Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2024. № 11.

DOI: http://doi.org/10.32702/2307-2105.2024.11.36

УДК 338.656

Н. В. Шевченко,

к. е. н, доцент, доцент кафедри менеджменту,

Львівський державний університет внутрішніх справ

ORCID ID: https://orcid.org/0000-0002-1815-7554

Г. З. Леськів,

к. т. н., доцент, завідувач кафедри менеджменту,

Львівський державний університет внутрішніх справ

ORCID ID: https://orcid.org/0000-0002-4900-9466

І. М. Горбан,

к. е. н, доцент, доцент кафедри фінансів та обліку,

Львівський державний університет внутрішніх справ

ORCID ID: https://orcid.org/0000-0002-0627-258X

О. М. Марченко,

к. е. н, доцент, доцент кафедри менеджменту,

Львівський державний університет внутрішніх справ

ORCID ID: https://orcid.org/0000-0001-5996-1330

ІННОВАЦІЙНІ ПІДХОДИ ДО УПРАВЛІННЯ КОРПОРАТИВНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ В СУЧАСНИХ УМОВАХ

N. Shevchenko,
PhD in Economics, Associate Professor of the Department of Management,
Lviv State University of Internal Affairs
H. Leskiv,
PhD in Technical Sciences, Head of the Department of Management,
Lviv State University of Internal Affairs
I. Horban
PhD in Economics, Associate Professor of the Department of Finance and Accounting, Lviv State University of Internal Affairs
O. Marchenko
PhD in Economics, Associate Professor of the Department of Management,
Lviv State University of Internal Affairs

INNOVATIVE APPROACHES TO CORPORATE SECURITY MANAGEMENT OF ENTERPRISES IN MODERN CONDITIONS

У статті досліджено сутність корпоративної безпеки підприємства, основні напрями управління та принципи управління корпоративною безпекою в сучасних умовах функціонування підприємств. Згруповано основні складові корпоративної безпеки: фінансова безпека, інформаційна безпека, фізична безпека, кадрова безпека, співпраця щодо формування системи захисту. Досліджено що до основних зовнішніх факторів, що впливають на ефективність управління корпоративною безпекою впливають: війна, постійні обстріли та руйнування інфраструктури; нестабільність економіки та національної грошової одиниці; агресивні дії конкурентів на ринку; політичні ризики; постійне збільшення податкового навантаження; кіберзагрози та отримання несанкціонованого доступу до даних; крадіжка інтелектуальної власності; соціальні фактори. До внутрішніх джерел відносять: кадрові ризики; ризики пов'язані з недотриманням корпоративної

культури; технологічні ризики; ризики пов'язані з неефективним управлінням фінансовими ресурсами; недостатньо налагоджені бізнес процеси.

Визначено, що для забезпечення високого рівня кадрової безпеки підприємствам доцільно застосовувати наступні інноваційні підходи: цифрова трансформація безпеки; блокчейн для забезпечення безпеки транзакцій; аналітика великих даних (Big Data) для управління ризиками; біометричні технології для захисту доступу; гібридні моделі управління корпоративною безпекою; інноваційні підходи до навчання персоналу підприємства.

The article defines the essence of corporate security of an enterprise, the main areas of management and the principles of corporate security management in the current conditions of enterprise functioning (including military aggression, constant shelling and economic and political instability in the country). The article groups the main components of corporate security: financial security, information security, physical security, personnel security, and cooperation in forming a protection system, which will allow for the most effective formation of directions for its optimization in the future.

It is investigated that the main external factors affecting the effectiveness of corporate security management include: war, constant shelling and destruction of infrastructure, equipment, machinery; instability of the economy and the national currency; aggressive actions of competitors in the market; political risks; constant increase in the tax burden; cyber threats and unauthorized access to data; theft of intellectual property; social factors, reduction of the purchasing power of the population. Internal sources include: human resources risks; risks associated with non-compliance with corporate culture, safety rules during air raids; technological risks, including lack of security; risks associated with inefficient management of financial resources, reduced profitability of the enterprise; insufficiently established business processes and business relationships.

It is determined that in order to ensure a high level of personnel security, enterprises should apply the following innovative approaches: digital transformation of security; blockchain to ensure transaction security; big data analytics for risk management; biometric technologies for access protection, in particular, the use of face recognition or fingerprints; hybrid models of corporate security management through the creation of security teams at the enterprise; innovative approaches to training enterprise personnel, the use of training; ensure cooperation with technology companies to develop corporate security management strategies for its components, taking into account external and internal factors.

Ключові слова: *корпоративна безпека, підприємства, економічна безпека, інновації, смарт-технології в управлінні, безпека, прибутковість, управління.*

Keywords: *corporate security, enterprises, economic security, innovations, smart technologies in management, security, profitability, management.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В сьогоденних умовах війни, економічної та політичної кризи, кібератак вітчизняні підприємства стикаються із значними загрозами, що негативно впливають на рівень корпоративної безпеки. У таких складних умовах виникає необхідність у розробці та впровадженні інноваційних методів (напрямів, стратегій, планів) управління корпоративною безпекою підприємств, які б максимально об’ємно враховували рівень сучасних загроз та швидко могли адаптуватися до змін.

Проблема управління корпоративною безпекою українських підприємств є особливо актуальною в умовах війни, постійної агресії зі сторони країни агресора, кризи, оскільки вони стикаються не лише з фізичними небезпеками (руйнування будівель, інфраструктури, офісів; загроза обстрілів, загроза життю працівників), а також економічними та інформаційними (зниження

фінансових показників, втрата даних, порушення логістичної діяльності). Традиційні підходи щодо управління корпоративною безпекою виявляються недостатньо ефективними, гнучкими чи такими, що враховують зовнішні ризики, у зв'язку з цим виникає необхідність розробки та застосування нових методів і прийомів управління корпоративною безпекою підприємств в сучасних умовах.

Головною ціллю запровадження інноваційних підходів до управління корпоративною безпекою є створення такого рівня захисту діяльності при якому економічних стан підприємства стане більш стійким та гнучким до загроз зовнішнього та внутрішнього середовища. При цьому підприємствам важливим є врахування можливостей використання штучного інтелекту, інтеграції інноваційно-технологічних програм, співпраці з кризовими бізнес-компаніями, розробка більш детальних стратегій враховуючи війну та військовий стан в Україні.

Аналіз останніх досліджень і публікацій. Дослідженням напрямів визначення та управління корпоративною безпекою вітчизняних підприємств присвячено праці багатьох економістів та вчених. Є. Давиденко визначає корпоративну безпеку як важливу складову забезпечення фінансової стійкості т успішності діяльності підприємств в умовах війни, а також визначає основні її складові [1].

П. Кравчук та О. Рудковський визначають сутність корпоративної безпеки як економічної категорії, основні функції яким відповідає корпоративна безпека, а також визначення впливу корпоративної безпеки на ефективність здійснення діяльності, виробництві товарів, наданні послуг та отриманні чистого доходу [2; 3]. Т. Шира розглядає корпоративну безпеку у контексті сукупних загроз які впливають на рівень фінансових показників діяльності компаній, обсягів виробництва і реалізації продукції, ефективності співпраці зі споживачами [4].

О. Линник та Н. Артеменко визначають основні фактори зовнішнього та внутрішнього середовища, що впливають не лише на корпоративну, а й на

загальну економічну безпеку підприємств, проте не враховують вплив війни та політичної кризи на діяльність українських підприємств [5]. Отже, потребує подальшого дослідження саме використання інноваційних підходів до управління корпоративною безпекою підприємств, як основа забезпечення подальшого розвитку та безпечного функціонування в Україні.

Формулювання цілей статті (постановка завдання). Метою даного дослідження є проведення аналізу та систематизації основних інноваційних підходів до управління корпоративною безпекою українських підприємств, які допоможуть знизити вплив внутрішніх та зовнішніх ризиків в умовах воєнних викликів та економічної нестабільності економіки; дослідження складових елементів корпоративної безпеки підприємств.

Виклад основного матеріалу. Корпоративна безпека являє собою комплекс заходів та стратегій, що спрямовані на захист матеріальних та нематеріальних ресурсів, фінансових, інформаційних, інтелектуальних та кадрових активів підприємства від зовнішніх та внутрішніх загроз. До складу корпоративної безпеки підприємства входить фінансова безпека, інформаційна безпека, фізична безпека, кадрова безпека, співпраця щодо формування системи захисту (рисунок 1).

Головною метою корпоративної безпеки є створення всіх необхідних умов для безпечної, безперервної та прибуткової діяльності підприємство, що сприяє її майбутньої фінансової стійкості та конкурентоспроможності на українському ринку. Відповідно управління корпоративною безпекою – це формування, розробку та впровадження таких напрямів, методів чи стратегій при якому забезпечується максимальний захист від внутрішніх та зовнішніх загроз.

На якість управління корпоративною безпекою впливають як зовнішні, так і внутрішні фактори. До основних зовнішніх загроз, які мають найбільший вплив можемо віднести:

– війна, постійні обстріли та руйнування інфраструктури, будівель, торгових приміщень підприємств, складів, техніки, обладнання, транспорту;

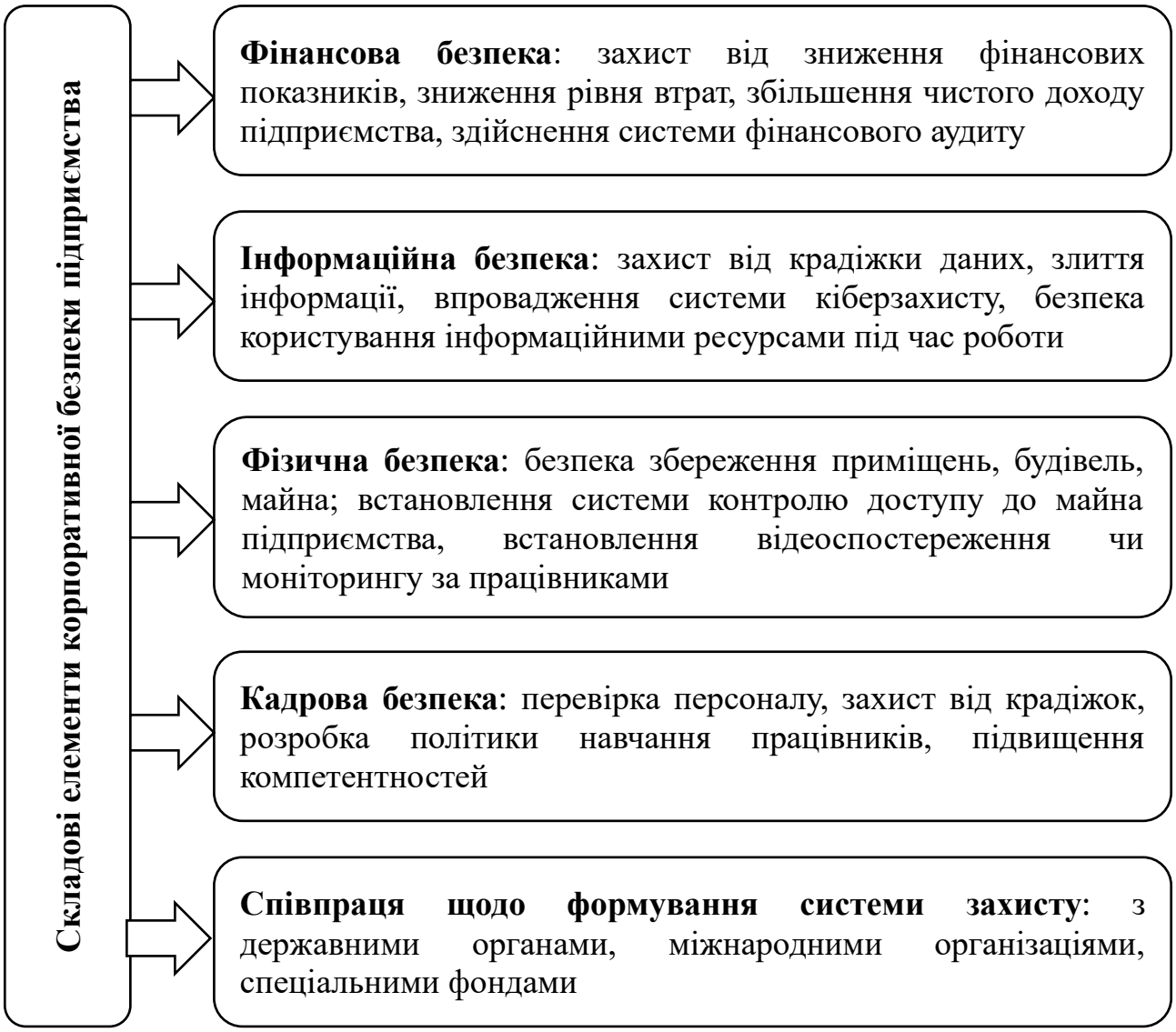

Рис. 1. Перелік основних складових елементів корпоративної безпеки підприємства

Джерело: Систематизовано за даними [1, 5]

- нестабільність економіки та національної грошової одиниці;
- агресивні дії конкурентів (враховуючи важкі умови функціонування вітчизняних підприємств);
- політичні ризики, які включають: постійну зміну законодавства, санкції, обмеження, збільшення розмірів штрафів та податкових підрахувань, що негативно впливають на стабільність функціонування підприємств;

- кіберзагрози, що пов’язані з викраденням особистих даних компаній, розробок чи клієнтської бази, маніпуляціями з комп’ютерними програмами чи системами, запуск вірусів, зломи системи;
- корпоративне шпигунство, крадіжка інтелектуальної власності чи корпоративних прав;
- соціальні фактори: зниження купівельної спроможності споживачів, клієнтів, зміна смаків та пріоритетів по відношенню до товарів, робіт, послуг, недостатня зацікавленість;
- енергетичні проблеми, які впливають на обсяги та постійність процесів виробництва і реалізації товарів, робіт, послуг.

До внутрішніх загроз, які сповільнюють процеси забезпечення корпоративної безпеки та напряму залежать від самого підприємства, доцільно віднести:

- кадрові ризики, що включають некомпетентність персоналу, небажання навчатися та отримувати нові здібності (за професійним спрямуванням), зловживання або шахрайство з баку співробітників, внутрішні крадіжки даних, злиття інформації конкурентам;
- ризики, що пов’язані з корпоративною культурою: недотримання професійних правил поводження на робочому місці, з клієнтами чи партнерами, недотримання правил безпеки на робочому місці (особливо під час повітряних тривог);
- технологічні ризики, які пов’язані із відсутністю надійних і сучасних технологій (відсутність надійних програм захисту на комп’ютерах, вільний доступ до обмеженої інформації чи даних);
- ризики спричинені неефективним управлінням фінансовими ресурсами, використання грошових коштів, зменшенням рівня прибутковості підприємства протягом звітного року, неправильними інвестиційними чи емісійними рішеннями;

– операційні ризики, що пов’язані з недостатньо налагодженими бізнес процесами, порушеннями логістичних зав’язків, наявність ненадійних партнерів та/або дебіторів тощо.

Така ситуація змушує вітчизняні підприємства шукати нові шляхи щодо забезпечення найвищого рівня корпоративної безпеки, які б враховували вплив зовнішніх та внутрішніх факторів, особливості галузі та напрями стратегічного розвитку підприємства. Враховуючи постійні зміни в оточуючому середовищі, підприємствам доцільно застосовувати інноваційні підходи та стратегії (рисунок 2). Інноваційні підходи до управління кадровою безпекою підприємства являють собою сукупність нових стратегій, методів чи технологій, що дозволяють сучасним підприємствам більш ефективно зменшувати вплив ризиків на фінансовий стан та діяльність, адаптуватися до змін економічного середовища, забезпечувати ефективну і безперебійну діяльність.

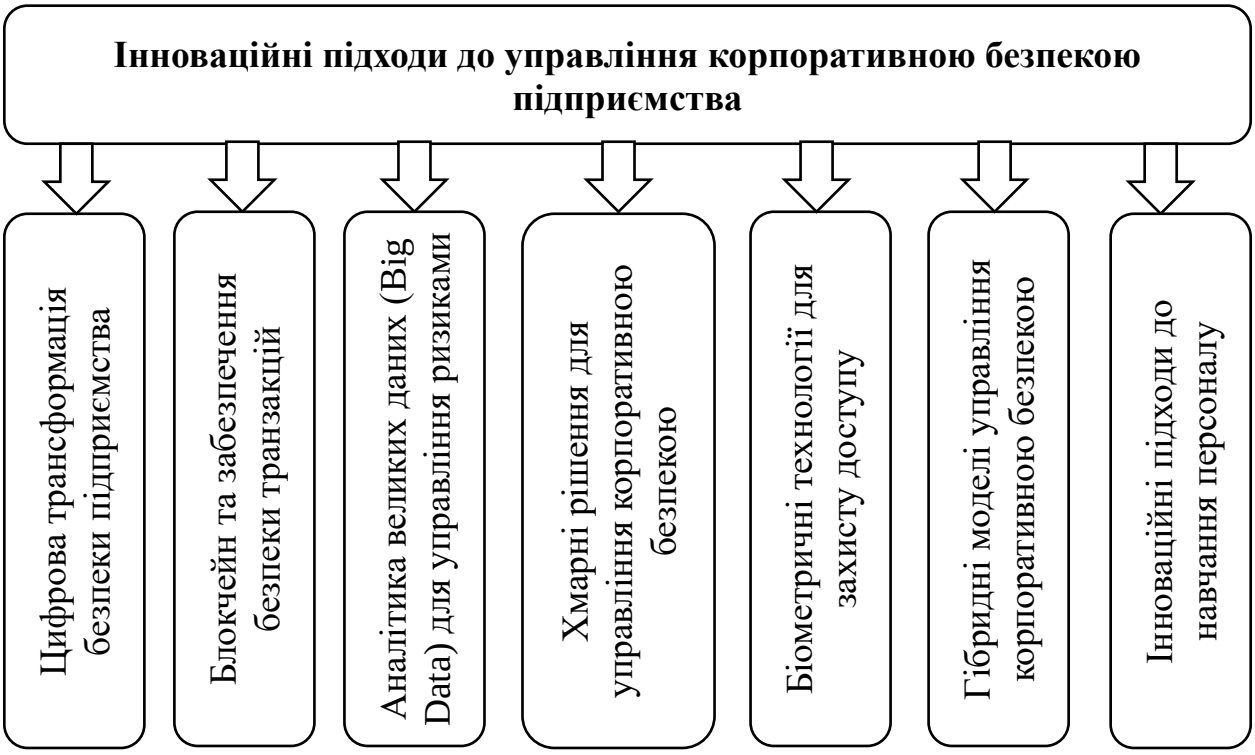

Рис. 2. Інноваційні підходи до управління корпоративною безпекою підприємства

Джерело: Сформовано за даними [1, 6, 7]

Ефективність подальшої реалізації інноваційної стратегії зменшення рівня корпоративної безпеки підприємства покладено не лише на власників, акціонерів чи керівників, а й на працівниках, які забезпечують ключові процеси забезпечення операційної, інвестиційної та фінансової діяльності підприємства на фінансовому ринку.

Цифрова трансформація безпеки підприємства повинна передбачати: впровадження системи кібербезпеки підприємства на основі застосування штучного інтелекту (AI) та машинного навчання для виявлення аномалій в діяльності підприємства чи здійснення фінансових розрахунків, формування стратегій та прогнозування загроз; використання хмарних технологій для подальшого зберігання та обробки даних що стосуються фінансової діяльності підприємства; застосування системи щодо забезпечення цілісності конфіденційних даних.

Використання блокчейн технологій дозволить забезпечити вітчизняним підприємствам (незалежно від галузі та стратегії розвитку) безпеку фінансових та ділових транзакцій між фінансовими партнерами. Оскільки система блокчейн забезпечує децентралізацію, чіткість та прозорість записів, це значною мірою мінімізує ризик шахрайства, втручання в ділові (економічні) процеси, зміну даних. Такий підхід є ефективним для захисту контрактів, управління поставками, створення системи логістичних маршрутів, проведення фінансових операцій. Система блокчейн у фінансових операціях та контрактах активно використовується американськими, канадськими, китайським компаніями.

Управління великими об’ємами даних (Big Data) дозволяє сучасним вітчизняним підприємствам проводити глибокий аналіз ризиків, виявляти нові тренди загроз (враховуючи постійні кібер атаки зі сторони країни агресора та цифрову війну), спрогнозувати можливі проблеми у майбутньому. За допомогою аналітики великих даних підприємства можуть краще розуміти поведінку ринку, тенденцій, виявляти шахрайські схеми, внутрішні проблеми, створювати різні стратегічні стратегії для їх подальшого уникнення.

Використання біометричних систем таких як: розпізнавання обличчя, відбитки пальців працівників підприємства, сканування райдужної оболонки ока, створення індивідуальних карточок пропуску тощо. Такі мірі безпеки та захисту забезпечать високий рівень захисту доступу до конфіденційної інформації підприємства (компанії, установи, фірми чи організації) або стратегічних ресурсів, інноваційних розробок. Практичне застосування біометрії значно підвищує рівень безпеки підприємства порівняно з поширеними традиційними, оскільки біологічні характеристики людини є унікальними та практично неможливими для підробки, копіювання чи заміни, що значно знижує потенційний ризик несанкціонованого доступу.

Впровадження біометричних систем у діяльність вітчизняних підприємств спрощує процедури щодо контролів доступу за поведінкою та корпоративною відповідальністю працівників, підвищує ефективність роботи підприємства та створює більш безпечне робоче середовище для керівників та самих працівників.

Гібридні моделі управління передбачають поєднання автоматизації за допомогою технологій (програмного забезпечення, автоматизованого устаткування) та людського контролю для забезпечення найбільш багаторівневого і ефективного захисту. Такий підхід включає створення спеціалізованих команд (груп) безпеки, які працюють над системами автоматичного моніторингу і реагування на загрози.

Інноваційні підходи до навчання передбачають використання підприємствами освітніх платформ, які орієнтовані на кібербезпеку, управління корпоративними ризиками та дозволяють проводити регулярне навчання персоналу підприємства щодо новітніх методів захисту і протидії загрозам. Таке застосування вебінарів, онлайн-тренінгів, інтерактивних симуляцій підвищує ефективність підготовки співробітників до можливих кризових загроз (ситуацій).

Також, до інноваційних рішень які забезпечать ефективне управління корпоративною безпекою можна віднести:

- система SIEM, яка дозволяє збирати та аналізувати дані з різних джерел з метою виявлення кібератак;
- SOAR-платформа – автоматизує повсякденні завдання, що покладені на менеджерів підприємства та дозволяє швидко реагувати на зміни, помилки, неточності;
- EDR-рішення – забезпечують виявлення та розслідування можливих кібератак, злиття чи викрадення даних та інших інцентдентів;
- платформи управління ідентичністю та доступом (IAM) – що допомагає централізувати управління даними компанії, оптимізувати весь доступ до інформаційних систем на різних рівнях управління.

Застосування інновацій у сфері корпоративної безпеки вже зараз є необхідністю через постійно зростаючі кіберзагрози та тенденцію до глобалізації. Нові технології та підходи дозволять підприємствам краще захищати свої активи, забезпечувати стабільну роботу та легше адаптуватися. По-перше, інновації дозволять підвищити ефективність системи безпеки. Постійне штучне навчання та штучний інтелект дозволять зробити рутинну аналітику та виявлення аномалій більш ефективним, в подекуд важче прогнозувати потенційно небезпечні ситуації. Це допоможе заощадити час і ресурси, а також зреагувати на інцидент швидше. По-друге, їх застосування підвищить рівень захисту. Наприклад, деякі складні загрози обнаружуватися не можна звичайними способами. Створювати гнучкі програмні продукти, які швидко змінюються, можливо лише завдяки інноваціям. Нарешті, вони можуть значна демонструвати високу довіру до підприємств.

Висновки та перспективи подальших досліджень у даному напрямі. Проведене в статті дослідження дає можливість визначити, що корпоративна безпека відіграє важливу роль у ефективному та прибутковому, конкурентоспроможному функціонуванні підприємства, забезпечуючи можливість оцінки ризиків внутрішнього та зовнішнього середовища. Незважаючи на значну кількість досліджень у цій галузі, залишається ще

багато невирішених питань, зокрема можливими напрямками подальшого дослідження доцільно визначити наступні:

- організація управління ризиками - створення інструментів оцінки та управління ризиками, пов'язаними з новими технологіями;
- моніторинг впливу геополітичних факторів на корпоративну безпеку;
- розробка практичних механізмів конфіденційності у відповідності з новими положеннями в законодавстві;
- дослідження споживчих властивостей користувачів в Інтернеті та запровадження заходів впливу на свідомість користувачів.

Література

1. Давиденко Є.А. Корпоративна безпека на українських підприємствах в умовах війни. *Економіка та суспільство*. № 58, 2023. С. 34-42.
2. Кравчук П.Я. Сутність та передумови виникнення поняття корпоративної безпеки підприємства. *Науковий вісник Волинського держ. ун-ту ім. Лесі Українки*. 2005. № 1. С. 165– 170.
3. Рудковський О.В. Формування функцій управління корпоративної безпеки. *Соціально-економічний розвиток регіонів в контексті міжнародної інтеграції*. 2013. № 12. С. 141–146.
4. Шира Т. Б. Корпоративна безпека підприємств в Україні: визначення ключових загроз. *Вчені записки Таврійського національного університету імені ВІ Вернадського. Серія: Економіка і управління*. № 6. 2018. С. 93-96.
5. Линник О.І., Артеменко Н.В. Стратегія економічної безпеки підприємства як фактор зменшення впливу зовнішніх та внутрішніх загроз. *Вісник Національного технічного університету ХПІ. Сер.: Технічний прогрес та ефективність виробництва*. 2013. № 67. С. 159 –169.
6. Леськів Г.З., Шевченко Н.В., Марченко О.М. Менеджмент інноваційними ресурсами із залученням технологій штучного інтелекту:

виклики сучасності. *Наукові інновації та передові технології*. № 4(32), 2024. С. 717-725

7. Погорєлова Т.О. Інноваційні технології в управлінні персоналом на сучасному підприємстві. Вісник Національного технічного університету "Харківський політехнічний інститут" (економічні науки) : зб. наук. пр. Харків : НТУ "ХПІ", 2018. № 15 (1291). –С. 101-104.

References

1. Davidenko, Ye.A. (2023), “Corporate security at Ukrainian enterprises in times of war”, *Ekonomika ta suspilstvo*, vol. 58, pp. 34-42.

2. Kravchuk, P.Ya. (2005), “The essence and prerequisites of the concept of corporate security of an enterprise”, *Naukovij visnik Volinskogo derzh. universytu Lesi Ukrayinki*, vol. 1, pp. 165-170.

3. Rudkovskij, O.V. (2013), “Formuvannya funkcij upravlinnya korporativnoyi bezpeki”, *Socialno-ekonomichnij rozvitok regioniv v konteksti mizhnarodnoyi integraciyi*, vol. 12, pp. 141-146.

4. Shira, T.B. (2018), “Formation of corporate security management functions”, *Vcheni zapiski Tavrijskogo nacionalnogo universitetu imeni V.I. Vernadskogo. Seriya: Ekonomika i upravlinnya*, vol. 6. pp. 93-96.

5. Linnik, O.I. and Artemenko, N.V. (2013), “The company's economic security strategy as a factor in reducing the impact of external and internal threats”, *Visnik Nacionalnogo tehnichnogo universitetu HPI. Ser.: Tehnichnij progres ta efektivnist virobnictva*, vol. 67. pp. 159-169.

6. Leskiv, G.Z. Shevchenko, N.V. and Marchenko, O.M. (2024), “Management of innovative resources with the involvement of artificial intelligence technologies: modern challenges”, *Naukovi innovaciyi ta peredovi tehnologiyi*, vol. 4. pp. 717-725.

7. Pogoryelova, T.O. (2018), “Innovative technologies in personnel management at a modern enterprise”. Visnik Nacionalnogo tehnichnogo universitetu "Harkivskij politehnichnij institut", vol. 15. pp. 101-104.

Стаття надійшла до редакції 22.10.2024 р.