

Ірина ДАНИЛЮК

кандидат економічних наук, доцент, Західноукраїнський національний університет,
Тернопіль, Україна, irynadanylyuk9@gmail.com
ORCID ID: 0000-0002-5090-0926

УПРАВЛІННЯ РИЗИКАМИ В ІТ-БІЗНЕСІ

Вступ. В умовах нестабільності особливої актуальності набувають питання аналізу, оцінки й управління ІТ-ризиками в бізнес-середовищі. Застосування відповідних технологій дає можливість компаніям ідентифікувати, оцінити та зменшити ризики в процесі ухвалення рішень. Такі технології охоплюють аналіз даних, моделювання ризиків та стимуляцію, а також стратегії управління ризиками. Аналіз даних дає змогу підприємствам ідентифікувати тенденції та прогнозувати можливі ризики на основі попередніх даних. Моделювання ризиків та стимуляція дають можливість компаніям оцінити реальні ризики та їхні наслідки.

Для ефективного управління бізнес-ризиками необхідно також розуміти, які види ризиків існують. Вони можуть бути пов'язані зі змінами управлінських рішень, фінансовою діяльністю, кадровою політикою, інфраструктурними проектами тощо. Важливим аспектом є управління ризиками, пов'язаними з безпекою. Вони стають все більш актуальними в контексті зростаючих кіберзагроз.

Мета – узагальнити види та методи дослідження ризиків в ІТ-бізнесі, систематизувати процеси управління ними та обґрунтувати заходи щодо їх попередження й уникнення.

Результати. Розглянуто види ІТ-ризиків, досліджено діяльність успішних компаній в ІТ-сфері з метою виявлення інструментів впливу на величину ризику. Досліджено технології аналізу, оцінки, управління бізнес-ризиками для систематизації та розробки заходів щодо їх попередження, уникнення. Теоретичне і практичне значення виявляється у тому, що аналіз ризиків в управлінні бізнес-процесами дає змогу підприємствам уникнути негативних наслідків для бізнесу та підвищити ефективність фінансово-господарської діяльності. Обґрунтовано фактори впливу на ризики в бізнесі, здійснено оцінку потенційних загроз безпеці, які можуть виникнути в процесі роботи з ІТ-системами.

Висновки. Проведений аналіз діяльності успішних ІТ-компаній свідчить про те, що зниження рівня ризику можна здійснити за допомогою впровадження технологій, вдосконалення продуктів/послуг компанії, використання страхових полюсів, впровадження фінансових заходів, інших інструментів. Ефективне управління ризиками на підприємстві є запорукою його успішної діяльності.

Ключові слова: бізнес-середовище, IT-ризик, бізнес-ризиками, управління IT-ризиками, бізнес-процеси, SWOT-аналіз, фінансові алгоритми.

Табл.: 5, рис.: 2, бібл.: 20.

Iryna DANYLYUK

Ph. D. (Economics), Assoc. Prof. West Ukrainian National University, Ternopil, Ukraine,
irynadanylyuk9@gmail.com
ORCID ID: 0000-0002-5090-0926

RISK MANAGEMENT IN IT-BUSINESS

Introduction. The article is devoted to topical issues of analysis, assessment and management of IT-risks in the business environment. The application of appropriate technologies enables companies to identify, assess and minimize risks in the decision-making process. Such technologies may include data analysis, risk modeling, and simulation, as well as risk management strategies. Data analysis can help businesses to identify trends and predict possible risks based on previous data. Risk modelling and simulations can help companies to estimate the possibilities that certain risks will become a reality and what are the consequences.

For effective business-risk management, it is also necessary to understand what risks types exist. Risks can be associated with changes in management decisions, financial, personnel and infrastructure risks, etc. An important aspect of risk management is the provision of security-related risks, which are becoming increasingly relevant in the context of growing cyber threats and other forms of cybercrimes.

The purpose of the article is to reveal the types, methods of risk research in the IT-business, their management and the justification of ways and measures to prevent and avoid them.

Results. The types of IT risks are considered, the activities of successful companies in the IT sphere are studied in order to identify tools for influencing the magnitude of risk. The technologies of analysis, evaluation, management of business risks for systematization and development of measures for their prevention and avoidance are studied. The theoretical and practical significance is manifested in the fact that risk analysis in the management of business processes allows enterprises to avoid negative consequences for business and increase the efficiency of financial and economic activities. The factors influencing risks in business are substantiated, an assessment of potential security threats that may arise in the process of working with IT systems is carried out.

Conclusions. The conducted analysis of the activities of successful IT companies shows that reducing the level of risk can be achieved with the help of the introduction of technologies, improvement of the company's products/services, the use of insurance poles, the implementation of financial measures, and other tools. Effective risk management at the enterprise is the key to its successful operation.

Keywords: business-environment, IT-risk, business-risks, IT-risk management, business-processes, SWOT-analysis, financial algorithms.

JEL Classification: D81.

Постановка проблеми. У сучасному світі, де бізнес-середовище є надзвичайно складним і непередбачуваним, питання аналізу, оцінки й управління бізнес-ризиками є надзвичайно важливими для успішної діяльності будь-якої компанії.

У широкому розумінні ризик визначають як можливість оцінити те, що певна подія може негативно вплинути на діяльність підприємства (організації), починаючи від економічних криз до природних катастроф, а також інших факторів – зміни законодавства або конкуренції на ринку.

Технології аналізу, оцінки, управління бізнес-ризиками дають змогу компаніям ідентифікувати, оцінити та зменшити ризики в процесі прийняття рішень. Вони охоплюють аналіз даних, моделювання ризиків та стимуляцію, а також стратегії управління ризиками. Аналіз даних дає змогу підприємствам ідентифікувати тенденції та прогнозувати можливі ризики на основі попередніх даних. Моделювання ризиків та стимуляція дають можливість оцінити вірогідність того, чи певні ризики стануть реальністю та які їхні наслідки. Також існують стратегії управління ризиками, такі як: розподіл ризиків між підприємствами, страхування, диверсифікація та ін.

Аналіз останніх досліджень і публікацій. Теоретичним обґрунтуванням сутності та дослідженням проблеми виявлення причин формування ризиків та їх елементів з метою ефективного управління підприємством займалися багато науковців, зокрема: В. В. Вітлінський [2], О. М. Крайнік [3], О. Луців [4], В. М. Іщенко [5], Т. Л. Мостенська [6], Н. С. Скопенко [6], І. А. Нечаєва [7] та ін.

Незважаючи на ґрунтовні дослідження змісту категорії “ризик” та причин його виникнення, на більшу увагу заслуговують питання впровадження системи управління

ризиками як одного з елементів корпоративного управління.

Метою статті є узагальнення видів та методів дослідження ризиків в ІТ-бізнесі, систематизація процесів управління ними, обґрунтування заходів щодо їх попередження й уникнення.

Виклад основного матеріалу дослідження. Ризик – це процес перетворення потенційних загроз на реальні, або настання небажаних наслідків, які можуть виникнути внаслідок різних дій чи подій, що впливають на бізнес. Це можуть бути економічні ризики, технічні, природні, фінансові, правові тощо. Такий процес дає змогу бізнесу бути готовим до можливих наслідків та застосовувати заходи щодо їхнього запобігання і зменшення впливу.

Фактори, що впливають на ризик в бізнесі, можуть бути різними і залежать від конкретного виду діяльності й особливостей ринку. Проте є загальні фактори, які можуть впливати на ризик в бізнесі, незалежно від його спрямованості.

Оскільки не можливо повністю уникнути ризику, важливо вирішувати проблеми, що виникають, та зменшувати їх наслідки.

Процес визначення ІТ-ризиків передбачає оцінку потенційних загроз безпеці, які можуть виникнути в результаті впливу різних факторів (рис.1). Існують різні методики, які складаються з певної послідовності (ідентифікація потенційних ІТ-ризиків, оцінка впливу ризиків, оцінка ймовірності виникнення ризиків, визначення пріоритетів, розробка плану управління ризиками, впровадження плану управління ризиками).

В результаті виконання зазначених етапів компанія має повну картину щодо ІТ-ризиків (табл.1), їх впливу на бізнес-процеси та можливості зменшення. ІТ-ризики та їх зв'язок з бізнес-ризиками є актуальною темою для бізнесу. За даними досліджень, збитки від кібератак у 2020 р. становили

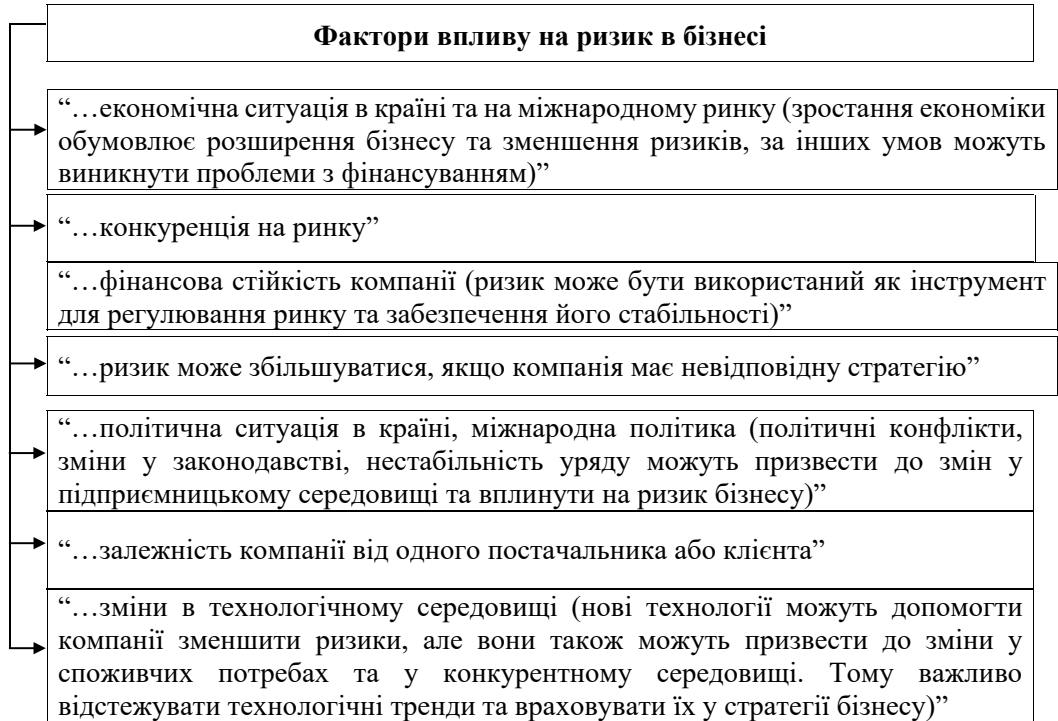


Рис. 1. Фактори, що впливають на ризик в бізнесі [1, 5, 9]

більше 1,5 трлн дол. США, що свідчить про важливість захисту інформації в бізнесі [10].

ІТ-ризиків можуть бути визначені як потенційні загрози, пов'язані з використанням технологій та інформації в бізнес-процесах. Основною метою управління ІТ-ризиками є забезпечення стійкості бізнес-процесів підприємства до можливих випадків порушення їх нормального функціонування.

Для успішного управління ІТ-ризиками важливо мати відповідну експертизу та знання про технології і стандарти безпеки. Наприклад, використання фреймворку NIST (National Institute of Standards and Technology) дає змогу компаніям розробити ефективні політики та процедури безпеки, що зменшують ризики та відновлюють роботу систем у разі виникнення інцидентів [11].

Зважаючи на ці ризики, важливо забезпечувати безпеку даних та розробляти від-

повідні політики безпеки. Наприклад, відповідно до звіту компанії Cisco, 61% компаній у світі мають політики безпеки для хмарних технологій, що забезпечує більшу захищеність від ІТ-ризиків [12].

Управління ІТ-ризиками є важливим аспектом діяльності будь-якого підприємства, оскільки керування ними забезпечує безпеку даних, знижує витрати на обслуговування ІТ-інфраструктури, підвищує та забезпечує продуктивність бізнес-процесів підприємства [11].

Успішні компанії, які працюють у складних умовах та змінному середовищі, мають декілька спільних рис, які дають змогу їм досягнути успіху навіть у непередбачуваних ситуаціях. До таких рис належать: гнучкість та адаптивність, інновації, конкурентні переваги, розуміння ризиків, командна робота, підтримка клієнтів, спрямованість на

Види ІТ-ризиків*

ІТ- ризик			
<i>Технічні ризики</i>			
Відмова обладнання	Помилки в програмному забезпеченні	Кібератаки	Втрата даних
<i>Людські ризики</i>			
Несумісність команди	Втрата ключових членів команди	Недостатня кваліфікація персоналу	Викрадення даних
<i>Природні ризики</i>			
Повені	Землетруси	Пожежі	Торнадо
<i>Безпека даних</i>			
Втрата конфіденційності даних	Неправомірний доступ до даних	Виток інформації	Віруси та шкідливе програмне забезпечення
<i>Ризики, пов'язані зі змінами в законодавстві</i>			
Зміни в регуляторному середовищі	Потенційні штрафи або судові позови	Несумісність з новими вимогами	Зміна політики конфіденційності
<i>Ризики, пов'язані зі змінами в технологіях</i>			
Застарілість технологій	Перехід до нових платформ	Нестабільність нових технологій	Конкуренція на ринку нових рішень

*Складено автором.

результат. У табл. 2 наведено перелік компаній, які успішно адаптуються до складних умов та працюють у змінному середовищі.

Успіх компанії в складних умовах також залежить від її здатності управляти ризиками та взаємодіяти із зацікавленими сто-

ронами, такими як клієнти, постачальники, регуляторні органи [10, 16].

Дослідження ризиків у бізнесі є важливим етапом для будь-якої компанії, а особливо для ІТ-компаній, які стикаються зі змінами у технологіях та вимогах клієнтів.

Таблиця 2

Характеристика адаптивних можливостей провідних міжнародних компаній у ризиковому середовищі [13,14,15,16]

Компанія	Характеристика адаптивних можливостей
Amazon	Змогла пережити економічну рецесію та зберегти свою позицію на ринку завдяки інноваційному підходу та здатності до адаптації у нових ринкових умовах
Tesla	Змінила автомобільну індустрію, роблячи електромобілі доступними та привабливими для споживачів. Вона здатна до інновацій та адаптації до нових технологій і ринкових умов
IBM	Успішно працює у складних умовах завдяки технологічним рішенням та адаптації до нових ринкових тенденцій та потреб
Procter & Gamble	Успішно працює у складних, змінних ринкових умовах та конкурентному середовищі завдяки маркетинговим стратегіям, здатності до інновацій та розвитку нових продуктів
McDonald's	Успішно працює у складних, змінних ринкових умовах та конкурентному середовищі завдяки здатності до інновацій й адаптації до різних культур, смаків споживачів
Google	Успішно працює у складних умовах завдяки своїм технологічним рішенням та здатності до адаптації до нових ринкових тенденцій і потреб

Однією з найпопулярніших ІТ-компаній є Alphabet Inc., материнська компанія Google [17, 18, 19]. Розглянемо ризики бізнесу Alphabet та можливі інструменти для їх зменшення.

Серед успішних компаній також варто виокремити Toyota, Unilever, Samsung, GE, Coca-Cola, Microsoft.

Для гарантування безпеки свого бізнесу успішні компанії активно застосовують технології аналізу, оцінки й управління бізнес-ризиками (табл.3).

Процес управління ризиками в Alphabet орієнтований на їх виявлення та зниження у всіх аспектах діяльності компанії. Для цього використовують, крім зазначених технологій, експертну оцінку, аналіз ризиків проєктів і програмного забезпечення, а також внутрішній аудит.

До зон ризику в Alphabet можна віднести фінансовий ризик, ризик технологій та інформації, ризик кадрів та ризик ділової репутації.

У діяльності Alphabet можна виокремити різні рівні ризику: стратегічний, ризик бізнесу, проєктний ризик. До методів зниження ризиків належать:

- зменшення ризику за допомогою технологій і вдосконалень у продуктах та послугах компанії;
- застосування страхових полюсів та інших фінансових інструментів для зменшення впливу ризику на фінансові результати компанії;
- розробка та виконання кризових планів і сценаріїв, які допоможуть компанії вирішити проблеми у разі виникнення кризи.

Alphabet застосовує різні методи аналізу ризиків, зокрема SWOT-аналіз (рис. 2.) та аналіз Портера (табл. 4). Також використовує експертну оцінку та різні інструменти для оцінки ризиків за допомогою Open FAIR (методика, яка дає змогу оцінити ризики з погляду їх впливу на бізнес та фінансові наслідки), інструменти моніторингу – Google Analytics, з метою відстеження трафіку та поведінки користувачів

Таблиця 3

Технології аналізу, оцінки та управління бізнес-ризиками компанії Alphabet [17, 18, 19]

№ з/п	Критерій	Характеристика
1	Ключові інструменти та технології	– моделі машинного навчання та штучного інтелекту для аналізу та проєктування ризиків у різних галузях бізнесу, включаючи кібербезпеку, фінанси та правові питання; – хмарні технології для зберігання й обробки даних з різних джерел, що дає змогу компанії виявляти та реалізувати ризики в реальному часі; – аналітика даних для візуалізації ризиків та їхнього рівня у різних галузях діяльності компанії; – технології блокчейну для забезпечення безпеки та відстежування даних у різних процесах компанії;
2	Методології та підходи	– підхід до оцінки ризиків, який дозволяє компанії оцінювати ризики на основі їх ймовірності та впливу на бізнес; – методика визначення критичності ризиків, що дає змогу компанії визначити та пріоритизувати ризики на основі їхнього впливу на ключові процеси та ресурси компанії; – підхід з управління ризиками, який охоплює розробку та впровадження стратегій і політик, що спрямовані на зменшення ризиків і забезпечення стійкості компанії.
3	Культура та організаційна структура	– у компанії високо цінують культуру безпеки та ризик орієнтованості; компанія має спеціальний підрозділ, що відповідає за управління ризиками та забезпечення безпеки; кожен працівник задіяний у забезпеченні безпеки, управлінні ризиками; організаційна структура дає змогу швидко й ефективно реагувати на ризики та управляти ними.
4	Результати та досягнення	компанія є одним з лідерів у галузі кібербезпеки та захисту персональних даних, активно розробляє та впроваджує нові технології для зменшення ризиків та забезпечення безпеки, таких як штучний інтелект, аналіз даних, машинне навчання.

<p>Сильні сторони (Strengths)</p> <ul style="list-style-type: none"> - лідер в галузі технологій та ІТ; - широкий спектр продуктів та послуг; - сильна фінансова база; - високі стандарти безпеки та приватності даних 	<p>Слабкі сторони (Weaknesses)</p> <ul style="list-style-type: none"> - залежність від рекламного бізнесу; - велика конкуренція в галузі технологій; - низький рівень міжнародного розширення; - нестабільність в роботі з деякими продуктами, наприклад, Google+
<p>Можливості (Opportunities)</p> <ul style="list-style-type: none"> - розвиток штучного інтелекту та машинного навчання; - розширення глобальної присутності на ринку; - розширення в галузі технологій та інтернету речей; - розвиток нових продуктів, наприклад, в сфері автономних транспортних засобів та медичних технологій 	<p>Загрози (Threats)</p> <ul style="list-style-type: none"> - регулювання технологічного сектору та приватних даних; - конкуренція в галузі технологій та зменшення популярності певних продуктів; - негативний вплив на здоров'я та благополуччя користувачів продуктів/послуг; - ризики кібератак та витоку даних

Рис. 2. SWOT-аналіз компанії Alphabet**

* Побудовано автором.

на своїх сайтах, програмах; систему моніторингу та захисту – Google Safe Browsing, яка дає змогу захистити користувачів від шкідливих сайтів і програм.

Актуальним для Alphabet є застосування різних програмних засобів для аналізу ризиків, зокрема Google Cloud Platform (має низку інструментів для безпеки та

Таблиця 4

Аналіз Портера компанії Alphabet [17, 18, 19]

Детермінанти конкуренції на ринку ІТ	Ступінь впливу	Характеристика
Загрози нових учасників	низький	ІТ-індустрія є високотехнологічною та капіталоємною, що ускладнює появу у ній нових учасників; має велику базу користувачів, займає лідерську позицію в своїй галузі, що робить її менш привабливою для інших учасників.
Постачальники	низький	Alphabet працює з великою кількістю постачальників, позиція на ринку послуг надзвичайно потужна, тому вільно впливає на ціни та умови контрактів; крім того, компанія має велику кількість постачальників, відповідно, зменшується вплив будь-якого постачальника.
Покупці	високий	У компанії Alphabet велика база користувачів, однак конкуренція в галузі надзвичайно висока, що може призвести до відтоку покупців в інші компанії (альтернативну продукцію).
Змінність товарів	низький	У компанії Alphabet широкий спектр продуктів та послуг, таких як пошук, реклама, хмарні обчислення, аналітика та інші, які є унікальними та важкозамінними.
Конкуренція в галузі	високий	ІТ-індустрія характеризується високим рівнем конкуренції, оскільки на ринку присутні багато гравців; конкурентами Alphabet є компанії Amazon, Microsoft, Facebook та інші; крім того, у цій галузі відбуваються інноваційні процеси, що змушують компанії змагатися за нові технології та продукти, а це може зменшити ринкову частку компанії.
Вплив уряду та законодавства	середній	Уряд та законодавство можуть мати значний вплив на ІТ-компанії щодо дотримання регулюючих вимог, конфіденційності даних та регулювання монополій; однак Alphabet має достатньо засобів, щоб виконувати вимоги та впливати на законодавство через лобіювання.

Управління ризиками компанії Alphabet [18]

Інструмент	Характеристика інструменту
Лобювання та співпраця зі змінами в законодавстві	Використання ресурсів для лобювання та адаптації до змін в законодавстві для відповідності вимогам.
Інвестиції в дослідження та розробки	Інвестування у дослідження та розробки нових технологій і продуктів з метою збільшення конкурентоспроможності.
Диверсифікація джерел прибутку	Розвиток інших напрямів бізнесу, таких як хмарні послуги, розробка програмного забезпечення, інтернет-послуги.
Стратегія ризик-менеджменту	Оцінка, контроль та зменшення ризиків у різних сферах діяльності компанії.
Забезпечення кібербезпеки	Використання методів, технологій для захисту систем, даних компанії від кібератак та інших загроз.
Аналіз ринку та конкурентів	Моніторинг ринку, конкурентів з метою розуміння тенденцій, прогнозування викликів і загроз.

захисту даних), Security Command Center, Cloud Identity, а також Cloud Armor.

Компанія складає кризовий план, який дає можливість діяти ефективно у разі нестабільної ситуації.

В Alphabet прибуток та ризик компанії взаємозалежні, оскільки великий потік коштів спрямовують у дослідження та розробки, які можуть бути ризиковими, але й одночасно можуть сприяти великим прибуткам. Ризики впливають на капіталізацію компанії, а отже, на фінансові показники та здатність залучати інвестиції. Інструменти управління ризиками зведено в табл. 5.

Отже, компанія Alphabet застосовує комплексний підхід до зменшення ризиків бізнесу, має досвід у розробці і впровадженні технологій, методологій управління ризиками та безпеки в бізнесі. Вона використовує підходи та методики, що дають змогу визначати й оцінювати ризики, розробляти стратегії управління ризиками, забезпечення безпеки, а також ефективно і вчасно реагувати на ризики, що виникли.

Висновки. Підсумовуючи вищезазначене, варто наголосити, що знання та розуміння ризиків, а також використання відповідних технологій, стратегій управління ризиками є надзвичайно важливими для

успішності будь-якої компанії у сучасному бізнес-середовищі. Без належної оцінки та управління ризиками підприємство може зазнавати значних втрат і, відповідно, негативних наслідків для бізнесу.

Одним із найважливіших аспектів управління ризиками є ідентифікація та аналіз видів ризиків, з якими компанія може зіткнутися. Зокрема, це можуть бути фінансові ризики, ризики, пов'язані зі змінами управлінських рішень, кадрові, інфраструктурні тощо. Особливу увагу потрібно звернути на ризики, що пов'язані з безпекою, оскільки кіберзагрози стають масовими.

Важливим для управління ризиками є застосування відповідних технологій і програмних рішень.

Список використаних джерел

1. Кері Д. Дж., Адамсон Х. Р. *Управління ризиками в бізнесі. Інтернаука.* 2019. URL : <https://www.google.com/search?client=avast-a-1&q>.
2. Вітлінський В. В., Верченко П. І. *Аналіз, моделювання та управління економічним ризиком : навч.-метод. посіб. для самост. вивч. дисц. Київ : КНЕУ, 2000. С. 292.*
3. Крайнік О. М. *Ризик-менеджмент як інструмент регулювання економічної поведінки суб'єктів господарювання в сучасних*

умовах. Інвестиції: практика та досвід. 2015. № 10. С. 28–31. URL : http://nbuv.gov.ua/UJRN/ipd_2015_10_7.

4. Луців О. Ризик-менеджмент як інструмент управління господарським ризиком у фармацевтії. Галицький економічний вісник. Економіка та управління національним господарством. 2014. Т. 45, № 2. С. 23–26.

5. Іщенко В. М. Ризик як фактор стабільності фінансового ринку. Економіка та держава. 2008. № 4. С. 71–74.

6. Мостенська Т. Л., Скопенко Н. С. Ризик-менеджмент як інструмент управління господарським ризиком підприємства. Вісник Запорізького національного університету. 2010. № 3(7). С. 74–79.

7. Нечаєва І.А., Дьордій Є. А. Управління ризиками підприємства в секторі іт-послуг як інструмент підвищення його конкурентоспроможності. Ефективна економіка. 2018. № 12. URL : http://nbuv.gov.ua/UJRN/efek_2018_12_67.

8. Старостіна А.О., Кравченко В.А. Ризик-менеджмент: теорія та практика : навч. посіб. для вузів. Київ : Кондор, 2004. 199 с.

9. Understanding financial statements: the balance sheet. Investopedia. URL : <https://www.investopedia.com/terms/b/balancesheet.asp>.

10. Cybersecurity Ventures. (2021, February, 23). Cybercrime to cost the world \$10.5 trillion annually by 2025. URL : <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>.

11. NIST framework for improving critical infrastructure cybersecurity, Version 1.1 (April 2018). URL : <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

12. Cisco Cloud Security Report 2020. URL : https://www.cisco.com/c/dam/en_us/products/security/cloud-security/2020-cloud-security-report.pdf.

13. Adaptation to change: characteristics of successful companies. URL : <https://www.jstor.org/stable/23259998>.

14. Effective leadership in successful companies. URL : <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4166803/>.

15. Hitt M. A., Ireland R. D., Hoskisson R. E. (2017). Strategic management: concepts and cases: competitiveness and globalization. Cengage Learning.

16. Kellermanns F. W., Eddleston K. A., Sarathy R., Murphy F. (2012). Innovativeness in family firms: a family influence perspective.

17. Alphabet Inc. Company Profile. Reuters. URL : <https://www.reuters.com/companies/GOOGL.O>.

18. Alphabet. About. URL : <https://abc.xyz/>.

19. Alphabet Inc. Market Watch. URL : <https://www.marketwatch.com/investing/stock/google>.

20. ISO/IEC 27001:2013 – Information security management, ISO. URL : <https://www.iso.org/standard/54534.html>.

References

1. Keri, D. Dzh., Adamson, Kh. R. (2019). Upravlinnia ryzykamy v biznesi [Risk management in business]. Internauka. Available at: <https://www.google.com/search?client=avast-a-1&>

2. Vitlinskyi, V. V., Verchenko, P. I. (2000). Analiz, modeliuvannya ta upravlinnia ekonomichnym ryzykom [Analysis, modeling and management of economic risk]. Kyiv: KNEU [in Ukrainian].

3. Krainik, O. M. (2015). Ryzyk-menedzhment yak instrument rehuliuвання ekonomichnoi povedinky subiektiv hospodariuvannya v suchasnykh umovakh [Risk management as a tool for regulating the economic behavior of business entities in modern conditions]. Investytsii: praktyka ta dosvid – Investment, Practice and Experience, 10, 28–31. Available at: http://nbuv.gov.ua/UJRN/ipd_2015_10_7.

4. Lutsiv, O. (2014). Ryzyk-menedzhment yak instrument upravlinnia hospodarskyim ryzykom u farmatsii [Risk management as a tool for economic risk management in pharmacy] Halytskyi ekonomichnykh visnyk. Ekonomika ta upravlinnia natsionalnym hospodarstvom – Galician Economic Bulletin. Economics and Management of the National Economy, 2, 23–26 (Vol. 45) [in Ukrainian].

5. Ishchenko, V. M. (2008). *Ryzyk yak faktor stabilnosti finansovoho rynku [Camelina as a factor of stability of the financial market]*. *Ekonomika ta derzhava – Economy and State*, 4, 71–74 [in Ukrainian].
6. Mostenska, T.L., Skopenko, N.S. (2010). *Ryzyk-menedzhment yak instrument upravlinnia hospodarskym ryzykom pidpriemstva [Risk management as a tool for managing the enterprise's economic risk]*. *Visnyk Zaporizkoho natsionalnoho universytetu – Bulletin of Zaporizhzhya National University*, 3(7), 74–79 [in Ukrainian].
7. Nechaieva, I.A., Dordii, Ye. A. (2018). *Upravlinnia ryzykamy pidpriemstva v sektori it-posluh yak instrument pidvyshchennia yoho konkurentospromozhnosti [Enterprise risk management in the IT services sector as a tool for increasing its competitiveness]*. *Efektivna ekonomika – Efficient Economy*, 12. Available at: http://nbuv.gov.ua/UJRN/efek_2018_12_67.
8. Starostina, A.O., Kravchenko, V.A. (2004). *Ryzyk-menedzhment: teoriia ta praktyka [Risk management: theory and practice]*. Kyiv: Condor [in Ukrainian].
9. *Understanding financial statements: the balance sheet*. Investopedia. Available at: <https://www.investopedia.com/terms/b/balancesheet.asp>.
10. *Cybersecurity Ventures*. (2021, February 23). *Cybercrime to cost the world \$10.5 trillion annually by 2025*. Available at: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>.
11. *NIST Framework for improving critical infrastructure cybersecurity, Version 1.1 (April 2018)*. Available at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
12. *Cisco Cloud Security Report 2020*. Available at: https://www.cisco.com/c/dam/en_us/products/security/cloud-security/2020-cloud-security-report.pdf.
13. *Adaptation to change: characteristics of successful companies*. Available at: <https://www.jstor.org/stable/23259998>.
14. *Effective leadership in successful companies*. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4166803/>.
15. Hitt, M. A., Ireland, R. D., Hoskisson, R. E. (2017). *Strategic management: concepts and cases: competitiveness and globalization*. Cengage Learning.
16. Kellermanns, F. W., Eddleston, K. A., Sarathy, R., Murphy, F. (2012). *Innovativeness in family firms: A family influence perspective*.
17. *Alphabet Inc. Company Profile*. Reuters. Available at: <https://www.reuters.com/companies/GOOGL.O>.
18. *Alphabet. About*. Available at: <https://abc.xyz/>.
19. *Alphabet Inc. Market Watch*. Available at: <https://www.marketwatch.com/investing/stock/googl>.
20. *ISO/IEC 27001:2013 – Information security management*, ISO. Available at: <https://www.iso.org/standard/54534.html>.