DOI: https://doi.org/10.32782/2524-0072/2024-63-81

УДК 338.24.021.8

# ОСНОВИ УПРАВЛІННЯ БЕЗПЕКОЮ В ОРГАНІЗАЦІЯХ КОРПОРАТИВНОГО ТИПУ

# FUNDAMENTALS OF SECURITY MANAGEMENT IN CORPORATE-TYPE ORGANIZATIONS

**Когут Мар'яна Володимирівна**
кандидат економічних наук, доцент,
Львівський національний університет природокористування
ORCID: https://orcid.org/0000-0001-8275-134X

**Содома Руслана Іванівна**
кандидат економічних наук, доцент,
Львівський державний університет безпеки життєдіяльності
ORCID: https://orcid.org/0000-0002-5020-6440

**Романів Володимир Ярославович**
аспірант,
Львівський державний університет безпеки життєдіяльності,
ORCID: https://orcid.org/0009-0000-4795-5849

**Kohut Maryana, Sodoma Ruslana**
Lviv National Environmental University

**Romaniv Volodymyr**
Lviv State University of Life Safety

Стаття розглядає роль корпоративних організацій у світовій економіці, акцентуючи на їх впливі на інновації, зайнятість і економічний розвиток через глобалізацію та міжнародну торгівлю. Розглядається складна структура управління таких організацій, яка містить різні рівні керівництва та корпоративну культуру, впливаючи на поведінку співробітників та їхнє ставлення до роботи. Розглядаються стратегії вирішення проблем управління ресурсами та оптимізації виробничих процесів. Вказано на важливість комплексного підходу до корпоративної безпеки для підтримки сталого розвитку та адаптації до змінних умов ринку. Окреслено дефініцію поняття «корпоративна безпека». У статті детально описано п'ять основних ризиків, які мають тривалий та значний вплив на корпоративну безпеку. Підкреслюється необхідність інтегрованого підходу та регулярного оновлення безпекових процедур, щоб впоратися з динамічними змінами в сучасному бізнес-середовищі та забезпечити всебічний захист компанії.

**Ключові слова:** безпека, безпека підприємства, корпоративна безпека, корпорація, загроза, стратегії.

The article examines the role of corporate organizations in the global economy, focusing on their impact on innovation, employment and economic development through globalization and international trade. The complex management structure of such organizations is considered, which contains different levels of management and corporate culture, influencing the behavior of employees and their attitude to work. Strategies for solving problems of resource management and optimization of production processes are outlined. The importance of a comprehensive approach to corporate security to support sustainable development and adaptation to changing market conditions is indicated. The definition of the concept of "corporate security" is outlined as a set of strategies that are integrated into all key areas of the company to avoid threats. Involvement of risk management departments, anti-crisis management and other areas ensures effective coordination and implementation of security measures. Corporate security, as an important part of strategic management, minimizes operational stress and helps focus on development and innovation. It is important that those responsible for security understand the organizational, legal and technical aspects to reduce risks and increase competitiveness. Modern technologies such as the Internet of Things bring new challenges to the field of cyber security, requiring continuous updating of protective strategies. The article describes in detail five main risks that have a long-term and significant impact on corporate security. In particular, cybercrime, insider threats, physical attacks, lack of regulatory compliance, and supplier-related risks are addressed.

It is important that corporate security acts not only as a response to potential threats, but also as a strategic advantage that allows companies to focus on development and innovation. The need for an integrated approach and regular updating of security procedures is emphasized in order to cope with dynamic changes in the modern business environment and ensure comprehensive protection of the company.

**Keywords:** security, enterprise security, corporate security, corporation, threat, strategies.

**Постановка проблеми.** Глобалізація та стрімкий прогрес у технологічній сфері відкрили для корпорацій нові можливості для росту та виходу на міжнародні ринки. Водночас, ці процеси супроводжуються різними загрозами, зокрема терористичними актами або ж порушеннями інформаційної безпеки, що підкреслює критичну важливість корпоративної безпеки. Освоєння передових практик у цій галузі є невід'ємним аспектом для забезпечення стабільності та безпеки. Кожна організація має бути підготовлена до несподіванок, які можуть виникнути у бізнесі, внутрішній структурі компанії або на глобальному рівні. Знання та застосування принципів корпоративної соціальної відповідальності та ефективне корпоративне управління стають ще важливішими. Завдяки системі корпоративної безпеки, що містить виявлення загроз та розробку стратегій їхнього зниження, компанії можуть ефективно здійснювати управління потенційними ризиками та захищати свої інтереси. Оновлення процесів управління безпекою компаній повинно стати ключовим завданням для вищого керівництва, щоб ефективно протидіяти загрозам і ризикам, які виникають у внутрішньому та зовнішньому середовищах. Розвиток інформаційної економіки та глобалізація ділового середовища демонструють переваги ризик-орієнтованих методів в забезпеченні економічної безпеки підприємств. Глобалізація та інтеграція можуть збільшити внутрішню та міжнародну конкуренцію, що вимагає більш глибокого аналізу існуючих та потенційних ризиків. Це означає, що для точної оцінки економічного стану суб'єктів господарювання потрібно використовувати все більше показників та перевірених досвідом діагностичних інструментів, оскільки традиційні методи, що використовувались у розвинених країнах, більше не забезпечують точних прогнозів.

**Аналіз останніх досліджень і публікацій.** Питання безпеки підприємств активно вивчають як вітчизняні, так і закордонні науковці, серед яких О. Ареф'єва, І. Бінько, З. Варналій, О. Власюк, Т. Васильців, З. Герасимчук, М. Єрмошенко, Я. Жаліло, З. Живко, О. Захаров, В. Ковальов, П. Кравчук, О. Ляшенко, Г. Пастернак-Таранушенко, В. Пономаренко, В. Франчук, Л. Шемаєва, В. Шлемко та інші. Однак слід зазначити, що існує недостатня увага до розробки чіткого визначення терміну «корпоративна безпека» та створення теоретичного та методологічного фундаменту для її забезпечення на українських підприємствах.

**Формулювання цілей статті.** Метою статті є аналіз та розкриття ключових стратегій та практик, які застосовують корпорації для забезпечення своєї безпеки.

**Виклад основного матеріалу дослідження.** Корпорації сьогодні мають вагомий вплив на економічні процеси в нашій країні, і їх роль з часом тільки зростатиме, слідуючи прикладам інших країн [8]. Варто зазначити, що організації корпоративного типу – - це великі, часто мультинаціональні компанії, що мають складну структуру управління та операцій. Вони можуть бути публічними або приватними і характеризуються різноманітністю бізнес-напрямків, що вимагає розгалуженої управлінської структури та стратегічного планування. Розглянемо основні ключові аспекти, які визначають організації корпоративного типу у табл. 1.

Корпоративні організації мають складну структуру управління та ієрархією, яка містить різні рівні керівництва, такі як генеральний директор (CEO), фінансовий директор (CFO) та інші; мають власну корпоративну культуру, що впливає на стандарти поведінки співробітників та їхнє ставлення до роботи та інновацій. Завдяки своїй глобальній присутності, такі компанії здатні конкурувати на міжнародних ринках, використовуючи переваги глобалізації. Вони зобов'язані дотримуватися строгих національного та міжнародного регулювання, що стосуються фінансової звітності, захисту даних та екологічних норм. Корпоративні організації також пропонують широкий спектр продуктів і послуг, розробляючи інноваційні рішення через значні інвестиції в дослідження та розвиток для підтримання своєї конкурентоспроможності [3].

Таким чином, такі організації грають значну роль у світовій економіці, здійснюючи значний вплив на інновації, зайнятість та економічний розвиток. Вони сприяють глобалізації ринків,

Таблиця 1

**Основні характеристики організацій корпоративного типу**

| | |
|---|---|
| Юридична структура | Зазвичай корпорації реєструються як юридичні особи, що мають права та обов'язки, незалежні від їхніх власників. Це включає можливість володіти майном, укладати договори та нести юридичну відповідальність. |
| Структура власності | Власність на корпоративні організації розділена на акції, які можуть бути вільно куплені та продані на відкритому ринку, що дозволяє їм залучати капітал через продаж акцій. |
| Управлінська ієрархія | Корпорації мають багаторівневу управлінську структуру з виразною делегацією відповідальностей. Верхівка зазвичай включає раду директорів, яка призначає вище керівництво, включаючи генерального директора (CEO). |
| Глобальна присутність | Багато корпоративних організацій мають глобальну присутність з філіями, виробництвами або представництвами у різних країнах, що вимагає комплексного управління та координації між регіонами. |
| Корпоративна культура та політика | Вони розробляють детальні внутрішні політики та процедури для забезпечення єдності та консистенції в управлінні, культурі та операціях по всьому світу. |
| Соціальна відповідальність | Корпоративні організації часто залучені у корпоративну соціальну відповідальність (КСВ), що включає зусилля на підтримку екологічних, соціальних та економічних ініціатив. |

*Джерело: розроблено на основі [3; 4; 5]*

посилюють міжнародну торгівлю та забезпечують масштабування технологічних нововведень. Крім того, корпоративні організації вносять вклад у соціальну стабільність, пропонуючи робочі місця та кар'єрні можливості на різних континентах, а також сприяють сталому розвитку через інвестиції в екологічні ініціативи та корпоративну соціальну відповідальність.

Значення корпоративної безпеки зростає у відповідь на складні виклики, з якими стикаються великі корпорації у сучасному динамічному світі. Важливість інтегрованого підходу до безпеки в корпоративному управлінні не може бути переоцінена, оскільки він дозволяє компаніям ефективно реагувати на внутрішні та зовнішні загрози, підтримувати стабільність та адаптуватися до умов ринку, що постійно змінюються.

У зв'язку з цим, корпоративна безпека набуває все більшого значення, оскільки вона охоплює ширший спектр завдань, ніж традиційні концепції "безпеки" чи "економічної безпеки". Вона містить моніторинг виробничих процесів та ринкової реалізації продукції, виявлення не використаних можливостей для оптимізації ресурсів компанії, розвиток інформаційної бази для підтримки прийняття управлінських рішень, захист комерційної таємниці та інформаційного поля підприємства [8]. Також важливим є забезпечення фізичної безпеки активів корпорації, управління конфліктами всередині організації, вдосконалення системи мотивації та використання потенціалу співробітників, захист прав учасників бізнесу, а також запобігання і вирішення протиріч між менеджментом і акціонерами. Це підкреслює необхідність комплексного підходу до управління корпоративною безпекою, який би гармонізував всі аспекти внутрішньої та зовнішньої діяльності корпорації для забезпечення її стійкого розвитку та конкурентоспроможності на ринку.

Термін «корпоративна безпека» найкраще розуміти як сукупність стратегій, оскільки він не стосується лише однієї сфери [4]. Зокрема, корпоративна безпека – це пошук найкращих стратегій і складання планів, які допоможуть уникнути ситуацій, які загрожують безпеці вашої компанії.

Корпоративна безпека є однією з основних функцій діяльності компанії, яка здійснюється в тісній співпраці з усіма іншими ключовими відділами компанії, такими як управління ризиками, антикризове управління, управління структурами безпеки в організації і навіть управління проєктними командами чи управління бізнес-проєктами.

Корпоративна безпека є невід'ємною частиною стратегічного управління будь-якої компанії, оскільки забезпечує не тільки захист, але й знижує оперативний стрес для співробітни-

ків і клієнтів. Вона дозволяє зосередитися на рості та інноваціях, зменшуючи тим самим екстрені витрати та підвищуючи загальну обізнаність щодо потенційних загроз. Також, добре організована система безпеки сприяє формуванню позитивного іміджу компанії.

З огляду на це, особи, відповідальні за корпоративну безпеку, повинні розуміти організаційні, правові та технічні аспекти, які допоможуть знизити ризики та підвищити конкурентоздатність на ринку. Вони мають відстежувати і управляти всіма аспектами безпеки та неперервності бізнесу, включаючи захист від внутрішніх та зовнішніх загроз.

Сучасні технології, такі як хмарні обчислення, штучний інтелект та Інтернет речей (IoT), принесли нові можливості для бізнесу, але також і нові виклики в сфері кібербезпеки. Враховуючи швидкий розвиток технологій, зростання інвестицій у галузі конфіденційності та безпеки є відповіддю на зростаючу кількість кібератак, що вимагає постійного вдосконалення захисних стратегій.

Керування корпоративною безпекою стає складнішим у світлі асиметричних і мережевих загроз, таких як організована злочинність і тероризм, а також у випадках політичних наворушень чи економічних криз. Таке середовище вимагає глибокого розуміння і впровадження передових практик у сфері фізичної і цифрової безпеки для зміцнення корпоративного управління і захисту активів компанії. Важливо використовувати ці практики обережно, адже неправильне їх застосування може непередбачувано збільшити ризики для бізнесу.

Варто зазначити, що існують три найкращі методи безпеки підприємства, а саме регулярний аналіз потреб компанії в безпеці, інтегрована корпоративна безпека для всієї компанії, детальні стратегії протидії ключовим загрозам [7]. Розглянемо їх детальніше.

***1. Регулярний аналіз потреб компанії в безпеці.*** Постійний огляд і оновлення потреб компанії у сфері корпоративної безпеки є критично важливим. Більше ніж просто впровадження програми безпеки, важливо регулярно переоцінювати і адаптувати ці потреби, враховуючи змінні умови та нові загрози. Моніторинг таких аспектів, як дотримання правил доступу до облікових записів, методи звітування про інциденти та виявлення порушень, є фундаментальним. Цілі безпеки повинні бути ясно сформульовані та однаково зрозумілі для всіх відділів. Комунікація є ключовою для забезпечення того, що всі члени команди залишаються інформованими про політики і процедури. Ефективний контроль, заснований на конкретних показниках ефективності, дозволяє не лише виявляти слабкі місця в системах безпеки, а й визначати нові потреби і забезпечувати постійне відповідність поточним стандартам безпеки.

Оцінка програми корпоративної безпеки має базуватися на об'єктивних даних та статистиці. Глибокий аналіз інформації про заходи безпеки, такі як захист персоналу, бренду чи продукції, може виявити вразливі місця. Наприклад, хоча на рецепції компанії може бути встановлено відеоспостереження, відсутність тривожної кнопки може підвищити ризик для співробітників і клієнтів у чотири рази. Використання статистичних методів дозволяє кількісно оцінити такі ризики і підтвердити необхідність впровадження змін.

Кількісний аналіз нових ризикових зон також важливий. Визначення потенційних прямих та нематеріальних витрат на відновлення після інцидентів допомагає оцінити необхідність інвестицій в заходи безпеки. На основі аналізу можливих наслідків від відсутності сигналізації, таких як вандалізм чи крадіжка, можна вирішити, чи виправдані витрати на встановлення тривожної кнопки. Важливо також представляти керівництву актуальні дані про ризики та варіанти їх мінімізації з бізнесової точки зору. Отримання підтримки від керівництва є ключовим для успішного впровадження та вдосконалення програм безпеки. Доцільно також аналізувати інциденти, які сталися у конкуруючих компаніях, використовуючи галузеві звіти, місцеві новини та цифрові публікації. Ці дані можуть стати основою для покращення власних заходів безпеки та стратегічного планування на майбутнє.

***2. Інтегрований підхід до корпоративної безпеки у компанії.*** Корпоративна безпека – це комплексна діяльність, яка залучає всю команду, а не ізольована сфера відповідальності. Для розробки або вдосконалення плану корпоративної безпеки важливо розуміти ключові аспекти: юридичні вимоги, поточні ризики, рівень інтеграції та співпрацю. Ці елементи спільно формують міцну основу для політики безпеки, і їх взаємодія гарантує захист всіх сегментів підприємства від зовнішніх і внутрішніх загроз [3].

Важливість загальної співпраці не можна недооцінювати, оскільки без цього компонента навіть найнадійніша система безпеки може зазнати збоїв. Корпоративна культура має значний вплив на успішність впрова-

дження практик безпеки; чим вона міцніша, тим більше ймовірність, що ініціативи будуть прийняті та ефективно інтегровані. Цей процес повинен розпочатися на вищому рівні – керівники та менеджери мають бути першими, хто ознайомиться з процедурами безпеки та почне їх впровадження, поширюючи ці знання та практики на решту команди. Такий підхід забезпечить, що лідери не тільки слугуватимуть прикладом, але й матимуть необхідні знання для забезпечення виконання цих практик.

***3. Стратегії протидії ключовим загрозам.*** Кожна організація має свою унікальну структуру та підходи до безпеки. Важливо проводити оцінку безпекових потреб, щоб не тільки ідентифікувати потенційні загрози, але й розробляти відповідні плани дій. Основна увага має бути зосереджена на п'яти основних ризиках, що мають безпосередній і довгостроковий вплив на корпорацію (рис. 1).

Кіберзлочинність містить такі ризики, як хакерські атаки на IT-системи, викрадення конфіденційної бізнес-інформації та персональних даних. Зловмисники можуть використовувати ці дані для своїх цілей або продажу на чорному ринку. Внутрішні загрози стосуються дій нечесних або непоінформованих співробітників, що можуть призвести до витоку конфіденційної інформації або несанкціонованого доступу до важливих матеріалів поза межами організації. Фізичні атаки охоплюють напади на корпоративні будівлі або транспортні засоби, що можуть викликати крадіжки, саботаж або пошкодження майна. Відсутність нормативної відповідності або ж недотримання законодавчих вимог, наприклад, у сфері захисту персональних даних, може призвести до штрафів, адміністративних санкцій, або навіть до втрати ділової репутації. Важливість вибору надійних постачальників IT-послуг та матеріалів, які проходять регулярну перевірку як частину аналізу ризиків у ланцюзі постачання. Аналіз ризиків та історій інцидентів повинен використовуватися для формування комплексних планів реагування, що забезпечують співпрацю між відділами для всебічного захисту організації [2].

Значення корпоративної безпеки для розвитку компанії відіграє ключову роль. Корпоративна безпека є критично важливою для будь-якої компанії, оскільки дозволяє зосередитися на розвитку замість витрати часу та ресурсів на боротьбу з загрозами. Ефективні заходи безпеки знижують частоту інцидентів, що перекладається на економію ресурсів, які


**Рис. 1. П'ять ключових ризиків з безпосереднім та довгостроковим впливом на корпорацію**

*Джерело: розроблено на основі [7; 8; 9]*

можна інвестувати у продуктивніші сфери, сприяючи успіху компанії.

Використання системи Corporate Security дозволяє компаніям переходити від пасивного реагування на загрози до проактивного планування та підготовки. Проведення попереднього навчання може значно знизити потенційні загрози та підготувати компанію до ефективного реагування на інциденти або порушення безпеки.

Хоча багато хто асоціює корпоративну безпеку із технічними аспектами, такими як системи моніторингу, вона також охоплює широкий спектр питань, зокрема мережеву безпеку та кібербезпеку. Підготовка до конкретних загроз не тільки підвищує обізнаність та почуття безпеки серед співробітників, клієнтів та партнерів, але й забезпечує, що персонал може ефективно ідентифікувати та реагувати на загрози. Завдяки зміцненню політик безпеки та проведенню тренінгів співробітники стають більш пильними та готовими до дій, знижуючи ризики, пов'язані з такими методами кіберзлочинності, як соціальна інженерія.

Важливо зазначити, що, згідно з дослідженням Forbes, близько 30% молодих професіоналів ігнорують корпоративні заходи безпеки для спрощення робочих процесів, несвідомо піддаючи компанії збільшеним ризикам [6]. Це підкреслює необхідність постійного вдосконалення політики безпеки та навчання персоналу.

Впровадження корпоративної безпеки несе численні переваги для будь-якої організації, незалежно від її галузі. Зокрема, ефективна політика безпеки забезпечує:

– *підвищене почуття безпеки* (співробітники та клієнти відчувають себе захищенішими, що сприяє позитивному робочому середовищу);

– *зменшення стресу* (наявність чітких процедур безпеки зменшує тривожність, пов'язану з потенційними загрозами);

– *підвищене усвідомлення загроз* (навчання та інформаційні кампанії сприяють кращому розумінню та ідентифікації потенційних ризиків);

– *готовність реагувати на інциденти* (співробітники знають, як діяти в критичних ситуаціях, знижуючи потенційні збитки);

– *зниження несподіваних витрат* (ефективне управління ризиками допомагає зменшити витрати на непередбачені інциденти);

– *покращення корпоративного іміджу* (здатність компанії захищати своїх співробітників та клієнтів покращує її репутацію на ринку) [5].

Ризики в сучасному бізнес-середовищі є неминучими, і компанія може зіткнутися з фізичними або цифровими загрозами. Впровадження стратегічно розробленої корпоративної безпеки забезпечує не тільки розуміння цих ризикових зон, але й проактивний захист від потенційних порушень. Така готовність є ключовою для управління ризиками і передбачення майбутніх викликів, що сприяє сталому розвитку та успіху компанії.

**Висновки.** Таким чином, компанії мають бути підготовлені до вирішення непередбачених викликів, які можуть виникнути як всередині бізнес-структур, так і на глобальному рівні. А це означає не лише знання та використання в практиці принципів корпоративної безпеки та корпоративної соціальної відповідальності, але й активне застосування принципів корпоративного управління для створення здорового робочого середовища.

Для підвищення рівня корпоративної безпеки важливо регулярно оновлювати підходи до управління ризиками, включаючи адаптацію до нових технологічних реалій та змін у законодавчому середовищі. Інвестиції в сучасні технології безпеки та підвищення обізнаності працівників щодо потенційних загроз можуть значно знизити ризики і забезпечити більш стабільне функціонування компаній. Таким чином, корпоративна безпека не лише захищає компанію, але й сприяє її сталому розвитку та довгостроковій стабільності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ареф'єва О. В., Кузьменко Т. Б. Планування економічної безпеки підприємств. Київ. Європ. ун-т, 2005. 170 с.

2. Єрмошенко М. М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення. Київ, 2001. 309 с.

3. Кравчук П. Я. Сутність та передумови виникнення поняття корпоративної безпеки підприємства. *Наук. вісник Волинського державного університету ім. Лесі Українки*. 2005. № 1. С. 165–170.

4. Рудковський О. В. Формування функцій управління корпоративною безпекою. *Соціально-економічний розвиток регіонів у контексті міжнародної інтеграції*. 2013. № 12(1). С. 141–146.

5. Франчук В. І. Теоретичні засади корпоративної безпеки. *Актуальні проблеми економіки.* 2009. № 7. С. 161–167.

6. Ansoff, H. I., Kipley, D., Lewis, A. O., Helm-Stevens, R., & An- soff, R. (2019). Using weak signals. In Implanting Strategic Management (pp. 449–468). Palgrave Macmillan, Cham. DOI: https://doi.org/10.1007/978-3-319-99599-1_20

7. Ilyash, O., Smoliar, L., Lupak, R., Duliaba, N., Dzhadan, I., Kohut, M., & Radov, D. (2021). Multidimensional analysis and forecasting the relationship between indicators of industrial-technological development and the level of economic security. *Eastern-European Journal of Enterprise Technologies*, 5(13 (113), 14–25. DOI: https://doi.org/10.15587/1729-4061.2021.243262

8. McKenzie-Skene, D. (2019). A practical guide to granting corpo- rate security in Scotland. *Edinburgh Law Review*, 2, 284–285. DOI: https://doi.org/10.3366/elr.2019.0559

REFERENCES:

1. Arefieva O. V., Kuzmenko T. B. (2005) Planuvannia ekonomichnoi bezpeky pidpryiemstv [Planning of economic security of enterprises]. Yevropeiskyi universytet. 170 p.

2. Yermoshenko M. M. (2001) Finansova bezpeka derzhavy: natsionalni interesy, realni zahrozy, stratehiia zabezpechennia [Financial security of the state: national interests, real threats, security strategy]. Kyiv. 309 p.

3. Kravchuk P. Ya. (2005) Sutnist ta peredumovy vynyknennia poniattia korporatyvnoi bezpeky pidpryiemstva [The essence and prerequisites of the emergence of the concept of corporate security of an enterprise]. *Naukovyi visnyk Volynskoho derzhavnoho universytetu im. Lesi Ukrainky – Scientific Bulletin of the Volyn State University named after Lesya Ukrainka*, vol. (1), pp. 165–170.

4. Rudkovskyi O. V. (2013) Formuvannia funktsii upravlinnia korporatyvnoiu bezpekoiu [Formation of corporate security management functions. Socio-economic development of regions in the context of international integration]. *Sotsialno-ekonomichnyi rozvytok rehioniv u konteksti mizhnarodnoi intehratsii – Socio-economic development of regions in the context of international integration,* vol. 12(1), pp. 141–146.

5. Franchuk V. I. (2009) Teoretychni zasady korporatyvnoi bezpeky [Theoretical principles of corporate security]. *Aktualni problemy ekonomiky – Actual problems of the economy*, vol. (7), pp. 161–167.

6. Ansoff, H. I., Kipley, D., Lewis, A. O., Helm-Stevens, R., & An- soff, R. (2019). Using weak signals. In Implanting Strategic Management (pp. 449–468). Palgrave Macmillan, Cham. DOI: https://doi.org/10.1007/978-3-319-99599-1_20

7. Ilyash O., Smoliar L., Lupak R., Duliaba N., Dzhadan I., Kohut M., & Radov D. (2021). Multidimensional analysis and forecasting the relationship between indicators of industrial-technological development and the level of economic security. *Eastern-European Journal of Enterprise Technologies*, 5(13 (113), 14–25. DOI: https://doi.org/10.15587/1729-4061.2021.243262

8. McKenzie-Skene, D. (2019). A practical guide to granting corporate security in Scotland. *Edinburgh Law Review*, 2, 284–285. DOI: https://doi.org/10.3366/elr.2019.0559