технічних ресурсів. Необхідність урахування взаємозалежностей під час планування відновлювальних заходів підтверджується результатами досліджень [9, 10].

Додаткові обмеження виникають у разі відновлення після кіберінцидентів, коли технічна готовність інформаційної системи не завжди означає можливість її безпечного повернення до експлуатації. Компрометація облікових записів, порушення цілісності даних або наявність шкідливого програмного забезпечення потребують проведення додаткових перевірок та усунення наслідків інциденту. Відповідно, передчасне відновлення взаємодії між інформаційними системами може створювати ризики повторної



компрометації. Важливість узгодження заходів інформаційної безпеки з процесами забезпечення неперервності бізнесу та відновлення після кіберінцидентів розглядається в роботах [3, 7].

Таким чином, виникає суперечність між необхідністю максимально швидкого відновлення критичних бізнес-функцій та потребою дотримання технологічних, ресурсних і безпекових обмежень. Пріоритезація відновлення за окремими показниками не завжди дозволяє врахувати сукупний вплив зазначених чинників на кінцевий результат. Це зумовлює необхідність переходу від визначення статичного рейтингу критичності інформаційних систем до формування допустимого розкладу відновлювальних операцій, у якому враховуються часові характеристики, взаємозалежності та умови безпечного повернення систем до продуктивного середовища.

Наукова проблема дослідження полягає в недостатній формалізації процесу планування відновлення інформаційних систем після інцидентів інформаційної безпеки з одночасним урахуванням їхньої бізнес-критичності, часових обмежень, технологічних залежностей, доступності ресурсів та вимог безпечного повернення до експлуатації. Її вирішення потребує розроблення математичної моделі, яка забезпечуватиме визначення оптимальної послідовності відновлювальних операцій із мінімізацією негативного впливу простою інформаційних систем на критичні бізнес-процеси.

Важливим аспектом є розмежування технічної готовності інформаційної системи та її готовності до безпечної експлуатації. Завершення технічного відновлення не завжди забезпечує можливість негайного повернення системи до продуктивного середовища через необхідність перевірки цілісності даних, виявлення залишкових ознак компрометації та підтвердження відповідності вимогам інформаційної безпеки. Неврахування таких операцій може призводити до заниження фактичного часу відновлення та нерационального розподілу ресурсів. Це обґрунтовує необхідність інтегрованого математичного планування технічного відновлення та безпекових перевірок з урахуванням часових, технологічних і ресурсних обмежень.

Аналіз останніх досліджень і публікацій. Питання забезпечення неперервності бізнесу, управління інцидентами інформаційної безпеки та відновлення інформаційних систем досліджуються в межах декількох взаємопов'язаних наукових напрямів. Зокрема, J. Järveläinen [1] досліджує вплив інцидентів інформаційних технологій на діяльність організацій та роль механізмів забезпечення неперервності бізнесу в зменшенні їхніх наслідків. У роботі M. Niemimäa та співавторів [2] розглянуто стійкість бізнес-моделей до порушень операційної діяльності. Зазначені дослідження обґрунтовують необхідність узгодження відновлення інформаційних ресурсів із потребами бізнесу, проте не зосереджуються безпосередньо на математичному визначенні послідовності відновлювальних операцій після кіберінцидентів.

Взаємозв'язок інформаційної безпеки та управління неперервністю бізнесу досліджено J. Järveläinen [3], зокрема в контексті міжорганізаційних інформаційно-технологічних відносин. G. Stamenkov [4] запропонував багаторівневу модель забезпечення неперервності бізнесу та аварійного відновлення, орієнтовану на узгодження відповідних організаційних і технічних заходів. Водночас ці роботи переважно формують концептуальну й організаційну основу управління відновленням, тоді як питання оптимізації конкретного розкладу відновлення інформаційних систем потребує окремого математичного опрацювання.

Окремий напрям досліджень присвячено кількісному оцінюванню кіберстійкості та відновленню після цілеспрямованих кібератак. S. M. AlHidaifi та співавтори [5] запропонували підхід до кількісного оцінювання кіберстійкості IT-інфраструктури. У дослідженні [6] розглянуто організаційні аспекти формування та реалізації кіберстійкості. Особливої уваги заслуговує робота С. Y. Chiu [7], у якій відновлення після ransomware-атак розглядається не лише як відновлення даних із резервних копій, а як процес повернення мінімально необхідної виробничої спроможності з урахуванням довіри до компонентів, технологічних залежностей та умов безпечного функціонування. Цей підхід є важливим для дослідження відновлення інформаційних систем після інцидентів інформаційної безпеки, оскільки підкреслює відмінність між технічною працездатністю системи та можливістю її безпечної експлуатації.

Суттєвий розвиток математичних методів планування відновлення представлено в дослідженнях взаємозалежних інфраструктурних мереж. Y. Almoghatwi, K. Barker та L. A. Albert [9] запропонували багатокритеріальну модель на основі змішаночислового програмування, спрямовану на підвищення стійкості взаємозалежних інфраструктурних систем та мінімізацію витрат на їх відновлення. Модель враховує часові й ресурсні обмеження, а також розподіл відновлювальних бригад між операціями. У роботі J. Zhou та співавторів [10] досліджено оптимізацію відновлення залежних мережесистем за умов каскадних відмов. Автори показали, що характеристики міжсистемних залежностей впливають на ефективність стратегій пріоритезації відновлення. Таким чином, зазначені дослідження підтверджують доцільність використання оптимізаційних моделей замість визначення черговості відновлення виключно за статичними показниками критичності.



Подальший розвиток цього напрямку пов'язаний з урахуванням часткового відновлення функціональності, різних умов прийняття рішень та координації доступних ресурсів. У роботі Y. Almoghatwī та співавторів [11] розглянуто оптимізацію відновлення структури взаємозалежних мереж за умов часткового порушення їх функціонування. М. Ху та співавтори [12] дослідили відновлення взаємозалежних інфраструктурних систем у різних середовищах прийняття рішень. A. Rangrazjeddi, A. D. González та K. Barker [13] запропонували теоретико-ігровий алгоритм координації відновлення в децентралізованому середовищі, де учасники можуть мати відмінні цільові функції. Такі дослідження розширюють можливості математичного планування відновлення, однак їхні постановки орієнтовані переважно на функціонування фізичних інфраструктурних мереж і не визначають як центральний предмет дослідження безпекові умови повернення корпоративних інформаційних систем до продуктивного середовища після компрометації.

Аналіз наукових публікацій засвідчує наявність розвинених підходів до управління неперервністю бізнесу, оцінювання кіберстійкості та оптимізації відновлення взаємозалежних систем. Водночас розглянуті роботи не дають достатніх підстав вважати повністю вирішеною задачу формування оптимального розкладу відновлення корпоративних інформаційних систем після інцидентів інформаційної безпеки за одночасного врахування бізнес-критичності, цільового часу відновлення, технологічних залежностей, ресурсних обмежень та умов безпечного повернення систем до експлуатації. Це визначає доцільність розроблення математичної моделі, у якій вимоги інформаційної безпеки формалізуються як обов'язкові обмеження процесу відновлення, а послідовність виконання операцій визначається на основі мінімізації негативного впливу простою на критичні бізнес-процеси.

Мета статті. Метою статті є розроблення математичної моделі пріоритезації та календарного планування відновлення взаємозалежних інформаційних систем після інцидентів інформаційної безпеки, яка забезпечує визначення послідовності й часових характеристик технічного відновлення та безпекових перевірок з урахуванням бізнес-критичності систем, RTO, технологічних залежностей і ресурсних обмежень для мінімізації негативного впливу простою на процеси забезпечення неперервності бізнесу.

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

- провести аналіз існуючих підходів до пріоритезації та планування відновлення інформаційних систем після інцидентів інформаційної безпеки;
- визначити основні параметри та обмеження, що впливають на послідовність відновлення інформаційних систем;
- розробити математичну модель пріоритезації відновлення інформаційних систем з урахуванням бізнес-критичності, RTO, технологічних залежностей, ресурсних обмежень та вимог інформаційної безпеки;
- сформулювати алгоритм визначення оптимальної послідовності відновлювальних операцій на основі запропонованої математичної моделі;
- провести обчислювальний експеримент на прикладі модельної IT-інфраструктури з визначеними характеристиками інформаційних систем та сценарієм інциденту інформаційної безпеки;
- порівняти результати застосування запропонованої моделі з підходами, що базуються на пріоритетності RTO та бізнес-критичності інформаційних систем;
- оцінити ефективність запропонованої моделі за показниками тривалості відновлення, порушення цільового часу відновлення та сукупних втрат від простою інформаційних систем;
- дослідити вплив інтегрованого врахування операцій безпекової перевірки на характеристики розкладу відновлення інформаційних систем шляхом порівняння запропонованої моделі з базовою постановкою календарного планування, у якій безпекові перевірки не включено до початкового оптимізаційного розкладу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для визначення послідовності відновлення інформаційних систем після інцидентів інформаційної безпеки запропоновано концептуальну модель, яка поєднує процеси управління інцидентами інформаційної безпеки, управління інформаційною безпекою та управління неперервністю бізнесу з урахуванням технологічних залежностей між системами й ресурсних обмежень. Основною метою моделі є формування обґрунтованого плану відновлення інформаційних систем, спрямованого на мінімізацію негативного впливу їх простою на критичні бізнес-процеси. Структуру запропонованої концептуальної моделі наведено на рис. 1.

У межах запропонованої моделі управління інцидентами інформаційної безпеки забезпечує визначення уражених інформаційних систем, характеру порушення та поточного стану відновлення.

Управління інформаційною безпекою формує вимоги до безпечного повернення систем до експлуатації, включаючи перевірку цілісності даних, усунення наслідків компрометації та виконання необхідних заходів захисту. Управління неперервністю бізнесу визначає бізнес-критичність інформаційних систем, RTO та потенційні втрати від простою, що формують основу для оцінювання пріоритетності відновлювальних операцій.

Важливими складовими моделі є технологічні залежності між інформаційними системами та ресурсні обмеження, які визначають допустиму послідовність відновлення, можливість паралельного виконання операцій та потребу в технічних і людських ресурсах. Їх урахування забезпечує формування реалістичного плану відновлення відповідно до наявних можливостей організації.

Центральним компонентом моделі є математична оптимізація послідовності відновлення, що передбачає мінімізацію негативного впливу простою інформаційних систем на бізнес-процеси з дотриманням часових, технологічних, ресурсних і безпекових обмежень. Результатом оптимізації є план відновлення інформаційних систем, який визначає послідовність і часові характеристики відновлювальних операцій з урахуванням вимог інформаційної безпеки та пріоритетів неперервності бізнесу.



Рис. 1. Концептуальна модель пріоритезації відновлення інформаційних систем після інцидентів

Таким чином, концептуальна модель формує основу для математичної постановки задачі пріоритезації відновлення інформаційних систем, що передбачає формалізацію вхідних параметрів, змінних рішення, цільової функції та системи обмежень.

Математична модель пріоритезації відновлення інформаційних систем після інцидентів

Для визначення оптимальної послідовності відновлення інформаційних систем після інцидентів інформаційної безпеки запропоновано математичну модель, яка враховує бізнес-критичність систем, RTO, технологічні залежності, обмеженість ресурсів та вимоги безпечного повернення систем до експлуатації.

За своєю математичною постановкою розглянута задача належить до розширеного класу задач календарного планування за обмежених ресурсів (Resource-Constrained Project Scheduling Problem, RCPSP). Задачі цього класу передбачають визначення часу виконання взаємозалежних операцій з урахуванням їхньої тривалості, технологічних залежностей та доступності ресурсів [16]. Подібні оптимізаційні підходи застосовуються для планування відновлення взаємозалежних інфраструктурних мереж з урахуванням ресурсних обмежень і розподілу відновлювальних команд [9].

З позицій управління IT-проектами процес відновлення інформаційних систем після інциденту інформаційної безпеки може розглядатися як комплекс взаємопов'язаних робіт, що характеризуються визначеною тривалістю, технологічними залежностями, ресурсними потребами та часовими обмеженнями. Планування такого комплексу робіт передбачає координацію діяльності технічних фахівців, команд інформаційної безпеки та відповідальних за забезпечення неперервності бізнесу. Застосування підходів календарного планування проектів із ресурсними обмеженнями дозволяє формалізувати послідовність виконання відновлювальних операцій, визначати можливості їх паралельного виконання та забезпечувати раціональний розподіл доступних ресурсів. Водночас специфіка відновлення після кіберінцидентів зумовлює необхідність доповнення традиційних моделей проектного



планування вимогами щодо бізнес-критичності інформаційних систем, дотримання RTO та підтвердження безпекової готовності перед поверненням систем до експлуатації.

У межах запропонованої моделі розрізняються два стани готовності інформаційної системи: технічна готовність, що досягається після завершення відповідних відновлювальних операцій, та готовність до безпечної експлуатації, яка додатково потребує завершення визначених безпекових перевірок. При цьому завершення технічного відновлення не розглядається як достатня умова повернення системи до продуктивного середовища. Момент допустимого відновлення її експлуатації визначається з урахуванням завершення обох етапів і виконання встановлених технологічних залежностей. Такий підхід дозволяє безпосередньо пов'язати вимоги інформаційної безпеки з часовими характеристиками оптимізаційного розкладу та оцінюванням дотримання RTO.

Нехай множина інформаційних систем, які потребують відновлення, визначається таким чином:

$$I = \{1, 2, \dots, n\}, \quad (1)$$

де n – кількість інформаційних систем, уражених наслідком інциденту інформаційної безпеки. Для кожної інформаційної системи $i \in I$ визначаються параметри наведені в таблиці 1.

Таблиця 1

Вхідні параметри математичної моделі

Позначення	Характеристика
w_i	Коефіцієнт бізнес-критичності системи
p_i	Тривалість технічного відновлення
v_i	Тривалість безпекової перевірки
RTO_i	RTO інформаційної системи
a_i	Найраніший допустимий момент початку відновлення
r_i	Ресурсна потреба технічного відновлення
q_i	Ресурсна потреба безпекової перевірки
R	Загальна кількість доступних ресурсних одиниць
λ	Коефіцієнт штрафу за перевищення RTO

Для формування плану відновлення вводяться змінні s_i – момент початку технічного відновлення, C_i^{tech} – момент завершення технічного відновлення, u_i – момент початку безпекової перевірки та C_i^{safe} – момент завершення перевірки й дозволеного повернення системи до експлуатації.

Тривалість технічного відновлення визначається співвідношенням:

$$C_i^{tech} = s_i + p_i, \quad \forall i \in I. \quad (2)$$

Безпекова перевірка може розпочинатися лише після завершення технічного відновлення:

$$u_i \geq C_i^{tech}, \quad \forall i \in I. \quad (3)$$

Момент безпечного повернення інформаційної системи до експлуатації визначається як:

$$C_i^{safe} = u_i + v_i, \quad \forall i \in I. \quad (4)$$

Таким чином, навіть після завершення технічного відновлення інформаційна система залишається недоступною для бізнес-процесів до завершення необхідних безпекових перевірок. У межах моделі передбачається, що ці перевірки завершуються позитивним результатом. У разі виявлення повторної компрометації параметри відновлення потребують перегляду.

Для оцінювання дотримання часових вимог використовується показник перевищення RTO:

$$T_i = \max(0, C_i^{safe} - RTO_i), \quad \forall i \in I, \quad (5)$$

де T_i – тривалість перевищення RTO. Важливо, що дотримання RTO оцінюється відносно моменту безпечного повернення системи до експлуатації, а не завершення її технічного відновлення. Часові параметри відраховуються від моменту виникнення інциденту, прийнятого за початок відліку.



Цільова функція математичної моделі передбачає мінімізацію зваженої тривалості простою інформаційних систем та штрафу за перевищення RTO:

$$\min Z = \sum_{i=1}^n w_i C_i^{safe} + \lambda \sum_{i=1}^n w_i T_i, \quad (6)$$

Перший компонент цільової функції характеризує сукупний зважений простій інформаційних систем, тоді як другий враховує додатковий негативний вплив порушення RTO. Коефіцієнт w_i відображає відносну бізнес-критичність системи. Якщо його значення визначається на основі грошових втрат за одиницю часу, цільова функція може використовуватися для оцінювання економічних наслідків простою.

Для забезпечення допустимості сформованого плану відновлення встановлюється система часових, технологічних, ресурсних і безпекових обмежень.

Обмеження початку відновлення визначає найраніший допустимий момент виконання технічних операцій:

$$s_i \geq a_i, \quad \forall i \in I. \quad (7)$$

Параметр a_i встановлюється на основі результатів реагування на інцидент інформаційної безпеки та характеризує момент, після якого дозволяється розпочати відновлення відповідної системи. Це дозволяє виключити плани, що передбачають виконання відновлювальних операцій до завершення необхідних заходів локалізації загрози.

Технологічні залежності між інформаційними системами представимо орієнтованим графом:

$$G = (I, E), \quad (8)$$

де E – множина залежностей між інформаційними системами. Наявність зв'язку $(i, j) \in E$ означає, що система j залежить від функціонування системи i . Для врахування таких залежностей встановлюється обмеження:

$$C_j^{safe} \geq C_i^{safe}, \quad \forall (i, j) \in E. \quad (9)$$

Наведене обмеження забезпечує дотримання допустимого порядку повернення взаємозалежних інформаційних систем до експлуатації. При цьому технічне відновлення та безпекові перевірки можуть виконуватися паралельно за наявності необхідних ресурсів. Для застосування моделі передбачається, що граф технологічних залежностей не містить циклів.

Ресурсні обмеження враховують необхідність залучення фахівців і технічних засобів як для відновлення, так і для безпекової перевірки. У межах моделі розглядається спільний обмежений ресурс із загальною доступною потужністю R . Для кожного моменту часу t встановлюється умова:

$$\sum_{i \in I: s_i \leq t \leq C_i^{tech}} r_i + \sum_{i \in I: u_i \leq t \leq C_i^{safe}} q_i \leq R, \quad \forall t \geq 0. \quad (10)$$

Перший доданок визначає ресурси, залучені до технічного відновлення, а другий — ресурси, необхідні для проведення безпекових перевірок. Таким чином, одночасне виконання зазначених операцій допускається лише за умови, що сумарна потреба в ресурсах не перевищує наявних можливостей організації. У межах дослідження передбачається, що кожна операція виконується без переривання, а її ресурсна потреба залишається сталою протягом виконання. Додатково встановлюються умови невід'ємності часових змінних:

$$s_i, C_j^{tech}, u_i, C_i^{safe}, T_i \geq 0, \quad \forall i \in I. \quad (11)$$

Для застосування методів лінійної оптимізації співвідношення (5) може бути представлене системою обмежень:

$$T_i \geq C_i^{safe} - RTO_i, \quad \forall i \in I. \quad (12)$$

За умови мінімізації цільової функції (6) з додатними вагами w_i та коефіцієнтом λ значення T_i відповідатиме фактичному перевищенню RTO. Для дискретного представлення часу моменти початку та завершення операцій додатково обмежуються обраним часовим кроком.

Таким чином, цільова функція (6) та система обмежень (2)–(5), (7)–(12) формують математичну модель пріоритизації відновлення інформаційних систем після інцидентів інформаційної безпеки.

Запропонована модель розширює постановку задачі календарного планування відновлювальних операцій шляхом окремого врахування технічного відновлення та перевірки безпекової готовності інформаційних систем. Це дозволяє врахувати тривалість і ресурсні потреби обох етапів, а також їхній вплив на фактичний момент повернення систем до експлуатації.

Результатом розв'язання оптимізаційної задачі є план, який визначає моменти початку та завершення технічного відновлення, проведення безпекових перевірок і безпечного повернення кожної інформаційної системи до експлуатації. Отриманий план спрямований на мінімізацію зваженого простого систем та перевищення RTO за дотримання технологічних, ресурсних і безпекових обмежень.

Алгоритм визначення оптимальної послідовності відновлення інформаційних систем

Для практичного застосування запропонованої математичної моделі розроблено алгоритм визначення оптимальної послідовності відновлення інформаційних систем після інцидентів інформаційної безпеки. Алгоритм передбачає послідовне формування вхідних даних, встановлення технологічних, ресурсних і безпекових обмежень, формування та розв'язання оптимізаційної задачі, а також отримання плану відновлення. Його основою є мінімізація цільової функції (6) за умови дотримання обмежень.

Для розв'язання оптимізаційної задачі використовується метод змішаночислового лінійного програмування (Mixed-Integer Linear Programming, MILP), який дозволяє визначати часові характеристики взаємозалежних операцій за обмежених ресурсів. Застосування цього методу передбачає дискретизацію часу та введення бінарних змінних, що визначають моменти початку технічного відновлення й безпекових перевірок інформаційних систем. Послідовність основних етапів алгоритму наведено на рис. 2

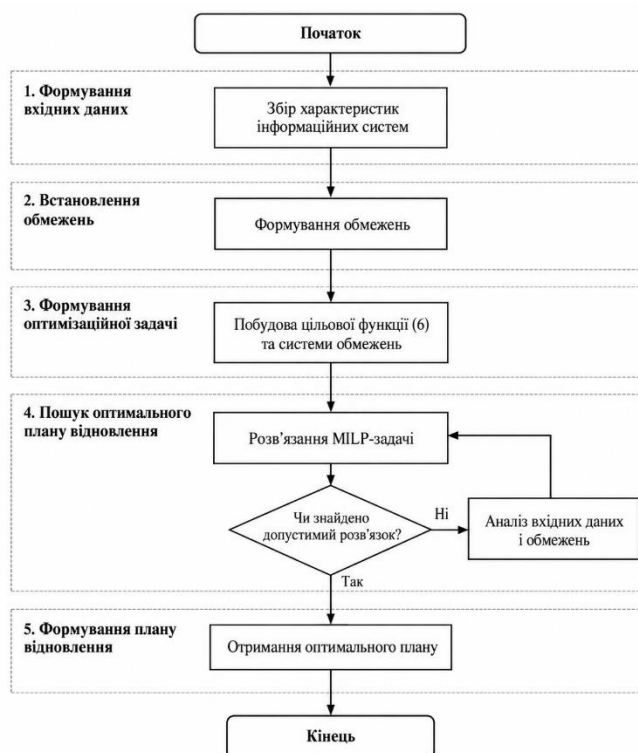


Рис. 2. Блок-схема алгоритму визначення оптимальної послідовності відновлення інформаційних систем

На першому етапі здійснюється формування вхідних даних: визначаються бізнес-критичність інформаційних систем, RTO, тривалість технічного відновлення та безпекових перевірок, а також потреба в ресурсах.

Другий етап передбачає встановлення обмежень на основі технологічних залежностей між системами, найраніших допустимих моментів початку відновлення та доступних ресурсів. Це забезпечує дотримання вимог інформаційної безпеки й допустимого порядку повернення систем до експлуатації.



На третьому етапі здійснюється формування оптимізаційної задачі на основі цільової функції (6) та встановленої системи обмежень. Для кожної інформаційної системи розглядаються дві послідовні операції: технічне відновлення та перевірка безпекової готовності. У межах дискретного часового горизонту вводяться бінарні змінні x_{it} та y_{it} , які набувають значення 1, якщо відповідна операція розпочинається в момент часу t , і 0 – в іншому випадку. Додаткові обмеження забезпечують одноразове виконання кожної операції, дотримання встановленої послідовності та неперевищення доступних ресурсів. Сформована MILP-задача забезпечує врахування тривалості операцій, технологічних залежностей, доступності ресурсів і вимог безпечного повернення інформаційних систем до експлуатації.

Четвертий етап передбачає пошук оптимального плану відновлення методом MILP. Оптимізатор визначає часові характеристики операцій, що забезпечують мінімізацію цільової функції. Якщо допустимого розв'язку не знайдено, здійснюється перевірка вхідних даних, часового горизонту та встановлених обмежень із подальшим повторним розв'язанням задачі.

На п'ятому етапі здійснюється формування плану відновлення, який містить моменти початку та завершення технічного відновлення, проведення безпекових перевірок і повернення кожної системи до експлуатації. Додатково визначаються показники перевищення RTO та значення цільової функції.

Таким чином, запропонований алгоритм забезпечує формування оптимізованого плану відновлення інформаційних систем з урахуванням бізнес-пріоритетів, технологічних залежностей, ресурсних обмежень і вимог інформаційної безпеки.

Постановка та умови обчислювального експерименту

Для перевірки працездатності запропонованої математичної моделі сформовано обчислювальний експеримент на основі сценарію інциденту інформаційної безпеки. Експеримент передбачає відновлення шести взаємопов'язаних інформаційних систем організації за умов обмеженості ресурсів, наявності технологічних залежностей та необхідності проведення безпекових перевірок перед поверненням систем до експлуатації.

Модельна IT-інфраструктура включає систему керування базами даних (DB), систему управління ідентифікацією та доступом (IAM), систему планування ресурсів підприємства (ERP), систему управління взаємовідносинами з клієнтами (CRM), вебпортал (Portal) та аналітичну систему (Analytics). Розглядається сценарій кібератаки, внаслідок якої порушено доступність зазначених систем. Для кожної з них визначено бізнес-критичність, RTO, тривалість технічного відновлення, тривалість безпекової перевірки, найраніший допустимий момент початку відновлення та потребу в ресурсах. Вхідні параметри наведено в табл. 2.

Таблиця 2

Вхідні параметри модельної IT-інфраструктури

Інформаційна система	w_i	p_i , год	v_i , год	a_i , год	r_i	q_i	RTO_i , год
DB	5	4	2	0	2	1	8
IAM	5	2	1	0	1	1	4
ERP	5	5	2	1	2	1	12
CRM	4	4	2	1	2	1	12
Portal	3	3	1	2	1	1	16
Analytics	2	4	1	2	1	1	24

Коефіцієнт бізнес-критичності визначається за п'ятибальною шкалою, де більше значення відповідає вищій значущості інформаційної системи для бізнес-процесів. Усі часові параметри виражено в годинах від початку інциденту. Технологічні залежності між системами зображені на рис. 3.

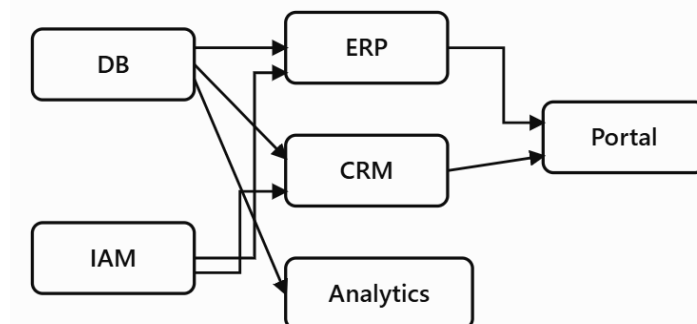


Рис. 3. Граф технологічних залежностей між інформаційними системами



У межах експерименту загальна кількість доступних ресурсних одиниць становить $R = 3$. Технічне відновлення окремих систем потребує від однієї до двох ресурсних одиниць, тоді як безпекова перевірка кожної системи – однієї ресурсної одиниці. Паралельне виконання операцій допускається за умови дотримання встановлених ресурсних обмежень.

Для розв'язання оптимізаційної задачі передбачено використання MILP-оптимізатора з дискретним представленням часу. Крок дискретизації становить одну годину, часовий горизонт планування – 26 годин, а коефіцієнт штрафу за перевищення RTO прийнято рівним $\lambda = 2$. Програмна реалізація виконана з використанням мови Python та бібліотеки SciPy з оптимізатором HiGHS.

Для порівняльного оцінювання визначено три стратегії планування відновлення. Перша передбачає мінімізацію цільової функції (6) методом MILP. Друга ґрунтується на підході RTO-first, за якого пріоритет надається системам із меншим значенням RTO. Третя використовує підхід Criticality-first, відповідно до якого першочергово розглядаються системи з вищим коефіцієнтом бізнес-критичності.

Для забезпечення коректності порівняння всі три стратегії використовують однакові вхідні параметри, технологічні залежності, ресурсні та безпекові обмеження. Ефективність сформованих планів оцінюється за значенням цільової функції, зваженою тривалістю простою, сумарним зваженим перевищенням RTO, кількістю систем із порушенням RTO та загальною тривалістю відновлення IT-інфраструктури. Відповідно сформований експериментальний сценарій дозволяє оцінити можливості запропонованої математичної моделі щодо визначення послідовності відновлення інформаційних систем та порівняти її ефективність із базовими стратегіями пріоритезації.

Оцінювання ефективності запропонованої математичної моделі

Для оцінювання ефективності запропонованої математичної моделі проведено обчислювальний експеримент із використанням параметрів шести інформаційних систем, наведених у табл. 2, та уточненого графа технологічних залежностей. Оптимізаційну задачу розв'язано методом MILP за допомогою оптимізатора HiGHS. Для прийнятих параметрів отримано оптимальне значення цільової функції $Z = 261$, що підтверджено результатом роботи оптимізатора з нульовим розривом оптимальності. Отримані результати наведено в табл. 3. Для кожної інформаційної системи визначено часові інтервали технічного відновлення та безпекової перевірки, момент безпечного повернення до експлуатації й величину перевищення RTO.

Таблиця 3

Результати оптимізації процесу відновлення інформаційних систем

Інформаційна система	$s_i - C_i^{tech}$, год	$u_i - C_i^{safe}$, год	C_i^{safe} , год	T_i , год
DB	0-4	4-6	6	0
IAM	0-2	2-3	3	0
ERP	4-9	9-11	11	0
CRM	9-13	13-15	15	3
Portal	6-9	14-15	15	0
Analytics	11-15	15-16	16	0

Аналіз отриманого плану показує, що відновлення інформаційних систем здійснюється з можливістю паралельного виконання операцій за умови дотримання ресурсних обмежень. Зокрема, технічне відновлення DB та IAM розпочинається одночасно, оскільки їхня сукупна потреба в ресурсах не перевищує встановленої місткості. Після завершення технічного відновлення IAM виконується її безпекова перевірка, а звільнені ресурси поступово залучаються до відновлення інших систем.

Особливістю сформованого плану є можливість виконання технічного відновлення залежних систем до моменту завершення всіх операцій із системами-попередниками. Наприклад, технічне відновлення Portal виконується в інтервалі 6–9 годин, тоді як ERP та CRM ще перебувають у процесі відновлення. Водночас безпечне повернення Portal до експлуатації відбувається лише на 15-й годині, після завершення безпекових перевірок ERP та CRM. Такий підхід дозволяє використовувати доступні ресурси без порушення встановлених технологічних залежностей.

Часову структуру отриманого плану відновлення наведено на рис. 4.

Як видно з рис. 4, сформований план передбачає послідовне використання обмежених ресурсів із можливістю паралельного виконання технічних і безпекових операцій. Загальна тривалість відновлення становить 16 годин. П'ять із шести інформаційних систем повертаються до експлуатації в межах установлених RTO. Для CRM спостерігається перевищення допустимого часу відновлення на 3 години.

Для кількісного оцінювання отриманого плану розраховано зважену тривалість простою інформаційних систем:

$$D = \sum_{i=1}^n w_i C_i^{safe} = 237. \quad (13)$$

Сумарне зважене перевищення RTO становить:

$$P = \sum_{i=1}^n w_i T_i = 12. \quad (14)$$

Відповідно значення цільової функції дорівнює $Z = D + \lambda P = 237 + 2 * 12 = 261$.

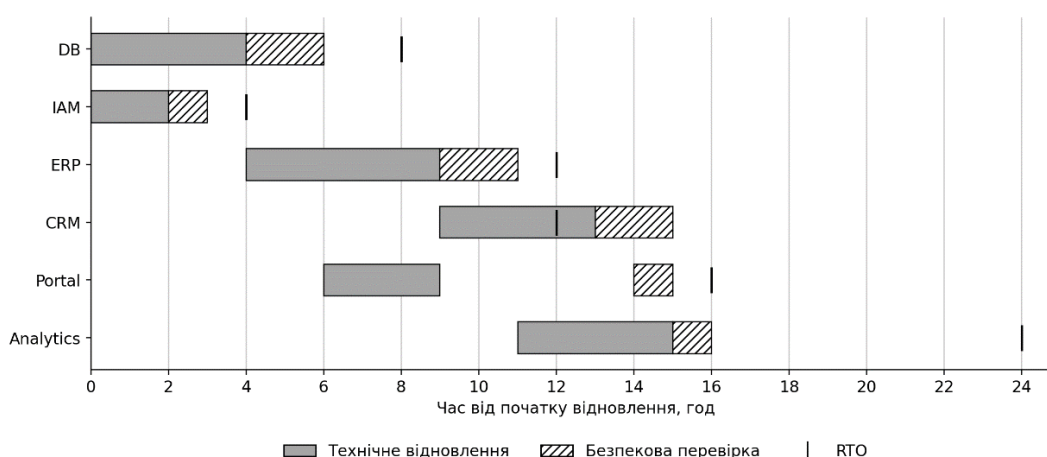


Рис. 4. Часова діаграма відновлення інформаційних систем за результатами MILP-оптимізації

Отже, основну складову цільової функції формує зважена тривалість простою інформаційних систем, тоді як штрафна складова враховує порушення встановленого RTO для CRM. Це дозволяє оцінювати ефективність відновлення не лише за моментом завершення всіх операцій, а й за впливом недоступності окремих систем на бізнес-процеси підприємства.

Для порівняльного оцінювання запропонованої математичної моделі розглянуто дві евристичні стратегії формування плану відновлення: RTO-first та Criticality-first. Перша стратегія передбачає визначення пріоритетності систем за зростанням встановленого RTO, тоді як друга – за спаданням коефіцієнта бізнес-критичності. За рівності основного критерію використовується другий критерій, а за подальшої рівності – алфавітний порядок назв систем.

Для забезпечення порівняльності результатів усі стратегії розглядаються за однакових вхідних параметрів, ресурсних обмежень, технологічних залежностей і вимог до безпекових перевірок. На відміну від MILP, евристичні підходи формують план на основі попередньо визначеного порядку пріоритетності, не здійснюючи глобальної мінімізації цільової функції. Результати порівняння наведено в табл. 4.

Таблиця 4

Порівняння ефективності стратегій відновлення інформаційних систем			
Показник	MILP	RTO-first	Criticality-first
D	237	240	240
P	12	12	12
Z	261	264	264
$N_{RTO} (\sum_i 1(T_i > 0))$	1	1	1
$\max_i C_i^{safe}$	16	16	16

За результатами експерименту запропонована математична модель забезпечила зменшення значення цільової функції на 1,14 % порівняно з евристичними стратегіями. Покращення досягнуто завдяки скороченню зваженої тривалості простою інформаційних систем із 240 до 237 умовних одиниць. Водночас показники перевищення RTO та загальної тривалості відновлення залишилися однаковими.

Однакові значення цільової функції для стратегій RTO-first та Criticality-first свідчать про те, що в межах розглянутого сценарію використання різних правил визначення пріоритетності не призводить до відмінностей за сукупними показниками ефективності. Водночас це не означає еквівалентності зазначених



стратегій для інших конфігурацій інформаційних систем, оскільки їхні результати можуть залежати від співвідношення бізнес-критичності, RTO, тривалості операцій і технологічних залежностей.

Важливою перевагою запропонованої математичної моделі є можливість формування оптимального плану з одночасним урахуванням декількох взаємопов'язаних чинників. На відміну від евристичних стратегій, які використовують локальні правила визначення пріоритетності, MILP дозволяє знаходити план, що мінімізує комплексний критерій ефективності в межах заданих обмежень. При цьому момент повернення інформаційної системи до експлуатації визначається не лише завершенням технічного відновлення, а й успішним виконанням безпекової перевірки.

Для оцінювання впливу інтегрованого врахування безпекових перевірок на ефективність відновлення інформаційних систем проведено абляційний обчислювальний експеримент (ablation study) на основі модельної IT-інфраструктури із шести взаємозалежних систем, характеристики яких наведено в табл. 2.

У межах експерименту порівняно два підходи до календарного планування. Перший передбачає двоетапне формування розкладу, за якого спочатку оптимізується та фіксується послідовність технічного відновлення, після чого плануються обов'язкові безпекові перевірки. Другий ґрунтується на запропонованій MILP-моделі, що забезпечує спільну оптимізацію технічних і безпекових операцій. Обидва підходи використовують однакові вхідні параметри, технологічні залежності та ресурсні обмеження, а повернення систем до експлуатації допускається лише після завершення безпекових перевірок.

Ефективність сформованих розкладів оцінено за зваженою тривалістю простою, перевищенням RTO, значенням цільової функції, кількістю систем із порушенням RTO та загальною тривалістю відновлення. Результати порівняння наведено в табл. 5.

Таблиця 5

Результати абляційного експерименту з оцінювання впливу інтегрованого планування безпекових перевірок

Показник	MILP	Двоетапне планування
D	237	313
P	12	72
Z	261	457
$N_{RTO} (\sum_i 1(T_i > 0))$	1	4
$\max_i C_i^{safe}$	16	15

Результати абляційного експерименту показали, що для дослідженого сценарію інтегроване планування технічного відновлення та безпекових перевірок забезпечує зменшення значення цільової функції з 457 до 261, або на 42,89 %, порівняно з реалізованим двоетапним підходом. Зважена тривалість простою інформаційних систем скоротилася з 313 до 237 умовних одиниць, а сумарне зважене перевищення RTO із 72 до 12. Кількість систем із порушенням RTO зменшилася з чотирьох до однієї.

Отримані відмінності зумовлені особливостями розподілу ресурсів між відновлювальними операціями. За двоетапного планування технічний розклад формується без урахування подальших ресурсних потреб безпекових перевірок, що може спричинити затримки повернення систем до експлуатації. Натомість інтегрована MILP-модель забезпечує узгоджене планування обох етапів з урахуванням бізнес-критичності систем, технологічних залежностей і часових обмежень.

Водночас загальна тривалість відновлення за інтегрованого підходу становила 16 годин проти 15 годин для двоетапного планування. Це свідчить, що скорочення часу завершення всіх операцій не обов'язково забезпечує мінімізацію зваженого простою та порушень RTO. Таким чином, отримані результати підтверджують доцільність спільної оптимізації технічного відновлення та безпекових перевірок для дослідженого сценарію. Величина покращення залежить від алгоритму формування базового розкладу та потребує подальшої перевірки на інших конфігураціях IT-інфраструктури.

З метою дослідження впливу вхідних параметрів на характеристики оптимального плану в наступному підрозділі проведено аналіз чутливості математичної моделі до доступності ресурсів, тривалості безпекових перевірок і коефіцієнта штрафу за перевищення RTO.

На першому етапі досліджено вплив кількості доступних ресурсних одиниць на ефективність відновлення інформаційних систем. Розглянуто чотири конфігурації з $R = 2, R = 3, R = 4, R = 5$ за незмінного коефіцієнта штрафу $\lambda = 2$. Отримані результати наведено в табл. 6.



Таблиця 6

Результати аналізу чутливості математичної моделі до доступності ресурсів

Показник	$R = 2$	$R = 3$	$R = 4$	$R = 5$
D	331	237	209	177
P	77	12	0	0
Z	485	261	209	177
$N_{RTO} (\sum_i 1(T_i > 0))$	5	1	0	0
$\max_i C_i^{safe}$	25	16	13	11

Результати свідчать про суттєвий вплив доступності ресурсів на ефективність процесу відновлення. За $R = 2$ значення цільової функції становить 485, а п'ять із шести інформаційних систем перевищують установлені RTO. Збільшення кількості ресурсних одиниць до трьох забезпечує зменшення значення цільової функції до 261, тобто на 46,19 %, та скорочення загальної тривалості відновлення з 25 до 16 годин. При $R = 4$ усі інформаційні системи повертаються до експлуатації в межах установлених RTO, а значення цільової функції зменшується до 209. Подальше збільшення кількості ресурсів до п'яти забезпечує додаткове скорочення зваженої тривалості простою та загального часу відновлення до 11 годин, проте вже не впливає на кількість порушень RTO.

На другому етапі досліджено вплив тривалості безпекових перевірок на часові характеристики відновлення інформаційних систем. Для цього сформовано три сценарії: без урахування тривалості перевірок, із базовими значеннями параметрів v_i , наведеними в табл. 2, та зі збільшенням тривалості перевірок на 50 %. В останньому випадку значення округлювалися до більшого цілого числа відповідно до годинного кроку дискретизації. Сценарій без урахування тривалості перевірок використано виключно як розрахунковий еталон для оцінювання додаткових часових витрат. Він не розглядається як рекомендований спосіб повернення інформаційних систем до експлуатації після інциденту інформаційної безпеки. Результати експерименту за незмінних $R = 3$ та $\lambda = 2$ наведено в табл. 7.

Таблиця 7

Результати аналізу чутливості до тривалості безпекових перевірок

Показник	$v_i = 0$	Базові v_i	v_i підвищена на 50 %
D	178	237	265
P	4	12	20
Z	186	261	305
$N_{RTO} (\sum_i 1(T_i > 0))$	1	1	1
$\max_i C_i^{safe}$	13	16	19

Отримані результати демонструють, що врахування безпекових перевірок суттєво впливає на характеристики оптимального плану. Порівняно з розрахунковим сценарієм без перевірок, у базовій конфігурації значення цільової функції збільшується зі 186 до 261, а загальна тривалість відновлення – із 13 до 16 годин. Збільшення тривалості безпекових перевірок на 50 % спричиняє подальше зростання значення цільової функції до 305 та збільшення загального часу відновлення до 19 годин. При цьому кількість систем із перевищенням RTO залишається незмінною, проте зважена величина такого перевищення зростає з 12 до 20.

Таким чином, неврахування безпекових перевірок призводить до заниження оцінки часу безпечного повернення інформаційних систем до експлуатації. Виділення цих процедур в окремі операції математичної моделі дозволяє точніше оцінювати потребу в ресурсах і враховувати вплив вимог інформаційної безпеки на виконання плану відновлення.

На третьому етапі досліджено чутливість математичної моделі до зміни коефіцієнта штрафу λ , який визначає відносну вагу перевищення RTO в цільовій функції. Розглянуто значення $\lambda = 0, \lambda = 1, \lambda = 2, \lambda = 5, \lambda = 10$ за незмінного ресурсного обмеження $R = 3$.

Оскільки зміна λ безпосередньо змінює структуру цільової функції, основну увагу приділено аналізу її складових D та P, а не порівнянню абсолютних значень Z. Результати наведено в табл. 8.

Таблиця 8

Результати аналізу чутливості до коефіцієнта штрафу

λ	D	P	Z	N_{RTO}	$\max_i C_i^{safe}$
0	236	16	236	1	16



1	237	12	249	1	16
2	237	12	261	1	16
5	237	12	297	1	16
10	237	12	357	1	16

За $\lambda = 0$ оптимізація спрямована виключно на мінімізацію зваженої тривалості простою, унаслідок чого $D = 236$, тоді як зважене перевищення RTO становить $P=16$. Збільшення коефіцієнта штрафу до $\lambda = 1$ забезпечує зменшення P до 12 за незначного збільшення D до 237.

Подальше збільшення коефіцієнта штрафу від 1 до 10 не змінює значень D та P . Це свідчить про те, що в межах досліджуваного сценарію компроміс між мінімізацією зваженої тривалості простою та обмеженням перевищення RTO досягається вже за $\lambda = 1$. Зростання значення Z за більших коефіцієнтів пояснюється збільшенням ваги штрафної складової, а не погіршенням часових характеристик відновлення.

Коефіцієнт λ дозволяє враховувати пріоритетність дотримання RTO під час формування оптимального плану. Водночас його вплив залежить від конкретної конфігурації інформаційних систем, технологічних залежностей і доступних ресурсів.

Проведений аналіз чутливості дозволив встановити, що найбільший вплив на ефективність відновлення інформаційних систем у досліджуваному сценарії має доступність ресурсів. Збільшення кількості ресурсних одиниць із двох до чотирьох забезпечує скорочення загальної тривалості відновлення з 25 до 13 годин, зменшення значення цільової функції з 485 до 209 та усунення перевищень RTO.

Тривалість безпекових перевірок також суттєво впливає на результати оптимізації. Її збільшення призводить до зростання зваженої тривалості простою та перевищення RTO, що підтверджує необхідність урахування безпекових процедур як самостійного етапу відновлення. Водночас дослідження коефіцієнта штрафу показало, що його вплив на характеристики оптимального плану має пороговий характер: після досягнення певного значення подальше збільшення штрафу не забезпечує додаткового покращення досліджуваних показників.

Отримані результати демонструють можливість використання запропонованої математичної моделі не лише для визначення оптимальної послідовності відновлення інформаційних систем, а й для обґрунтування управлінських рішень щодо необхідного обсягу ресурсів, оцінювання часових витрат на безпекові перевірки та вибору пріоритетів відновлення. Водночас установлені закономірності характеризують сформований синтетичний сценарій і потребують подальшої перевірки для інших конфігурацій IT-інфраструктури та умов виникнення інцидентів інформаційної безпеки.

З погляду управління IT-проектами практична цінність запропонованої математичної моделі полягає у можливості використання результатів оптимізації як інструменту підтримки управлінських рішень під час планування та координації відновлювальних робіт. Сформований розклад визначає часові характеристики виконання операцій, послідовність залучення ресурсів і допустимі моменти повернення інформаційних систем до експлуатації, що створює основу для контролю виконання плану та узгодження діяльності залучених команд. У разі зміни ресурсної доступності, тривалості окремих операцій або умов безпекової готовності інформаційних систем можливе повторне розв'язання оптимізаційної задачі з актуалізованими вхідними параметрами. Таким чином, запропонований підхід може використовуватися для обґрунтованого календарного планування та перепланування відновлювальних робіт, забезпечуючи узгодження операційних пріоритетів, ресурсних можливостей і вимог неперервності бізнесу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті вирішено актуальне науково-практичне завдання розроблення математичної моделі пріоритезації відновлення інформаційних систем після інцидентів інформаційної безпеки для підвищення ефективності процесів забезпечення неперервності бізнесу. Проведений аналіз наявних підходів засвідчив необхідність комплексного врахування бізнес-критичності інформаційних систем, установлених RTO, технологічних залежностей, ресурсних обмежень і вимог безпечного повернення систем до експлуатації.

У межах дослідження розроблено математичну модель на основі змішаночислового лінійного програмування, яка забезпечує мінімізацію зваженої тривалості простою інформаційних систем і штрафів за перевищення RTO. Особливістю запропонованого підходу є формалізація технічного відновлення та перевірки безпекової готовності як окремих взаємопов'язаних операцій, що дозволяє визначати допустимий момент повернення систем до експлуатації з урахуванням часових, технологічних і ресурсних обмежень.

Експериментальне оцінювання на прикладі шести взаємозалежних інформаційних систем показало, що запропонована модель забезпечує значення цільової функції 261, що на 1,14 % менше порівняно з



евристичними стратегіями RTO-first та Criticality-first. За результатами абляційного експерименту встановлено зменшення значення цільової функції на 42,89 % порівняно з реалізованим двоетапним підходом до планування, а також скорочення кількості систем із порушенням RTO з чотирьох до однієї. Аналіз чутливості показав, що збільшення кількості доступних ресурсних одиниць із двох до чотирьох скорочує загальну тривалість відновлення з 25 до 13 годин та забезпечує дотримання RTO всіма інформаційними системами. Отримані результати демонструють доцільність інтегрованого планування відновлювальних і безпекових операцій за умов обмеженості ресурсів.

Практичне значення отриманих результатів полягає в можливості використання запропонованої моделі для обґрунтування пріоритетів відновлення інформаційних систем, календарного планування відновлювальних робіт, раціонального розподілу ресурсів і підтримки прийняття управлінських рішень у процесах забезпечення неперервності бізнесу.

Перспективи подальших досліджень пов'язані з удосконаленням математичної моделі шляхом урахування невизначеності тривалості відновлювальних операцій, динамічної зміни доступності ресурсів і результатів безпекових перевірок. Подальший розвиток запропонованого підходу доцільно спрямувати на розроблення механізмів адаптивного перепланування, дослідження масштабованості оптимізаційного алгоритму та перевірку його ефективності для складніших конфігурацій ІТ-інфраструктури. Також передбачається проведення експериментальної апробації запропонованої математичної моделі на різних типах інформаційних систем, що відрізняються архітектурою, функціональним призначенням, рівнем критичності та характером взаємозалежностей. Особливу увагу буде приділено оцінюванню ефективності моделі в умовах реальних інцидентів інформаційної безпеки, різної доступності ресурсів і масштабів ІТ-інфраструктури. Це дозволить перевірити універсальність запропонованого підходу, його масштабованість та практичну придатність для підтримки прийняття рішень щодо відновлення інформаційних систем у процесах забезпечення неперервності бізнесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, 33(3), 583–590. <https://doi.org/10.1016/j.ijinfomgt.2013.03.001>
2. Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management*, 49, 208–216. <https://doi.org/10.1016/j.ijinfomgt.2019.04.010>
3. Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, 20(5), 332–349. <https://doi.org/10.1108/09685221211286511>
4. Stamenkov, G. (2022). Layered business continuity and disaster recovery model. *Continuity & Resilience Review*. <https://doi.org/10.1108/crr-05-2022-0008>
5. AlHidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). Towards a cyber resilience quantification framework (CRQF) for IT infrastructure. *Computer Networks*, 110446. <https://doi.org/10.1016/j.comnet.2024.110446>
6. Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: from sensemaking to practice. *Computers & Security*, 103372. <https://doi.org/10.1016/j.cose.2023.103372>
7. Chiu, C. Y. (2026). From backup restoration to Minimum Viable Factory Recovery: A systematization of ransomware recovery in manufacturing systems. *International Journal of Critical Infrastructure Protection*, 54, 100882. <https://doi.org/10.1016/j.ijcip.2026.100882>
8. Liu, L., Sajid, Z., Kravaris, C., & Khan, F. (2025). RESPONSE- a Resilient Framework to Manage Cyber-attacks on Cyber-physical Process Systems. *Digital Chemical Engineering*, 100238. <https://doi.org/10.1016/j.dche.2025.100238>
9. Almoghathawi, Y., Barker, K., & Albert, L. A. (2019). Resilience-driven restoration model for interdependent infrastructure networks. *Reliability Engineering & System Safety*, 185, 12–23. <https://doi.org/10.1016/j.res.2018.12.006>
10. Zhou, J., Coit, D. W., Felder, F. A., & Wang, D. (2021). Resiliency-based restoration optimization for dependent network systems against cascading failures. *Reliability Engineering & System Safety*, 207, 107383. <https://doi.org/10.1016/j.res.2020.107383>
11. Almoghathawi, Y., Selim, S., & Barker, K. (2022). Community Structure Recovery Optimization for Partial Disruption, Functionality, and Restoration in Interdependent Networks. *Reliability Engineering & System Safety*, 108853. <https://doi.org/10.1016/j.res.2022.108853>



12. Xu, M., Li, G., & Chen, A. (2023). Resilience-driven post-disaster restoration of interdependent infrastructure systems under different decision-making environments. *Reliability Engineering & System Safety*, 109599. <https://doi.org/10.1016/j.res.2023.109599>
13. Rangrazjeddi, A., González, A. D., & Barker, K. (2024). Game-theoretic algorithm for interdependent infrastructure network restoration in a decentralized environment. *Risk Analysis*. <https://doi.org/10.1111/risa.14269>
14. Garay-Sianca, A., & Nurre Pinkley, S. G. (2021). Interdependent integrated network design and scheduling problems with movement of machines. *European Journal of Operational Research*, 289(1), 297–327. <https://doi.org/10.1016/j.ejor.2020.07.013>
15. Li, Y.-l., Lin, J., Li, G.-j., Liu, B.-s., & Wang, C. (2020). Restoration of Interdependent Critical Infrastructure Network: A Model for Joint Optimization of Scheduling and Routing. In *Construction Research Congress 2020*. American Society of Civil Engineers. <https://doi.org/10.1061/9780784482858.001>
16. Hartmann, S., & Briskorn, D. (2021). An updated survey of variants and extensions of the resource-constrained project scheduling problem. *European Journal of Operational Research*. <https://doi.org/10.1016/j.ejor.2021.05.004>

**Mariia Stadnyk**

PhD, Associate Professor

Associate Professor of the Department of Cybersecurity
Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

ORCID: 0000-0002-0287-2254

stadnyk_m@tntu.edu.ua

Dmytro Tymoshchuk

PhD,

Senior Lecturer at the Department of Cybersecurity

Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

ORCID: 0000-0003-0246-2236

dmytro.tymoshchuk@tntu.edu.ua

Maryna Derkach

PhD, Associate Professor

Associate Professor of the Department of Cybersecurity

Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

ORCID: 0000-0001-8977-2776

m_derkach@tntu.edu.ua

MATHEMATICAL MODEL FOR PRIORITIZING INFORMATION SYSTEMS RECOVERY AFTER INFORMATION SECURITY INCIDENTS IN BUSINESS CONTINUITY MANAGEMENT PROCESSES

Abstract. This article investigates and formalizes the optimal scheduling problem for information system recovery activities and associated security checks following information security incidents within business continuity management processes, taking into account technical dependencies, resource constraints, and recovery time objectives (RTOs). The study substantiates the applicability of mathematical optimization methods for determining recovery priorities based on system business criticality, time-related characteristics, and information security requirements. Existing approaches to recovery planning are analyzed, highlighting the need to jointly consider resource constraints, technological dependencies, and security verification procedures. A mathematical model based on Mixed-Integer Linear Programming (MILP) is proposed to minimize the weighted downtime of information systems and penalties for exceeding RTOs. A distinctive feature of the model is the representation of technical recovery and security verification as separate but interdependent operations that are jointly optimized to determine when systems can safely return to operation. An algorithm for generating an optimal recovery schedule is developed, taking into account resource availability and technological dependencies. A computational experiment is conducted using six interdependent information systems. The proposed model achieves a 1.14 % reduction in the objective function value compared with the RTO-first and Criticality-first heuristic strategies. An ablation study demonstrates a 42.89 % reduction in the objective function value compared with the implemented two-stage planning approach, while reducing the number of systems exceeding their RTOs from four to one. Sensitivity analysis confirms the significant impact of resource availability and security verification duration on recovery performance. The practical significance of the results lies in the potential application of the proposed model to justify information system recovery priorities, allocate limited resources efficiently, and support managerial decision-making in business continuity management processes.

Keywords: information security, information security incidents, business continuity, information systems recovery, IT project management, project scheduling, recovery prioritization, mathematical optimization, mixed-integer linear programming, RTO, resource constraints, security verification.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, 33(3), 583–590. <https://doi.org/10.1016/j.ijinfomgt.2013.03.001>



2. Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management*, 49, 208–216. <https://doi.org/10.1016/j.ijinfomgt.2019.04.010>
3. Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, 20(5), 332–349. <https://doi.org/10.1108/09685221211286511>
4. Stamenkov, G. (2022). Layered business continuity and disaster recovery model. *Continuity & Resilience Review*. <https://doi.org/10.1108/crr-05-2022-0008>
5. AlHidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). Towards a cyber resilience quantification framework (CRQF) for IT infrastructure. *Computer Networks*, 110446. <https://doi.org/10.1016/j.comnet.2024.110446>
6. Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: from sensemaking to practice. *Computers & Security*, 103372. <https://doi.org/10.1016/j.cose.2023.103372>
7. Chiu, C. Y. (2026). From backup restoration to Minimum Viable Factory Recovery: A systematization of ransomware recovery in manufacturing systems. *International Journal of Critical Infrastructure Protection*, 54, 100882. <https://doi.org/10.1016/j.ijcip.2026.100882>
8. Liu, L., Sajid, Z., Kravaris, C., & Khan, F. (2025). RESPONSE- a Resilient Framework to Manage Cyber-attacks on Cyber-physical Process Systems. *Digital Chemical Engineering*, 100238. <https://doi.org/10.1016/j.dche.2025.100238>
9. Almoghathawi, Y., Barker, K., & Albert, L. A. (2019). Resilience-driven restoration model for interdependent infrastructure networks. *Reliability Engineering & System Safety*, 185, 12–23. <https://doi.org/10.1016/j.res.2018.12.006>
10. Zhou, J., Coit, D. W., Felder, F. A., & Wang, D. (2021). Resiliency-based restoration optimization for dependent network systems against cascading failures. *Reliability Engineering & System Safety*, 207, 107383. <https://doi.org/10.1016/j.res.2020.107383>
11. Almoghathawi, Y., Selim, S., & Barker, K. (2022). Community Structure Recovery Optimization for Partial Disruption, Functionality, and Restoration in Interdependent Networks. *Reliability Engineering & System Safety*, 108853. <https://doi.org/10.1016/j.res.2022.108853>
12. Xu, M., Li, G., & Chen, A. (2023). Resilience-driven post-disaster restoration of interdependent infrastructure systems under different decision-making environments. *Reliability Engineering & System Safety*, 109599. <https://doi.org/10.1016/j.res.2023.109599>
13. Rangrazjeddi, A., González, A. D., & Barker, K. (2024). Game-theoretic algorithm for interdependent infrastructure network restoration in a decentralized environment. *Risk Analysis*. <https://doi.org/10.1111/risa.14269>
14. Garay-Sianca, A., & Nurre Pinkley, S. G. (2021). Interdependent integrated network design and scheduling problems with movement of machines. *European Journal of Operational Research*, 289(1), 297–327. <https://doi.org/10.1016/j.ejor.2020.07.013>
15. Li, Y.-l., Lin, J., Li, G.-j., Liu, B.-s., & Wang, C. (2020). Restoration of Interdependent Critical Infrastructure Network: A Model for Joint Optimization of Scheduling and Routing. In *Construction Research Congress 2020*. American Society of Civil Engineers. <https://doi.org/10.1061/9780784482858.001>
16. Hartmann, S., & Briskorn, D. (2021). An updated survey of variants and extensions of the resource-constrained project scheduling problem. *European Journal of Operational Research*. <https://doi.org/10.1016/j.ejor.2021.05.004>

Отримано редакцією журналу / Received: 03.09.26

Прорецензовано / Revised: 16.09.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.