Minimization of risks associated with changing the business behavior of IT enterprises

Kompanets, N. I. [1]

Received: 2023-12-20
Accepted: 2024-01-29
DOI: https://doi.org/10.5281/zenodo.11123298

Annotation. It has been demonstrated that the risk management model associated with changes in the business behavior of IT enterprises due to war takes on a variable, scenario-based nature, which is formed for each enterprise depending on three key variables: response to war, success in operating under martial law, and readiness for post-war changes. The key features of IT enterprises' risk management are detailed, emphasizing its importance for achieving organizational goals in wartime conditions. The interrelations between risk management and business behavior of the enterprise are specified, taking into account key strategic decisions, tactics, and operational decisions in the organization. The paradox of security and enterprise development, arising against the backdrop of managing conflicting goals of achieving security while simultaneously fostering innovative and risky development in wartime, is characterized. Internal and external security factors of the enterprise are classified, and a refined classification of risks and threats manifested in the operation of IT enterprises is provided. A resolution to the security-development paradox is proposed, considering the theoretical peculiarities and practice of managing IT enterprises, features of risk management, risks, and threats in wartime, and in the context of post-war recovery prospects through the implementation of scenario-based planning for the transformation of business behavior. Considering previous results from the analysis of the peculiarities of managing the business behavior of IT enterprises under martial law, pessimistic, realistic, and optimistic scenarios are described. The main risks associated with changes in the business behavior of IT sector enterprises in Ukraine under different scenarios are detailed. To minimize risks associated with changes in the business behavior of IT enterprises during and post-war, a multi-level system of measures for different levels of enterprise management has been developed, based on the principles of risk management but also considering the prospects of post-war economic recovery and the necessity for future enterprise development to succeed in competitive battles on national and international markets. A model calculation of the balance of costs for security and development depending on the scenarios of business behavior development is substantiated, and detailed recommendations for effective balancing are developed. To strengthen the substantiated recommendations, key managerial competencies necessary for implementing the recommendations are briefly described.

Keywords: model, risk management, business behavior, scenarios, recommendations.

[1] Ph.D. candidate at the Lviv University of Business and Law ORCID ID: 0009-0000-6615-8810

Вступ

Як доведено у попередніх підрозділах, управління бізнес-поведінкою підприємств у сфері ІТ, як одній з найдинамічніших сфер національної і світової економіки, безпосередньо пов'язане із гнучкістю, адаптивністю, а у загальному – із змінами на різних рівнях управління, від стратегічного до мікроуправління. На перших етапах повномасштабної війни зміни головним чином стосувались оперативного вирішення безпосередніх загроз, що постали перед підприємствами сфери ІТ на тлі вторгнення – скорочення попиту у зв'язку з неготовністю іноземних замовників працювати в умовах форс-мажорних обставин, фізична загроза і релокація бізнесу, виїзд або мобілізація співробітників. За два роки діяльності в умовах воєнного стану підприємства сфери адаптувались до ризиків і продовжили працювати або ж припинили свою діяльність. Зараз ситуація умовно стабілізувалась, однак ризики, пов'язані зі зміною бізнес-поведінки через адаптацію до функціонування в умовах воєнного стану усе ще зберігаються. З іншого боку, існує розуміння того, що війна не триватиме вічно, а отже необхідно готуватись до переходу до функціонування у нормальних умовах, які, утім, суттєво відрізнятимуться від довоєнних.

Таким чином, модель управління ризиками, пов'язаними із зміною бізнес-поведінки підприємств сфери ІТ у зв'язку з війною набуває варіативного, сценарного характеру, що для кожного підприємства формується у залежності від трьох ключових змінних: реакції на війну, успішності діяльності в умовах воєнного стану, готовності до повоєнних змін. Таким чином, системний підхід до управління підприємствами сфери ІТ на тлі часового горизонту, що включає період від переходу до воєнного стану до повоєнної відбудови вимагає проведення сценарного аналізу, з урахуванням попередніх результатів дослідження, й, відтак, побудови системи заходів щодо мінімізації явних та прихованих ризиків.

Метою статті є обгрунтувати систему заходів мінімізації ризиків, пов'язаних зі зміною бізнес-поведінки підприємств сфери ІТ в умовах війни і повоєнний час.

Результати

Ризик-менеджмент є ключовим елементом стратегічного управління будь-якою організацією. Його важливість полягає в ідентифікації, аналізі та вжитті заходів щодо різних видів ризиків, які можуть вплинути на досягнення поставлених цілей. Цей процес дозволяє організаціям не тільки уникнути потенційних загроз, а й оптимізувати використання своїх ресурсів.

Перш за все, ефективне управління ризиками забезпечує стабільність організації, дозволяючи їй підготуватися до можливих криз та мінімізувати їх вплив. Такий стан досягається через систематичний підхід до оцінки ризиків, які можуть виникнути з різних джерел, включаючи фінансові коливання, правові обмеження, технологічні несподіванки, політичні зміни та природні катастрофи.

Ризик-менеджмент допомагає підвищити прозорість прийняття рішень у компанії. Відкритість процесів ідентифікації та аналізу ризиків дозволяє зацікавленим сторонам, включаючи інвесторів, кредиторів і акціонерів, краще розуміти стратегічні вибори та управлінські рішення, що сприяє зміцненню довіри і підтримки на довгострокову перспективу.

Врешті-решт, комплексне управління ризиками сприяє оптимізації вартості капіталу та ресурсів. Забезпечуючи адекватний контроль над можливими ризиками та

їх наслідками, організації можуть не тільки знизити витрати, пов’язані з неочікуваними втратами, але й ефективно розподілити свій капітал на найбільш прибуткові та безпечні інвестиції. Таким чином, управління ризиками є не просто захисним механізмом, а стратегічною перевагою, яка може забезпечити довгострокову стійкість організації.

Ризик-менеджмент демонструє глибокі та важливі взаємозв'язки з бізнес-поведінкою підприємства, визначаючи як стратегічні тактики, так і операційні рішення в організації. Основні напрямки взаємозв'язків можливо описати наступним чином.

1. Ризик-менеджмент відіграє ключову роль у стратегічному плануванні компанії допомагаючи визначити потенційні загрози та можливості, які можуть вплинути на досягнення корпоративних цілей. Інтеграція ризик-менеджменту у процес стратегічного планування забезпечує, що рішення приймаються з урахуванням повного спектру внутрішніх і зовнішніх чинників, зміцнюючи спроможність компанії адаптуватися та відреагувати на зміни в бізнес-середовищі.

2. Ризик-менеджмент формує культуру ризику в організації, впливаючи на ставлення і поведінку співробітників стосовно ризиків. Здорова культура ризику сприяє відкритості, де члени команди вільно обговорюють потенційні проблеми і виклики, вносячи свій вклад у рішення, що мінімізують загрози і максимізують можливості.

3. На операційному рівні, ризик-менеджмент впливає на повсякденні рішення і процедури забезпечуючи, щоб всі операції проводяться з урахуванням їхнього потенційного впливу на безпеку, стабільність і правову відповідність. Таким чином, ризик-менеджмент допомагає запобігати фінансовим збиткам і юридичним проблемам, одночасно зберігаючи довіру клієнтів і партнерів.

4. Ефективне управління ризиками також сприяє покращенню стосунків з інвесторами, кредиторами та іншими зацікавленими сторонами. Інформування про стратегії управління ризиками зміцнює довіру стейкхолдерів до компанії, забезпечуєбільш вигідні умови фінансування та загалом покращує репутацію організації.

Таким чином, ризик-менеджмент в умовах воєнного стану та з урахуванням перспектив повоєнної відбудови набуває характеру невід'ємною складовою стратегії бізнес-поведінки, що впливає на кожен аспект діяльності підприємства, від стратегічного планування до операційної ефективності. Поряд з цим, впровадження ризик-менеджменту вимагає докладного дослідження парадоксу безпеки і розвитку.

Парадокс безпеки та розвитку підприємства полягає у виявленні та управлінні здається суперечливими цілями: забезпечення максимальної безпеки, при одночасному сприянні інноваційному та ризикованому розвитку. З одного боку, підприємства прагнуть до безпеки для мінімізації ризиків та збереження стабільності. З іншого боку, для досягнення зростання та конкурентоспроможності вони повинні приймати ризики, що нерідко включають інновації та експерименти.

Безпека у даному контексті включає комплекс заходів для захисту активів компанії, зокрема її фінансових ресурсів, репутації, внутрішніх данних та фізичних активів. Підприємства впроваджують строгі контрольні системи, процедури дотримання норм і політики, щоб уникнути збитків і забезпечити довготривалу стійкість.

Розвиток натомість вимагає інвестицій у нові технології, входження на нові ринки, розвиток нових продуктів, що може супроводжуватися значними ризиками. Інновації

потребують вільного простору для творчості та можливості помилки, що вступає в конфлікт з політиками безпеки.

Описаний парадокс можливо подолати шляхом коректного балансування між ризиком та безпекою. Ефективний ризик-менеджмент дозволяє ідентифікувати, оцінити та контролювати ризики, давати простір для інновацій при одночасному забезпеченні необхідних запобіжних заходів. Таким чином, для підтримання здатності підприємства досягати довгострокових переваг необхідним завданням постає створення культури, яка визнає важливість ризиків та прийняття обґрунтованих рішень.

Безпека підприємства є критичним аспектом його стабільності та успішності, що включає заходи захисту від різноманітних ризиків, що можуть впливати на активи, репутацію, персонал та інформаційні ресурси. Внутрішні та зовнішні фактори безпеки підприємства формують комплексну систему, яка вимагає постійної уваги та управління.

I. Внутрішні фактори:

1. Людський фактор – непрофесіоналізм або ненавмисні помилки співробітників можуть привести до значних фінансових втрат або аварій. Тому, систематичне навчання та розвиток персоналу, а також створення культури відповідальності є важливими для забезпечення внутрішньої безпеки.

2. Корпоративна культура – відсутність чітко визначених політик управління ризиками та контролю може підвищити вразливість компанії до внутрішніх загроз. Зміцнення корпоративної культури, заснованої на прозорості та етичних стандартах, сприяє підвищенню внутрішньої безпеки.

3. Фізичні умови безпеки – адекватне утримання та оновлення фізичних активів та обладнання є ключовим для запобігання несправностей та аварій, які можуть негативно вплинути на безпеку персоналу та продуктивність процесів.

4. Безпека інформаційних систем – – захист даних та систем від кібератак є особливо актуальним у сучасному цифровому світі. Надійні технологічні рішення та регулярне оновлення захисних систем мінімізують ризики витоку даних і кіберзлочинності.

II. Зовнішні фактори:

1. Політико-правові ризики – зміни у законодавстві, вплив військової агресії рф.

2. Економічні умови – економічні коливання, такі як інфляція, курсові ризики, глобальні фінансові кризи.

3. Природні катастрофи – землетруси, повені, урагани та інші природні катастрофи.

4. Технологічні зміни – швидкий розвиток технологій що призводить до застарілості існуючих бізнес-моделей та процесів.

Забезпечення безпеки підприємства вимагає комплексного підходу до управління внутрішніми та зовнішніми ризиками. Відповідна стратегія та систематичне її втілення дозволяють не тільки знизити потенційні ризики, але й створити основу для стійкого розвитку та успішного майбутнього.

В академічній літературі та професійній практиці часто використовуються терміни «загроза» і «ризик», які мають відмінності у значенні та застосуванні. Розуміння цих відмінностей є критично важливим для ефективного управління безпекою та ризиками на підприємстві.

Термін «загроза» відноситься до будь-якої потенційної причини небажаної події, яка може завдати шкоди системі, організації або процесу. Загрози можуть мати різне походження: природне (наприклад, землетруси або повені), технологічне (наприклад, збій обладнання), людське (наприклад, помилки персоналу або зловмисні дії).

Ключовою характеристикою загрози є її потенціал спричинити втрату або шкоду, без оцінки ймовірності чи впливу цих подій [Костюк].

Ризик, у свою чергу, є поняттям, яке описує потенційний вплив на організацію в результаті реалізації загрози, при цьому враховуються ймовірність виникнення негативної події та можливі наслідки. Ризик може бути виражений як комбінація ймовірності події та її впливу на організацію. Оцінка ризиків включає ідентифікацію потенційних загроз, аналіз їх можливих наслідків та визначення ймовірності їх виникнення. Ризик завжди має кількісну або якісну оцінку [Рудніченко].

Між досліджуваними поняттями спостерігаються наступні основні відмінності:

1. Природа понять:

- загроза – це потенційний збудник негативної події.

- ризик – це оцінка потенційного впливу цієї події на організацію, з урахуванням її ймовірності.

2. Фокус оцінки:

- загрози оцінюються з точки зору їх наявності та потенціалу спричинити шкоду.

- ризики оцінюються через призму можливих втрат та ймовірності реалізації цих втрат.

3. Управлінський аспект:

- управління загрозами зосереджене на мінімізації та уникненні потенційних причин негативних подій.

- управління ризиками включає стратегії зниження ймовірності негативних подій або зменшення їх впливу на організацію.

Класифікація загроз і ризиків для підприємств включає різні категорії, кожна з яких має свої специфічні особливості та потребує відповідних методів управління. Нижче наведено універсальну класифікацію загроз та ризиків, яка може застосовуватися до більшості організацій, незалежно від їхнього розміру чи галузі. Загрози можливо класифікувати наступним чином.

Кожен вид загроз або ризиків вимагає індивідуального підходу до управління, включаючи адекватне страхування, розробку планів відновлення після надзвичайних ситуацій, тренінги персоналу та впровадження передових технологічних рішень для захисту. Розуміння та відповідне реагування на ці загрози та ризики є ключовим для забезпечення стійкості та успішного розвитку підприємства.

Українська IT-індустрія, зіткнувшись із викликами воєнного стану, демонструє необхідність адаптації бізнес-поведінки до змінюваних умов. Розглянемо песимістичний, реалістичний та оптимістичний сценарії розвитку підприємств цієї сфери в контексті воєнного стану та майбутнього відновлення.

У песимістичному сценарії, воєнний стан продовжує серйозно впливати на економіку, що призводить до зниження інвестицій в IT-сектор. Через збільшення ризиків, іноземні замовники відмовляються від послуг українських розробників, обираючи стабільніші ринки. Внутрішній ринок також стикається з проблемами, оскільки малі та середні підприємства зазнають фінансових втрат і скорочують бюджети на IT-проекти. В результаті, багато IT-спеціалістів емігрують у пошуках кращих можливостей, що призводить до відтоку мозків та зниження інноваційного потенціалу країни.

В реалістичному сценарії, IT-сектор продемонструє свою стійкість завдяки гнучкості та адаптації до нових умов. Підприємства активно переходять на дистанційну роботу, що дозволяє зберегти більшість проектів і робочих місць. Хоча деяке зниження іноземних

інвестицій спостерігається, значна частина замовників залишається вірною українським розробникам, оцінюючи їх як висококваліфікованих та економічно вигідних партнерів. Відновлення економіки поступово покращує ситуацію, і починають з'являтися нові можливості для розширення та інновацій, особливо у сферах, пов'язаних з цифровою трансформацією і кібербезпекою.

В оптимістичному сценарії, IT-індустрія не тільки встоїть, а й відіграє ключову роль у відновленні економіки. Висока адаптація до дистанційної роботи та збереження міжнародних клієнтів підкреслюють надійність і професіоналізм українських IT-фахівців. Збільшення державних інвестицій в технологічну інфраструктуру сприяє зростанню нових стартапів та інноваційних проектів. Підприємства не тільки відновлюють свої позиції, але й розширюються на нові ринки, залучаючи інвестиції та створюючи нові робочі місця. Крім того, акцент на кібербезпеку та розробку власних технологічних продуктів зміцнює міжнародну конкурентоспроможність України.

Описані сценарії підкреслюють необхідність гнучкого підходу до управління змінами та адаптації стратегій, залежно від зовнішніх обставин і внутрішніх можливостей підприємства. Розвиток IT-сектору в Україні, особливо в умовах воєнного стану та відновлення після війни, буде залежати від здатності підприємств адаптувати свою бізнес-модель та використовувати нові можливості для росту та інновацій.

З урахуванням попередніх досліджень практики управління підприємствами сфери IT, узагальнимо основні ризики у зв'язку зі зміною бізнес-поведінки підприємств IT-сектору України за різними сценаріями.

У контексті мінливих умов бізнес-середовища, особливо для IT-сектору України, який вимагає постійної адаптації до нових викликів, зокрема в умовах воєнного стану та перспектив повоєнного відновлення, розробка загальної стратегії управління ризиками є ключовою. Така стратегія повинна бути всебічною та враховувати специфіку сектору, включаючи технологічні, ринкові, геополітичні та соціальні аспекти. Основні вимоги до такої стратегії представимо наступним чином.

1. Ідентифікація та оцінка ризиків – аналіз вразливостей. Необхідно систематично ідентифікувати потенційні загрози для бізнесу, що можуть виникати з внутрішніх та зовнішніх джерел. Важливо оцінити ймовірність кожного ризику та потенційний вплив, який він може мати на діяльність підприємства.

2. Розробка стратегій реагування – планування дій. Важливо розробити стратегії, які дозволять мінімізувати або нейтралізувати ризики. Прикладами таких стратегій є страхування, диверсифікацію ринків, технічні рішення для забезпечення кібербезпеки, а також навчання персоналу для підвищення їхньої обізнаності та здатності ефективно реагувати на виклики.

3. Інтеграція у корпоративну культуру – залучення персоналу. Ризик-менеджмент повинен стати неодмінною частиною корпоративної культури. У цьому контексті є важливим забезпечення того, щоб усі рівні організації були інформовані та готові діяти у відповідності до політик управління ризиками.

4. Моніторинг та перегляд – неперервне оновлення. Оскільки зовнішнє середовище та внутрішні умови підприємства непередбачувані та змінюються, стратегія управління ризиками повинна постійно актуалізуватися. Регулярний перегляд та оновлення стратегії, базуючись на нових даних та змінах у середовищі,

гарантує, що підприємство матиме змогу справитись з можливими загрозами.

5. Використання технологій – технологічна інтеграція. Використання передових технологій для моніторингу, аналізу та управління ризиками є необхідним. Як приклад можливо навести автоматизовані системи для трекінгу ризиків, кібербезпеку, використання штучного інтелекту для прогнозування потенційних проблем та автоматизацію відповідей на інциденти.

Для мінімізації ризиків, пов'язаних зі зміною бізнес-поведінки підприємств сфери ІТ в умовах війни і повоєнного часу, необхідним є впровадження багаторівневої системи заходів для різних рівнів управління:

I. Стратегічний рівень:

1. Створення резервних планів діяльності:

- розробка планів дій на випадок різних сценаріїв, включаючи повне або часткове припинення бізнес-операцій;

- диверсифікація ринків та пошук нових напрямків діяльності для зменшення залежності від одного ринку чи сегменту.

2. Інвестиції в безпеку та відновлення:

- розробка та впровадження системи комплексної безпеки, що включає кібербезпеку, фізичну безпеку та безпеку даних;

- створення фондів на відновлення та відшкодування втрат у випадку кризових ситуацій.

II. Оперативний рівень:

1. Управління ланцюгами поставок:

- забезпечення наявності декількох надійних постачальників для критичних компонентів і послуг;

- моніторинг та регулярна оцінка стабільності постачальників та їх здатності виконувати зобов'язання у складних умовах.

2. Комунікаційна стратегія:

- підтримка відкритого діалогу з клієнтами, партнерами, та співробітниками для забезпечення прозорості діяльності та оперативного реагування на зміни умов;

- розробка кризових комунікаційних планів для випадків зміни умов ринку або політичної ситуації.

III. Тактичний рівень

1. Тренінги та підвищення кваліфікації:

- організація регулярних тренінгів для співробітників з питань безпеки, управління ризиками та ефективної роботи в умовах кризи;

- підвищення кваліфікації технічних команд для роботи з новітніми технологіями та методиками забезпечення стабільності систем.

2. Мінімізація фінансових ризиків:

- розробка бюджетів, що передбачають можливі кризові витрати та резервування коштів на непередбачені обставини;

- застосування фінансових інструментів для хеджування курсових ризиків та інших фінансових варіацій.

IV. Технологічний рівень

1. Забезпечення кібербезпеки:

- впровадження розширених засобів захисту даних, антивірусного захисту, шифрування і мережевої безпеки;

- регулярний аудит та оновлення безпекових систем для протидії новітнім загрозам.

2. Розробка відновлювальних стратегій:

- створення резервних копій важливих даних та систем, географічне розподілення серверних потужностей для мінімізації впливу локальних подій на роботу компанії;

- плани швидкого відновлення діяльності після кібератак або технічних збоїв.

Запропонована багаторівнева система заходів дозволяє не тільки знизити потенційні ризики, пов'язані з веденням бізнесу в умовах війни та

відновлення після неї, а й забезпечити стійкість і гнучкість ІТ-підприємств, адаптувавши їх до змінних умов.

Для ефективного управління ризиками в рамках песимістичного сценарію, коли ІТ-підприємства в Україні надалі стикатимуться з серйозними викликами через воєнний стан та його наслідки, необхідно застосувати конкретні та цілеспрямовані заходи. Ці заходи мають забезпечити стабільність підприємства, мінімізувати фінансові втрати та зберегти ключові кадрові ресурси.

Окреслені стратегії слід доповнити модельним розрахунком балансу витрат на безпеку та розвиток залежно від сценаріїв розвитку бізнес-поведінки підприємств. Таблиця має ілюстративний характер; у її основі закладено спостереження за бізне-поведнікою підприємств ІТ, власний досвід автора щодо управління таким підприємством, а формулювання відосоткових співвідношень здійснено за правилом Парето.

Додатково пропонуємо наступні основні рекомендації для ефективного балансування:

І. Песимістичний сценарій:

1. Приоритет безпеці – через високий рівень зовнішніх загроз і внутрішніх викликів, інвестиції в заходи безпеки повинні бути максимальними для захисту активів і ресурсів.

2. Обмеження витрат на розвиток – розвиток обмежується виживанням в складних умовах, з основним фокусом на підтримці існуючих потужностей і мінімізації втрат.

ІІ. Реалістичний сценарій:

1. Збалансовані інвестиції – інвестування в безпеку для забезпечення надійного функціонування бізнесу, одночасно підтримуючи розвиток нових продуктів та входження на нові ринки.

2. Гнучке реагування на зміни – постійний моніторинг ринкової ситуації для адаптації стратегії і бюджетів відповідно до поточних потреб і можливостей.

ІІІ. Оптимістичний сценарій:

1. Фокус на розвитку – використання стабільної ситуації для активних інвестицій у розвиток, дослідження та інновації; також напрямки розвитку можуть включати розширення на нові ринки та впровадження новітніх технологій.

2. Мінімізація витрат на безпеку – при стабілізації умов, витрати на безпеку можуть бути знижені, зберігаючи при цьому адекватний рівень захисту.

Запропонована модель дозволяє гнучко підходити до управління витратами в залежності від зовнішніх і внутрішніх умов, забезпечуючи підприємствам можливість максимізувати свої стратегічні переваги в різних сценаріях.

Ідентифікація оптимального набору заходів управління ризиками вимагає від менеджерів наявності специфічних компетенцій, які дозволять ефективно керувати підприємством в умовах складних та непередбачуваних обставин. Основні компетенції, необхідні для менеджерів, включають стратегічне мислення, аналітичні навички, лідерські якості, здатність до інновацій, а також високий рівень емоційного інтелекту.

Висновки

У сучасних умовах, коли бізнес-середовище охоплене невизначеністю, особливо в контексті воєнного стану у зв’язку з повномасштабним вторгненням рф, ефективний ризик-менеджмент стає критичним елементом забезпечення стійкості та адаптивності підприємств. Особливо важливим ризик-менеджмент у сучасних умовах залишається для ІТ-сектору, який є за свою природою високотехнологічним та вкрай чутливим до змін у зовнішньому середовищі. Реалізація системи мінімізації ризиків в умовах воєнного

стану дозволяє не тільки знизити потенційні загрози, але й надає можливість для планування дій в повоєнний період. Застосування сценарного планування є умовою визначення найбільш вірогідних варіантів розвитку подій та підготовки відповідних стратегій дій, що сприяє підвищенню загальної ефективності управління підприємством. Зрештою, компетентності менеджерів у сфері кризового управління, адаптивності до змін та стратегічного бачення майбутнього є необхідною умовою впровадження системи мінімізації ризиків, що, в свою чергу, забезпечує не тільки виживання, але й розвиток підприємств у складних умовах війни та повоєнного відновлення.

References

Пуцентейло, П. Р., & Гуменюк, О. О. (2016). Стратегічний аналіз як важливий елемент управління підприємством. http://dspace.wunu.edu.ua/bitstream/316497/3490/1/InnEko_3-4_2016_196-205.pdf

Дуднєва, Ю. Е., Антипцева, О. Ю., & Обидєннова, Т. С. (2019). Ризик-менеджмент: інтегрований підхід до організації. *Економіка і суспільство*, (20), 229-236.

Вербіцька, І. І. (2013). Ризик-менеджмент як сучасна система управління ризиками підприємницьких структур. *Сталий розвиток економіки*, (5), 282-291.

Гомба, Л. А., & Федорова, В. О. (2013). До питання сутності категорії економічної безпеки. *Вісник Чернівецького торговельно-економічного інституту. Економічні науки*, (4), 10-13. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Vchtei_2013_4_3.pdf

Шевченко, І. (2008). Особливості формування системи економічної безпеки підприємства.

Жихарєва, В. В., & Савельєва, Т. М. (2017). Формування стратегії розвитку підприємства в умовах невизначеності. *Економіка і суспільство*, *9*. https://eprints.cdu.edu.ua/4705/2/shkolna.pdf#page=417

Костюк, Ж. С. (2013). Поняття ризику, небезпеки та загрози як базових категорій розкриття сутності економічної безпеки підприємства. *Вісник економіки транспорту і промисловості*, (43), 142-149.

Рудніченко, Є. М. (2013). Загроза, ризик, небезпека: сутність та взаємозв'язок із системою економічної безпеки підприємства. *Економіка. Менеджмент. Підприємництво*, (25 (1)), 188-195. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/ecmepi_2013_25(1)__23.pdf

Українське IT у війну: як було, як зараз і які прогнози (дослідження). https://ain.ua/2022/12/09/ukrayinske-it-u-vijnu/