https://doi.org/10.31891/2307-5740-2023-322-5-20
УДК 338.28

Ірина ІВЧЕНКО
Національний університет «Одеська політехніка»
https://orcid.org/0000-0002-1977-0342
Тетяна ФІЛАТОВА
Національний університет «Одеська політехніка»
https://orcid.org/0000-0001-9373-4756
Олег ІВЧЕНКО
Національний університет «Одеська політехніка»
https://orcid.org/0000-0002-9540-1637

РОЗВИТОК НОВИХ ПІДХОДІВ ДО МОДЕЛЮВАННЯ ПРОЦЕСІВ ДІАГНОСТИКИ ТА АНАЛІЗУ РИЗИКІВ В ІТ КОМПАНІЯХ

У сучасному світі ІТ компанії стикаються зі значними ризиками, пов'язаними зі швидким технологічним розвитком, змінами на ринку та загрозами кібербезпеки. Ця стаття присвячена розвитку нових підходів до моделювання процесів діагностики та аналізу ризиків в інформаційно-технологічних (ІТ) компаніях. В рамках статті розглядаються три ключових джерела ризиків: швидкий технологічний прогрес, загрози кібербезпеки та необхідність працювати з великими об'ємами даних. Описуються основні ризики, пов'язані з цими факторами, і пояснюється необхідність розробки нових підходів для їх моделювання. Акцентується увага на кібербезпеці та кібератаках, які становлять серйозну загрозу для ІТ компаній. Саме тому особливу увагу зосереджено на економіко-математичному моделюванні кіберризиків, напрямах їх дослідження та управлінні ними. Показано, як використання нових методів моделювання ризиків може допомогти виявити потенційні загрози та розробити ефективні заходи для їх запобігання. В результаті дослідження стверджується, що розвиток нових підходів до моделювання ризиків в ІТ компаніях має великий потенціал для покращення управління ризиками та забезпечення стійкості бізнесу.

Ключові слова: моделювання ризиків, інформаційні технології, ІТ компанія, кіберризики, технологічний розвиток ІТ сфери, штучний інтелект.

Iryna IVCHENKO, Tetiana FILATOVA, Olen IVCHENKO
Odesa Polytechnic National University

DEVELOPMENT OF NEW APPROACHES TO MODELING DIAGNOSTIC PROCESSES AND RISK ANALYSIS IN IT COMPANIES

The article considers the topical issue of developing new approaches to modeling the processes of diagnostics and risk analysis in IT companies. The rapid technological progress of recent years necessitates innovative risk management methods. The authors highlight that conventional risk assessment methods often fail to account for the swift changes within the IT sector and may prove inadequate for dynamic environments. Consequently, the task at hand involves formulating and adapting new risk modeling approaches that consider the specific nature of the IT industry and propose enhancements to risk management. The article underscores that one of the primary sources of risk for IT companies is the rapid technological progress within the IT realm. Novel technologies frequently employed by IT companies can be less predictable and stable compared to those utilized by traditional businesses. Conventional risk models, founded on historical statistical data, may be ill-suited for such dynamic environments, necessitating fresh approaches to modeling technological and innovative risks.

Within the article, three key risk sources within the IT domain are examined: rapid technological progress, cybersecurity threats, and the need to handle extensive data volumes. The main risks associated with these factors are described, highlighting the need for developing new approaches to their modeling. Emphasis is placed on cybersecurity and cyberattacks, which present significant threats to IT companies. Thus, particular attention is dedicated to the economic-mathematical modeling of cyber risks, avenues of research in this field, and effective risk management. The authors underscore the importance of leveraging cutting-edge technologies, notably artificial intelligence, in modeling risks for IT companies. The article demonstrates how the utilization of new risk modeling methods can assist in identifying potential threats and devising effective measures for prevention. As a result of this research, it is affirmed that the development of innovative risk modeling approaches in IT companies holds substantial potential for ensuring business resilience.

Keywords: risk modeling, information technologies, IT company, cyber risks, technological development of the IT sphere, digitalization.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими та практичними завданнями

Невизначеність та високий рівень ризику при розробці сучасних програмних продуктів вимагають нових підходів та методів обґрунтування економічних рішень в ІТ сфері. За останні роки проведено велику кількість досліджень з цієї проблематики та знайдено цікаві шляхи ідентифікації та розв'язання проблем управління ризиками на основі можливостей сучасного економіко-математичного інструментарію та інформаційно-інтелектуальних технологій. ІТ компанії зазнають значних ризиків, пов'язаних зі швидким технологічним розвитком, змінами на ринку та загрозами кібербезпеки. Ці ризики можуть негативно

вплинути на фінансові показники, репутацію, конкурентоспроможність та навіть насамперед на існування самої компанії.

Традиційні підходи до моделювання ризиків, які широко використовуються в інших галузях, можуть бути недостатніми для врахування специфічних особливостей ІТ сектору. Проблема полягає в тому, що існуючі моделі ризиків в ІТ компаніях часто базуються на статистичних даних з минулого, які можуть бути непридатними або недостатньо репрезентативними в умовах швидкого технологічного змінного середовища. Крім того, вони можуть не враховувати специфічні які є актуальними саме для ІТ сфери. Тому виникає необхідність у розробці нових підходів до моделювання ризиків в ІТ компаніях, які враховуватимуть швидкий технологічний прогрес, зміни на ринку та кібербезпеку. Процес діагностики в ІТ компаніях направлено на виявлення проблем, несправностей, відхилень або вразливостей в інформаційних системах, програмних продуктах чи технологічних процесах. Це може включати в себе знаходження помилок в програмному коді, ідентифікацію системних проблем, а також виявлення можливих загроз безпеці даних. Аналіз ризиків – це процес визначення, оцінки та управління можливими небезпеками та ризиками, пов'язаними з інформаційними системами, проектами, програмними продуктами або технологічними ініціативами. Він включає в себе ідентифікацію потенційних загроз, оцінку ймовірності їх виникнення та впливу на діяльність компанії, а також розробку стратегій та заходів для зменшення ризиків або зниження їх наслідків. Отже, актуальною є постановка завдання щодо розробки та адаптації нових підходів до моделювання ризиків, які враховуватимуть специфіку ІТ індустрії та дозволять більш ефективно виявляти, аналізувати та управляти ризиками, забезпечуючи стійкість та зростання ІТ компаній у сучасному конкурентному середовищі в умовах зростаючих викликів і невизначеності.

Аналіз останніх досліджень і публікацій

Останні дослідження та публікації в області моделювання ризиків висвітлюють нові підходи та методи, які допомагають вдосконалити управління підприємствами. Сучасна ризикологія накопичила великий обсяг знань, що доводять результати досліджень українських вчених. Вивчення аспектів аналізу економічних ризиків, методик його здійснення та систем оцінки управління проектами разом з проблемами розвитку ІТ-компаній акцентується в дослідженнях таких вчених, як В. В. Вітлінський [1], Є. М. Крижановський [2], О. В. Козирєва [3], Посохов І. М. [4], Хаустова В.Є. [5] та інших.

Оцінка ризику визначається за допомогою якісних та кількісних методів. Якісні методи дозволяють ідентифікувати ризики, оцінити впливаючи фактори. Кількісні методи включають числові показники, їх розрахунок, а також аналіз чинників, що створюють ризик. Вони враховують інтервали часу, що витрачається на управління ризиком, ступень ризику та навіть рівень професіоналізму приймача рішень. Але нажаль, деякі аспекти управління проектними ризиками в ІТ-компаніях та можливі способи їх вдосконалення в сучасних економічних умовах не були належним чином досліджені та вимагають більш ретельного аналізу.

Формулювання цілей статті

Мета статті є дослідження останніх тенденцій в області моделювання ризиків ІТ компаній у сучасних економічних умовах, зокрема використання штучного інтелекту, адаптивного управління технологічними ризиками та інших новаторських підходів та визначення Поставлена задача визначити переваги, які можуть принести нові підходи до моделювання ризиків для ІТ компаній, а також виявити можливі труднощі та виклики, пов'язані з їх впровадженням.

Виклад основного матеріалу

В сучасних умовах ІТ-сфера є одним з найбільш динамічних сегментів національної економіки України та джерелом надходження коштів до країни. Бізнес акцентує свою увагу на інноваціях та просуванні ІТ-технологій як найбільш перспективних напрямків для досягнення економічного зростання. На даний момент майже в усіх ІТ компаніях основним елементом у загальній системі управління є "управління проектами", тоді як "управління ризиками" часто розглядається як допоміжний процес. Але важливо зауважити, що навіть при успішності ІТ-сфери, для розвитку вітчизняних ІТ-компаній є важливим вдосконалення існуючої системи управління проектними ризиками.

Традиційні підходи до моделювання ризиків, які успішно використовуються в інших сферах бізнесу, недостатньо адаптовані до особливостей ІТ індустрії. ІТ компанії стикаються з унікальними викликами, такими як швидкі зміни технологічного ландшафту, постійна загроза кібератак, необхідність ефективного управління персоналом та інші аспекти, які вимагають інноваційного підходу до оцінки та управління ризиками. Традиційні методи можуть бути недостатньо гнучкими та адаптивними, щоб відповідати вимогам швидкозмінного середовища. Однією з ключових проблем є відсутність підходів, які б ураховували динамічний характер ІТ індустрії та швидкозмінність її факторів ризику.

Розглянемо відмінності до моделювання ризиків в ІТ компаніях в порівнянні зі звичайними підприємствами.

По-перше, одним із ключових джерел ризиків для ІТ компаній є швидкий технологічний розвиток ІТ сфери. ІТ компанії стикаються зі значними інноваційними ризиками, пов’язаними з науково-технічним та технологічним прогресом. ІТ галузь постійно удосконалюється, нові технології з'являються швидко, а існуючі технології стають застарілими. Нові технології, з якими часто працюють ІТ-компанії, можуть бути менш передбачуваними та менш стабільними, ніж ті, що використовуються у звичайних компаніях. Це створює нестабільність та невизначеність, оскільки компанії мають швидко адаптуватися до нових технологій та інновацій, щоб залишатися конкурентоспроможними. Традиційні моделі ризиків, засновані на статистичних даних з минулого, можуть бути непридатними в такому змінному середовищі. Тому виникає потреба у нових підходах до моделювання технологічних та інноваційних ризиків.

По-друге, в сучасному цифровому світі постійно існують загрози кібербезпеки. Кібератаки можуть призвести до серйозних наслідків, таких як втрата даних, порушення конфіденційності та фінансові збитки. Моделювання ризиків, пов'язаних з кібербезпекою, вимагає аналізу таких загроз та вразливостей. ІТ компанії зазвичай використовують спеціалізовані підходи до моделювання ризиків, які дозволяють оцінити загрози, пов’язані з кібербезпекою, та визначити ефективні заходи для їх запобігання. Наприклад, для виявлення аномальної активності та попередження можливих кібератак актуальним є використання технологій штучного інтелекту та аналізу великих обсягів даних.

По-третє, ІТ компанії оперують великою кількість даних. Для моделювання таких ризиків важливо використовувати прогнозування та аналіз трендів. Це дозволяє визначити потенційні переваги та небезпеки нових технологій, оцінити їх вплив на бізнес-процеси та прийняти відповідні рішення. Тому вони мають використовувати складну аналітику даних для оцінки ризиків та прийняття рішень. Нові підходи до моделювання можуть включати в себе використання методів швидкого прототипування та сценарного аналізу, що дозволяє оцінити можливі ризики та виявити шляхи їх зниження.

Зміни на ринку є ще одним важливим джерелом ризиків для ІТ компаній. Динамічний характер ІТ індустрії та швидкозмінність її факторів ризику, ринкова конкуренція, зміни вимог клієнтів та зміна попиту на продукти та послуги можуть вплинути на прибутковість та успішність компаній. Щоб прогресувати в цьому напрямку, необхідно проводити подальші дослідження в напрямку розробки сучасних математичних моделей аналізу ризиків. Рекомендовано проводити дослідження впливу сучасних технологій, таких як штучний інтелект та аналіз великих обсягів даних, для розробки пропозицій щодо ефективного управління ризиками в компаніях сфери ІТ. Серед перспектив забезпечення стійкості бізнесу в галузі ІТ – створення нових методик моделювання ризиків та сучасних математичних моделей, які враховуватимуть специфіку цього сектору. На сьогоднішній день в ІТ-компаніях загалом використовуються традиційні методи управління ризиками в проектах, які включають чотири ключові етапи: ідентифікацію ризиків, оцінку ризиків, розробку стратегій реагування на ризики та моніторинг ризиків [6].

Якісний аналіз можливих ризиків проводиться на етапі ідентифікації ризиків. Основна мета цього аналізу – отримання інформації про властивості об'єкта та його структуру, а також наявних ризиків. Це допомагає виявити джерела, причини та фактори ризиків, ідентифікувати можливі зони ризиків та їх види.

Етапу оцінки ризиків відповідає їх кількісний аналіз. Проводиться чисельне визначення як окремих ризиків так і ризику проекту в цілому. На цьому кроці розраховується ступень ризику та визначаються кількісні показники припустимого рівня ризику. Для цього розраховуються ймовірності виникнення ризиків та розміри їх наслідків. Таким чином етап оцінки ризику передбачає визначення імовірності та масштабу можливих збитків та враховує імовірність комерційного і технічного успіху в залежності від характеру проекту.

Наступний етап – розробка стратегій реагування на ризики. Це набір правил, на основі яких надаються методи вибору рішень у ситуаціях з ризиком. Серед цих правил традиційно виділяють наступні:

– максимізація виграшу;
– досягнення оптимальної ймовірності результату;
– забезпечення оптимального рівня коливання результату;
– поєднання оптимального балансу між виграшем і рівнем ризику.

Моніторинг ризиків – це останній крок у процесі керування ризиками. Він включає контроль та коригування результатів виконання вибраної стратегії з урахуванням нової інформації. Під час контролю здійснюється отримання від ризик-менеджерів даних про виниклі збитки та прийняті заходи для їх мінімізації.

Для моделювання ризиків, пов'язаних зі змінами на ринку, необхідно враховувати фактори, такі як ринкові тенденції, стратегічне планування та аналіз конкурентів. Тут важливим елементом є аналіз маркетингових даних, що дозволяє виявити зміни відносно попиту, конкурентної ситуації та інших факторів.

Основними методами моделювання ризиків в звичайних компаніях є:

– SWOT Analysis, який визначає сильні та слабкі сторони компанії, а також можливості та загрози в зовнішньому середовищі.
– метод VaR (Value at Risk), який використовується для визначення максимального можливого збитку, який компанія може понести внаслідок ризикованих подій.

– метод аналізу сценаріїв для оцінки впливу можливих сценаріїв на фінансовий стан компанії.

– метод дерева рішень, що використовується для визначення ризиків та можливих варіантів дій у прийнятті рішень.

– метод аналізу чутливості, який визначає, як зміна певних параметрів впливає на ризики та результати компанії [1, 6].

Але традиційні методи ризик-менеджменту можуть бути недостатньо гнучкими та адаптивними, щоб відповідати вимогам швидкозмінного IT середовища.

Підходи до моделювання ризиків в IT компаніях мають відрізнятися від підходів до моделювання ризиків в звичайних компаніях через специфічність і особливості IT індустрії. Однією з таких особливостей є те, що IT компанії стикаються з унікальними технічними ризиками, пов'язаними з використанням цифрових технологій. Це можуть бути проблеми з програмними багами, вразливостями програмного забезпечення, а також невідомими вразливостями, які можуть бути використані зловмисниками. Додамо, що IT компанії перебувають на передовому рівні технологій, і на їх ризики впливають зміни технологічних тенденцій та впровадженням новаторських рішень. Розвиток нових технологій, таких як нейронні мережі, штучний інтелект, Інтернет речей (IoT) може призвести до нових типів загроз. Відповідно, підходи до моделювання ризиків повинні враховувати вплив цифрових технологій та інновацій на бізнес-процеси та визначати можливі ризики та вигоди.

У сучасному цифровому світі одним із найбільш актуальних ризиків для IT сфери стала кібербезпека. Кібератаки можуть призвести до втрати даних, порушення конфіденційності, порушення роботи систем та серйозних фінансових збитків. Варто відзначити, що в кібербезпеці ключовими поняттями є кіберризики та кіберзагрози, і їх розуміння допомагає оцінити рівень вразливості та вплив на цифрові активи та інформацію. Кіберризики та кіберзагрози відображають два відмінних поняття. Кіберзагрози представляють собою конкретні дії або методи, якими зловмисники користуються для атак на системи, мережі та інші цифрові ресурси. Це може бути, наприклад, використання вразливостей програмного забезпечення, фішингові атаки або експлуатація розширень для злому систем, вони також включають можливість підвищення привілеїв. Кіберзагрози є особливою формою небезпеки, яка може викликати кіберризики. Ця ситуація створює потенціал для втрати конфіденційності, цілісності та доступності цифрових активів. Вплив кіберзагроз на ризик також може включати фактори, такі як шахрайство, фінансові злочини, втрату даних або обмеження доступності системи [6].

Кіберризики є більш широким поняттям. Вони виникають з можливості вразливості системи або мережі перед реальними кіберзагрозами. Це означає, що хоча певні загрози можуть існувати, їх вплив на дійсний ризик залежить від рівня захищеності системи та можливостей зловмисників. Але кіберризик можна розглядати як одну з форм ризику, а точніше, як певний вид операційного ризику в цифровій сфері. Цей вид ризику може викликати різноманітні негативні наслідки, такі як фінансові втрати, пошкодження репутації та інші негативні впливи, які пов'язані з продуктивністю та регулюванням. Крім того, цей вид ризику може мати наслідки і в фізичній сфері, призводячи до збитків, наприклад, пошкодження операційного обладнання.

Математичні моделі та методи допомагають оцінити та управляти ризиками як в інформаційно-технологічних компаніях, так і в звичайних компаніях, враховуючи їхні специфічні аспекти та потреби.

В таблиці 1 наведено порівняння основних аспектів між методами моделювання ризиків в інформаційно-технологічних компаніях та звичайних компаніях. Відмінності полягають в специфіці і особливостях IT індустрії, таких як швидкозмінний технологічний ландшафт, важливість кібербезпеки, технічні ризики, інновації та інші.

Таблиця 1

Особливості моделювання ризиків в залежності від сфери діяльності зрілості систем управління

Аспекти порівняння	**Критерії моделювання**	
	Математичні моделі в IT компаніях	**Математичні моделі в звичайних компаніях**
Технологічні зміни	Враховують швидкозмінність технологічного ландшафту	Можуть бути менше вираженими
Кібербезпека та кіберризики	Враховують імовірність кібератак, захисту та вплив на бізнес-процеси	Можуть не враховувати кібербезпеку
Статистичні дані	Використовують статистику з кіберподій та технічних ризиків	Використовують загальну статистику
Адаптивність	Можуть бути адаптивними до швидких змін	Зазвичай менше адаптивні
Інновації та зміни	Враховують вплив інновацій на ризики	Враховують вплив інновацій
Гнучкість та адаптація	Можуть бути розроблені для гнучкого врахування змін	Зазвичай менше гнучкі
Фінансові аспекти	Враховують можливий вплив ризиків на фінансовий стан	Аналізують загальний фінансовий стан

Джерело: складено автором

Застосовування нових методів моделювання ризиків з використанням штучного інтелекту та аналітики даних може істотно покращити виявлення потенційних загроз в роботі IT підприємств. Такі

методи та математичні моделі дозволяють аналізувати величезний обсяг інформації, зокрема журналів подій та інших даних, що стосуються кібербезпеки (це дозволяє виявити підозрілі активності, аномалії та відновити вирішення загроз), аналізувати тренди та прогнозувати майбутні ризики за допомогою аналізу статистичних даних, прогнозувати та оцінювати зміни серед багатьох факторів, які можуть впливати на ризики в IT середовищі. Нові підходи до моделювання можуть використовувати методи аналізу Big Data та машинного навчання для отримання більш точних прогнозів та оцінки ризиків. Використання нових методів дозволяє враховувати ці тенденції та визначати можливі ризики вперед.

Математичні моделі використовують методи інтелектуальної обробки інформації в поєднанні з експертними методами прийняття рішень. Прикладами моделей штучного інтелекту та аналітики даних, які можуть бути використані для моделювання кіберризиків та виявлення загроз в роботі IT підприємств є:

– модель виявлення вторгнень (IDS) використовує алгоритми машинного навчання та аналізу даних для виявлення аномальних або небезпечних активностей в комп'ютерних системах.;

– модель передбачення загроз (Threat Intelligence) використовує дані з різних джерел, таких як форуми, блоги та бази даних з попередніми інцидентами, щоб передбачити можливі кіберзагрози. Вона використовує аналіз текстів та обробку природної мови для виявлення згадок можливих атак;

– модель виявлення фішингу та шахрайства (Anti-Phishing) використовує аналіз ланцюжків електронних листів та URL-адрес для виявлення підозрілих повідомлень, що можуть бути спробами фішингу або шахрайства;

– модель прогнозування вразливостей використовує дані про вразливості програмного забезпечення та сторонніх джерел для прогнозування можливих місць уразливості в майбутньому. Вона використовує аналітику даних для ідентифікації потенційних ризиків [8, 9].

Розширення та поглиблення середовища штучного інтелекту та забезпечення його ефективного існування в різних предметних областях дозволяє своєчасно приймати заходи для забезпечення безпеки та захисту від можливих загроз в IT компаніях. Використання методів прогнозування та аналізу трендів при моделюванні ризиків в IT компаніях дозволяє виявити потенційні переваги та загрози нових технологій, а також оцінити їх вплив на бізнес-процеси компанії. Наприклад, використання аналітики даних та машинного навчання може допомогти передбачити тенденції розвитку технологій та ідентифікувати можливі ризики, що дозволить компаніям приймати обґрунтовані рішення щодо їх впровадження.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

В результаті проведеного аналізу можна відзначити, що нові підходи до моделювання ризиків в IT компаніях мають значний потенціал для забезпечення стійкості цифрового бізнесу. Вони дозволяють компаніям більш точно визначати ризики, а також розробляти ефективні стратегії управління, що сприяє забезпеченню їх успішності та конкурентоспроможності. Однак, важливо пам'ятати, що це постійний процес, оскільки технологічний розвиток та загрози змінюються з часом. Тому подальші дослідження у цій області є важливими для розвитку ефективних методів моделювання ризиків в IT компаніях. Розвиток нових підходів до моделювання ризиків дозволить компаніям адаптуватися до змін, забезпечити стійкість та досягнення своїх стратегічних цілей. Це буде важливим внеском у розвиток IT галузі та створення стійких та інноваційних організацій.

Література

1. Вітлінський В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємництві : монографія. Київ : КНЕУ, 2004. 480 с.

2. Крижановський Є. М., Ящолт А. Р., Жуков С. О., Козачко О. М. Моделювання бізнес-процесів та управління IT-проєктами. Вінниця : ВНТУ, 2018. 91 с.

3. Козирєва О. В., Іванов М. Є. Теоретичні аспекти управління проектними ризиками в IT-компаніях. Бізнес Інформ. 2019. № 12. С. 420– 425. URL: https://doi.org/10.32983/2222-4459-2019-12-420-425

4. Посохов І. М. Теоретичні та практичні аспекти управління ризиками корпорацій : монографія. Харків : Слово, 2014. 499 с.

5. Хаустова В.Є., Козирєва О.В., Іванов М.Є. Удосконалення системи управління проектними ризиками в IT-компаніях України. Наукові записки Національного університету «Острозька академія». Серія «Економіка» : науковий журнал. Острог : Вид-во НаУОА, березень 2021. № 20(48). С. 53–58. DOI: 10.25264/2311-5149-2021-20(48)-53-58

6. Івченко І. Ю. Моделювання економічних ризиків і ризикових ситуацій : навч. посібник. К. : Центр учбової літератури, 2007. 344 с. URL:https://www.twirpx.com/file/605996/

7. Калініна І.В., Лісовиченко О.І. Використання генетичних алгоритмів в задачах оптимізації. Міжвідомчий науково-технічний збірник. 2015. № 1(26).

8. Іваніченко Є.В., Сабліна М. А., Кравчук К.В., Використання машинного навчання в кібербезпеці, Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»: Том 4 № 12. 2021

References

1. Vitlinskyi V. V., Velykoivanenko H. I. Ryzykolohiia v ekonomitsi ta pidpryiemnytstvi : monohrafiia. Kyiv : KNEU, 2004. 480 s.

2. Kryzhanovskyi Ye. M., Yashcholt A. R., Zhukov S. O., Kozachko O. M. Modeliuvannia biznes-protsesiv ta upravlinnia IT-proiektamy. Vinnytsia : VNTU, 2018. 91 s.

3. Kozyrieva O. V., Ivanov M. Ye. Teoretychni aspekty upravlinnia proektnymy ryzykamy v IT-kompaniiakh. Biznes Inform. 2019. № 12. S. 420– 425. URL: https://doi.org/10.32983/2222-4459-2019-12-420-425

4. Posokhov I. M. Teoretychni ta praktychni aspekty upravlinnia ryzykamy korporatsii : monohrafiia. Kharkiv : Slovo, 2014. 499 s.

5. Khaustova V.Ie., Kozyrieva O.V., Ivanov M.Ie. Udoskonalennia systemy upravlinnia proektnymy ryzykamy v IT-kompaniiakh Ukrainy. Naukovi zapysky Natsionalnoho universytetu «Ostrozka akademiia». Seriia «Ekonomika» : naukovyi zhurnal. Ostroh : Vyd-vo NaUOA, berezen 2021. № 20(48). S. 53–58. DOI: 10.25264/2311-5149-2021-20(48)-53-58

6. Ivchenko I. Yu. Modeliuvannia ekonomichnykh ryzykiv i ryzykovykh sytuatsii : navch. Posibnyk. K. : Tsentr uchbovoi literatury, 2007. 344 s. URL: https://www.twirpx.com/file/605996/

7. Kalinina I.V., Lisovychenko O.I. Vykorystannia henetychnykh alhorytmiv v zadachakh optymizatsii. Mizhvidomchyi naukovo-tekhnichnyi zbirnyk. 2015. № 1(26).

8. Yevhen Ivanichenko, Mylana Sablina, Kateryna Kravchuk, Vykorystannia mashynnoho navchannia v kiberbezpetsi, Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika»: Tom 4 № 12. 2021