Хоменко Інна Олександрівна
д.е.н., професор
Сорока Анастасія Володимирівна
здобувачка вищої освіти 3 курсу
Національний університет «Чернігівська політехніка»
(м. Чернігів, Україна)

РИЗИКИ ТА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ СУЧАСНОГО БІЗНЕСУ: НАУКОВИЙ ОГЛЯД ТА АНАЛІЗ

Сучасний бізнес, без сумніву, є складною та динамічною системою, яка підлягає впливу численних ризиків та загроз, що ставлять під загрозу його економічну безпеку. Застосування новітніх технологій, глобалізація, зміни в політичному, економічному та соціальному середовищі створюють унікальні виклики для підприємств із різних галузей.

По-перше, сучасна глобалізація та швидкі технологічні зміни створюють нові можливості для бізнесу, але й супроводжуються збільшенням ризиків. По-друге, ростуть вимоги та очікування споживачів, що також спонукає компанії приділяти більше уваги економічній безпеці. По-третє, зростаюча кількість кіберзагроз та кібератак свідчить про необхідність адекватного аналізу ризиків і впровадження заходів щодо кібербезпеки.

Однією з найважливіших причин вивчення ризиків та загроз економічній безпеці сучасного бізнесу є необхідність забезпечення стійкості та конкурентоспроможності компаній. Зовнішні та внутрішні загрози можуть впливати на фінансові результати, репутацію, імідж, стосунки зі зацікавленими сторонами та інші аспекти діяльності підприємств. Розуміння та управління ризиками стає ключовим елементом стратегічного планування та прийняття рішень в бізнесі.

Дослідження ризиків та загроз економічній безпеці також має важливе значення для розвитку економічної теорії та практики. Вивчення різних типів ризиків, їхніх причин та наслідків, а також впливу загроз на економіку допомагає вдосконалювати моделі та методи аналізу ризиків, розробляти ефективні практики управління ризиками. Це дозволяє підприємствам ефективніше прогнозувати та управляти ризиками, знижувати втрати та максимізувати можливості.

Крім того, розгляд ризиків та загроз економічній безпеці сучасного бізнесу стає особливо актуальним у контексті глобальних викликів та кризових ситуацій. Природні катаклізми, екологічні проблеми, фінансові кризи, пандемії та інші події можуть значно підірвати економіку та стабільність бізнесу. Розуміння та аналіз ризиків допомагає компаніям підготуватися до подібних ситуацій, розробляти плани надійності та реагування, а також встановлювати стратегії резервування та відновлення.

Також слід відзначити, що розгляд ризиків та загроз економічній безпеці сучасного бізнесу має перехресну наукоємність і включає в себе елементи економіки, менеджменту, фінансів, права, соціології та інших наукових дисциплін. Інтеграція цих підходів дозволяє отримати більш повне уявлення про ризики та загрози, а також розробити комплексні стратегії їх управління.

Питання гарантування економічної безпеки сучасних підприємств вивчалися в роботах різних вітчизняних і зарубіжних науковців, таких як Ляшенко О.М., Камлик М.І., Шликова В.В.,

Мінаєва Г.А., Захарова О.І., Андрощук Г.А., Крутова В.В. та інших. Вони досліджували цю проблему як в теоретичному, так і в практичному аспектах [1].

Незважаючи на те, що вже проведено певне дослідження щодо гарантування економічної безпеки, питання визначення і класифікації існуючих загроз і їх ранжування в умовах економічної кризи залишаються актуальними. Це пояснюється постійною зміною економічного середовища та появою нових ризиків і викликів, з якими стикаються підприємства.

Такі дослідження мають велике значення для практичного застосування, оскільки вони дозволяють підприємствам ідентифікувати і аналізувати потенційні загрози, розробляти ефективні стратегії їх запобігання та управління. Відповідне класифікування і ранжування загроз дає змогу підприємствам сконцентрувати свої ресурси та заходи на найбільш критичних аспектах економічної безпеки.

Сучасні вчені економісти все частіше використовують поняття економічної безпеки як важливий аспект стабільності підприємств. Варто відзначити, що в більш розвинених країнах це поняття вже давно відоме і активно використовується в управлінській діяльності підприємств.

Кожне підприємство, незалежно від свого типу та галузі, функціонує в умовах постійного впливу конструктивних і деструктивних факторів. Ці фактори можуть бути зовнішніми, тобто неконтрольованими менеджментом підприємства, але впливають на його економічну діяльність в умовах ринкового середовища, або внутрішніми, що пов'язані з недоліками та прорахунками в самій діяльності підприємства.

Зовнішнє середовище підприємства складається з різних факторів, які можуть мати як позитивний, так і негативний вплив на його діяльність. Це економічні, політичні, адміністративні, правові, соціальні, науково-технічні, освітні, криміногенні, географічні, погодно-кліматичні та інші фактори. Важливо враховувати, що зовнішнє середовище постійно змінюється, що ускладнює його прогнозування та вимагає від підприємства гнучкості та адаптації до нових умов.

Внутрішнє середовище підприємства включає фактори, що контролюються менеджментом і безпосередньо пов'язані з його власною діяльністю. Ці фактори можуть включати недоліки, помилки та прорахунки у рішеннях, неефективне контролювання та несвоєчасну реакцію на проблеми. Недостатня ефективність у внутрішньому середовищі може призводити до негативних наслідків для підприємства.

Таким чином підприємство знаходиться у постійному пошуку балансу між зовнішніми впливами та внутрішніми факторами, які можуть створювати ризики, небезпеки та загрози. Розуміння та аналіз цих факторів є важливим для ефективного управління економічною безпекою підприємства та прийняття стратегічних рішень, спрямованих на забезпечення стійкості та успішності [2].

Загрози економічній безпеці підприємства можуть мати різні причини, як на макрорівні, так і на мікрорівні. На макрорівні, загрози походять від загальноекономічних факторів, які негативно впливають на велику кількість підприємств і становлять загрозу для національної економічної безпеки. Це можуть бути помилки у формулюванні та впровадженні реформ, неефективна науково-промислова та інноваційна політика держави, втрата контролю над економічними процесами тощо.

З іншого боку, загрози на мікрорівні пов'язані з помилками та неефективними управлінськими рішеннями, що приймаються самим підприємством. Це можуть бути помилки в стратегічному плануванні, недостатня увага до інновацій та досліджень, недосконаліть організаційної структури, недостатній контроль над фінансовим станом та ризиками тощо.

Отже, загрози економічній безпеці підприємства виникають внаслідок впливу зовнішніх макроекономічних факторів та внутрішніх управлінських проблем. Розуміння цих причин дозволяє підприємству приймати відповідні заходи та стратегічні рішення для забезпечення економічної безпеки і збереження стійкості в динамічному бізнес-середовищі (табл. 1).

Таблиця 1

Класифікація загроз економічній безпеці бізнесу

Фактор класифікації	**Загрози**			
Місце знаходження джерела загрози	Зовнішня		Внутрішня	
Джерело виникнення загрози	Об’єктивна		Суб’єктивна	
Можливості прогнозування загрози	Передбачувана		Непередбачувана	
Ступінь вірогідності	Невірогідна	Маловірогідна	Вірогідна	Дуже вірогідна
Ступінь очевидності	Явна		Прихована	
Частота виникнення	Постійна		Випадкова	
Момент існування	Актуальна		Потенційна	
Об’єктивність існування	Реальна		Надумана	
Віддаленість у часі	Безпосередня	Близька (до року)	Далека (більше року)	
Віддаленість у просторі	На території підприємства	На прилеглій до підприємства території	На території регіону, країни	На закордонній території
Суб’єкт загрози	Кримінальні структури	Недобросовісні конкуренти	Контрагенти	Власні працівники
Форми прояву	Кількісні		Якісні	
Об’єкт посягань	Загрози підприємству		Загрози стейкхолдерам підприємства	
Вид збитків	Загрози, що несуть прямий збиток		Загрози, що призводять до втраченої вигоди	

Джерело: складено авторами на основі [3]

Економічна безпека сучасного бізнесу піддається різноманітним ризикам та загрозам, які можуть вплинути на його стійкість, прибутковість та існування. Нижче наведений науковий огляд та аналіз основних ризиків та загроз економічній безпеці сучасного бізнесу [4]:

1. Фінансові ризики: Включають кредитні ризики, коливання валютних курсів, процентні ризики та ризики ліквідності. Недостатня фінансова стійкість може спричинити проблеми з оплатою кредиторів, зростанням витрат на позики або недостатньою ліквідністю для виконання поточних зобов'язань.

2. Конкурентний тиск: Бізнеси зазнають загрози від конкуренції з боку інших підприємств, які можуть привести до зменшення частки ринку, зниження цін на товари та послуги, втрати клієнтів тощо. Недостатня конкурентоспроможність може призвести до погіршення фінансових результатів та зменшення прибутку.

3. Політичні ризики: Включають політичну нестабільність, зміни в законодавстві, введення нових регуляторних обмежень та податкових політик, корупцію тощо. Такі фактори можуть вплинути на економічну стратегію бізнесу, його здатність до розвитку та прибутковості.

4. Технологічні загрози: Швидкий темп технологічного розвитку може створювати загрози для бізнесу, особливо для тих, які не можуть швидко адаптуватися до нових технологій. Нові технології можуть змінити попит на продукцію, методи виробництва, а також конкурентну ситуацію на ринку.

5. Загрози кібербезпеки: З розвитком цифрової економіки зростає ризик кібератак, які можуть призвести до витоку конфіденційної інформації, порушення роботи систем управління та втрати довіри клієнтів. Недостатня кібербезпека може негативно позначитися на репутації бізнесу та призвести до значних фінансових втрат.

6. Демографічні ризики: Зміни в демографічній структурі населення, зростання пенсійного віку, зміни в робочій силі можуть мати вплив на бізнес. Недостатність кваліфікованої робочої сили, зростання витрат на пенсії та соціальні програми можуть створювати економічний тиск на підприємства.

7. Екологічні ризики: Зміна клімату, екологічні катастрофи та посилення вимог щодо екологічної стійкості можуть впливати на діяльність бізнесу. Забруднення довкілля, виснаження природних ресурсів та потенційні санкції можуть мати великий вплив на економічну продуктивність та репутацію компаній.

Враховуючи ці ризики та загрози, сучасні бізнеси повинні розробляти стратегії управління ризиками, впроваджувати інновації та бути гнучкими, щоб протистояти негативним впливам. Також важливим є постійний моніторинг зовнішнього середовища, аналіз трендів та здатність до адаптації до нових умов.

Рейдерські атаки та недружнє поглинання є серйозною загрозою для економічної безпеки підприємств. Ці загрози виникають з бажання сторонніх осіб захопити успішно функціонуюче підприємство з метою контролю над ним і отримання стабільного прибутку. Такі атаки зазвичай спрямовані на підприємства з ліквідними активами, стратегічним місцезнаходженням, налагодженим виробничим циклом, ексклюзивним обладнанням та інтелектуальною власністю.

Рейдерство і недружнє поглинання призводять до встановлення тотального контролю над підприємством незважаючи на бажання його власника. Це може мати наслідком втрату власності, фінансову нестабільність і порушення бізнес-процесів. Для "загарбників" особливий інтерес представляють корпоративна інформація (документи, положення, протоколи), фінансово-економічна інформація (бухгалтерські баланси, заборгованість, контрагенти) і відомості про менеджмент та власників підприємства [3].

Ці загрози існують в Україні з 90-х років минулого століття і залишаються актуальними і досі. Для підприємств важливо приділяти достатню увагу заходам безпеки, зокрема, забезпеченню правового захисту своєї власності, контролю над доступом до конфіденційної інформації, і розробці стратегій протидії рейдерським атакам.

Для успішного розвитку підприємства та забезпечення його інформаційної безпеки необхідно використовувати сучасні технології обробки великих обсягів даних. В сучасному світі інформація стала надзвичайно важливим ресурсом. Кожен день генерується величезна кількість цифрових даних, які не тільки потребують зберігання, але й можуть бути використані

компаніями для підтримки бізнесу. Щоб використати всі можливості доступної інформації, її потрібно зібрати, структурувати та проаналізувати. Цифрова трансформація підприємства вимагає використання передових технологій, таких як великі дані (Big Data) та штучний інтелект (AI). Ці технології спрямовані на обробку великого обсягу інформації, що дозволяє приймати рішення, адаптувати пропозиції для клієнтів та прогнозувати їх поведінку.

Цифрова трансформація підприємства надає унікальні можливості для забезпечення його економічної безпеки шляхом впровадження сучасних технологій у бізнес-процеси. Цей підхід включає не тільки встановлення нового обладнання та програмного забезпечення, але й глибокі зміни в управлінні, корпоративній культурі та зовнішніх комунікаціях. В результаті підвищується продуктивність працівників та задоволеність клієнтів, що сприяє побудові репутації прогресивної та сучасної організації. Тому цифрова трансформація має важливе значення не тільки для окремих підприємств, але й для цілих галузей, оскільки допомагає адаптуватися до швидкозмінюючого оточення. Завдяки цифровізації промисловості, роздрібної торгівлі, державного сектору та інших сфер життя людей і роботи підприємств уже сьогодні відчувають зміни [5].

Одним з найважливіших завдань системи економічної безпеки є захист конфіденційної інформації підприємства. Ця інформація включає різноманітні ноу-хау, комерційні таємниці, секрети виробництва та інші конфіденційні дані. У сучасних умовах конкуренції навіть такі відомості, як дані про клієнтів або постачальників і умови співпраці з ними, можуть серйозно підірвати фінансовий стан підприємства, якщо вони потраплять у недоброчесні руки.

Зловживання корпоративними даними та промислове шпигунство стали нещодавно нерідкістю. Крадіжки конфіденційної інформації можуть мати серйозні наслідки для підприємства, такі як втрати клієнтів, порушення довіри, втрата конкурентної переваги та навіть фінансовий збиток. У зв'язку з цим, захист конфіденційної інформації стає важливим завданням для підприємств у всіх сферах діяльності.

Для забезпечення захисту конфіденційних даних підприємство повинно впровадити комплексний підхід до інформаційної безпеки. Це включає використання сучасних технологій шифрування даних, контроль доступу до інформації, системи моніторингу та виявлення вторгнень, а також проведення навчання персоналу з питань кібербезпеки. Крім того, важливо розробити і впровадити політику безпеки даних, яка включатиме процедури резервного копіювання, управління ризиками та виявлення і реагування на інциденти безпеки.

Збереження конфіденційності інформації підприємства є критично важливим для його успішної діяльності і збереження конкурентної переваги на ринку. Дотримання високих стандартів інформаційної безпеки допоможе запобігти можливим загрозам і зберегти довіру клієнтів і партнерів.

Один з відомих прикладів крадіжки інформації бізнесу і порушення економічної безпеки стався у 2014 році, коли компанія Sony Pictures Entertainment стала жертвою кібератаки. У результаті цього кіберінциденту, хакерська група, яка стверджувала, що представляє себе як групу "Гвардія віртуального каліфату", зламала систему компанії і отримала доступ до значної кількості конфіденційної інформації. Зловмисники поширили в Інтернеті велику кількість конфіденційних документів, включаючи фінансову інформацію, особисті дані співробітників, недопущені фільми та сценарії, а також листування внутрішньої корпоративної пошти [6].

Цей інцидент сильно пошкодив репутацію компанії, спричинив значні фінансові втрати та порушив конфіденційність клієнтів та співробітників. Крім того, він викликав серйозні проблеми з кібербезпекою та викликав глобальну обуреність.

Цей приклад підкреслює важливість захисту конфіденційної інформації та необхідність використання сучасних технологій і стратегій для попередження кібератак та забезпечення економічної безпеки компанії.

Недостатній рівень компетенцій працівників служби економічної безпеки створює ще більшу проблему для забезпечення економічної безпеки підприємства. У сучасному господарському середовищі вимоги до спеціалістів в цій галузі постійно зростають, оскільки кіберзлочинці та інші зловмисники постійно вдосконалюють свої методи атак. Проте, при наборі персоналу на посади керівників і заступників начальника служби економічної безпеки підприємства, більшість рекрутерів надає перевагу кандидатам з попереднім досвідом роботи в правоохоронних органах або органах внутрішніх справ. Це може створювати дисбаланс в складі персоналу, оскільки важливо також мати спеціалістів з глибоким розумінням сучасних кіберзагроз, кібербезпеки та методів захисту підприємства.

Для забезпечення економічної безпеки підприємства, необхідно створити та підтримувати власну систему безпеки. Система економічної безпеки включає спеціальні органи, служби, методи і заходи, які забезпечують захист важливих інтересів підприємства від внутрішніх і зовнішніх загроз. Варто зазначити, що кожна система безпеки є унікальною для конкретного підприємства, оскільки вона залежить від виду діяльності, розміру, виробничого потенціалу, ризиків, наявності конфіденційної інформації та інших факторів.

Система безпеки підприємства повинна бути комплексною, забезпечуючи майнову, фінансову, інтелектуальну, інформаційну, науково-технічну та екологічну безпеку. Вона повинна бути ефективною та дієвою, що залежить від чіткого визначення завдань, які система повинна виконувати. Основні завдання системи економічної безпеки підприємства включають захист прав і інтересів підприємства і його співробітників, збір, аналіз і оцінку даних, вивчення партнерів, конкурентів, споживачів та майбутніх співробітників, виявлення можливих загроз зовнішнього середовища, протидію проникненню структур економічної розвідки, забезпечення збереження комерційної таємниці, отримання необхідної інформації для управлінських рішень, формування позитивного іміджу підприємства, контроль за ефективністю системи безпеки та її вдосконалення.

Ефективна система економічної безпеки створює умови для успішного функціонування підприємства, досягнення бізнес-цілей в умовах конкуренції та господарських ризиків. Вона дозволяє вчасно виявляти та нейтралізувати різноманітні загрози та небезпеки.

Основні завдання системи економічної безпеки суб'єкта господарювання можуть варіюватися залежно від контексту та специфіки конкретної ситуації. Проте, деякі загальні завдання можна визначити як типові складові економічної безпеки. Основні з них включають [3]:

1. Захист фінансових ресурсів: Суб'єкт господарювання повинен забезпечувати захист своїх фінансових активів від ризиків, таких як фінансові шахрайства, злочини, корупція, втрати в результаті нестабільності ринків тощо. Це може включати встановлення ефективних систем контролю, аудиту та фінансового моніторингу.
2. Забезпечення стабільності виробництва: Економічна безпека вимагає забезпечення неперервного виробництва та постачання товарів або послуг. Для досягнення цієї мети суб'єкт господарювання повинен бути готовим до управління ризиками, пов'язаними зі збоїв в постачанні сировини, проблемами з виробництвом, недостатньою кваліфікацією працівників, технологічними загрозами тощо.

3. Захист інтелектуальної власності: Для забезпечення конкурентоспроможності суб'єкт господарювання повинен захищати свої інтелектуальні права, які включають патенти, авторські права, товарні знаки тощо. Це важливо, оскільки порушення інтелектуальної власності може призвести до фінансових втрат та втрати конкурентної переваги.

4. Мінімізація ризиків та кризового управління: Суб'єкт господарювання повинен розробити стратегії та плани мінімізації ризиків, що можуть загрожувати його діяльності. Це включає аналіз ризиків, розробку системи попередження кризових ситуацій, створення планів невідкладних заходів та відновлення після кризи.

5. Забезпечення конкурентоспроможності: Економічна безпека також передбачає забезпечення конкурентоспроможності суб'єкта господарювання на ринку. Це охоплює вивчення ринку, розробку стратегій маркетингу та продажу, вдосконалення продукту або послуги, впровадження інновацій, залучення та розвиток талановитих працівників тощо.

Основні принципи формування стратегічної економічної безпеки підприємства можуть включати такі аспекти [7]:

1. Аналіз і прогнозування ризиків: Ретельний аналіз і оцінка потенційних ризиків, які можуть вплинути на діяльність підприємства, допомагає виявити загрози і розробити стратегії їх управління.

2. Диверсифікація діяльності: Розширення спектру продукції або послуг, або розвиток на різних ринках дозволяє зменшити залежність від конкретного сегменту або регіону, тим самим знижуючи ризик збитків в разі проблем у певній галузі.

3. Фінансова стабільність: Раціональне фінансове планування, ефективне управління обіговими коштами, залучення інвестицій та підтримка стабільного фінансового стану підприємства.

4. Кадровий потенціал: Розвиток та збереження висококваліфікованого персоналу, проведення навчання та підвищення кваліфікації співробітників з метою забезпечення конкурентоспроможності підприємства.

5. Інновації та дослідження: Спрямування зусиль на пошук нових ідей, технологій та ринків, впровадження інноваційних рішень і покращення продукції з метою забезпечення конкурентної переваги.

6. Співпраця та партнерство: Розвиток довгострокових партнерських відносин з постачальниками, клієнтами та іншими зацікавленими сторонами для створення взаємовигідних умов співробітництва та забезпечення стійкості.

7. Конкурентна реакція: Активне відстеження діяльності конкурентів та вчасна реакція на зміни в ринкових умовах, здатність адаптуватися до конкурентних тиску та забезпечити свою позицію на ринку.

8. Інформаційна безпека: Захист конфіденційної інформації підприємства, використання захисних технологій та систем забезпечення інформаційної безпеки.

9. Гнучкість та адаптивність: Здатність швидко реагувати на зміни в економічному середовищі та змінювати свою стратегію відповідно до нових умов.

10. Соціальна відповідальність: Дотримання принципів етичного бізнесу, взаємодія зі спільнотою, врахування соціальних та екологічних факторів у діяльності підприємства.

Формування економічної безпеки підприємства вимагає виконання широкого спектру заходів та програм забезпечення безпеки на різних рівнях: державному, регіональному, сфери економічної діяльності та самого підприємства. Основні аспекти, які потрібно враховувати при формуванні економічної безпеки підприємства, включають наступні [8]:

1. Законодавча база: Держава повинна розробляти та приймати ефективні закони, правила та нормативи, які регулюють економічну діяльність і забезпечують стабільність та прогнозованість бізнес-середовища. Це включає законодавство, що регулює питання власності, оподаткування, корпоративного управління, контролю за фінансовою діяльністю тощо.

2. Макроекономічна стабільність: Держава повинна підтримувати стабільну макроекономічну ситуацію, контролювати інфляцію, забезпечувати фінансову стабільність і ефективну монетарну політику. Це допомагає зменшити ризики, пов'язані з економічними коливаннями і фінансовою нестабільністю.

3. Забезпечення безпеки інвестицій: Для залучення інвестицій підприємству важливо мати стабільне та привабливе інвестиційне середовище. Держава повинна розробляти заходи для протидії корупції, забезпечення правової інституціональної бази, створення сприятливих умов для інвестиційного клімату, включаючи спрощення процедур інвестування та зниження бюрократичних бар'єрів.

4. Фінансова стабільність: Підприємство повинно мати ефективну фінансову політику, забезпечуючи стабільність фінансових потоків, ефективне управління ризиками, адекватне фінансування та достатні резерви для покриття можливих втрат.

5. Захист інтелектуальної власності: Захист прав інтелектуальної власності є важливим аспектом економічної безпеки підприємства. Держава повинна розробляти і реалізовувати правові механізми для захисту інтелектуальної власності та запобігання порушенням авторських прав, патентів, товарних знаків тощо.

6. Розвиток людського капіталу: Підприємство повинно надавати належну увагу розвитку та підвищенню кваліфікації свого персоналу. Держава може сприяти цьому шляхом створення системи професійної освіти, підтримки науково-дослідницьких робіт, розвитку технологічних інновацій та підприємництва.

7. Забезпечення фізичної безпеки: Заходи забезпечення фізичної безпеки на підприємстві включають контроль за доступом до приміщень, встановлення систем відеоспостереження, протипожежні заходи, охоронні послуги тощо. Такі заходи допомагають запобігати крадіжкам, диверсіям та іншим формам незаконної діяльності.

Ці заходи та програми сприяють формуванню економічної безпеки підприємства, зменшують ризики і підвищують стійкість бізнесу до внутрішніх і зовнішніх загроз. Окрім державних заходів, саме підприємство повинно ретельно аналізувати свої потенційні ризики, розробляти плани економічної безпеки та впроваджувати внутрішні процедури та політики, що сприяють забезпеченню стабільності та успішності своєї діяльності.

У цьому науковому огляді та аналізі були визначені ризики та загрози економічній безпеці сучасного бізнесу. Дослідження виявило, що в сучасному світі бізнес стикається з різноманітними викликами, які можуть негативно впливати на його економічну безпеку. Основні ризики та загрози можна узагальнити наступним чином:

1. Глобальна економічна нестабільність: Зміни в глобальній економіці, такі як фінансові кризи, рецесії, коливання валютних курсів та торгові війни, можуть створювати негативні наслідки для бізнесу. Вони можуть призвести до зменшення попиту на товари та послуги, зростання цін на сировинні матеріали та зниження прибутків.

2. Технологічні загрози: Швидкий темп технологічного розвитку може створювати ризики для бізнесу. Введення нових технологій може призвести до застаріння продуктів та послуг, які не встигли адаптуватися до нових реалій. Крім того, технологічні загрози такі як

кібератаки та крадіжка конфіденційної інформації можуть негативно впливати на безпеку даних бізнесу та порушити його функціонування.

3. Регуляторні ризики: Зміни у законодавстві та регулюванні можуть мати серйозні наслідки для бізнесу. Впровадження нових правил та обмежень може змінити умови ведення бізнесу, збільшити витрати на виконання вимог, а також налагодження та збереження відповідних систем контролю.

4. Загрози конкуренції: Конкуренція на ринку постійно зростає, і це може становити ризик для бізнесу. З'явлення нових конкурентів, їхнє здатність залучати клієнтів та інновації можуть вплинути на позицію бізнесу на ринку та його прибутковість.

5. Недостатня кадрова безпека: Наявність кваліфікованих та мотивованих кадрів є ключовим фактором успіху бізнесу. Однак, бізнес стикається з ризиком втрати талановитих співробітників, конфліктами в колективі, нестачею необхідних навичок та знань у працівників.

Для ефективного управління ризиками та забезпечення економічної безпеки бізнесу, компаніям рекомендується прийняти наступні заходи:

1. Ретельний аналіз ринку та розуміння глобальних економічних тенденцій, що дозволить прогнозувати можливі зміни та адаптувати бізнес-стратегію.

2. Інвестиції в дослідження та розробки, щоб бути в курсі новітніх технологій та забезпечити конкурентоспроможність.

3. Регулярне оновлення знань про законодавство та регулювання, а також налагодження систем внутрішнього контролю для виконання вимог.

4. Розвиток стратегій конкурентоспроможності, таких як інновації, партнерства та розвиток унікальних пропозицій споживачам, щоб забезпечити своє місце на ринку.

5. Розвиток програм набору, навчання та утримання талановитих працівників, а також створення стимулюючого та задовільного робочого середовища.

В цілому, розуміння ризиків та загроз економічній безпеці є важливим елементом успішного управління сучасним бізнесом. Сприйняття цих ризиків і прийняття відповідних заходів дозволить компаніям протистояти негативним впливам та забезпечити стійкість та стабільність свого бізнесу.

Для сучасного бізнесу існує широкий спектр ризиків та загроз економічній безпеці. Глобальна економічна нестабільність може викликати зміни у попиті та прибутковості бізнесу, технологічні загрози можуть призвести до застаріння продуктів та кібератак, регуляторні ризики можуть вимагати додаткових витрат та змін у веденні бізнесу, загрози конкуренції можуть підірвати позицію на ринку, а недостатня кадрова безпека може впливати на продуктивність та успішність бізнесу.

Однак, компанії можуть успішно управляти цими ризиками та загрозами, приймаючи певні заходи. Дослідження, розуміння глобальних економічних тенденцій, інвестиції в дослідження та розробки, оновлення знань про законодавство та регулювання, розвиток стратегій конкурентоспроможності та програм набору та навчання кадрів - усе це може допомогти забезпечити економічну безпеку бізнесу.

Важливим елементом успішного управління ризиками є постійний моніторинг та аналіз ситуації, прогнозування можливих змін і прийняття вчасних заходів для їх запобігання або мінімізації впливу. Компанії повинні бути гнучкими, інноваційними та відкритими до змін, щоб успішно протистояти ризикам та використовувати можливості, які вони можуть принести.

Запобігання ризикам та забезпечення економічної безпеки повинні бути постійним пріоритетом для керівництва компаній. Це вимагає систематичного планування, внутрішнього

контролю, співпраці зі зацікавленими сторонами та постійного вдосконалення процесів управління ризиками.

В цілому, свідоме управління ризиками та загрозами економічній безпеці допоможе сучасному бізнесу забезпечити стійкість, зростання та конкурентоспроможність у непередбачуваних умовах ринку.

Список використаних джерел

1. Лаптєв М.С. Загрози економічній безпеці підприємств в сучасних умовах // Вчені записки Університету «КРОК». – 2016. – Випуск 44. – С.111-116
2. Камлик М.І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект: Навчальний посібник. – К.: Атіка, 2005. – 432 с
3. Пашнюк Л. Загрози економічній безпеці підприємства та засоби їх нейтралізації // ВІСНИК Київського національного університету імені Тараса Шевченка. – 2013. – Випуск 10(151). – С.93-97
4. Burkynskyi, B., & Gryshchenko, V. (2020). Factors of ensuring economic security in the process of innovative development of entrepreneurship. *Economic Innovations*, *22*(3(76), 6-29. https://doi.org/https://doi.org/10.31520/ei.2020.22.3(76).6-29
5. Бакай В.Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій // Вісник Хмельницького національного університету 2020, № 4, Том 1. – С.32-35
6. Офіційний сайт газети Washingtonpost. URL: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/
7. Валіков В.П., Македон В.В. Економічна безпека підприємства в концепті процесного управління // Нобелівський вісник. 2017. № 1 (10). – С.12-22
8. Барташевська Ю.М. Економічна безпека підприємства: фактори впливу та шляхи забезпечення // Науковий вісник Мукачівського державного університету. Серія «Економіка і суспільство». Випуск 7, 2016. – С.189-194
9. Волинець Л.М., Хоменко І.О., Халацька І.І., Нагорний П.В., Сопоцько О.Ю. Зовнішньоекономічна безпека підприємств України в умовах інтеграції логістичних ланцюгів поставок. Вісник НТУ. К.: НТУ, 2022. Серія «Економічні науки». Випуск 2 (52), 2022. С.57-64.
10. Хоменко І.О, Садчикова І.В., Колоток М.О. Контролінг як інструмент підтримки достатнього рівня економічної безпеки та конкурентоспроможності промислового підприємства. Проблеми і перспективи економіки та управління. 2021. № 2 (26). С. 25-36.
11. Хоменко І.О, Волинець Л.М, Халацька І.І., Божок Ю.О., Пенківська К.С. Формування системи управління ризиками в логістичній діяльності підприємств. Вісник НТУ. К.: НТУ, 2021. Серія «Економічні науки». Випуск 2 (49), 2021. С.22-31.