

Додаток № 5 ___ до наказу
Міністерства освіти і науки
України
від ____.____.2021 року № ___

Форма проєкту прикладного дослідження

Секція: Інформатика та кібернетика

Назва проєкту: Дослідження інтелектуалізованих систем підтримки прийняття рішень з інвестування у розвиток Smart City

Назва пріоритетного напрямку розвитку науки і техніки:

2. Інформаційні та комунікаційні технології

Назва напрямку секції (згідно із паспортом секції обирається до 2-х напрямів):

3. Математичне та програмне забезпечення обчислювальних машин і систем
(3.10. Інтелектуальні прикладні програмні системи, експертні системи, інтелектуальні системи підтримки прийняття рішень)

7. Інформаційні технології (7.10. Моделювання предметних галузей інформаційних систем (аналітичне, імітаційне, інфологічне, об'єктно-орієнтоване, тощо) на підґрунті створення і застосування відповідних інформаційних технологій).

Організація-виконавець: Національний університет біоресурсів і природокористування України
(повна назва)

Адреса: Україна, 03041, м. Київ, вул. Героїв Оборони, 15.

АВТОРИ ПРОЄКТУ:

Керівник проєкту (П.І.Б.) Лахно Валерій Анатолійович

(основним місцем роботи керівника проєкту має бути організація, від якої подається проєкт)

Науковий ступінь доктор технічних наук, вчене звання професор

Місце основної роботи Національний університет біоресурсів і природокористування України

Посада завідувач кафедри комп'ютерних систем і мереж

Тел.:(044) 527-81-99 E-mail: valss21@ukr.net

Відповідальний виконавець проєкту (П.І.Б., науковий ступінь, вчене звання, посада):

Тел.: _____ E-
mail: _____

Проєкт розглянуто й погоджено рішенням наукової (вченої, науково-технічної ради) (назва закладу вищої освіти/наукової установи) від « _____ » _____ 20__ р., протокол № _____.

Керівник проєкту

Лахно Валерій Анатолійович

Підпис: _____

« _____ » _____ 202__ р.

Керівник Національного університету
біоресурсів і природокористування України
ПІБ: Ніколаєнко С.М.

Підпис: _____

« _____ » _____ 202__ р.

М.П.

Секція: Інформатика та кібернетика

П Р О Е К Т
прикладного дослідження,
(непотрібне викреслити)

що виконуватиметься за рахунок видатків загального фонду державного бюджету

Назва проекту: **Дослідження інтелектуалізованих систем підтримки прийняття рішень з інвестування у розвиток Smart City**

Пропоновані терміни виконання проекту (до 24 місяців)
з 03.01.2022 р. по 31.12.2023 р.

Орієнтовний обсяг фінансування проекту: 1000 тис. грн.

1. АНОТАЦІЯ (до 15 рядків)

Проект прикладного дослідження спрямовано на розробку інтелектуалізованої системи підтримки рішень з безперервного взаємного інвестування в технології Smart City. В результаті дослідження буде запропоноване математичне рішення та відповідний програмний продукт, які засновані на розгляді білінійної диференціальної гри якості з двома термінальними поверхнями. Наукова новизна результатів, отриманих в ході досліджень, базується на розв'язанні питання про застосування нового класу білінійних диференціальних ігор для задач оцінювання різно варіантні стратегії інвестування в Smart City. У процесі досліджень будуть розроблені програмні продукти для операційних систем Windows і Android в яких реалізована запропонована модель. Програмні продукти орієнтовані на потенційних інвесторів і можуть бути використані в процесі зменшення розбіжності при оцінюванні даних щодо прогнозування отримання прибутку від інвестування в Smart City. Результати виконання проекту актуальні для суміжних галузей, а також будуть мати суттєву соціальну значущість у розбудові великих міст.

2. ПРОБЛЕМАТИКА ДОСЛІДЖЕННЯ (до 15 рядків)

2.1. Проблема, на вирішення якої спрямовано проект.

Прикладне дослідження проводиться на стику таких розділів математики як теорія ймовірності, математична статистика, теорія ігор, а також галузі інформаційних технологій, програмування та кібербезпеки. Проблема ефективного фінансового інвестування в надсучасні інформаційні технології, що використовуються при створенні Smart City, є однією з найважливіших у сфері урбанізації промислово розвинених держав. Подібні проекти характеризуються високим ступенем невизначеності та ризикованості. Для підвищення результативності та ефективності оцінювання подібних великих проектів, що стосуються Smart City, доцільно задіяти потенціал різних комп'ютеризованих систем підтримки прийняття рішень (СППР). Особливо це актуально для аналізу різно варіантних стратегій інвесторів. Безсумнівно, це відноситься і до великих міждержавних або міжрегіональних проектів розвитку Smart City. Як показав аналіз останніх досліджень у цій галузі, релевантною залишається проблема подальшого розвитку моделей для СППР у завданнях безперервного взаємного інвестування в Smart City. Практичні результати роботи дадуть поштовх розвитку зазначених наук.

2.2. Об'єкт дослідження.

Процеси інвестування в технології Smart City в межах схеми диференціальної гри якості з декількома термінальними поверхнями.

2.3. Предмет дослідження.

Методи диференціальних ігор якості, моделі взаємного інвестування та інформаційні технології для систем підтримки прийняття рішень в процесі інвестування у технології Smart City.

3. СТАН ДОСЛІДЖЕНЬ ПРОБЛЕМИ І НАПРЯМУ (до 70 рядків)

3.1. Аналіз результатів, отриманих авторами проекту за напрямом, проблемою, тематикою, об'єктом та предметом дослідження; у чому саме полягає внесок згадуваних вчених і чому їх напрацювання потребують продовження, доповнення, вдосконалення (до 20 рядків).

Авторами напрацьовані методики дослідження та побудови моделей для СППР із взаємного інвестування в технології для Smart City. Запропонована для наукового дослідження модель, на відміну від існуючих, дає конкретні наукові та методичні рекомендації при виборі інвестиційних стратегій. Можливе корегування параметрів процесу інвестування при незадовільному прогнозі для одного з інвесторів. Розглянуто новий клас білінійних диференціальних ігор, який дозволив адекватно описати процес інвестування в технології для Smart City. Розробляється програмний продукт «Invest-SmSy» для платформи Android, який буде заснований на вже отриманих і нових математичних моделях інвестиційних процесів в технології для Smart City. У «Invest-SmSy» будуть реалізовані запропоновані моделі, що базуються на застосуванні методів теорії диференціальних ігор.

3.2. Аналіз результатів, отриманих іншими вітчизняними та закордонними вченими (аналогічно наведеному у п.3.1); окремо проаналізувати напрацювання цих учених за останні 5 років із посиланням на конкретні публікації (до 30 рядків).

Серед вітчизняних науковців описом динамічних керованих об'єктів за допомогою диференціальних рівнянь займалися Л.С. Понтрягін та М.М. Красовський. Ними пропонуються ті чи інші методи теорії ігор, що дозволяють вирішувати реальні практичні завдання. Академіком Л.С. Понтрягіним були розроблені методи знаходження оптимальних стратегій гравцями в такій взаємодії. Школа академіка М.М. Красовського пододала ці обмеження і запропонувала розглядати дискретні аналоги диференціальних рівнянь, але при цьому не зробивши заключного переходу від диференціальних рівнянь до дискретних систем. Ця обставина привела до того, що клас протидій гравця-супротивника повинен бути хоча б функціями, що мають виміри.

Тематиці ефективного фінансового інвестування в технології для створення Smart City в останні роки було присвячено значне число робіт закордонними вченими [1-10]. Однак, слід зазначити, що реальних рекомендацій з розробки стратегій взаємного фінансового інвестування в Smart City авторами R. G. Hollands (2015), M. Angelidou (2014), не було запропоновано. Самостійним напрямком досліджень в даній галузі стали роботи, присвячені застосуванню різних експертних систем (ЕС) з праці M. Angelidou (2014), Z. Irani, A. Sharif (2014) [7, 8] і СППР для вибору раціональних стратегій інвестування в Smart City у працях S. Altuntas & T. Dereli (2015), J. Gottschlich & O. Hinz, (2014). Розроблені авторами [1-10] підходи для вирішення цієї проблеми не дозволяють знаходити ефективні рекомендації і стратегії управління інвестиціями в Smart City. Ця обставина обумовлює необхідність розробки нових моделей для СППР, які б дали можливість знаходити оптимальні стратегії взаємного фінансового інвестування в передові технології Smart City. Досягнення мети можливе за рахунок застосування методів теорії диференціальних ігор якості з декількома термінальними поверхнями. Слід зазначити, що для таких диференціальних ігор незастосовні підходи викладені в роботах V. Albino, U. Berardi & R. Dangelico (2015). Останнє обумовлено тим, що, в рамках, запропонованих моделей рішень гравець-протидія (наприклад, інвестор з іншої держави) може застосовувати вимірні управління. У нашому підході, який пропонується, допустимі будь-які види управління, зокрема, невимірні функції.

3.3. Перелік основних публікацій (не більше 10-ти) закордонних і вітчизняних вчених (окрім публікацій авторів, що наведені у доробку), що містять аналоги та прототипи, є основою для проекту (до 20 рядків).

Таблиця 1

№	Повні дані про статті
1	Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions,

	performance, and initiatives. Journal of Urban Technology, 22(1), pp. 3-21.
2	Angelidou, M. (2015). Smart cities: A conjuncture of four forces. Cities, 47, pp. 95-106.
3	Glasmeier, Amy, and Susan Christopherson. "Thinking about smart cities." (2015): pp. 3-12.
4	Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things journal, 1(1), pp. 22-32.
5	Paroutis, S., Bennett, M., & Heracleous, L. (2014). A strategic view on smart city technology: The case of IBM Smarter Cities during a recession. Technological Forecasting and Social Change, 89, pp. 262-272.
6	Hollands, R. G. (2015). Critical interventions into the corporate smart city. Cambridge Journal of Regions, Economy and Society, 8(1), pp. 61-77.
7	Angelidou, M. (2014). Smart city policies: A spatial approach. Cities, 41, S3-S11.
8	Irani, Z., Sharif, A., Kamal, M. M., & Love, P. E. (2014). Visualising a knowledge mapping of information systems investment evaluation. Expert Systems with Applications, 41(1), pp. 105-125.
9	Altuntas, S., & Dereli, T. (2015). A novel approach based on DEMATEL method and patent citation analysis for prioritizing a portfolio of investment projects. Expert systems with Applications, 42(3), 1003-1012.
10	Gottschlich, J., & Hinz, O. (2014). A decision support system for stock investment recommendations using collective wisdom. Decision support systems, 59, pp. 52-62.

4. МЕТА, ОСНОВНІ ЗАВДАННЯ ТА ЇХ АКТУАЛЬНІСТЬ (до 70 рядків)

4.1. Ідеї та робочі гіпотези проекту.

Ідея проекту полягає у розробці інтелектуалізованої системи підтримки прийняття рішень при інвестуванні у проекти по розвитку Smart City. Моделі, алгоритми та безпосередньо СППР, яка розробляється у межах проекту, базуються на білінійних диференціальних рівняннях з залежними рухами, що дозволяє конструктивно знаходити оптимальні стратегії та давати конкретні рекомендації інвесторам в проекти Smart City, або інші великі інвестиційні проекти.

Робоча гіпотеза проекту - передбачається, що якщо здійснити розробку інтелектуалізованої системи підтримки прийняття рішень при інвестуванні у високотехнологічні та водночас ризикові проекти по розвитку Smart City, то завдяки тому, що базові моделі СППР базуються на білінійних диференціальних рівняннях з залежними рухами, можна підвищити ефективність вибору раціональних варіантів стратегій для залучення фінансових ресурсів під завдання інвестування в Smart City.

4.2. Мета і завдання, на вирішення яких спрямовано проект.

Метою проекту є розробка моделей, методів та алгоритмів для побудови ефективної системи підтримки прийняття рішень у галузі інвестування у проекти по розвитку Smart City, з подальшою можливістю поширити досвід використання СППР на інші великі інвестиційні проекти.

Для досягнення поставленої мети потрібно вирішити наступні завдання:

- провести аналіз існуючих науково-теоретичних і практичних знань з проблеми, що досліджується. Виконати огляд та аналіз наявних методів, моделей та інформаційних технологій для вибору стратегій інвестування потенційними інвесторами, зокрема, у складні проекти, пов'язані із розбудовою Smart City;

- розробити нові та удосконалити існуючі методи та моделі для СППР зі взаємного інвестування у високотехнологічні проекти розбудови Smart City;

- обґрунтувати архітектуру СППР, сформувати її параметри та відносини між компонентами, визначити цільову функцію та обмеження, що накладаються на область рішень диференціальної гри якості з декількома термінальними поверхнями;

- розробити програмний продукт (СППР) та провести його апробацію на рівні структурних підрозділів великих міст України, які займаються плануванням розбудови інфраструктури відповідно до концепції Smart City.

4.3. Обґрунтування актуальності та/або доцільності виконання завдань, виходячи із: стану досліджень проблематики за напрямом проекту; ідей та робочих гіпотез проекту.

В ході завчасно проведеного аналізу встановлено, що основними проблемами, з якими стикаються компанії та організації в ході оцінювання і вибору раціональних стратегій інвестування в Smart City залишаються: відсутність методології визначення точних значень для оцінки ризиків, пов'язаних з інвестуванням передових інформаційних технологій застосовуваних в Smart City; складність пропонованих моделей і методів, зокрема, коли мова заходить про їх алгоритмізацію і подальшу реалізацію, наприклад, в системах підтримки прийняття рішень (СППР) за вибором стратегій взаємного інвестування; відсутність методології оцінювання стратегій контрагента взаємного інвестування, наприклад, коли фінансовий ресурс обмежений, тощо.

Все це загалом робить актуальним завдання продовження досліджень у напрямку розробки нових методів і моделей за вибором раціональних стратегій інвестування в Smart City. Зокрема, для ситуацій, коли, виникають додаткові запити на розвиток передових інформаційних технологій для Smart City, що викликані зміною рівня ризиків для інвесторів. А, отже, веде до необхідності перегляду власних стратегій взаємного інвестування.

Практична цінність проекту полягає в розробці програмних продуктів для платформ Windows і Android в яких реалізується запропонована модель. Програмні продукти будуть орієнтовані на потенційних інвесторів і можуть бути використані в процесі зменшення розбіжності при оцінюванні даних під час прогнозування прибутків інвестування в Smart City.

5. ПІДХІД, МЕТОДИ, ЗАСОБИ ТА ОСОБЛИВОСТІ ДОСЛІДЖЕНЬ ЗА ПРОЕКТОМ

5.1. Визначення підходу щодо проведення досліджень, обґрунтування його новизни.

Для проведення досліджень в рамках проекту обрано підхід, який базується на застосуванні методів теорії диференціальних ігор якості з декількома термінальними поверхнями. Новизна підходу, який пропонується полягає в тому, що він дозволяє конструктивно знаходити оптимальні стратегії і, отже, це дозволяє давати конкретні рекомендації інвесторам.

Слід зазначити, що опис динамічних керованих об'єктів відбувається за допомогою диференціальних рівнянь. І в залежності від правих частин цих рівнянь пропонуються ті чи інші методи теорії ігор, що дозволяють вирішувати реальні практичні завдання. У разі лінійності правої частини диференціальних рівнянь відносно фазової змінної, академіком Л.С. Понтрягіним були розроблені методи знаходження оптимальних стратегій гравцями в такій взаємодії. Ці методи носять назви першого прямого методу Л.С. Понтрягіна і методу альтернованого інтегралу. Однак у такого підходу є недоліки, а саме - важливою обставиною є те, що для таких лінійних диференціальних рівнянь може бути застосована формула Коші для знаходження рішення системи диференціальних рівнянь і крім того, керуючі збурення є функціями часу, але не функціями фазових координат. Це істотно обмежує застосування даного підходу.

Під час виконання проекту автори використовують сучасну матеріально-технічну базу, обладнані лабораторії НУБіП України (начальні лабораторії «Вбудованих та інтернет-речей», «Інформаційних управляючих систем і технологій» «Технологій програмування»). Також апробація результатів дослідження буде відбуватися у центрах колективного користування, з використанням обладнання НАН України. Виконавці матимуть доступ до сучасних електронних баз даних, в т.ч. Scopus та WoS.

Результати дослідження будуть запропоновані для прикладного практичного використання меріям великих мість, які розбудовують інфраструктуру у відповідності до концепції Smart City, а також зацікавленим підрозділам МінАПК, НААН України.

5.2. Нові або оновлені методи та засоби, методика та методологія досліджень, що створюватимуться авторами у ході виконання проекту.

У проекті пропонується використати методику досліджень і, на її основі, методологію досліджень, яка базується на рішенні дискретних аналогів диференціальних ігор, що дозволить

зняти всі обмеження на класи стратегій, які застосовуються інвесторами в процесі пошуку раціональної стратегії інвестування.

СППР, яка буде розроблена та відповідна методика її використання мають враховувати процеси та особливості взаємного інвестування у технології Smart City. Математичне рішення, що пропонується в проекті, засноване на розгляді білінійної диференціальної гри якості з двома термінальними поверхнями. Наукова новизна результатів, отриманих в ході реалізації проекту, базується на вирішенні питання про застосування нового класу білінійних диференціальних ігор для задач оцінювання різно варіантності стратегій інвестування в Smart City.

5.3. Особливості структури та складових проведення досліджень.

На першому етапі дослідження буде проведено аналіз наявних науково-теоретичних і практичних знань з проблеми, що досліджується. Також на цьому етапі буде виконано огляд та аналіз наявних методів, моделей та інформаційних технологій для вибору стратегій інвестування потенційними інвесторами, зокрема, у складні проекти, пов'язані із розбудовою Smart City.

На другому етапі дослідження будуть розроблені нові та удосконалені існуючі методи та моделі для СППР зі взаємного інвестування у високотехнологічні проекти розбудови Smart City. Також на другому етапі буде обґрунтована архітектура СППР, сформовано її параметри та відносини між компонентами СППР. Буде визначено цільову функцію та обмеження, що накладаються на область рішень диференціальної гри якості з декількома термінальними поверхнями.

На завершальному третьому етапі дослідження буде розроблено програмний продукт (СППР) та проведена його апробація на рівні структурних підрозділів великих міст України. Під час апробації планується підтвердити, що інвестори у проекти Smart City зможуть отримувати конкретні рекомендації по вибору стратегій інвестування.

Базою виконання досліджень буде слугувати сучасні лабораторії НУБіП України, зокрема, початкові лабораторії «Вбудованих та інтернет-речей», «Інформаційних управляючих систем і технологій» «Технологій програмування». Також автори проекту мають доступ сучасних реферативних баз Scopus та WoS.

6. ОЧІКУВАНІ РЕЗУЛЬТАТИ ВИКОНАННЯ ПРОЕКТУ ТА ЇХ НАУКОВА НОВИЗНА

6.1. Докладно представити очікувані результати – попередні описи теорій, концепцій, закономірностей, моделей, інших положень, що створюватимуться, змінюватимуться та/або доповнюватимуться авторами.

Передумовою проекту стали ідеї опису динамічних керованих об'єктів за допомогою диференціальних рівнянь. У відповідності до цієї концепції, яка була запропонована академіком Л.С. Понтрягіним, були розроблені методи знаходження оптимальних стратегій гравцями в різних ситуаціях. Пізніше було запропоновано розглядати дискретні аналоги диференціальних рівнянь, але при цьому не зробивши заключного переходу від диференціальних рівнянь до дискретних систем. Ця обставина привела до того, що клас протидій гравця-супротивника повинен бути хоча б функціями, що мають виміри. Розроблені авторами проекту підходи, дозволяють досягти мети за рахунок застосування методів теорії диференціальних ігор якості з декількома термінальними поверхнями. В результаті реалізації Проекту можливо стане знаходити оптимальні стратегії інвесторів та генерувати за допомогою СППР конкретні рекомендації щодо коригування параметрів інвестування для досягнення бажаного для інвесторів результату.

Для вирішення сформульованої задачі авторами проекту запропоновано підхід, заснований на застосуванні методів теорії багатокрокових і диференціальних ігор якості з декількома термінальними поверхнями. Даний підхід дозволяє враховувати безліч факторів невизначеності, таких як неповнота інформації, протидію як з боку можливих контрагентів взаємодії, так і природи, а також цілий ряд інших факторів, що дозволяють адекватно описувати функціонування таких складних об'єктів як Smart City. Застосування теорії ігор для

вирішення практичних завдань вже давно не потребує додаткових аргументів для підтвердження обґрунтованості такого застосування. Без теорії ігор в даний час неможливо конструювати управління технічними об'єктами як у військовій сфері, так і цивільної області. Для таких задач розроблені методи диференціальних ігор, на підставі яких створені алгоритми з подальшою їх програмною реалізацією.

6.2. Визначити, які з очікуваних результатів можуть бути науково-обґрунтованими та доведеними, спиратимуться на закономірності (і які саме) природи, а які – корисними методичними і технічними напрацюваннями на основі практичного досвіду.

Всі отримані результати будуть науково обґрунтованими, так як вони спираються на суцільно науковому доведенні відповідних результатів в галузі багатокрокових, диференціальних ігор якості з декількома термінальними поверхнями.

Наукова новизна наведених положень і результатів підтверджується науковою новизною результатів в галузі теорії багатокрокових і диференціальних ігор якості з декількома термінальними поверхнями.

6.3. Довести наукову новизну наведених положень на основі їх змістовного порівняння із існуючими аналогами у світовій науці на основі посилань на конкретні публікації (наведені у Таблиці 1), довести переваги результатів, які будуть отримані, над існуючими.

Результатом реалізації проекту є СППР, яка може бути корисна не тільки при вирішенні проблеми інвестування в Smart City, а й при вирішенні інших проблем, таких як знаходження стратегії інвестування захисника інформаційних систем для нейтралізації хакера; для знаходження фінансової стратегії банку при взаємодії з контрагентом банку тощо. Результатом роботи СППР будуть отримані рішення в ході пошуку оптимальних стратегій гравців і траєкторії руху фінансових ресурсів інвесторів при застосуванні ними їх оптимальних стратегій. У разі, коли інвесторів не буде задовольняти результат інвестування у них буде можливість так змінити їх власні параметри, які їм дозволять їм отримати прийнятний для них результат взаємодії.

Отримані в ході реалізації проекту результати є новими, аналогів у світовій науці не мають. Тому запропонована методика має перевагу в тому, що вдалося отримати результати, які мають практичне значення для реальних економічних і фінансових процесів.

7. ПРАКТИЧНА ЦІННІСТЬ ДЛЯ ЕКОНОМІКИ ТА СУПІЛЬСТВА

7.1. Обґрунтувати цінність очікуваних результатів для потреб розвитку країни та загальнолюдської спільноти.

Для прикладного дослідження визначити та обґрунтувати використання очікуваних результатів для конкретної галузі науки та суспільної практики, що досліджується, потреб розвитку соціально-економічної системи України (з можливим підтвердженням листами-підтримки від потенційних замовників).

Цінність очікуваних результатів для потреб розвитку країни полягає в тому, щоби їх використання дало можливість ефективно використовувати фінансові кошти країни при вирішенні важливих соціально-господарських проблем а, отже, це дасть можливість використання «зекномлених» фінансових коштів в інших важливих економічних і фінансових сферах.

7.2. Для прикладних досліджень довести, що задля одержання наведених наукових результатів варто витратити відповідні кошти державного бюджету, тобто, що економічний, соціальний або інший ефект від використання результатів проекту перевищить витрати.

Концептуальні підходи, що стосуються створення і розвитку інфраструктури Smart City були озвучені ще на початку 2000-х років. Є очевидним, щоб максимально трансформувати або адаптувати традиційні міста (тобто міста знайомі нам сьогодні) в Smart City, необхідно максимально використовувати весь потенціал інформаційно-комунікаційних технологій (ІКТ). При цьому як відзначають багато дослідників, передові інформаційно-комунікаційні системи

(ІКС) є ключовим елементом для досягнення цілей подібної трансформації. Крім того, використання сучасних ІКТ сприяє вирішенню та інших супутніх завдань, наприклад, таких як, поліпшення суспільних послуг, підвищення ефективності та безпеки міського середовища, поліпшення міської логістики та мобільності населення, впровадження енергоефективних та ресурсозберігаючих технологій в системах енерго- і водопостачання та багато іншого .

У теперішній час велика кількість дослідницьких ініціатив зі створення нових Smart City і процесу вдосконалення існуючих, зосереджені саме на технічних аспектах цього завдання. А саме технологіям розвитку нових сенсорних пристроїв, мереж зв'язку, систем зберігання та обробки даних, нових хмарних платформах, здатних управляти міськими службами, відкриваючи величезні можливості для компаній в цьому секторі.

Зауважимо, що всі подібні інноваційні технології та шляхи їх впровадження безпосередньо в системи Smart City вимагають ретельного опрацювання для потенційних інвесторів стратегій фінансування. Дуже багато гравців на ринку інвестицій, в тому числі в системи і технології Smart City розглядали їх ІКТ в розрізі оцінювання параметрів невизначеності і ризикованості подібних фінансових вкладень. Для підвищення результативності та ефективності оцінювання подібних проектів, доцільно задіяти потенціал різних комп'ютеризованих систем підтримки рішень (СППР). Особливо таке завдання актуальне для ситуацій, коли на ринку інвестицій взаємодіє кілька груп інвесторів. При цьому інтереси інвесторів можуть бути діаметрально протилежні.

Вище зазначене зумовлює актуальність і необхідність фінансування тематики нашого дослідження. Зокрема, в аспекті необхідності розробки нових моделей для СППР щодо інвестування у великі інноваційні рішення, до яких, безумовно, відносяться і проекти з розвитку ІКТ Smart City. Подібні моделі, що будуть реалізовані у відповідні алгоритмічні та програмні розробки моделей СППР, дозволять зменшити розбіжності даних прогнозування і реальної віддачі від інвестування в технології Smart City.

Економічний, соціальний и інший ефект від використання результатів проекту буде істотно перевищувати витрати на его реалізацію.

7.3. Обґрунтувати цінність очікуваних результатів для світової та вітчизняної науки.

Цінність очікуваних результатів для світової і вітчизняної науки полягає в тому, що їх використання дасть можливість визначити напрямки перспективного наукового пошуку у проблемах ефективного використання фінансових коштів при вирішенні важливих соціально-господарських проблем, що в свою чергу дасть можливість використання «зеконномлених» фінансових коштів в інших важливих економічних і фінансових сферах.

Розроблені моделі, на відміну від існуючих рішень, дадуть конкретні рекомендації при виборі інвестиційних стратегій в технології Smart City. Можливе корегування параметрів процесу інвестування при незадовільному прогнозі для одного з інвесторів. Буде розглянуто новий клас білінійних диференціальних ігор, який дозволить адекватно описати процес інвестування в технології для Smart City.

7.4. Довести цінність результатів для підготовки фахівців у системі освіти, зокрема наукових кадрів вищої кваліфікації, навести ПБ та тематику кваліфікаційних робіт магістрантів, аспірантів і докторантів, що будуть брати участь у виконанні проекту з оплатою праці.

На підставі дослідження планується підготувати протягом 2021-2022 року одну дисертацію на здобуття наукового ступеню к.н.т. за спеціальністю 122 Комп'ютерні науки. Тема «Методи, моделі та інформаційні технології кластерного аналізу надзвичайних ситуацій в Smart City», та протягом 2021-2022 років дисертацію на здобуття наукового ступеня д.т.н. за спеціальністю 122 Комп'ютерні науки на тему «Методи та моделі в інтелектуалізованих системах підтримки прийняття рішень з розвитку Smart City».

Цінність результатів для підготовки фахівців в системі освіти полягає в тому, що вони отримують навички наукового дослідження, підкріплені навичками практичної реалізації отриманих результатів. Також результати дослідження планується використовувати при читанні наступних дисциплін «Комп'ютерні системи штучного інтелекту», «Теорія і

проектування комп'ютерних систем», «Технології програмування комп'ютерних систем», «Інтелектуальний аналіз даних та розробці методичних рекомендації для практичних та лабораторних занять по цим дисциплінам.

7.5. Навести запланований перелік розробок, інформаційно-аналітичних матеріалів, рекомендацій, пропозиції тощо, що можуть бути передані для використання поза межами організації-виконавця на підставі укладання договорів, зокрема господарчих і грантових угод, продажу ліцензій тощо.

Розроблений програмний продукт СППР з безперервного взаємного інвестування в технології Smart City може бути переданий будь-якому замовнику, який розглядає питання про вибір раціональних стратегій інвестування в передові інформаційні технології Smart City або інші великі інвестиційні проекти.

8. ФІНАНСОВЕ ОБГРУНТУВАННЯ ВИТРАТ ДЛЯ ВИКОНАННЯ ПРОЕКТУ

8.1. Обсяг витрат на заробітну плату (розрахунок фонду оплати праці за кількістю працівників, залучених до виконання (загальний).

На період виконання проекту обсяг витрат на оплату праці становить 400,0 тис. грн.

Загальна кількість виконавців передбачає 6 осіб (6 сум.):

головний науковий співробітник – сумісник (0,5 ст.), заробітна плата – 4,566 тис. грн., доплата за вчене звання – 1,507 тис. грн., доплата за науковий ступінь – 1,142 тис. грн., середньомісячна заробітна плата – 7,215 тис. грн., кількість місяців – 12. Фонд заробітної плати – 86,58 тис. грн.

провідний науковий співробітник – сумісник (0,5 ст.), заробітна плата – 4,285 тис. грн., доплата за вчене звання – 1,071 тис. грн., доплата за науковий ступінь – 1,071 тис. грн., середньомісячна заробітна плата – 6,427 тис. грн., кількість місяців – 12. Фонд заробітної плати – 77,124 тис. грн.

провідний науковий співробітник – сумісник (0,5 ст.), заробітна плата – 4,285 тис. грн., доплата за вчене звання – 1,071 тис. грн., доплата за науковий ступінь – 0,643 тис. грн., середньомісячна заробітна плата – 5,999 тис. грн., кількість місяців – 12. Фонд заробітної плати – 71,988 тис. грн.

старший науковий співробітник: – сумісник (0,5 ст.), заробітна плата – 4,005 тис. грн., доплата за вчене звання – 1,001 тис. грн., доплата за науковий ступінь – 0,601 тис. грн., середньомісячна заробітна плата – 5,607 тис. грн., кількість місяців – 12. Фонд заробітної плати – 67,284 тис. грн.

старший науковий співробітник: – сумісник (0,5 ст.), заробітна плата – 4,005 тис. грн., доплата за науковий ступінь – 0,601 тис. грн., середньомісячна заробітна плата – 4,606 тис. грн., кількість місяців – 12. Фонд заробітної плати – 55,272 тис. грн.

старший науковий співробітник: – сумісник (0,5 ст.), заробітна плата – 3,445 тис. грн., середньомісячна заробітна плата – 3,445 тис. грн., кількість місяців – 12,1. Фонд заробітної плати – 41,752 тис. грн.

Витрати за статтею «Нарахування на оплату праці» розраховані з урахуванням єдиного внеску у розмірі 22% відповідно до Закону України № 2464-VI і становлять 88,0 тис. грн.

8.2. Обсяг витрат на матеріали, обладнання та інвентар, орієнтовний розрахунок (загальний).

На виконання проекту обсяг витрат на матеріали передбачено в обсязі 292,0 тис. грн., з них картридж 5 од. загальною вартістю 17,000 тис. грн, комплектуючі до комп'ютерної техніки на суму 275,0 тис. грн., а саме:

- процесор AMD Ryzen 5 2600 3,4 GHz (країна виробник США) на суму 76 000 грн. в кількості 16 шт.

- материнська плата Gigabyte B450 Arous Elite sAM4, AMD B450, PCI-Ex16 на суму 44 000 грн. в кількості 16 шт.

- оперативна пам'ять Hyper-x DDR4 -2400 8190 MB на суму 22 000 грн. в кількості 16 шт.

- Жорсткий диск Samsung 860 Evo-Series 500GB 2.5" SATA III V-NAND MLC на суму 42 400 грн. в кількості 16 шт.

- відеокарта ASUS GeForce GTX1650 4096Mb TUF OC D6 4GB GDDR5 128 bit на суму 90 600 грн. в кількості 16 шт.

Призначені для розгортання та побудови навчально-наукового кластеру для розподілених обчислень великих даних та моделювання роботи Smart City.

8.3. Обсяг витрат на енергоносії, інші комунальні послуги (загальний).

Розрахунок потреби в коштах на оплату комунальних послуг та енергоносіїв здійснено з урахуванням показників Прогнозу економічного і соціального розвитку України на 2021 рік і становитимуть 30,0 тис. грн. це 2% від загального обсягу фінансування проекту.

Оплата теплопостачання на весь період виконання проекту становить 12,6 тис. грн. (1,82239 тис. грн. x 6,9 Гкал)

Оплата водопостачання та водовідведення на весь період виконання проекту становить 2,5 тис. грн. (0,022992 тис. грн. x 109,6 м. куб).

Оплата електроенергії на весь період виконання проекту становить 14,9 тис. грн.. (0,001826 x 8149,0 кВт/год).

8.4. Інші витрати (за видами, із обґрунтуванням їх необхідності (загальний).

Непрямі витрати, передбачені на управління, становлять 20% від загального обсягу проекту і дорівнюють 200,000 тис. грн.

8.5 Зведений кошторис проекту (загальний).

Загальний зведений кошторис проекту на період 03.01.2022 р. – 31.12.2023 р. становить 1000,000 тис. грн.

8.6. Перелік обладнання (із зазначенням цін та виробників), необхідного для виконання наукової роботи, науково-технічної (експериментальної) розробки.

На виконання проекту обсяг витрат на придбання обладнання і предметів довгострокового користування передбачено в обсязі 200,0 тис. грн., а саме сервер Supermicro SYS-5039R-T (Middle Tower, один процесор Intel Xeon W, чипсет Intel C422, до 512GB пам'яті DDR4-2666 ECC, до 4-х дисків SAS/SATA hot-swap, два порти Gigabit Ethernet, IP KVM, Virtual DVD/FDD, 1 блок живлення на суму 200 тис. грн. в кількості 1 шт. Країна виробник – Україна.

Призначено для обробки даних по моделюванню у Smart City в рамках науково-дослідних робіт по реалізації пропонованої системи та організації на його базі кластеру системи.

9. НАУКОМЕТРИЧНІ ПОКАЗНИКИ АВТОРІВ ПРОЕКТУ

Сумарний h-індекс керівника та 4 авторів проекту згідно БД Scopus або WoS – складає 26.

Ляхно Валерій Анатолійович, h-індекс – 10 у БД Scopus, кількість публікацій у Scopus – 80.

<https://www.scopus.com/authid/detail.uri?authorId=57162971300>

Малюков Володимир Павлович, h-індекс – 7 у БД Scopus, кількість публікацій у Scopus – 22,.

<https://www.scopus.com/authid/detail.uri?origin=AuthorProfile&authorId=57200609600&zone=>

Шкарупило Вадим Вікторович, h-індекс – 3 у БД Scopus, кількість публікацій у Scopus – 8,

<https://www.scopus.com/authid/detail.uri?authorId=57189326576>

Касаткін Дмитро Юрійович, h-індекс – 2 у БД Scopus, кількість публікацій у БД Scopus – 5,

<https://www.scopus.com/authid/detail.uri?authorId=57204879318>

Третиник Віолета Вікентіївна, h-індекс – 4 у БД Scopus, кількість публікацій у БД Scopus – 8,

<https://www.scopus.com/authid/detail.uri?origin=AuthorProfile&authorId=57202218122&zone=>

10. НАУКОВИЙ ДОРОБОК ТА ДОСВІД АВТОРІВ ЗА НАПРЯМОМ ПРОЕКТУ

(за попередні 5 років (включно з роком подання запиту))

10.1. Перелік опублікованих статей у наукових журналах, збірниках наукових праць, матеріалах конференції тощо, що входять до науково-метричних баз даних WoS та/або Scopus (в тому числі у наукових фахових журналах України, що відносяться до категорії «А»)

Таблиця 2

№	Повні дані про статті з веб-адресою електронної версії; <u>обрати прізвища авторів</u> , які належать до списку авторів, індекс SNIP видань (Source	Наукоме тр.	Індекс SNIP
---	---	-------------	-------------

Normalized Impact Per Paper)	бази даних	
1. Lakhno, V., Akhmetov, B., Korchenko, A., Alimseitova, Z., Grebenuk, V. Development of a decision support system based on expert evaluation for the situation center of transport cybersecurity (2018) Journal of Theoretical and Applied Information Technology, 96 (14), pp. 4530-4540. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051110127&partnerID=40&md5=1e083859243e9ae15a271b37e2e7a387	Scopus	0,42
2. Lakhno, V., Malyukov, V., Parkhuts, L., Buriachok, V., Satzhanov, B., Tabylov, A. Funding model for port information system cyber security facilities with incomplete Hacker information available (2018) Journal of Theoretical and Applied Information Technology, 96 (13), pp. 4215-4225. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85050159836&partnerID=40&md5=85e044eb895e1c28973dfefaf374011b	Scopus	0,42
3. Akhmetov, B., Lakhno, V. System of decision support in weakly formalized problems of transport cybersecurity ensuring (2018) Journal of Theoretical and Applied Information Technology, 96 (8), pp. 2184-2196. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046369231&partnerID=40&md5=9563d116cc140dfdb1d9698f8d522367	Scopus	0,42
4. Lakhno, V.A., Kravchuk, P.U., Malyukov, V.P., Domrachev, V.N., Myrutenko, L.V., Piven, O.S. Developing of the cyber security system based on clustering and formation of control deviation signs (2017) Journal of Theoretical and Applied Information Technology, 95 (21), pp. 5778-5786. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85037719607&partnerID=40&md5=6dafd66465b64177f3da8fb962230da1	Scopus	0,42
5. Lakhno, V.A., Kravchuk, P.U., Mekhed, D.B., Mohylnyi, H.A., Donchenko, V.U. Development of a support system for managing the cyber protection of an information object (2017) Journal of Theoretical and Applied Information Technology, 95 (6), pp. 1263-1272. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85016941583&partnerID=40&md5=38a790e0d5fdaa40e20ac4e16911f610	Scopus	0,42
6. Lakhno, V.A., Nikolaievskiy, O.Y., Skliarenko, E.V., Lytvynenko, L.O. Models and tools for automatization of the linguistic research (2017) Journal of Theoretical and Applied Information Technology, 95 (5), pp. 989-999. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85015409280&partnerID=40&md5=c8128894b2f3acca1ca33ed94dbfbd64	Scopus	0,42
7. Lakhno, V.A., Kravchuk, P.U., Pleskach, V.L., Stepanenko, O.P., Tishchenko, R.V., Chernyshov, V.A. Applying the functional effectiveness information index in cybersecurity adaptive expert system of information and communication transport systems (2017) Journal of Theoretical and Applied Information Technology, 95 (8), pp. 1705-1714. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85018374791&partnerID=40&md5=c9c0edbaa38787d4db705cd3a97532bb	Scopus	0,42
8. Lytvynenko, L., Nikolaievskiy, O., Lakhno, V., Skliarenko, E. Development of knowledge-oriented system of machine translation based on the analyticsynthetic text processing (2017) EasternEuropean Journal of Enterprise Technologies, 1 (2-85), pp. 15-24. https://www.scopus.com/inward/record.uri?eid=2-s2.0-5014034379&doi=10.15587%2f1729-4061.2017.92021&partnerID=40&md5=59855e71833edac225c47b0c51c746c6	Scopus	0,503
9. Lakhno, V., Malyukov, V., Gerasymchuk, N., Shtuler, I. Development of the decision making support system to control a procedure of financial investment (2017) EasternEuropean Journal of Enterprise Technologies, 6 (3-90), pp. 35-41. https://www.scopus.com/inward/record.uri?eid=2-s2.0-	Scopus	0,503

<p>5039955576&doi=10.15587%2f1729-4061.2017.119259&partnerID=40&md5=cd1d878eed8355db27245b5f1b3a157b</p> <p>10. Akhmetov, B., Lakhno, V., Boiko, Y., Mishchenko, A. Designing a decision support system for the weakly formalized problems in the provision of cybersecurity (2017) EasternEuropean Journal of Enterprise Technologies, 1 (2-85), pp. 4-15. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85014001217&doi=10.15587%2f1729-4061.2017.90506&partnerID=40&md5=5e760ac5b845a0eeb2dcb58c4cba30db</p>	Scopus	0,503
<p>11. Lakhno, V., Kozlovskiy, V., Boiko, Y., Mishchenko, A., Opirskyy, I. Management of information protection based on the integrated implementation of decision support systems (2017) EasternEuropean Journal of Enterprise Technologies, 5 (9-89), pp. 36-42. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85031719951&doi=10.15587%2f1729-4061.2017.111081&partnerID=40&md5=abc762ff6412664feb771e57890dc280</p> <p>12. Lakhno, V., Malyukov, V., Domrachev, V., Stepanenko, O., Kramarov, O. Development of a system for the detection of cyber attacks based on the clustering and formation of reference deviations of attributes (2017) EasternEuropean Journal of Enterprise Technologies, 3 (9-87), pp. 43-52. https://www.scopus.com/inward/record.uri?eid=2-s2.0-5020825988&doi=10.15587%2f1729-4061.2017.102225&partnerID=40&md5=2843c6e3c822cac9dbb8a4e26967e2f4</p>	Scopus	0,503
<p>13. Lakhno, V., Boiko, Y., Mishchenko, A., Kozlovskii, V., Pupchenko, O. Development of the intelligent decisionmaking support system to manage cyber protection at the object of informatization (2017) EasternEuropean Journal of Enterprise Technologies, 2 (9-86), pp. 53-61. https://www.scopus.com/inward/record.uri?eid=2-s2.0-5018724374&doi=10.15587%2f1729-4061.2017.96662&partnerID=40&md5=53ab4778e4627997aaf33108756fe3b6</p> <p>14. Lakhno, V.A., Petrov, O.S., Hrabariyev, A.V., Ivanchenko, Y.V., Beketova, G.S. Improving of information transport security under the conditions of destructive influence on the information-communication system (2016) Journal of Theoretical and Applied Information Technology, 89 (2), pp. 352-361. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84980043588&partnerID=40&md5=a4290326c6dfd817d5eb766667c8230f</p>	Scopus	0,503
<p>15. Lakhno, V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering (2016) EasternEuropean Journal of Enterprise Technologies, 2 (9), pp. 18-25. https://www.scopus.com/inward/record.uri?eid=2-s2.0-4969920390&doi=10.15587%2f1729-4061.2016.66015&partnerID=40&md5=a30ebcdcc8240af1c0931502f58ee9c2</p> <p>16. Lakhno, V., Hrabariyev, A. Improving the transport cyber security under destructive impacts on information and communication systems (2016) EasternEuropean Journal of Enterprise Technologies, 1 (3), pp. 4-11. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84960362860&doi=10.15587%2f1729-4061.2016.60711&partnerID=40&md5=ef80f26fc0e23bcc993b356c281202bd</p>	Scopus	0,42
<p>17. Lakhno, V., Kazmirchuk, S., Kovalenko, Y., Myrutenko, L., Zhmurko, T. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features (2016) EasternEuropean Journal of Enterprise Technologies, 3 (9), pp. 30-38. https://www.scopus.com/inward/record.uri?eid=2-s2.0-4984605124&doi=10.15587%2f1729-4061.2016.71769&partnerID=40&md5=85365d9779279cac472dbf0d2e1c8b3a</p>	Scopus	0,503

18. Lakhno, V., Tkach, Y., Petrenko, T., Zaitsev, S., Bazylevych, V. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks (2016) EasternEuropean Journal of Enterprise Technologies, 6 (9-84), pp. 32-44. https://www.scopus.com/inward/record.uri?eid=2-s2.0-5010223689&doi=10.15587%2f1729-4061.2016.85600&partnerID=40&md5=ebf935fbc4ae44e01bb8e7e3fed57862	Scopus	0,503
19. Lakhno, V., Mohylnyi, H., Donchenko, V., Smahina, O., Pyroh, M. A model developed for teaching an adaptive system of recognising cyberattacks among nonuniform queries in information systems (2016) EasternEuropean Journal of Enterprise Technologies, 4 (9), pp. 27-36. https://www.scopus.com/inward/record.uri?eid=2-s2.0-4994207006&doi=10.15587%2f1729-4061.2016.73315&partnerID=40&md5=95c3260cfe508e7674d655ad6811180f	Scopus	0,503
20. Al Hadidi, M., Ibrahim, Y.K., Lakhno, V., Korchenko, A., Tereshchuk, A., Pereverzev, A. Intelligent systems for monitoring and recognition of cyber attacks on information and communication systems of transport (2016) International Review on Computers and Software, 11 (12), pp. 1167-1177. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85019277094&doi=10.15866%2firecos.v11i12.9108&partnerID=40&md5=c3a9850741434c776dde5b8a180744e8	Scopus	0,471

Анотації українською мовою статей наведені у Додатку 1

10.2. Перелік опублікованих статей у наукових фахових журналах України, що відносяться до категорії «Б», статті у закордонних наукових виданнях, що не оцінені за п.10.1.

Таблиця 3

№	Повні дані про статті з веб-адресою електронної версії; позначити прізвища авторів, які належать до списку авторів проекту
1	Касаткін Д.Ю., Рудик Я.М., Шостак В.А. Principles of information support for scientific and pedagogical staff motivation in the research university (Стаття у Web of Science виданні «Інформаційні технології і засоби навчання»), 2017, Том 61, No5. С. 73-87. Режим доступу: https://journal.iitta.gov.ua/index.php/itlt/article/view/1803
2	Lakhno, V.A., Tretynyk, V.V. Information technologies for maintaining of management activity of universities (2019). Advances in Intelligent Systems and Computing, 754, pp. 663-672. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85047481124&doi=10.1007%2f978-3-319-91008-6_65&partnerID=40&md5=a400bd58824540515261cf56e52be0c4
3	Akhmetov, B., Lakhno, V., Akhmetov, B., Alimseitova, Z. Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity (2019) Advances in Intelligent Systems and Computing, 860, pp. 162-171. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85053593918&doi=10.1007%2f978-3-030-00184-1_15&partnerID=40&md5=ae280607d74f381148682ffa85330fd2
4	Lakhno, V., Zaitsev, S., Tkach, Y., Petrenko, T. Adaptive expert systems development for cyber attacks recognition in information educational systems on the basis of signs' clustering (2019) Advances in Intelligent Systems and Computing, 754, pp. 673-682. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85047484067&doi=10.1007%2f978-3-319-91008-6_66&partnerID=40&md5=5686e9ff8f96e7e5412abf78eee02f8c
5	Akhmetov, B., Lakhno, V., Akhmetov, B., Myakuhin, Y., Adranova, A., Kydyralina, L. Models and algorithms of vector optimization in selecting security measures for higher education institution's information learning environment (2019) Advances in Intelligent Systems and Computing, 860, pp. 135-142. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85053624876&doi=10.1007%2f978-3-030-00184-1_13&partnerID=40&md5=5e75749f3e1ab0d3d59d9d19a7fa8338
6	Lakhno, V., Malyukov, V., Bochulia, T., Hipters, Z., Kwilinski, A., Tomashevskaya, O. Model of managing of the procedure of mutual financial investing in information technologies and smart city systems (2018) International Journal of Civil Engineering and Technology, 9 (8), pp. 1802-1812. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054353565&partnerID=40&md5=2a9f02b6a7aad4a2c75359303d259e5d

- 7 Lakhno, V., Petrov, A., Petrov, A. Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport (2018) *Advances in Intelligent Systems and Computing*, 656, pp. 113-127. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85029475839&doi=10.1007%2F978-3-319-67229-8_11&partnerID=40&md5=303cb241006a13fa46fbd7b26c1ce117
- 8 Lakhno V.A., Kasatkin D.Y., Blozva A.I., Gusev B.S. (2020) Method and Model of Analysis of Possible Threats in User Authentication in Electronic Information Educational Environment of the University. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) *Advances in Computer Science for Engineering and Education II. ICCSEEA 2019*. vol 938.(pp. 600-609) First Online 29 March 2019. https://link.springer.com/chapter/10.1007%2F978-3-030-16621-2_56
<https://www.scopus.com/record/display.uri?eid=2-s2.0-85064533966&origin=resultslist&sort=plf-f&src=s&sid=62ccf5aef77f798fc6656f76ee808b88&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857204879318%29&relpos=0&citeCnt=0&searchTerm=>
- 9 Lakhno, V.A., Kasatkin, D.Y., Kartbayev, T.S., Togzhanova, K.O., Alimseitova, Z.K., Tussupova, B.B. Analysis of methods and information technologies for dynamic planning of smart city development (2020) *International Journal of Advanced Trends in Computer Science and Engineering*, 9 (5), art. no. 83, pp. 7496-7505. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85092671147&doi=10.30534%2Fijatse%2F2020%2F83952020&partnerID=40&md5=b551cde52722a996255d73def7cdeb3d>
- 10 Lakhno V., Malyukov V., Kraskevich, V., Kasatkina, O. et al. Computer support system for choosing the optimal managing strategy by the mutual investment procedure in smart city (2021) *Advances in Intelligent Systems and Computing*, 1194 AISC, pp. 278-287. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85087039619&doi=10.1007%2F978-3-030-50454-0_26&partnerID=40&md5=7e4ba105288f4f5a809c4819cd798343
- 11 Лахно В.А. Інформаційна безпека інтелектуальних транспортних систем, *Захист інформації*, 2015, Том 17, № 4, С. 298-305.
Petrov A., Lakhno V., Korchenko A. Models, Methods and Information Technologies of Protection of Corporate Systems of Transport Based on Intellectual Identification of Threats, *Decision Making in Manufacturing and Services*, 2015, Vol. 9, no. 2, P. 19-37.
Lakhno V. Mathematical model for the intelligential traffic management system of the buses, *MEST Journal*, 2016, Vol. 4, No 2, P. 120-129.
- 12 Лахно В.А., Терещук А.М., Петренко Т.А. Вдосконалення кіберзахисту інформаційних систем за рахунок адаптивних технологій розпізнавання кібератак, *Захист інформації*, 2016, Том 18, № 2, С. 99-106.
- 13 Лахно В.А., Петренко Т.А., Пирог М. В. Моделювання роботи адаптивної системи розпізнавання кібератак в умовах неоднорідних потоків запитів в модулях e-business, *Безпека інформації*, 2016, Том 22, № 2, с. 135-142.
- 14 Бекетова Г., Ахметов Б., Корченко А., Лахно В. Разработка модели интеллектуального распознавания аномалий и кибератак с использованием логических процедур, базирующихся на покрытиях матриц признаков, *Безпека інформації*, 2016, Том 22, № 3, С. 242-254.
- 15 Лахно В.А. Кібербезпека комп'ютерних систем транспорту, *Електротехнічні та комп'ютерні системи*, 2016, № 21, (97), С. 76-80.
- 16 Лахно В.А., Касаткін Д.Ю., Блозва А.І., Місюра М.Д., Гусев Б.С. Проектування бази знань для систем кібербезпеки на основі методу змістовної ідентифікації об'єктів. Том 4 № 8 (2020): *Кібербезпека: освіта, наука, техніка*, стр. 135-148. Стаття - <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/163>
- 17 Лахно В.А., Малуков В.П., Касаткін Д.Ю., Блозва А.І., Литовченко Т.О. (2019). Модель підтримки рішень групи інвесторів проектів для smart city з урахуванням багатофакторності. *Кібербезпека: освіта, наука, техніка*, 2(6), 57-70. (Стаття) - <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/111>
- 18 Lakhno, V., Matus, Y., Malyukov, V., Desyatko, A., Hnatchenko, T. Smart City Cybersecurity Projects Financing Model in Case of Description of Investors' Resources with Fuzzy Sets (2019) *2019 IEEE International Conference on Advanced Trends in Information Theory, ATIT 2019 - Proceedings*, art. no. 9030499, pp. 249-252. Тези доповіді - <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85082685197&doi=10.1109%2FATIT49449.2019.9030499&partnerID=40&md5=a7a27a14e3dcb19882e7>

19	24f0587ecfef Lakhno, V., Kasatkin, D., Blozva, A. Modeling cyber security of information systems smart city based on the theory of games and markov processes (2019) 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, art. no. 9061383, pp. 497-501. Тези доповіді - https://www.scopus.com/inward/record.uri?eid=2-s2.0-85083636001&doi=10.1109%2FICST47496.2019.9061383&partnerID=40&md5=645bf91cd000e6af5168ed6d32d5328e
20	Ляхно В. А., Гусєв Б. С., Блозва А. І. Касаткін Д. Ю., Осипова Т. Ю. Кластеризація ознак мережесих атак в задачах аналізу захищеності інформації, Кібербезпека: освіта, наука, техніка, No 1(9), 2020, с. 45-58. https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/179/168

Переклад анотацій статей українською мовою наведено у Додатку 2

10.3. Перелік монографії (розділів монографії) за напрямом проекту, виданих офіційними мовами Європейського Союзу в провідних міжнародних видавництвах (перелік видавництв затверджений наказом МОН від 03.11.2020 р. № 1362, враховуються друковані аркуші тільки авторського внеску).

Таблиця 4

№	Повні дані про монографії; позначити прізвища авторів, зі списку розділу 13	Кількість друк. арк.
1	Petrov, O., Borowik, B., Karpinskyu, M., Korchenko, O., & Lakhno, V. (2016). Immune and defensive corporate systems with intellectual identification of threats. Pszczyna: Śląska Oficyna Drukarska.	17

Анотації українською мовою монографій наведені у Додатку 3

10.4. Перелік монографії (розділів монографій) за напрямом проекту, що не оцінені за п.10.3 (враховуються друковані аркуші тільки авторського внеску)

Таблиця 5

№	Повні дані про монографії; позначити прізвища авторів, зі списку розділу 13	Кількість друк. арк.
1	Production Engineering and Management monografia / red. nauk.. Editing by Marek Dudek Chapter XV. Modeling information security system of transport enterprises, Valerie Lakhno , Alexander Petrov, pp. 221-248.	1,5
2	Informacje i marketing w działalności organizacji : monografia / red. nauk. Honorata Howaniec, Irena Szewczyk, Wiesław WASZKIELEWICZ. — Bielsko-Biała : Chapter X . Application of the theory of games at the choice of information security, Valerie Lakhno , Alexander Petrov, Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej, 2013. — S. 69–92.	1,6
3	The contemporary problems of management – value-based marketing, social responsibility and other factors in process of development – micro, meso and macro aspect / H. Howaniec, W. Waszkielewicz. Chapter Ensuring of information processes' safety and security in application data processing systems for transport. Valerie Lakhno , Alexander Petrov. Poland, University of Bielsko-Biala. - Bielsko-Biała: University of Bielsko-Biala Press, 2014. – 350 p.	1,5
4	Финансовые аспекты поддержания кибербезопасности ситуационных центров и информационных систем транспорта / Ахметов Б.С., Ахметов Б.Б., Ляхно В.А. , Малюков В.П. – Алматы: изд-во университета «Туран», 2019. – 196с., табл 6, ил.50, библиограф.назв.81	5,96

Анотації українською мовою розділів монографій навести у Додатку 4

10.5. Захищені дисертації доктора філософії (кандидата наук) авторами проекту або під керівництвом авторів проекту

Таблиця 6

№	Дані про дисертації (автор, назва дисертації, спеціальність, науковий керівник, рік та місце захисту); <u>позначити прізвища авторів/керівників, які належать до списку авторів проекту</u>
1	Литвиненко Леонід Олександрович , «Моделі та методи аналітико-синтетичної обробки різномовної текстової інформації в знання-орієнтованій системі машинного перекладу», захист жовтень, 2017 р. Київський національний університет будівництва і архітектури (Спеціальність 05.13.06 – інформаційні технології). Керівник – Лахно В.А.
2	Петренко Тарас Анатолійович, "Методи та моделі експертних систем розпізнавання кібератак на основі кластеризації реалізацій ознак", захист липень 2019 р., Національний авіаційний університет (Спеціальність 05.13.21 – системи захисту інформації). Керівник – Лахно В.А.

10.6. Захищені дисертації доктора наук авторами проекту або під консультуванням авторів проекту

Таблиця 7

№	Дані про дисертації (автор, назва дисертації, спеціальність, науковий консультант, рік та місце захисту); <u>позначити прізвища авторів/консультантів, які належать до списку авторів проекту</u>
1	Свідоцтво про авторське право на твір №90553 від 09.07.2019 р. Комп'ютерна програма «Система підтримки прийняття рішень про інвестування Смарт Сіті (IDSS)»
2	Свідоцтво про авторське право на твір №90554 від 09.07.2019 р. Комп'ютерна програма «Система підтримки прийняття рішень для вибору технічних засобів захисту систем кібербезпеки. (Pareto DSS)»

10.7. Перелік загальноуніверситетських наукових грантів, за якими працювали автори проекту, що фінансувались закордонними організаціями.

Таблиця 9

№	ПІБ виконавців	Назва гранту	Кількість місяців	Фінансування, тис. грн.
1	Лахно В.А.	<u>«Разработка адаптивных экспертных систем в области кибербезопасности критически важных объектов информатизации»</u> Некоммерческое акционерное общество "Алматинский университет энергетики и связи" 2018 - 2020 Конкурс на грантовое финансирование по научным и (или) научно-техническим проектам на 2018-2020 г.	36	294 000

10.8. Авторами проекту виконано договорів з наукової тематики, що фінансуються із спеціального фонду на суму (тис. грн.) (з відповідним підтвердженням довідкою з бухгалтерії закладу/установи)

Таблиця 9

№	ПІБ виконавців	Назва роботи	Замовник	Обсяг фінансування, тис. грн.
1	Касаткін Д.Ю.	У рамках проекту НДР за договором №15/28 від 01.06.2017 р. виконувались наукові дослідження «Удосконалення програмного забезпечення з автоматизації проведення кваліфікаційної експертизи на придатність до поширення сорту (ПСП) в Українському інституті експертизи сортів рослин» кошти в сумі 184 800 грн (сто вісімдесят чотири тисячі вісімсот гривень).	Український інститут експертизи сортів рослин	184 800 грн
2	Касаткін Д.Ю.	Навчально-науково-виробничим підрозділом «Центр комп'ютерних систем і мереж» (особовий рахунок 15.04.01) – виконавець Касаткін Д.Ю., протягом 2018-2019 років надавались науково-консультаційні та організаційні послуги на суму 101225 грн 00 коп (2018 р. – 54510 грн 00 коп.; 2019 р. – 46715 грн 00 коп)	НУБіП України	101225 грн 00 коп (2018 р. – 54510 грн 00 коп.; 2019 р. – 46715 грн 00 коп)

10.9. Перелік отриманих охоронних документів на об'єкти права інтелектуальної власності (ОПІВ)

Таблиця 10

№	Повні дані про охороні документи на ОПІВ з веб-адресою електронної версії; <u>позначити прізвища авторів, які належать до списку авторів проекту</u>
1	Свідоцтво про авторське право на твір №90553 від 09.07.2019 р. Комп'ютерна програма «Система підтримки прийняття рішень про інвестування Смарт Сіті (IDSS)»
2	Свідоцтво про авторське право на твір №90554 від 09.07.2019 р. Комп'ютерна програма «Система підтримки прийняття рішень для вибору технічних засобів захисту систем кібербезпеки. (Pareto DSS)»

10.10. Наявність матеріально-технічної бази, яка буде використана для виконання проекту (Центри колективного користування науковим обладнанням (ЦККНО), державні ключові лабораторії, наукові об'єкти, що становлять національне надбання).

Таблиця 11

№	Назва об'єкту	Назва документу, що свідчить про надання об'єкту відповідного статусу, та його реєстраційні дані
1		

10.11. Наявність у авторів проекту нагород: державних премій України в галузі науки і техніки, освіти та інші, премій Кабінету Міністрів України за розроблення і впровадження інноваційних технологій, премій Президента України та премій Верховної ради України для молодих вчених (без строку давності).

Таблиця 12

№	ПІБ лауреата	Назва премії	Назва документу, що свідчить про присудження премії, та його реєстраційні дані
1			

11. ОЧІКУВАНІ РЕЗУЛЬТАТИ ЗА ТЕМАТИКОЮ ПРОЕКТУ

Таблиця 13

№ з/п	Назви показників очікуваних результатів	Значення
1	Створення макету, експериментального/дослідного зразка, інженерної моделі (конструкції, технології, матеріалу)	назва та функціонал
2	Буде укладено господарчі договори, продані ліцензії, отримано грантові угоди поза межами організації-виконавця як впровадження наукових або науково-практичних результатів проекту	5%
3	Отримання охоронних документів на об'єкти права інтелектуальної власності (у тому числі свідоцтв на авторський твір)	1
4	Буде захищено дисертацій доктора наук авторами проекту або під консультуванням авторів проекту	1
5	Буде захищено дисертацій доктора філософії (кандидата наук) авторами проекту або під керівництвом авторів проекту	1
6	Будуть опубліковані монографії (розділи монографій) за напрямом проекту, виданих офіційними мовами Європейського Союзу в провідних міжнародних видавництвах (в друкованих аркушах авторського внеску)	4 д.а.
7	Будуть опубліковані монографії (розділи монографій) за напрямом проекту, що не оцінені п.6 (в друкованих аркушах авторського внеску)	7 д.а.
8	Будуть опубліковані статті у наукових журналах, збірниках наукових праць, матеріалах конференції тощо, що входять до науково-метричних баз даних WoS та/або Scopus (в тому числі у наукових фахових журналах України, що відносяться до категорії «А»)	статті у наукових журналах WoS та/або Scopus – 4 матеріалах конференції – 4 у наукових фахових журналах України - 4
9	Будуть опубліковані статті у наукових фахових журналах України, відносяться до категорії «Б», статті у закордонних наукових виданнях, що не оцінені за п.8.	4

12. ЕТАПИ ВИКОНАННЯ ПРОЕКТУ

Таблиця 14

Етапи роботи (рік)	Назва та зміст етапу	Обсяг фінансування етапу, тис.грн	Очікувані результати етапу (вказати конкретні наукові результати та наукову і науково-технічну продукцію). Звітна документація (вказати кількість запланованих публікацій, захистів магістерських, кандидатських та докторських дисертацій, отримання охоронних документів на об'єкти права інтелектуальної власності).
2021	<p>Назва етапу. Оцінка стану та перспектив розвитку інтелектуалізованих систем підтримки прийняття рішень з інвестування у розвиток Smart City.</p> <p>Зміст етапу.</p> <ul style="list-style-type: none"> - аналіз наявних науково-теоретичних і практичних знань з проблеми, що досліджується; – аналіз наявних методів, моделей та інформаційних технологій для вибору стратегій інвестування потенційними інвесторами, зокрема, у складні проекти, пов'язані із розбудовою Smart City. – розробка нових та удосконалення існуючих методів та моделей для СППР зі взаємного інвестування у високотехнологічні проекти розбудови Smart City. – обґрунтування архітектури СППР. – формування параметрів та відносини між компонентами СППР. 	500	<p>Очікувані результати етапу.</p> <p>Оглядовий розділ звіту, який містить розгляд оцінювання шляхів підвищення ефективності застосування інтелектуалізованих систем підтримки прийняття рішень для оцінювання великих інвестиційних проектів, зокрема із розвитку Smart City.</p> <p>Розроблені моделі, на відміну від існуючих рішень, дадуть конкретні рекомендації при виборі інвестиційних стратегій в технології Smart City. Можливе корегування параметрів процесу інвестування при незадовільному прогнозі для одного з інвесторів. Математичний опис нового класу білінійних диференціальних ігор, який дозволить адекватно описати процес інвестування в технології для Smart City.</p> <p>Звітна документація: Магістерська робота, 2 статі у журналах, що індексуються у Скопус, 2 статті у фахових журналах України, 2 участі у міжнародних конференціях з опублікуванням тез, 1 авторське свідоцтво на твір.</p>
2022	<p>Назва етапу. Розробка та апробація СППР.</p> <p>Зміст етапу.</p> <ul style="list-style-type: none"> – визначення цільової функції та обмежень, що накладаються на область рішень диференціальної гри якості з декількома термінальними поверхнями. – розробка СППР; – апробації СППР на рівні структурних підрозділів великих міст України. 	500	<p>Очікувані результати етапу.</p> <p>Результатом реалізації є комп'ютерна система СППР, яка корисна при вирішенні проблеми інвестування в Smart City, при вирішенні інших проблем, таких як знаходження стратегії інвестування інвесторів.</p> <p>Звітна документація: дві магістерських роботи, 2 статі у журналах, що індексуються у Скопус або WoS, 2 статті у фахових журналах України, 2 участі у міжнародних конференціях з опублікуванням тез, Монографія. Підготовлена дисертація на здобуття наукового ступеню д.т.н.</p>

13. ВИКОНАВЦІ ПРОЕКТУ (з оплатою в межах запиту):

- доктори наук: 2, кандидати наук: 2;
- молоді вчені до 35 років 2, з них кандидатів наук 2;
- наукові працівники без ступеня 1;
- аспіранти: 2; студенти 1.

Р а з о м : 8 осіб.

Таблиця 15. **Основні виконавці (автори) проекту*** (з оплатою в межах запиту):

№ з/п	Прізвище, ім'я, по батькові	Науковий ступінь	Вчене звання	Посада і місце основної роботи (тел.; E-mail)	Вік та дата народження
1.	Лахно Валерій Анатолійович	д.т.н.	професор	Завідувач кафедри комп'ютерних систем і мереж НУБіП України (050-6029690, lva964@nubip.edu.ua)	56, 1964
2.	Малюков Володимир Павлович	д.фіз-мат.н.	доцент	Професор кафедри комп'ютерних систем і мереж НУБіП України (067-1059943, volod.malyukov@gmail.com)	69, 1951
3.	Касаткін Дмитро Юрійович	к.пед.н.	доцент	Доцент кафедри комп'ютерних систем і мереж НУБіП України (098-7341617, d.kasatkin@nubip.edu.ua)	46, 1975
4.	Шкарупило Вадим Вікторович	к.т.н.	доцент	Доцент кафедри комп'ютерних систем і мереж НУБіП України (066-1297345, shkarupylo.vadym@nubip.edu.ua)	32, 1988
5.	Блозва Андрій Ігорович	к.пед.н.	-	Доцент кафедри комп'ютерних систем і мереж НУБіП України (098-9782817, andriy.blozva@nubip.edu.ua)	31, 1989
6.	Касаткіна Ольга Михайлівна	-	-	Ст. викладач кафедри інформаційних систем НУБіП України (097-3115251, olga_kasat@nubip.edu.ua)	41, 1979
Дослідники, що працюють за основним місцем роботи в інших організаціях					
7.	Третиник Віолета Вікентіївна	д.фіз-мат.н.	доцент	Доцент, НТУУ «Київський політехнічний інститут імені Ігоря Сікорського» Факультет прикладної математики Кафедра прикладної математики (097-1534646, viola.tret@gmail.com)	50, 1970
8.	Литвиненко Леонід Олександрович	к.т.н.	Ст. викладач	Старший викладач кафедри інформаційних систем та математичних ПВНЗ «Європейський університет» (093-9181785, l.lytvynenko@gmail.com)	35, 1985

*вносяться дані про основних виконавців (авторів) (до 6 осіб), окрім допоміжного персоналу та студентів. **середній вік – 43 роки**

До складу основних виконавців (авторів) проекту може входити за необхідності не більше 30 % (2 особи) дослідників, що працюють за основним місцем роботи в інших організаціях (з відповідним

обґрунтуванням необхідності їх залучення до виконання проекту або досвідом попередньої співпраці – спільні проекти, публікації).

До запиту додається письмова згода основних виконавців (авторів) проекту щодо участі в ньому.

Додаток 1. Анотації українською мовою статей, що наведені у Таблиці 2

№ з/п	Назви статей та їх анотації
1	<p>Розробка системи підтримки прийняття рішень на основі експертної оцінки ситуаційного центру транспортної кібербезпеки</p> <p>Анотація. Робота присвячена розробці математичної підтримки інформаційної системи підтримки прийняття рішень (DSS) з кібербезпеки інформаційно-комунікаційних транспортних систем (ICTS). Удосконалено алгоритм на основі методу Delphi для проведення опитування для оцінки безпеки ICTS за допомогою DSS. Алгоритм адаптований для он-лайн режиму для вирішення завдань прогнозування розвитку ситуацій, пов'язаних з інформаційною безпекою, та запобігання руйнівного впливу кібернападів на ICTS. Запропоновано модель структурування гетерогенної інформації, отриманої шляхом опитування експертів та формування бази знань DSS. Однією з мотивуючих причин цього дослідження була необхідність розробки досить простих по алгоритмічній реалізації, але ефективних інструментів для роботи експертів в мережі, оцінки інформаційної безпеки певного інформаційного об'єкта. На основі запропонованої моделі розроблені та протестовані автоматизовані засоби для аналізу безпеки ICTS в режимі on-line з використанням генерації анкет для проведення досліджень методом Delphi. Представлені результати апробації розроблених інструментів для практичних завдань забезпечення кібербезпеки ICTS. Показано, що запропоновані рішення дозволяють скоротити фінансові та часові витрати в процесі організації on-line експертної оцінки та сприяти її якості та ефективності.</p>
2	<p>Фінансування моделі порту інформаційних об'єктів системи кібер-безпеки з неповною інформацією про хакера</p> <p>Анотація. У статті описується модель, розроблена для модуля портів інформаційної системи кіберзахисту об'єктів фінансування системи прийняття рішень. Модель побудована на основі багатоетапного інструментарію теорії ігор. Запропоноване рішення дає можливість керівникам систем інформаційної безпеки, особливо інформаційних систем і технологій порту, проводити попередню оцінку фінансових стратегій для розробки ефективних систем кібербезпеки. Відмінною рисою моделі є припущення, що сторона, що захищається, не має повної інформації про стратегії фінансування атакуючої сторони та про стан її фінансових ресурсів, які використовуються для розриву кібер-бар'єрів безпеки інформаційної системи порту. Розроблено математичний апарат білінійної покрової багатоступеневої якісної гри з декількома термінальними поверхнями. Для забезпечення достовірності моделі було проведено експеримент з моделювання з декількома варіантами. Результати експерименту також будуть описані тут. Таким чином, у статті вперше було показано рішення гри для всіх випадків співвідношення параметрів гри для сторони захисту портової інформаційної системи (ПІС) та хакерів, які прагнуть подолати межі кібербезпеки. Знайдене в статті рішення буде корисним для створеної системи підтримки прийняття рішень, зокрема, для ситуації, коли зловмисник використовує змішану фінансову стратегію злому інформаційної системи.</p>
3	<p>Система підтримки прийняття рішень в забезпеченні слабоформалізованих проблем транспортної кібербезпеки</p> <p>Анотація. У даній роботі вирішується актуальне завдання розробки математичних програмних систем підтримки прийняття рішень (DSS) кібербезпеки критично важливих інформаційних систем транспорту (CRIST) в погано структурованих і складних завданнях формалізації інформаційної безпеки та оцінки інформаційних ризиків. У статті представлена розроблена система підтримки прийняття рішень в слабо формалізованих задачах CRIST і кібербезпеки об'єктів інформатизації галузі. Система базується на моделях опису завдань інформаційної безпеки, оцінки ризиків та кіберзахисту транспорту в концептуальних та функціональних аспектах. Також у статті представлено опис процесу формування бази знань СППР щодо обставин, пов'язаних з виявленням важкодоступних ознак аномалій і нападів.</p>
4	<p>Розробка системи кібербезпеки на основі кластеризації та формування ознак відхилення контролю</p> <p>Анотація. Розроблено адаптивну систему кібербезпеки (CS). Вона заснована на вдосконалених алгоритмах аномалій ознак просторового розбиття і нападів на кластери. Запропоновано новий підхід до вирішення актуальної наукової та прикладної проблеми підвищення ефективності систем інтелектуального розпізнавання кібератак та аномалій. На відміну від існуючих, даний підхід дозволяє враховувати сучасні статистичні та віддалені параметри кластеризації атрибутів кібер-атак і дає можливість одночасно змінювати допустимі відхилення допуску для всіх атрибутів, а також швидко визначати нові типи складних комбінованих атак з обмеженими обчислювальними ресурсами і мінливістю умов. На відміну від існуючих алгоритмів, вдосконалені алгоритми дозволяють враховувати особливості предметної області, включаючи правові характеристики побудови кіберзлочинів космічних знаків. Серед PTC Mathcad Prime 4.0, MATLAB (Simulink), за допомогою встановлених моделювань, продуктивність запропонованих алгоритмів перевіряється в системах КС різних компаній.</p>

5	<p>Розробка системи підтримки керування кіберзахистом інформаційного об'єкта</p> <p>Анотація. Архітектура системи управління інформаційним об'єктом безпеки та підсистема інтелектуальної підтримки прийняття рішень щодо операційного керування кібербезпекою пропонується особливо в умовах невизначеності, неузгодженості та відсутності знань про стан безпеки об'єкта. Розроблено інформаційний об'єкт операційної системи управління кібербезпекою та формування моделі раціональних множин методів захисту, заснованої на морфологічному підході. Ця модель дозволяє генерувати різні варіанти наборів захисту, які відповідають комп'ютерній системі з урахуванням морфологічних матриць для кожного периметра безпеки, підготовлених за допомогою інтелектуальної системи підтримки прийняття рішень (IDSS). Він знайде оптимальний варіант периметра набору інформаційної безпеки з використанням об'єктної функції, що максимізує співвідношення консолідованого показника «інформаційної безпеки» до консолідованої цифри «витрати». Розроблено програмний комплекс для IDSS в схемах організаційно-технічного та оперативного управління інформаційною системою безпеки. Доведено, що використання розробленого IDSS дозволяє знизити витрати на розробку системи інформаційної безпеки та скоротити час для інформування окремих відповідальних осіб про інциденти інформаційної безпеки. © 2005 - продовження JATIT & LLS.</p>
6	<p>Моделі та засоби автоматизації лінгвістичних досліджень</p> <p>Анотація. Стаття присвячена вирішенню проблеми побудови засобів автоматизації лінгвістичних досліджень, зокрема морфологічного та семантичного багатомовного аналізу. Отримані результати мають велике значення для розвитку лінгвістичних досліджень. Розроблено процедуру автоматичного створення словникових квазі-перегинів словоформ як мовних компонентів, що забезпечують автоматичний морфологічний аналіз. Розроблена система автоматичного робочого місця AWP PARADIGM, що дозволяє автоматизувати процес побудови компонентів лінгвістичних програм для автоматичного морфологічного аналізу в системі машинного перекладу, а також забезпечити функціональну повноту. Розроблена система AWP EXPERT, що дозволяє автоматизувати процес побудови компонентів лінгвістичного програмного забезпечення для автоматичного передпредметного аналізу і визначення семантичної інформації в системі машинного перекладу (SMT). Розроблений програмний продукт підтримує англійську, російську та українську мови. Доведено, що запропонований спосіб кодування лексико-граматичної інформації та підхід до автоматичного морфологічного аналізу з використанням квазіінфекцій має суттєві переваги порівняно з існуючими методами. © 2005 - продовження JATIT & LLS.</p>
7	<p>Застосування індексу інформації про функціональну ефективність в адаптивній експертній системі кібербезпеки інформаційно-комунікаційних транспортних систем</p> <p>Анотація. Розробка моделі для визначення інформаційного критерію функціональної ефективності для вивчення експертної системи для визначення стану кібербезпеки, з урахуванням відомих статистичних та дистанційних кластеризаційних показників кіберзагроз, кібер-атак (СА), аномалій, а також помилок третього типу, що може виникнути при визнанні комплексу цілеспрямованих СА на критичних комп'ютерних системах, включаючи транспортний сектор. Розроблено модель визначення інформаційного критерію функціональної ефективності експертної системи машинного навчання. Вона заснована на модифікованому інформаційному критерію розбіжності ентропії і Кульбака - Лейблера при особливостях кластеризації СА і аномаліях, які можуть отримати вхідну нечітку класифіковану навчальну матрицю, яка використовується як об'єкт дослідження, і побудувати правильні правила прийняття рішень для розпізнавання складних СА. Проведено випробування розробленої експертної системи. Встановлено, що запропонована модель може істотно підвищити аномалії та ефективність виявлення СА при постійному збільшенні кількості та складності деструктивних впливів на інформаційну безпеку комп'ютерних систем. Розроблено модель для визначення інформаційного критерію функціональної ефективності, здатного до самонавчальної експертної системи інформаційної безпеки. Він враховує потенційні помилки третього типу, які можуть виникати та накопичуватися під час вивчення інтелектуальної системи комплексного цільового виявлення СА.</p>
8	<p>Розробка знання орієнтованої системи машинного перекладу на основі аналітичної синтетичної обробки тексту</p> <p>Анотація. Розроблено метод автоматизованого аналізу синтаксичного тексту на основі декларативного представлення правил синтаксичної комбінованості. У цьому методі, на відміну від існуючих, таблиці синтаксичних правил використовуються не тільки для аналізу контексту, але і для визначення предмета, предиката, вторинних частин речення, а також суперфазних синтаксичних комбінацій. Розроблено метод розподілу програмно-аналітично-синтетичної обробки тексту мови природного мовлення в системах машинного перекладу. Розроблений метод, на відміну від відомих методів, враховує умови переходу на паралельну обробку даних як на рівні завдань обробки, так і в залежності від типу даних. Програми C #, де були реалізовані розроблені методи аналітично-синтетичної обробки багатомовних російських, українських та англійських текстів, були реалізовані програмним забезпеченням. Експериментально доведено, що розроблене програмне забезпечення для текстів з військової предметної області дозволяє знизити кількість помилок семантичного характеру на 14-16% у порівнянні з існуючими системами машинного перекладу шляхом автоматизованої обробки тексту на рівні знакової системи та введення синтезу над фрази.</p>
9	<p>Розробка системи підтримки прийняття рішень для управління процедурою фінансових інвестицій</p> <p>Анотація. Запропоновано модель безперервного контролю процедури взаємних фінансових інвестицій для системи підтримки прийняття рішень. Модель дозволяє оптимізувати пошук багатоваріантних стратегій</p>

	<p>взаємного фінансового інвестування проектів. З математичної точки зору ця модель базується на розв'язанні білінійної диференціальної якості гри з декількома поверхнями терміналів. Особливістю цієї гри є те, що правою частиною системи диференціальних рівнянь є білінійні функції з довільними коефіцієнтами. Модель реалізована на мові високого рівня C++ в програмному продукті "Система підтримки прийняття рішень для взаємного інвестування - SSDMI", яка була протестована в ряді інвестиційних проектів. Модель дозволяє вирішити проблему підвищення ефективності процедури взаємних фінансових інвестицій для учасників при різних співвідношеннях параметрів взаємодії. Тут можна знайти умову, за якої процедура взаємних фінансових інвестицій стає вигідною для всіх учасників. Запропоновано апарат теорії диференціальних ігор як інструментарій для розробки ефективної стратегії взаємних фінансових інвестицій. У рамках даного дослідження досліджується процес взаємодії між інвестором з однієї країни та її контрагентом з іншої країни. Вибраний підхід дозволяє визначити області можливих початкових станів ресурсів (фінансових капіталів) взаємодіючих об'єктів. Передбачається, що об'єкти мають таке властивість: якщо взаємодія починається з цих початкових станів, то може виникнути втрата фінансового капіталу або однією взаємодіючою стороною, або іншою в один з моментів часу. Рішення гри полягає в ідентифікації наборів переваг сторін і стратегій (контрольних дій) сторін, шляхом застосування яких можна отримати результати, краще для кожної сторони. На основі отриманих висновків були зроблені висновки та надані рекомендації інвесторам щодо їх подальших дій з метою отримання максимально можливого результату в умовах фінансових інвестицій та зменшення інвестиційних ризиків.</p>
10	<p>Розробка системи підтримки прийняття рішень для слабо формалізованих задач в забезпеченні кібербезпеки</p> <p>Анотація. Ми розробили систему підтримки прийняття рішень (DSS) для слабо формалізованих проблем захисту інформації та забезпечення кібербезпеки на об'єктах інформатизації. Система базується на моделях, що описують завдання інформаційної безпеки та кіберзахисту в концептуальних та функціональних аспектах. Описано процес складання бази знань DSS для обставин, пов'язаних з виявленням важкодоступних атрибутів аномалій і атак. Розроблена нами система DSS "Система підтримки прийняття рішень з управління захистом інформації - DMSSCIS" дозволяє поліпшити розуміння аналізованих ситуацій, що відбуваються в процесі кіберзахисту критично важливих комп'ютерних систем. Під час тестування на підприємствах було встановлено, що система "DMSSCIS" давала можливість ефективної візуалізації та інтерпретації результатів поточної оцінки виявлених важкодоступних атрибутів аномалій і кібератак, а також дозволила описати поточну ситуацію в Перебіг багатоступеневих цільових кібератак. Встановлено, що застосування DSS "DMSSCIS" у взаємодії з іншими системами для розумного розпізнавання незаконних перешкод в операціях комп'ютерних систем дозволило підвищити ефективність прийняття рішень з інформаційної безпеки. Під час тестування було встановлено, що застосування системи "DMSSCIS" дозволило скоротити час, необхідний для інформування осіб, відповідальних за кібербезпеку, про інциденти в 6,9-7,2 рази.</p>
11	<p>Управління захистом інформації на основі інтегрованої реалізації систем підтримки прийняття рішень</p> <p>Анотація. Розроблено метод і модель управління захистом об'єктів інформатизації на основі інтегрованої реалізації систем підтримки прийняття рішень для задач з кібербезпеки. Запропоновані рішення відрізняються від існуючих можливістю автоматизації процедури генерування варіантів для керування діями за допомогою системи підтримки прийняття рішень, розробленої як веб-додаток. Описана модель координації думок експертів ґрунтується на методі Delphi. Запропонований підхід дозволяє узгоджувати експертні висновки, в тому числі враховувати різні інтервальні оцінки ступеня захисту та метрики інформаційної безпеки об'єктів інформатизації. Представлені результати тестування за реальними умовами на підприємствах України програмного комплексу "Система підтримки прийняття рішень для управління кібербезпекою підприємства - DMSSCSE". DSS адаптована для он-лайн роботи експертів. Встановлено, що ДП «ДМСКГС» дозволяє підвищити ефективність застосованих організаційно-технічних заходів щодо захисту об'єктів інформатизації. Запропоновані рішення дозволили знизити витрати на організацію комплексних систем захисту інформації на 12-15% у порівнянні з існуючими методами.</p>
12	<p>Розробка системи виявлення кібер-атак на основі кластеризації та формування еталонних відхилень атрибутів.</p> <p>Анотація. Розроблено адаптивну систему виявлення кібератак, яка базується на вдосконалених алгоритмах розбиття простору ознак на кластери. Вдосконалено процедуру розпізнавання шляхом одночасного кластерування та формування перевірки допустимих відхилень атрибутів аномалій та кібератак. Запропоновані модифікації алгоритму розбиття простору ознак на кластери в процесі реалізації процедури розпізнавання аномалій і кібератак, на відміну від існуючих, дозволяють одночасно формувати довідкові допуски при обробці складних атрибутів розпізнавання об'єктів (RO). Це дає можливість, на кожному етапі підготовки адаптивної системи розпізнавання, змінювати перевірку допустимих відхилень для всіх атрибутів аномалій і кібератак одночасно. Запропоновані алгоритми дозволяють запобігти можливим випадкам поглинання одного класу RO базовими атрибутами аномалій і кібератаками іншого класу. Отримано предикатні вирази для ASR, здатних до самонавчання. Верифікація запропонованих алгоритмів проводилася на імітаційних моделях в MatLab і Simulink. Доведено, що запропоновані алгоритми кластеризації атрибутів RO дозволяють отримувати ефективні матриці навчання для ASR як частина інтелектуальних систем для виявлення кібератак.</p>
13	<p>Розробка інтелектуальної системи підтримки прийняття рішень для управління кіберзахистом на об'єкті інформатизації</p>

	<p>Анотація. Запропоновано архітектуру системи управління захистом об'єкта інформатизації (ОІ) з підсистемою інтелектуальної підтримки для прийняття рішень з оперативного управління кіберзахистом. Запропонована архітектура, зокрема, може бути використана в умовах неповноти знань про стан захисту ОІ. Ми розробили модель оперативного управління кіберзахистом в ЗОІ і сформуваємо раціональний комплекс засобів захисту. Модель базується на морфологічному підході. Модель, враховуючи морфологічні матриці для кожного з п'яти запропонованих периметрів, підготовлена інтелектуальною системою підтримки прийняття рішень (IDMSS), генерація варіантів множин, що враховують сумісність програмно-апаратних засобів захисту інформації. Пропонується зробити вибір на оптимальному варіанті набору для периметра з використанням цільової функції, що максимізує співвідношення сумарного показника «захист інформації» до сумарного показника «витрати». Програмне забезпечення реалізується та перевіряється в реальних умовах IDMSS в контурах для організаційно-технічного та оперативного управління захистом ОІ. Поліпшена архітектура відрізняється від існуючих рішень можливістю одночасної оптимізації наборів програмно-апаратних засобів для досліджуваних периметрів ОБІ, як для централізованих, так і для децентралізованих варіантів обробки інформації. У цьому випадку аналіз рівня захисту ОБІ виконується в реальному часі. Доведено, що використання розробленого IDMSS дозволяє значно скоротити заплановані витрати на систему захисту інформації, а також скоротити час, необхідний для інформування осіб, які приймають рішення, про інциденти інформаційної безпеки.</p>
14	<p>Покращення безпеки інформаційного транспорту в умовах руйнівного впливу на інформаційно-комунікаційну систему</p> <p>Анотація. Інформаційно-комунікаційне середовище транспорту (ICET) орієнтоване на взаємодію з іншими секторами з метою зменшення затримок при перевезенні товарів, обробці морських і річкових суден, контейнерів, вагонів і вантажів на прикордонних переходах за допомогою електронних рахунків-фактур «Клієнт-Банк» Система, електронний бізнес, взаємодія з клієнтами і партнерами тощо. Важливість системного відмови цього рівня складності вимагає нових досліджень з інформаційної безпеки (IS) ICET з акцентом на доступність і стійкість систем і цілісність інформації, що зберігається і обробляється в інформаційних системах (IS) і автоматизованих системах управління (ACS) промисловості. У статті наведені результати досліджень, спрямованих на подальший розвиток методів і моделей, що розпізнають загрози ICET і вдосконалення IS в умовах формування єдиного інформаційно-комунікаційного середовища, впровадження нових і модернізації існуючих ІС транспорту, а також збільшення кількості дестабілізуючий вплив на доступність, безпеку та цілісність інформації. Метод розпізнавання загроз на основі дискретних обробок з використанням апаратів логічних функцій і нечітких множин, які покращують ефективність розпізнавання, створюють ефективні аналітичні, схематичні та програмні рішення інтегрованих систем інформаційної безпеки (ISIS) ICET.</p>
15	<p>Створення адаптивної системи виявлення кіберзагроз на основі кластеризації нечітких ознак</p> <p>Анотація. Наведено результати досліджень, спрямованих на подальший розвиток методів і алгоритмів виявлення кіберзагроз і найпоширеніших класів аномалій і кібератак в критичних інформаційних системах (СНД). Розглянуто проблеми посилення опору СНД в умовах впровадження нових та модернізації існуючих інформаційно-автоматизованих систем управління, із збільшенням кількості дестабілізуючих впливів на доступність інформації, конфіденційність та цілісність. Показано, що кіберзахист СНД відстежується та аналізується за кількома параметрами особливостей аномалій або кібератак. Це, у свою чергу, дозволяє проводити попередню оцінку інформаційної безпеки шляхом кластеризації набору ознак аномалій або спроб кібератак. Запропоновано категоріальну модель побудови адаптивної інтелектуальної системи виявлення кіберзагроз (ICTDS). За допомогою процедури нечіткої кластеризації розроблено алгоритм навчання ІКТД з можливістю гіперліпсодної корекції правил прийняття рішень. Це дозволяє створити адаптивні механізми самореалізації ІКТДС. Перевіряється ефективність алгоритму інформаційно-екстремального навчання ІКТС. Для оцінки якості розділення простору ознак аномалій, вразливостей та кібер-атак зроблено вибір раціональної кількості кластерів та індексу нечіткості кластерів у просторі ознак. Доведено, що запропонований підхід дозволяє вирішувати складні задачі управління кіберзахистом СНД і може бути використаний при розробці програмних рішень для систем кіберзахисту.</p>
16	<p>Покращення транспортної кібербезпеки під деструктивним впливом на інформаційні та комунікаційні системи</p> <p>Анотація. Інформаційно-комунікаційне середовище транспорту (ICET) орієнтоване на взаємодію з іншими секторами економіки з метою зменшення затримок у перевезенні, обробці морських і річкових суден, контейнерів, вагонів, фургонів за допомогою електронних платіжних систем». -Банк "і т.д. Можливі збої, викликані кібер-атаками в системах такого рівня складності, вимагають нового дослідження інформаційної безпеки (IC) ICET з акцентом на доступність, стабільність і цілісність інформації, що зберігається і обробляється в інформаційних системах (IS) і автоматизованих системах управління (АСУ) транспортної галузі. У статті представлені результати досліджень, спрямованих на розробку методів та моделей виявлення кіберзагроз для ICET та підвищення їх стабільності при формуванні єдиного інформаційного простору, впровадження нових та модернізації існуючих ІС та АСУ в транспорті та збільшення кількості дестабілізуючих ефектів. про доступність, безпеку та цілісність інформації. Запропоновано метод інтелектуального виявлення кіберзагроз на основі дискретних процедур з використанням апарату логічних функцій і нечітких множин. Це покращить ефективність виявлення кібер-атаки, а також може бути</p>

	використана для розробки нових апаратних і програмних рішень для систем кіберзахисту ICET.
17	<p>Проектування адаптивної системи виявлення кібер-атак на основі моделі логічних процедур і матриць покриття ознак.</p> <p>Анотація. Останні десятиліття ознаменувалися стрімким розвитком критично важливих комп'ютерних систем та мереж, для забезпечення кіберзахисту яких розроблено безліч систем для розпізнавання аномалій, кіберзагроз та атак, які дозволяють виявити нелегітимні дії атакуючої сторони. Запропоновано модель розпізнавання аномалій і кібератак, яка базується на покриттях матриць ознак і понятті елементарного класифікатора, що дозволяє мінімізувати кількість навчальних вибірок для ідентифікації кіберзагроз, атак і аномалій.</p>
18	<p>Розробка адаптивної експертної системи інформаційної безпеки з використанням процедури кластеризації атрибутів аномалій і кібератак.</p> <p>Анотація. У статті представлені результати досліджень, спрямованих на подальший розвиток моделей інтелектуальних систем розпізнавання кіберзагроз, аномалій та кібератак. Запропоновано структурну схему адаптивної експертної системи (АЕС) інформаційної безпеки, здатної до самонавчання, яка враховує потенційні помилки третього виду, які можуть виникати і накопичуватися при підготовці системи інтелектуального виявлення комплексного цільового кібер атаки і попередній процес розщеплення простору атрибутів об'єктів розпізнавання. Розроблено модель для розрахунку інформаційного критерію функціональної ефективності на основі ентропійних і дистанційних критеріїв Кульбака-Лейблера в процесі кластеризації атрибутів об'єктів розпізнавання в комп'ютерних системах, що дозволяє отримати вхідну нечітку класифікаційну матрицю навчання. Процедура експлуатації АЕС як елемента системи інтелектуального розпізнавання кіберзагроз (SIRCT) була досліджена в режимі навчання апріорною класифікованою навчальною матрицею, що дозволило нам побудувати правильні вирішальні правила для розпізнавання кібератак. Ми розробили АЕС «Аналізатор загроз» і провели його тестові дослідження в умовах реальної продуктивності КС на декількох підприємствах. Встановлено, що запропонована модель навчання АЕС дозволяє досягти результатів розпізнавання стандартних класів кібер-атак на рівні від 76,5% до 99,1%, що на рівні ефективності розпізнавання кращими гібридними нейронними мережами. і генетичні алгоритми.</p>
19	<p>Розроблена модель навчання адаптивної системи розпізнавання кібератак серед неоднорідних запитів в інформаційних системах.</p> <p>Анотація. У роботі представлені результати, спрямовані на подальшу розробку моделей інтелектуальних та самоосвітніх систем розпізнавання аномалій та кібератак у критично важливих інформаційних системах (MCIS). Доведено, що існуючі системи кіберзахисту все ще значно покладаються на використання моделей і алгоритмів розпізнавання кібератак, які дозволяють враховувати інформацію про структуру вхідних потоків або зміну інтенсивності запитів, швидкість атаки. і тривалість імпульсу. Запропоновано математичну модель для системного модуля інтелектуальної ідентифікації кібератак в гетерогенних потоках запитів і мережевих форм кібератак. Модель визнає гетерогенні вхідні потоки запитів і будь-яку можливу зміну інтенсивності запитів та інших параметрів цільової кібератаки, спрямованої на MCIS. Модельні моделі, які були створені в MATLAB і Simulink, використовувалися для дослідження динаміки змін у станах підсистеми блокування запитів у процесі виявлення кібератак в MCIS. Імовірність розв'язання задачі розпізнавання кібератак в гетерогенних потоках запитів і мережевих форм кібератак становить 85-98%, залежно від типу кібератаки. Результати моделювання дозволяють вибрати способи протидії та нейтралізації наслідків таких цілеспрямованих атак і допомагають аналізувати більш складні кібератаки. Запропонована модель розпізнавання складних кібератак, якщо зловмисники використовують неоднорідні потоки запитів, більш точна, на 5-7%, ніж інші існуючі моделі. Розроблені імітаційні моделі дозволяють зменшити час на встановлення проєктів систем кібердефенту на 25-30%, включаючи SIRCA для СНД або MCIS.</p>
20	<p>Інтелектуальні системи моніторингу та розпізнавання кібератак на інформаційно-комунікаційні системи транспорту</p> <p>Анотація. Для поліпшення інформаційної безпеки транспортних систем необхідно, щоб спільні дослідження були спрямовані на подальший розвиток моделей визнання кіберзагроз в інформаційно-комунікаційному середовищі транспорту (ICET) та прийняття рішень з нечітко визначеною введеною інформацією. Запропоновано новий підхід до прийняття рішень для кібербезпеки критично важливих інформаційних систем та автоматизованих систем управління наземним транспортом. Було розглянуто випадок кіберзахисту ICET на основі нечіткої регресії механізмів логічного висновку для підтримки прийняття рішень з нечіткими вхідними даними.</p>

Додаток 2. Анотації українською мовою монографій, що наведені у Таблиці 5

№	Назви монографій та їх анотації
1	<p>Монографія містить результати досліджень, спрямованих на подальший розвиток методів та моделей інтелектуального розпізнавання загроз інформаційно-комунікаційному середовищу транспорту, зокрема міського для Smart City (IKCT).</p> <p>Вперше розроблено метод інтелектуального розпізнавання загроз на основі дискретних процедур з</p>

<p>використанням апарату логічних функцій і нечітких множин, що дозволяє проводити ефективний аналіз кіберзагроз для ІКСТ.</p> <p>Вперше розроблена модель для прийняття рішення, яка ґрунтується на дискретних процедурах виявлення кіберзагроз для транспортних систем.</p> <p>Вперше розроблена модель інтелектуального розпізнавання складних комп'ютерних вторгнень, зокрема, таких, як "відмова в обслуговуванні", в якому система виділяє найбільш інтенсивні вхідні потоки, що дозволяє оцінити можливість зміни інтенсивності запитів, швидкість атак та інші.</p> <p>Уточнені математичні моделі для оптимізації структурно-технологічного резерву ІКСТ.</p>
--

Додаток 3. Анотації українською мовою розділів монографій, що наведені у Таблиці 6

№	Назви монографій та їх анотації
1	<p>Production Engineering and Management monografia / red. nauk.. Editing by Marek Dudek Chapter XV. Modeling information security system of transport enterprises, Valerie Lakhno, Alexander Petrov, pp. 221-248.</p> <p>В розділі містяться результати досліджень, що дозволяють підвищити рівень захисту автоматизованих та інтелектуальних інформаційних систем автотранспортних підприємств Smart City в умовах інтенсифікації перевезень. Також розглядаються питання дослідження та захисту інформаційних систем за умови декількох потоків запитів конфліктних даних.</p>
2	<p>Informacje i marketing w działalności organizacji : monografia / red. nauk. Honorata Howaniec, Irena Szewczyk, Wiesław WASZKIELEWICZ. — Bielsko-Biała : Chapter X. Application of the theory of games at the choice of information security, Valerie Lakhno, Alexander Petrov, Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej, 2013. — S. 69–92.</p> <p>Запропоновано метод використання тесту Вальда та критерію Гурвіца для вибору ефективного захисту від DoS (DDoS) – атак для Smart City. Розглянуто умови для ефективного захисту.</p>
3	<p>The contemporary problems of management – value-based marketing, social responsibility and other factors in process of development – micro, meso and macro aspect [Текст] / H. Howaniec, W. Waszkielewicz. Poland, University of Bielsko-Biala. - Bielsko-Biala: University of Bielsko-Biala Press, 2014. – 350 p.</p> <p>Chapter Ensuring of information processes' safety and security in application data processing systems for transport. Valerie Lakhno, Alexander Petrov. Запропоновано використовувати методи системного аналізу для вирішення проблем інформаційної безпеки інформаційних транспортних систем Smart City. Запропоновано доповнення метод формування політики безпеки для забезпечення високонадійної обробки інформації у Smart City, що відрізняється використанням нової проблемно-графічно-теоретичної одиниці стандартної моделі автоматизованої системи.</p>
4	<p>Финансовые аспекты поддержания кибербезопасности ситуационных центров и информационных систем транспорта / Ахметов Б.С., Ахметов Б.Б., Лакно В.А., Малюков В.П. – Алматы: изд-во университета «Туран», 2019. – 196с., табл 6, ил.50, библиограф.назв.81</p> <p>ГЛАВА 1. Состояние, перспективы и основные направления развития кибербезопасности информационно-коммуникационных систем</p> <p>Рассмотрены цели и задачи, решаемые информационно-коммуникационными системами; критически важные компьютерные системы как объект кибератак.</p> <p>ГЛАВА 2. Математическая модель управления взаимодействующими информационными системами</p> <p>Сравниваются модели конфликтного взаимодействия информационных: Модель конфликтного взаимодействия информационных систем, функционирующих в дискретные моменты времени; Модель конфликтного взаимодействия информационных систем, функционирующих непрерывно во времени.</p> <p>Решение многошаговых игр качества информационных систем с полной информацией; многошаговой игры с неполной информацией с фиксированным временем окончания взаимодействия.</p> <p>Задачи о конфликтном взаимодействии информационных систем в рамках модели с неполной информацией; о конфликтном взаимодействии двух информационных систем с неполной информацией.</p>

Решение дифференциальных игр качества экономических систем с полной информацией.

ГЛАВА 3. Модель стратегий инвестирования в системы кибербезопасности ситуационных центров

Сравниваются: модели нахождения оптимальной стратегии управления процедурой взаимного финансового инвестирования в ситуационный центр по кибербезопасности; модель финансирования в кибербезопасность в рамках схемы билинейной дифференциальной игры качества; модель финансирования системы кибербезопасности в условии не полной информации о финансовом состоянии атакующей стороны (хакеров); модель финансирования средств кибербезопасности с процедурой получения дополнительных данных стороной защиты; модель принятия оптимального решения по финансированию средств кибербезопасности в условиях активного противодействия стороне взломщиков объектов информатизации.

ГЛАВА 4. Системы поддержки решений в слабо формализуемых задачах обеспечения кибербезопасности

Рассматривается модель описания метазнаний в интеллектуализированных системах поддержки принятия решений по обеспечению кибербезопасности. Менеджмент защиты информации на основе комплексного внедрения систем поддержки решений.