ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ

Кафедра: менеджменту, економіки, статистики та цифрових технологій

# БАКАЛАВРСЬКА РОБОТА

на здобуття освітнього ступеня бакалавра

на тему:

**Менеджмент корпоративної безпеки на підприємстві (на матеріалах Хмельницького РЕМ ПАТ «Хмельницькобленерго»)**

**Виконав(ла):** студент(ка)
5 курсу спеціальності
073 Менеджмент
Патик В. Р.
(прізвище та ініціали)

**Керівник:** к.е.н., доцентка, доцентка кафедри
Арзянцева Д. А.
(науковий ступінь, вчене звання, прізвище та ініціали)

**Рецензент:** Кузьмін Ф. В.
(науковий ступінь, вчене звання, прізвище та ініціали)

**Хмельницький – 2026 рік**

## Анотація

**ПІП. Менеджмент корпоративної безпеки на підприємстві (на матеріалах Хмельницького РЕМ АТ «Хмельницькобленерго»**). Кваліфікаційна наукова праця на правах рукопису. Бакалаврська робота на здобуття освітнього ступеня бакалавра за спеціальністю 073 Менеджмент. Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький, 2026. 83 с.

Бакалаврська робота спрямована на вирішення актуального науково-практичного завдання, пов'язаного з удосконаленням системи менеджменту корпоративної безпеки підприємства в умовах підвищеного рівня внутрішніх і зовнішніх загроз. У роботі визначено сутність категорій «корпоративна безпека підприємства» та «менеджмент корпоративної безпеки», систематизовано основні підходи до оцінювання рівня корпоративної безпеки.

Проведено комплексну оцінку складових корпоративної безпеки АТ «Хмельницькобленерго». Здійснено аналіз фінансово-економічної, кадрової, інформаційної, техніко-технологічної та силової складових корпоративної безпеки; виявлено ключові загрози та ризики функціонування підприємства. Оцінювання рівня корпоративної безпеки здійснено із застосуванням інтегрального підходу та методів експертного аналізу.

Сформульовано пріоритетні напрями підвищення рівня корпоративної безпеки АТ «Хмельницькобленерго» з урахуванням галузевих особливостей та стадії життєвого циклу підприємства. Запропоновано комплекс організаційно-економічних, управлінських та превентивних заходів, спрямованих на мінімізацію загроз, зниження ризиків та забезпечення сталого функціонування підприємства в сучасних умовах.

Ключові слова: корпоративна безпека; менеджмент корпоративної безпеки; загрози; ризики; система корпоративної безпеки.

## Annotation

**ІІІІІ. Corporate security management of the enterprise (based on the materials of Khmelnytskyi REM JSC "Khmelnytskoblenergo"»).** Qualification scientific work in manuscript form. Bachelor's thesis for obtaining a bachelor's degree in specialty 073 Management. Khmelnytsky University of Management and Law named after Leonid Yuzkov, Khmelnytsky, 2026. 83 p.

The bachelor's thesis is aimed at solving a relevant scientific and practical problem related to improving the corporate security management system of an enterprise under conditions of increased internal and external threats. The essence of the concepts "corporate security of the enterprise" and "corporate security management" is defined, and the main approaches to assessing the level of corporate security are systematized.

A comprehensive assessment of the components of corporate security Khmelnytskyi REM JSC "Khmelnytskoblenergo" is carried out. The financial-economic, personnel, information, technical-technological, and physical security components are analyzed, and key threats and risks affecting the enterprise's activity are identified. The level of corporate security is assessed using an integrated approach and expert evaluation methods.

Priority directions for improving the level of corporate security of Khmelnytskyi REM JSC "Khmelnytskoblenergo» are formulated, taking into account industry specifics and the stage of the enterprise life cycle. A set of organizational, economic, managerial, and preventive measures aimed at minimizing threats, reducing risks, and ensuring the sustainable operation of the enterprise in modern conditions is proposed.

Keywords: corporate security; corporate security management; threats; risks; corporate security system.

# ЗМІСТ

ВСТУП 5

РОЗДІЛ 1 ..... 8

ТЕОРЕТИЧНІ ОСНОВИ МЕНЕДЖМЕНТУ КОРПОРАТИВНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ..... 8

1.1. Сутність та значення корпоративної безпеки в системі управління підприємством ..... 8

1.2. Механізми та інструменти менеджменту корпоративної безпеки..... 16

РОЗДІЛ 2 ..... 25

ДОСЛІДЖЕННЯ СИСТЕМИ КОРПОРАТИВНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ ХМЕЛЬНИЦЬКИЙ РЕМ АТ «ХМЕЛЬНИЦЬКОБЛЕНЕРГО» ..... 25

2.1. Характеристика Хмельницького РЕМ АТ «Хмельницькобленерго» та організаційного забезпечення корпоративної безпеки ..... 25

2.2. Аналіз загроз корпоративній безпеці та оцінка ефективності діючих заходів їх нейтралізації ..... 39

РОЗДІЛ 3 ..... 50

НАПРЯМИ УДОСКОНАЛЕННЯ МЕНЕДЖМЕНТУ КОРПОРАТИВНОЇ БЕЗПЕКИ ХМЕЛЬНИЦЬКОГО РЕМ ..... 50

3.1. Концептуальні засади удосконалення корпоративної безпеки на підприємстві..... 50

3.2. Запровадження інноваційних технологій корпоративної безпеки..... 57

ВИСНОВКИ..... 62

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ..... 65

ДОДАТКИ..... 70

# ВСТУП

**Актуальність теми.** У сучасних умовах нестабільного економічного середовища, високої конкуренції, технологічної динамічності та посилення зовнішніх і внутрішніх загроз питання забезпечення корпоративної безпеки підприємств набуває особливої ваги. Підприємства енергетичної сфери, зокрема об'єкти критичної інфраструктури, стикаються з широким спектром ризиків: від фінансово-економічних та інформаційних до технологічних, кадрових та соціальних. У таких умовах традиційні підходи до захисту ресурсів підприємства виявляються недостатніми, що зумовлює необхідність формування ефективної системи менеджменту корпоративної безпеки.

Корпоративна безпека виступає комплексною характеристикою здатності підприємства протистояти загрозам і забезпечувати стабільність своєї діяльності. Значна кількість сучасних досліджень присвячена питанням економічної, інформаційної, кадрової безпеки, однак недостатньо опрацьованими залишаються аспекти інтегрованого менеджменту корпоративної безпеки, що охоплює весь спектр функціональних напрямів та передбачає системну взаємодію між підрозділами. Для підприємств енергетичної галузі, зокрема Хмельницького РЕМ АТ «Хмельницькобленерго», ефективне управління корпоративною безпекою є критично необхідним, адже стабільне постачання електроенергії прямо залежить від здатності підприємства забезпечити надійність технологічних процесів, інформаційних потоків, захист кадрового потенціалу та фінансових ресурсів. Це обумовлює наукову та практичну необхідність дослідження сучасних механізмів менеджменту корпоративної безпеки та розробки шляхів їх удосконалення.

Актуальність дослідження корпоративної безпеки підтверджується численними роботами вітчизняних та зарубіжних науковців таких як Шира Т. [51], Б., Кіпчарська Я. М. [22], Марущак С. М. [30], Грішина В. П. [15], Мігус І. П. [32], Рудковський О. В. [42]. Разом з тим попри наявність значної

кількості наукових праць, присвячених проблематиці корпоративної безпеки, питання формування та впровадження ефективної системи корпоративної безпеки на підприємствах енергетичної галузі, зокрема на рівні регіональних підрозділів, залишаються недостатньо дослідженими та потребують подальшого наукового опрацювання.

**Мета та завдання роботи**. Метою бакалаврської роботи є обґрунтування теоретичних засад і розроблення практичних рекомендацій щодо удосконалення менеджменту корпоративної безпеки на підприємстві на матеріалах Хмельницького РЕМ.

Для досягнення поставленої мети необхідно вирішити такі **завдання:**

– вивчити сутність корпоративної безпеки та її ролі в системі управління підприємством;

– дослідити механізми та інструменти менеджменту корпоративної безпеки;

– надати характеристику діяльності Хмельницького РЕМ та оцінити організаційне забезпечення корпоративної безпеки;

– ідентифікувати загрози корпоративній безпеці підприємства та здійснити оцінку ефективності існуючих заходів їх нейтралізації;

– обґрунтувати напрями удосконалення менеджменту корпоративної безпеки;

– запропонувати інноваційні технології підвищення рівня корпоративної безпеки Хмельницького РЕМ.

**Об’єкт дослідження** – процес управління корпоративною безпекою підприємства.

**Предмет дослідження** – теоретико-методичні засади та практичні рекомендації щодо менеджменту корпоративної безпеки підприємства АТ «Хмельницькобленерго».

У процесі виконання роботи використано сукупність загальнонаукових і спеціальних **методів дослідження.** Методи узагальнення та систематизації застосовано для аналізу наукових підходів до визначення сутності

корпоративної безпеки та менеджменту корпоративної безпеки підприємства. Методи економічного та структурного аналізу використано для дослідження стану системи корпоративної безпеки Хмельницького РЕМ АТ «Хмельницькобленерго» та її складових. Порівняльний аналіз застосовано для зіставлення показників рівня загроз і ефективності заходів корпоративної безпеки в динаміці. Методи математичної статистики використано для обробки та інтерпретації кількісних показників фінансово-економічної та кадрової безпеки підприємства. Метод експертних оцінок застосовано з метою ідентифікації та ранжування основних загроз корпоративній безпеці підприємства. Елементи економіко-математичного моделювання використано для оцінювання ефективності заходів менеджменту корпоративної безпеки та обґрунтування напрямів їх удосконалення. Соціологічні методи (опитування та аналіз кадрової інформації) застосовано для дослідження кадрових ризиків і оцінки рівня кадрової складової корпоративної безпеки підприємства. Практична значущість полягає в можливості застосування отриманих результатів у діяльності Хмельницького РЕМ для підвищення рівня корпоративної безпеки, удосконалення системи ідентифікації загроз, оптимізації механізмів управління ризиками та впровадження сучасних технологічних рішень у сфері інформаційної й кадрової безпеки.

**Апробація результатів дослідження.** Окремі положення та отриманні результати бакалаврської роботи були оприлюднені на Міжнародній науково-практичній конференції «SCIENCE AT THE FRONTIER OF PROGRESS» (27-29 січня 2026 року м. Париж, Франція) [56].

Структура роботи. Бакалаврська робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 67 сторінок.

# РОЗДІЛ 1
# ТЕОРЕТИЧНІ ОСНОВИ МЕНЕДЖМЕНТУ КОРПОРАТИВНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

## 1.1. Сутність та значення корпоративної безпеки в системі управління підприємством

Корпоративна безпека є комплексною системою заходів, спрямованих на захист підприємства від внутрішніх і зовнішніх загроз, здатних порушити стабільність його функціонування або негативно вплинути на фінансові результати. У сучасних умовах динамічного та часто нестабільного ринкового середовища корпоративна безпека розглядається як превентивний механізм, що забезпечує підприємству чіткий план дій у разі виникнення ризиків, інцидентів або кризових ситуацій. Вона інтегрується в усі рівні управління та охоплює як традиційні напрями захисту, так і сучасні підходи до управління ризиками, інформаційної безпеки, відповідності нормативним вимогам та забезпечення безперервності бізнес-процесів.

За своєю сутністю корпоративна безпека являє собою керовану систему, яка пов'язує фізичний, технічний, інформаційний, кадровий, процедурний та управлінський аспекти діяльності підприємства. Така багатовимірність пояснюється тим, що загрози можуть виникати як у матеріальному середовищі, так і у цифровому просторі або внаслідок людського фактора. Тому ефективна система корпоративної безпеки повинна забезпечувати своєчасне виявлення потенційних ризиків, їх аналіз і нейтралізацію ще до того, як вони призводять до збитків.[55]

Значення корпоративної безпеки для системи управління підприємством полягає насамперед у її здатності гарантувати стабільність роботи, захист комерційних і особистих даних, збереження інтелектуальних і матеріальних ресурсів, а також підтримання позитивної ділової репутації. Успішне функціонування підприємства багато в чому залежить не лише від

компетентності менеджменту та конкурентних переваг продукції, але й від здатності підприємства протидіяти загрозам, сконцентрованим у цифровій сфері, у сфері трудових відносин і в операційних процесах. Саме тому корпоративна безпека виступає інструментом стратегічного управління, який сприяє забезпеченню довгострокової стійкості та конкурентоспроможності підприємства.

Формування ефективної корпоративної безпеки потребує врахування особливостей галузі, масштабів діяльності та рівня ризиковості бізнес-процесів підприємства. Наприклад, виробничі підприємства зосереджуються передусім на дотриманні вимог охорони праці, екологічної та технічної безпеки, тоді як установи фінансового сектору традиційно приділяють підвищену увагу інформаційній безпеці, кіберзахисту та запобіганню шахрайству. Водночас, у будь-якій галузі важливо забезпечити узгодженість дій персоналу, прозорість процедур доступу, належну комунікацію між структурними підрозділами та вчасність управлінських рішень.[23]

У контексті сучасної digital-економіки особливого значення набувають питання захисту даних та дотримання вимог законодавства у сфері конфіденційності інформації, адже витоки інформації стають однією з найбільш поширених та дороговартісних загроз. Додатковим викликом для підприємств є управління мобільною та дистанційною роботою працівників. Коли працівники працюють поза офісом, підприємство має подбати про спеціальні засоби безпеки, щоб ніхто сторонній не отримав доступ до корпоративної інформації [1].

З огляду на це корпоративна безпека займає ключове місце в системі управління підприємством, оскільки дозволяє не лише запобігти кризовим ситуаціям, але й забезпечує безперервність виробничих і бізнес-процесів, підвищуючи таким чином ефективність діяльності і загальну конкурентоздатність підприємства. Її значення полягає у здатності створювати умови, за яких підприємство може розвиватися, інвестувати, впроваджувати інновації та підтримувати стабільні стосунки з партнерами, споживачами й

іншими стейкхолдерами. Саме тому корпоративна безпека є невід'ємним компонентом сучасної системи менеджменту та важливим чинником довгострокового успіху підприємства.

На основі критичного переосмислення наукових підходів [2-5] структура корпоративної безпеки може бути подана у вигляді таких взаємопов'язаних складових (рис. 1.1).

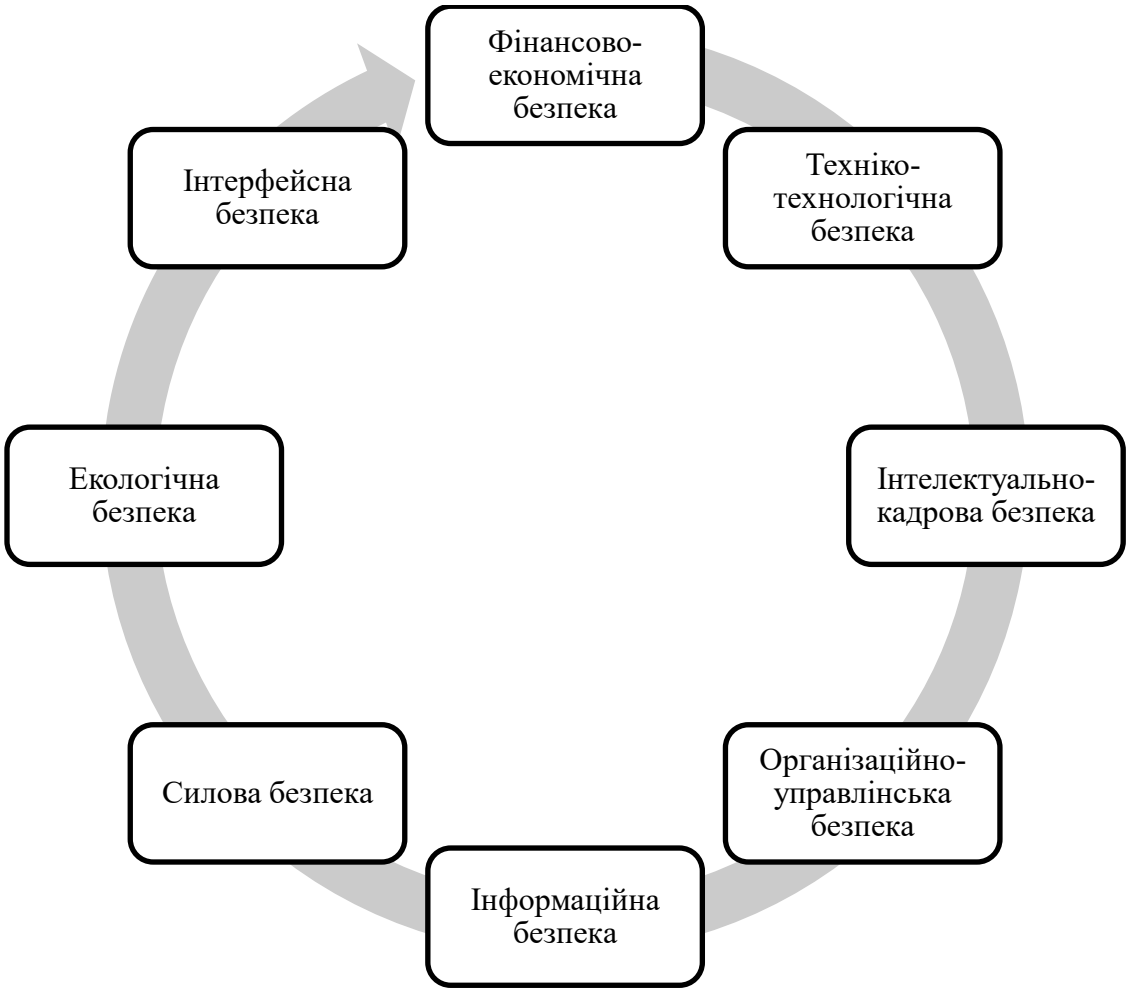


Рисунок 1.1. Структура корпоративної безпеки

*Джерело: складено за [2-5]*

Фінансово-економічна безпека характеризує ефективність використання корпоративних ресурсів, забезпечення фінансової стійкості, ліквідності та прибутковості підприємства. У цю складову включають фінансову, економічну та ринкову підсистеми, що відображають здатність підприємства забезпечувати стабільний розвиток, підтримувати конкурентні позиції та

адаптуватися до змін ринкової кон’юнктури.

Техніко-технологічна безпека забезпечує відповідність технічного оснащення і технологічних процесів сучасним стандартам, включає технічну, технологічну та екологічну підсистеми. Її ключова роль полягає у зниженні технологічних ризиків, підвищенні ефективності виробництва та дотриманні екологічних нормативів.

Інтелектуально-кадрова безпека пов’язана з рівнем професійної підготовки персоналу, мотивацією, морально-психологічним кліматом та захистом інтелектуальних ресурсів підприємства. До її складу входять кадрова, мотиваційна, морально-психологічна та інтелектуальна підсистеми, що визначають здатність підприємства формувати висококваліфікований і лояльний персонал.

Організаційно-управлінська безпека є визначальною для корпоративного підприємства, оскільки охоплює гарантування прав акціонерів, прозорість корпоративного управління та ефективність менеджменту. Правова безпека також є невід’ємною частиною цієї складової, оскільки убезпечує підприємство від юридичних ризиків та забезпечує дотримання внутрішніх регламентів.[20]

Інформаційна безпека спрямована на захист інформаційних ресурсів, ефективне інформаційно-аналітичне забезпечення та формування позитивного іміджу підприємства. Вона включає безпеку документообігу, аналітичну й іміджеву складові.

Силова безпека забезпечує фізичний захист персоналу, об’єктів та майна, а також мінімізацію ризиків протиправних дій.

Екологічна безпека полягає в забезпеченні відповідності діяльності підприємства екологічним нормам, мінімізації негативного впливу на довкілля та дотриманні екологічних стандартів продукції.

Інтерфейсна безпека відображає надійність взаємодії підприємства з контрагентами (постачальниками, споживачами, інвесторами та

посередниками). Зміна умов співробітництва в ринковому середовищі може створювати суттєві ризики, що потребують відповідного управління.

Об’єктами корпоративної безпеки є фінансові ресурси, персонал, репутація власників та підприємства, активи, технології та бізнес-процеси. Суб’єктами корпоративної безпеки виступають керівництво підприємства, внутрішні служби або спеціалізовані зовнішні організації (аутсорсинг), а також змішані моделі. На практиці доцільним є поєднання внутрішніх і зовнішніх механізмів: внутрішні підрозділи відповідають за організацію, координацію та контроль заходів безпеки, а зовнішнім структурам передаються функції, що потребують спеціальної експертизи (кібербезпека, юридичний супровід, аудит безпеки тощо) [6].

Корпоративна безпека є невід'ємною складовою системи управління сучасним підприємством, адже забезпечує захищеність ресурсів, стабільність функціонування та здатність ефективно реагувати на внутрішні й зовнішні загрози. Формування дієвої системи корпоративної безпеки потребує опори на низку методологічних основ (табл. 1.1).

Таблиця 1.1. Методологічні основи формування корпоративної безпеки та їх значення в системі управління підприємством

| Основа безпеки | Сутність | Значення для системи управління підприємством |
|---|---|---|
| 1 | 2 | 3 |
| Унікальність | Корпоративна безпека формується з урахуванням індивідуальних характеристик підприємства: форми власності, виду діяльності, масштабів, організаційної структури, специфіки ринку та умов функціонування. | Дозволяє створити безпекову систему, яка відповідає реальним потребам підприємства та забезпечує ефективний захист від специфічних загроз. |
| Узгодженість | Забезпечення тісної інтеграції служби безпеки з усіма підрозділами підприємства, побудова вертикальних і горизонтальних комунікацій. | Підвищує швидкість реагування на ризики, сприяє кращому обміну інформацією, забезпечує комплексність рішень і мінімізує управлінські збої. |
| Комплексність | Спрямованість заходів безпеки на всі ключові сфери діяльності підприємства, а не лише на окремі аспекти. | Дозволяє усувати загрози системно, запобігаючи їх поширенню на інші сфери та мінімізуючи ризики мультиплікативних втрат. |

Продовження табл. 1.1

| 1 | 2 | 3 |
|---|---|---|
| Автономність | Виділення власних фінансових, кадрових та організаційних ресурсів для підтримання та розвитку системи безпеки незалежно від коливань фінансових результатів підприємства. | Забезпечує стабільність функціонування служби безпеки та дає можливість реалізовувати довгострокові превентивні програми. |
| Наявність резерву | Формування двох бюджетів: базового — для поточної діяльності служби безпеки, та резервного — для реагування на критичні загрози. | Підвищує готовність підприємства до непередбачуваних подій, скорочує час реакції та мінімізує збитки. |
| Дієвість | Активна позиція служби безпеки: своєчасне виявлення ризиків, аналіз загроз, формування інформації для управлінських рішень. | Забезпечує проактивне управління ризиками, зменшує імовірність реалізації загроз та покращує стабільність діяльності підприємства. |
| Адаптивність | Гнучкість системи безпеки щодо змін у внутрішньому та зовнішньому середовищі, можливість швидкого коригування заходів. | Дає підприємству здатність ефективно функціонувати в умовах невизначеності та турбулентності ринку. |
| Своєчасність реакції | Прогнозування потенційних змін у рівні безпеки та оперативне впровадження відповідних заходів. | Дозволяє попереджувати загрози на ранніх етапах, економити ресурси та підтримувати стабільний рівень безпеки. |

Примітка: складено автором за джерелом[7]

У період поширення дистанційних форм зайнятості, зростання кіберзагроз, інформаційної вразливості та технологічної залежності бізнесу особливої важливості набуває формування цілісної культури корпоративної безпеки. Вона виступає не лише як набір регламентів і технічних рішень, а як соціально-організаційний механізм, що інтегрується у всі бізнес-процеси та визначає поведінку працівників, якість управлінських рішень та стратегічні можливості компанії.

Значення корпоративної безпеки проявляється в тому, що вона забезпечує цілісність бізнесу як системи, де кожен співробітник усвідомлює свою відповідальність за захист інформаційних, фінансових, матеріальних та репутаційних активів. У ситуації, коли робота організацій дедалі більше ґрунтується на цифрових сервісах, а дистанційна діяльність відкриває

додаткові канали ризику, навіть один необачний крок працівника може поставити під удар цілісну інфраструктуру компанії. Тому корпоративна безпека стає не лише технічною чи адміністративною функцією, вона перетворюється на елемент корпоративної культури, що формує модель поведінки персоналу, рівень довіри, атмосферу відповідальності та дисципліни.

Ефективне управління підприємством передбачає, що безпекова складова інтегрована у кожен процес (від стратегічного планування до щоденних операцій). Коли безпековий компонент є невід'ємною частиною управлінських рішень, підприємство здатне системно виявляти загрози, оперативно реагувати на ризики та мінімізувати наслідки можливих інцидентів.

Корпоративна безпека – це не вузька функція окремого підрозділу, а спільний процес, що охоплює все підприємство. Її ефективність залежить від здатності керівників підрозділів демонструвати особисту відповідальність, від рівня усвідомленості персоналу, якості комунікації між службами та наявності наскрізних механізмів контролю ризиків.[41]

Культура корпоративної безпеки передбачає, що працівники не тільки знають правила, але й добровільно їх дотримуються, використовуючи їх як частину повсякденної роботи. Вони розуміють важливість комплексного підходу до захисту (від кібергігієни до протидії шахрайству, від роботи з конфіденційною інформацією до взаємодії з контрагентами). Ключову роль відіграє й людський фактор, тому підприємства мають здійснювати системну оцінку благонадійності персоналу, аналіз норм поведінки та мотивації, оскільки саме персонал найчастіше стає джерелом ризиків, як ненавмисних, так і цілеспрямованих.

Важливе місце у забезпеченні корпоративної безпеки займає аналітика. Підприємства, які системно аналізують дані щодо безпеки, отримують вагомі конкурентні переваги, оскільки здатні швидше реагувати на зміни та запобігати збиткам, ще до того як загроза проявляється в реальних

наслідках[8].

Практика українських підприємств підтверджує, що ефективність корпоративної безпеки значною мірою залежить від організації внутрішнього контролю. Як зазначає В. Пантелеєв, однією з найбільших проблем є розпорошеність контрольних функцій, відсутність координації та несвоєчасність контрольних заходів, що призводить до надмірного нагляду за одними об’єктами та недостатнього – за іншими [9]. Навіть за наявності ревізійних комісій у більшості акціонерних товариств, їх діяльність майже не впливає на реальний контроль за управлінськими рішеннями, оскільки частота засідань є критично низькою, а кадровий склад – недостатнім [10]. Усе це свідчить, що без належного внутрішньокорпоративного контролю корпоративна безпека втрачає свою дієвість.

У контексті забезпечення корпоративної безпеки внутрішньокорпоративний контроль слід розглядати як систему спостереження й перевірки, яка орієнтована на інформаційні потреби власників та менеджменту, спрямовані на досягнення корпоративних інтересів, раціональне використання ресурсів та захист від зовнішніх і внутрішніх загроз. На відміну від узагальненого підходу І. Дмитренко, яка трактує внутрішньокорпоративний контроль як механізм реалізації волі власників на всіх рівнях управління [11], у сфері корпоративної безпеки він виконує більш специфічну функцію – забезпечує виявлення загроз, оцінку ризиків і формує інформаційну базу для своєчасних управлінських рішень щодо їх нейтралізації.

Суттєве значення має також поділ внутрішньокорпоративного контролю на внутрішній аудит і внутрішньогосподарський контроль, оскільки ці компоненти дозволяють по-різному оцінювати вплив управлінських дій на безпеку підприємства, виявляти ознаки корпоративних конфліктів чи низької ефективності менеджменту. Внутрішньокорпоративний контроль забезпечує своєчасне формування сигналів про посилення ризиків, а відтак, створює умови для оперативного реагування. Мета такого контролю у системі

корпоративної безпеки полягає не лише у гармонізації стратегічних і поточних завдань, але й у тому, щоб забезпечити керівництво достовірною інформацією про безпекові аспекти діяльності, стан ресурсів, наявність загроз і можливість їх попередження.

Отже, корпоративна безпека в системі управління підприємством є не просто частиною операційної діяльності, а стратегічним інструментом забезпечення стійкості, конкурентоспроможності та довгострокового розвитку бізнесу. Вона формує основу довіри всередині компанії, зміцнює її репутацію на ринку, знижує потенційні втрати і створює умови для ефективного функціонування в умовах динамічних ризиків сучасного ринку.

## 1.2. Механізми та інструменти менеджменту корпоративної безпеки

Менеджмент корпоративної безпеки підприємства складається з сукупності механізмів і інструментів, які забезпечують захист організації від внутрішніх і зовнішніх загроз, підтримують її стабільність і здатність до розвитку, а також інтегровані у загальну систему управління. Таке розуміння підтверджується як українськими, так і міжнародними науковими джерелами [12].

Перш за все, менеджмент корпоративної безпеки ґрунтується на організаційно-управлінських механізмах, що створюють правові та адміністративні рамки для діяльності усіх служб безпеки підприємства. Це включає формування чіткої структури відповідальності, розподіл повноважень та інтеграцію служби безпеки у загальну систему корпоративного управління, що забезпечує координацію дій між різними підрозділами та сприяє своєчасному обміну інформацією про потенційні загрози. Суттєве значення такого підходу підкреслено в роботах з корпоративної безпеки підприємств, де організаційно-правові механізми розглядаються як фундамент для побудови дієвої безпекової системи та

запобігання ризикам, що виникають в умовах мінливого зовнішнього середовища [13].

Економічні механізми управління безпекою виконують важливу функцію збереження фінансових і матеріальних ресурсів. Вони включають управління ризиками, бюджетування безпекових заходів, фінансове планування та страхування, що дозволяють підприємству мінімізувати можливі економічні втрати, забезпечити ліквідність і стійкість до кризових явищ. Так, у контексті управління економічною безпекою вітчизняні дослідники розглядають механізми попереджуючого та антикризового управління, що передбачають аналіз, прогнозування ризиків, планування необхідних заходів і оперативне реагування при настанні подій, які можуть поставити під загрозу діяльність підприємства [14] (табл. 1.2).

Таблиця 1.2. Складові механізму управління економічною безпекою підприємства

| Вид управління економічною безпекою | Основний зміст | Ключові дії / механізми |
|---|---|---|
| Стратегічне управління | Формування довгострокових цілей та пріоритетів економічної безпеки підприємства | Розробка стратегії безпеки, інтеграція з корпоративною стратегією, аналіз зовнішнього середовища |
| Попереджуюче (превентивне) управління | Запобігання виникненню потенційних загроз економічній безпеці | Аналіз і прогнозування загроз, планування змін, моніторинг ризиків, раннє реагування |
| Оперативне управління | Забезпечення поточного рівня економічної безпеки в процесі діяльності підприємства | Контроль показників безпеки, координація підрозділів, коригування управлінських рішень |
| Антикризове управління | Реалізація заходів з мінімізації втрат у разі настання загроз | Швидке реагування, локалізація кризових ситуацій, оперативне прийняття рішень |
| Контрольне управління | Оцінювання результативності заходів забезпечення економічної безпеки | Аудит безпеки, аналіз відхилень, коригування стратегії та інструментів |

Примітка: створено автором на основі джерела[26].

Це підтверджує, що адекватне розуміння та реалізація таких економічних механізмів є важливою складовою корпоративної безпеки в системі управління підприємством.

Значну роль у системі менеджменту корпоративної безпеки відіграють інформаційно-аналітичні інструменти, що забезпечують якісну обробку, оцінку та прогнозування даних про ризики та загрози. Завдяки застосуванню сучасних інформаційних систем, платформ бізнес-аналітики (BI), CRM/ERP-систем та технологій штучного інтелекту підприємство отримує можливість якісно оцінювати стан безпеки, виявляти аномалії, моделювати сценарії розвитку загроз і приймати обґрунтовані рішення щодо їх нейтралізації. Методи управління корпоративною інформаційною безпекою, включаючи аналіз уразливостей та моніторинг загроз, розглядаються як невід'ємна частина сучасного менеджменту безпеки, що дозволяє суттєво підвищити ефективність захисних заходів та адаптуватись до цифрових ризиків [15]. Ключовими елементами механізму корпоративної інформаційної безпеки є об'єкти, суб'єкти, мета, завдання, функції та методи впливу. Об'єктами безпеки виступають структурні елементи корпоративного інформаційного простору, такі як інформаційне поле, віртуальна реальність, інформаційні процеси, інформаційна культура, технічні та технологічні засоби, а також внутрішні регламенти та нормативи. Суб'єктами є служба безпеки, IT-служба, юридичні підрозділи, топ-менеджери та відповідальні особи, які мають доступ до конфіденційної інформації. Метою корпоративної безпеки є забезпечення реалізації економічних інтересів підприємства шляхом захисту інформації, а завдання включають забезпечення цілісності, конфіденційності та доступності даних. Функції механізму охоплюють ідентифікацію загроз, оцінювання та аналіз ризиків, формування організаційної структури служби безпеки, розробку стратегії захисту корпоративної інформації та координацію роботи між підрозділами.[28]

Інструменти (методи) управління корпоративною безпекою можна класифікувати на економічні, організаційно-правові та технічні.

Економічні методи включають аналіз бізнес-процесів, систему збалансованих показників, стратегічні карти, карту ризиків, прикладний інформаційний аналіз, оцінку доданої та вихідної економічної вартості,

управління портфелем активів, функціонально-вартісний аналіз, метод життєвого циклу штучних систем, методи інтегрального аналізу та експертних оцінок. Використання цих методів дозволяє ідентифікувати загрози, здійснювати аналіз та планування заходів з управління інформаційною безпекою.

Організаційно-правові методи включають моделювання бізнес-процесів, впровадження комплаєнсу та розробку регламентних документів. Моделювання бізнес-процесів забезпечує систематизацію діяльності підприємства та оптимізацію процесів захисту інформації. Найпоширенішими методами є SADT (Structured Analysis and Design Technique), IDEF0 та IDEF3, DFD (Data Flow Diagrams), ARIS, Ericsson-Penker та Rational Unified Process, які дозволяють аналізувати послідовність дій, потоки даних, взаємозалежності процесів та бізнес-модель підприємства. Комплаєнс є важливим інструментом корпоративної культури та управління ризиками невідповідності законодавству або внутрішнім стандартам. Він орієнтований на запобігання умисному та неумисному витоку конфіденційної інформації та може реалізовуватись за підходом «Rule based» або «Risk based», де останній вважається більш ефективним для інтеграції з іншими інструментами корпоративної безпеки.[31]

Технічні методи включають моделювання корпоративної інформаційної безпеки та автоматизовані системи управління ризиками. Основними моделями є Bell-LaPadula (BLP), Biba, Clark-Wilson (CW), дискреційна (матрична) модель, Adept-50, MITER ATT&CK, «алмазна модель» та «піраміда болю», які дозволяють формалізовано оцінювати рівень безпеки та взаємодії суб’єктів і об’єктів інформаційної системи. Автоматизовані системи, такі як CRAMM, CORAS, OCTAVE, Risk Watch та Oracle Crystal Ball, забезпечують якісне та кількісне оцінювання ризиків, оптимізацію витрат на захист та прогнозування можливих загроз. [35]

Таким чином, менеджмент корпоративної безпеки підприємства реалізується через поєднання економічних, організаційно-правових та

технічних методів, що дозволяє забезпечити захист корпоративної інформації, мінімізувати ризики та підтримувати стратегію ефективного функціонування підприємства в умовах сучасного динамічного середовища.

Правові інструменти менеджменту корпоративної безпеки забезпечують правову основу для діяльності підприємства щодо дотримання законів, регламентів, внутрішніх політик та процедур безпеки. Це включає механізми нормативного регулювання реалізації безпекових програм, побудови систем контролю та аудиту, а також управління конфліктами інтересів. Правове забезпечення створює умови для захисту корпоративних прав власників і менеджерів, мінімізує ризики юридичної відповідальності та сприяє створенню прозорої системи корпоративного управління, що підвищує довіру інвесторів та партнерів.[44]

У контексті сучасних викликів не менше значення мають технічні та технологічні механізми, зокрема системи кібербезпеки, засоби контролю доступу, відеоспостереження, шифрування даних та резервного копіювання, які забезпечують безперервність технологічних процесів і захист інформаційних активів підприємства. Міжнародні дослідження підкреслюють, що інтеграція таких технологій у загальну систему корпоративної безпеки сприяє зниженню вразливості до кібератак, забезпечує відповідність стандартам захисту даних і зменшує операційні ризики [16].

Крім того, суттєвою складовою механізмів менеджменту корпоративної безпеки є управління кадровою безпекою, яке спрямоване на створення умов для відбору, навчання та мотивації персоналу відповідно до вимог безпеки. У межах цього механізму розробляються політики щодо професійної підготовки, оцінювання компетенцій персоналу у сфері безпеки, а також управління поведінкою працівників для мінімізації людського фактору як джерела ризиків. Управління кадровою безпекою розглядається в наукових працях як один із важливих елементів загальної системи захисту підприємства, що забезпечує формування відповідального та компетентного колективу [17].

Формування системи корпоративної безпеки починається з прийняття

стратегічного рішення про створення та розробку концепції кадрової безпеки, що включає визначення мети, завдань, функцій, принципів та стратегій забезпечення безпеки персоналу. Система управління кадровою безпекою на підприємстві визначається як сукупність взаємопов'язаних заходів, спрямованих на забезпечення нормального функціонування, розвитку та ефективного використання персоналу при одночасному збереженні стабільності економічної безпеки підприємства. Основною метою корпоративної безпеки в контексті кадрового менеджменту є формування та утримання висококваліфікованого та відповідального персоналу, здатного мінімізувати вплив внутрішніх і зовнішніх загроз на економічну безпеку підприємства. Завдання системи включають ефективне використання персоналу, вибір оптимального стилю управління, забезпечення координації та співпраці між підрозділами, підвищення якості організації робочих місць, визнання особистих досягнень працівників, а також впровадження системи оплати та стимулювання.[40]

Ключовими механізмами реалізації корпоративної безпеки з позиції кадрової безпеки є організаційний, мотиваційний, соціальний та економічний механізми. Організаційний механізм передбачає прогнозування структури персоналу, визначення потреб у кадрах, підбір та розміщення співробітників, укладання трудових договорів та контрактів. Мотиваційний механізм зосереджується на оцінці потенціалу працівників, їхніх навичок, компетенцій та бажань, що дозволяє планувати навчання, підвищення кваліфікації і ефективне закріплення або заміну персоналу. Соціальний механізм включає управління кар'єрою, підтримку морально-психологічного клімату в колективі та створення стабільного складу персоналу і робочих місць. Економічний механізм охоплює управління витратами на персонал, стимулювання та забезпечення діяльності служби економічної безпеки.

Інструменти менеджменту кадрової безпеки охоплюють нормативно-правове регулювання, функціональні складові системи та методологію оцінки стану безпеки. Нормативно-правове забезпечення ґрунтується на Конституції

України, міжнародних правових актах, ратифікованих ВРУ, Податковому кодексі Україні, Кодексі Законів про працю, інших Законах України («Про зайнятість населення» тощо), підзаконних актах, внутрішніх документах підприємства (Статут, Положення про Службу економічної безпеки, Положення про комерційну таємницю, Положення про мотивацію персоналу, Колективний догорів тощо). [45] Функціональні складові системи включають фінансову, корпоративну, правову, майнову, кадрову, технологічну, інформаційну та екологічну складові. Методологія комплексної оцінки стану системи передбачає використання показників витрат на персонал, якості процесів управління, результативності управління та стану кадрової безпеки (табл. 1.3).

Таблиця 1.3. Складові механізму управління кадровою безпекою підприємства

| Механізм | Основні функції та завдання |
|---|---|
| Організаційний | Планування структури та потреб у персоналі, залучення та відбір співробітників, розміщення кадрів, укладання договорів і контрактів. |
| Мотиваційний | Створення бази даних щодо рівня кваліфікації, професійних умінь, бажань та результатів оцінки праці працівників для визначення потенціалу, організації навчання, підвищення кваліфікації, закріплення або звільнення персоналу. |
| Соціальний | Управління кар'єрою, професійно-кваліфікаційне та посадове переміщення працівників, формування стабільного складу персоналу та робочих місць, покращення морально-психологічного клімату у колективі. |
| Економічний | Управління витратами на персонал, стимулювання працівників, контроль витрат на створення та забезпечення діяльності служби економічної безпеки. |

Примітка: складено автором за джерелом[19]

Важливо, що ефективний менеджмент корпоративної безпеки сприяє не лише зменшенню ризиків, а й підвищенню корпоративного іміджу, стабільності роботи та мотивації співробітників. Чіткі процедури, навчання персоналу та належне планування дозволяють знизити стрес і непередбачені витрати, підвищити готовність до реагування на кризові ситуації та забезпечити стратегічну стійкість компанії в умовах динамічного бізнес-середовища [18].

Успішне функціонування системи корпоративної безпеки значною мірою залежить від роботи штатного підрозділу безпеки, який підпорядковується безпосередньо керівництву підприємства та координує свої дії з іншими структурними підрозділами і зовнішніми державними та недержавними органами. Основною метою підрозділу є попередження, мінімізація та протидія небезпекам, загрозам і ризикам, що забезпечує стабільне функціонування і розвиток підприємства. Одним із ключових механізмів є інформаційно-аналітичне забезпечення, яке включає збір, систематизацію, обробку та аналіз інформації про конкурентне середовище, зміни на ринку та потенційні загрози для діяльності підприємства. На основі аналітичних даних готуються довідки та рекомендації для керівництва, що дозволяє приймати стратегічні рішення, визначати політику компанії та планувати розвиток. Важливим інструментом тут є оцінка достовірності інформації та її впливу на внутрішнє та зовнішнє середовище, що дозволяє своєчасно виявляти ризики та розробляти відповідні заходи безпеки.[32]

Планування діяльності корпоративної безпеки виступає наступним важливим механізмом. Воно охоплює визначення пріоритетів захисту економічних, кадрових та інформаційних ресурсів підприємства, узгодження завдань різних підрозділів і створення процедур протидії потенційним загрозам. Інструментами планування є розробка політик безпеки, стратегічних профілів захисту та систем технологічного контролю, що дозволяє відстежувати стан активів і своєчасно реагувати на ризики.

Взаємодія підрозділу безпеки з державними органами, силовими структурами та зовнішніми партнерами є ще одним механізмом менеджменту корпоративної безпеки. Вона забезпечує протидію реальним і потенційним загрозам економічної безпеки та дозволяє захищати комерційну та інтелектуальну власність підприємства. Сюди входить захист інформації на електронних носіях, протидія корпоративній шпигунській діяльності та контроль за дотриманням законодавчих вимог.[42]

Стратегічні інструменти менеджменту корпоративної безпеки

спрямовані на гармонізацію інтересів підприємства та його персоналу, діагностику фінансово-економічної стійкості, формування профілів захисту стратегічних планів, підтримку інноваційної активності та адаптивності організації, а також забезпечення екологічної та соціальної відповідальності. Вони включають комплекс заходів, які дозволяють підприємству ефективно управляти ризиками, знижувати фінансові та операційні втрати, підтримувати конкурентну позицію на ринку та забезпечувати сталий розвиток [34].

Узагальнюючи, менеджмент корпоративної безпеки підприємства охоплює комплекс механізмів та інструментів (організаційно-управлінських, економічних, правових, інформаційно-аналітичних, технологічних і кадрових), які взаємодіють між собою, створюючи цілісну систему захисту та розвитку підприємства. Їхня взаємодія сприяє підвищенню стійкості до загроз, зміцненню корпоративних позицій на ринку, покращенню управлінських рішень та створенню умов для сталого функціонування і розвитку в умовах сучасної економіки.

Таким чином, механізми і інструменти менеджменту корпоративної безпеки включають комплексну оцінку потреб компанії, інтегрований підхід до захисту всіх бізнес-процесів, використання сучасних технологій і розробку стратегій протидії ключовим загрозам. Їх ефективне застосування дозволяє компаніям зменшувати ризики, підвищувати конкурентоспроможність і забезпечувати сталий розвиток у сучасних економічних умовах.

# РОЗДІЛ 2
# ДОСЛІДЖЕННЯ СИСТЕМИ КОРПОРАТИВНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ ХМЕЛЬНИЦЬКИЙ РЕМ АТ «ХМЕЛЬНИЦЬКОБЛЕНЕРГО»

## 2.1. Характеристика Хмельницького РЕМ АТ «Хмельницькобленерго» та організаційного забезпечення корпоративної безпеки

Хмельницький район електричних мереж (Хмельницький РЕМ) є відокремленим підрозділом акціонерного товариства АТ «Хмельницькобленерго», який виконує функції з експлуатації та обслуговування розподільчих мереж, обліку електроенергії та надання суміжних послуг споживачам у межах визначеної території.

Основні функції Хмельницький РЕМ:

1) експлуатація розподільчих мереж та ліній електропередачі середньої й низької напруги;

2) технічне обслуговування і ремонт обладнання електромереж;

3) виконання робіт з приєднання споживачів та заміни/пломбування/монтажу засобів обліку (лічильників);

4) організація аварійно-відновлювальних робіт та оперативне реагування на відключення;

5) взаємодія з населенням і бізнес-клієнтами щодо послуг та графіків планових робіт.

На сайті АТ «Хмельницькобленерго» перелік відокремлених підрозділів містить контакти Хмельницького РЕМ (телефон, e-mail), інформацію про відділення (наприклад, Ярмолинецьке відділення) та послуги, які надаються через районну структуру. РЕМ виконує й сервісну/адміністративну функцію взаємодії зі споживачами. На офіційному сайті наведено перелік відокремлених відділень, які входять до складу Хмельницького РЕМ

(наприклад, Хмельницьке відділення та Ярмолинецьке відділення), з телефонами і e-mail для прийому заяв і повідомлень. Хмельницький РЕМ має територіальний поділ оперативних зон для більш оперативного обслуговування споживачів у місті Хмельницькому та навколишніх районах.

Хмельницький РЕМ надає типові для районних електромереж послуги: приєднання споживачів, монтаж і заміну електролічильників, пломбування вузлів обліку, виконання електромонтажних робіт, оперативне усунення аварій, планові вимкнення для ремонту та реконструкції. На сайті публікується переліки послуг і вартість деяких платних робіт, а також інструкції для замовлення послуг (через особистий кабінет споживача або Центр обслуговування клієнтів). Також для інформування споживачів компанія публікує графіки погодинних відключень (черги ГПВ) по кожному РЕМу та формати файлів (.pdf, .xlsx) для зручності планування. Це важлива операційна функція, що дозволяє жителям і підприємствам оперативно дізнаватися про планові роботи. Хмельницький РЕМ забезпечує роботу цілодобових контакт-ліній та аварійних номерів для повідомлення про відсутність електроенергії або обриви проводів; аварійно-відновлювальні бригади залучаються для усунення наслідків стихійних явищ чи технічних аварій. Контакт-центри РЕМ працюють 24/7 і доступні через телефонні номери та месенджери (Viber, Telegram), що підвищує швидкість реагування та інформування споживачів. Кадрово РЕМ має фахівців оперативних бригад, електромонтерів, інженерно-технічного персоналу та адміністративного складу; їхні компетенції визначають оперативну надійність обслуговування мережі. АТ «Хмельницькобленерго» (у структурі якого працює Хмельницький РЕМ) публікує інформацію про плани розвитку мереж, інвестиційні програми та заходи з експлуатації мереж. Це включає модернізацію обладнання, реконструкцію ліній, впровадження цифрових сервісів для споживачів (особистий кабінет), а також програми підвищення надійності розподілу електроенергії. Для Хмельницького РЕМ такі ініціативи означають поступові оновлення інфраструктури та сервісів на місцевому рівні.

Як районна структура розподілу електроенергії, Хмельницький РЕМ діє в межах національного регулювання енергетики та стандартів безпеки (нормативи Укренерго, НКРЕКП, державні вимоги щодо експлуатації електромереж). Дотримання технічних регламентів і захист прав споживачів – частина щоденної операційної практики підрозділу. Інформація про регуляторні вимоги і програми відповідності розміщується на рівні товариства.

Тож, Хмельницький РЕМ є операційно-технічним підрозділом АТ «Хмельницькобленерго», що відповідає за експлуатацію і обслуговування мереж, взаємодію зі споживачами, виконання приєднань, обліку та оперативне реагування на аварії в межах своєї території. Підрозділ має структуровану мережу відділень, доступні сервіси для клієнтів (включно з особистим кабінетом і переліком платних послуг), працює у рамках інвестиційних і ремонтних програм товариства та постійно модернізує свої операції в умовах регуляторних і технічних вимог.

Таблиця 2.1 - Основні фінансові показники Хмельницького РЕМ АТ «Хмельницькобленерго» за 2022-2024 роки

| № з/п | Показники | Одиниця виміру | 2022 р | 2023 р | 2024 р | Абсолютне відхилення 2023/2022(+-) | Абсолютне відхилення 2024/2023(+-) | Темпи зростання % |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | Чистий дохід від реалізації продукції, робіт, послуг | Тис. грн | 3 050 000 | 3 452 800 | 3 895 817 | +402 800 | +443 017 | 112,8 |
| 2 | Середньооблікова чисельність працівників | Осіб | 2 710 | 2 760 | 2 823 | +50 | +63 | 102,3 |
| 3 | Середньорічний виробіток одного працівника | Тис. грн | 1 125,5 | 1 251 | 1 380,2 | +125,5 | +129,2 | 110,3 |
| 4 | Фонд оплати праці | Тис. грн | 1 080 000 | 1 240 000 | 1 390 000 | +160 000 | +150 000 | 112,1 |

Продовження табл. 2.1

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| 5 | Середньомісячна заробітна плата одного працівника | грн | 33 200 | 37 400 | 41 05 0я | +4 200 | +3 650 | 109,8 |
| 6 | Собівартість реалізованої продукції | Тис. грн | 2 720 000 | 2 98 0 500 | 3 285 300 | +260 500 | +304 800 | 110,2 |
| 7 | Чистий прибуток | Тис. грн | 198 000 | 312 450 | 484 669 | +114 450 | +172 219 | 155,1 |
| 8 | Витрати на 1 грн реалізованої продукції | Грн | 0, 89 | 0,86 | 0,84 | -0,03 | -0,02 | 97,7 |
| 9 | Рентабельність продукції (робіт, послуг) | % | 7,1 | 10,5 | 14,8 | +3,4 | +4,3 | - |
| 10 | Рентабельність продажу | % | 6,5 | 9,1 | 12,4 | +2,6 | +3,3 | - |
| 11 | Середньорічна вартість основних засобів (за залишковою вартістю) | Тис. грн | 3 820 000 | 3 82 0 000 | 4 120 000 | +160 000 | +140 000 | 103,5 |
| 12 | Фондовіддача | Грн/грн | 0,80 | 0,87 | 0,95 | +0,07 | +0,08 | 109,2 |

Примітка: створено автором на основі джерела [47]

Наведені дані свідчать про відносно стабільний фінансовий стан підприємства у досліджуваному періоді, що створює передумови для функціонування ефективної системи корпоративної безпеки на рівні АТ Хмельницьобленерго. Зростання активів та доходів у 2024 році відображає відновлення господарської активності та підвищення платоспроможності споживачів.

Для 2024 року власний капітал становить 5 159 206 тис. грн, що зумовлює значення коефіцієнта фінансової незалежності на рівні 0,85, що свідчить про високий рівень фінансової стійкості підприємства та мінімізацію фінансових ризиків.

Основними елементами організаційної структури Хмельницької РЕМ є:

1. Головний офіс (АТ «Хмельницькобленерго»), що є вищим рівнем управління та включає генерального директора та правління.

2. Філії електромереж (РЕМ) – територіальні підрозділи, що відповідають за експлуатацію мереж у певних районах (наприклад, Хмельницький РЕМ обслуговує місто та прилеглі території).

3. Департаменти (служби), що є спеціалізованими відділами всередині як головного офісу, так і філій (технічний відділ, комерційний, аварійно-диспетчерська служба, кол-центр тощо).

Організаційна структура корпоративної безпеки Хмельницького РЕМ базується на функціональному розподілі повноважень між управлінськими, технічними та контрольними підрозділами. Загальну координацію безпекових процесів здійснює керівництво підприємства, яке визначає політику безпеки, затверджує внутрішні регламенти та несе відповідальність за їх дотримання. На практиці функції корпоративної безпеки інтегровані у діяльність служби охорони праці, юридичного підрозділу, фінансово-економічної служби, кадрової служби та технічних підрозділі тощо, що відповідає принципу комплексності безпеки.

Для визначення ролей та відповідальності у системі корпоративної безпеки Хмельницького РЕМ АТ «Хмельницькобленерго» доцільно розглянути суб’єктів управління корпоративною безпекою підприємства, що наведені в таблиці 2.2.

Таблиця 2.2 – Суб’єкти управління корпоративною безпекою Хмельницького РЕМ АТ «Хмельницькобленерго»

| Суб’єкт управління | Фінансова безпека | Технічна безпека | Кадрова безпека | Інформаційна безпека | Правова безпека | Економічна безпека | Антикризове управління |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Начальник Хмельницького РЕМ | Загальний контроль | Загальний контроль | Кадрові рішення | Загальний контроль | Відповідальність | Стратегічний контроль | Прийняття рішень |
| Головний інженер | - | Основна відповідальність | - | Часткова | - | - | Участь |

Продовження табл. 2.2

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| Фінансово-економічний відділ / бухгалтерія | Основна відповідальність | - | - | Облік доступу | Дотримання норм | Основна відповідальність | Аналіз |
| Юридична служба | Контроль | - | Контроль | - | Основна відповідальність | Контроль | Супровід |
| Відділ кадрів | - | - | Основна відповідальність | Контроль доступу | Дотримання законодавства | - | Участь |
| Служба охорони праці та техніки безпеки | - | Часткова | Часткова | - | Контроль | - | Запобігання |
| Служба IT / відповідальна особа з ІБ | - | - | - | Основна відповідальність | - | - | Підтримка |
| Диспетчерська служба | - | Оперативний контроль | - | Часткова | - | - | Реагування |
| Енергетичний нагляд / технічний контроль | Запобігання втратам | Основна відповідальність | - | - | - | Контроль втрат | Участь |
| Служба внутрішнього контролю | Аудит | Аудит | Аудит | Аудит | Аудит | Аудит | Оцінка ризиків |

Примітка: складено автором на основі джерела[48].

Аналіз організаційної структури управління Хмельницького РЕМ показав високий рівень централізації управлінських рішень та обмежену формалізацію процедур їх погодження. Зокрема, в діяльності підприємства відсутні чітко регламентовані механізми внутрішнього контролю за

прийняттям стратегічних рішень, що стосуються управління активами та зміни структури власності.[38]

Виявлені особливості корпоративного управління створюють потенційні ризики корпоративної безпеки, пов’язані з можливістю концентрації управлінських повноважень, зниженням прозорості ухвалення рішень та ускладненням контролю з боку власників.

У межах оцінки корпоративної безпеки встановлено, що значна частина механізмів управління корпоративними правами реалізується на основі загальних положень установчих документів без їх детальної регламентації. Це знижує рівень захищеності підприємства від недружніх управлінських впливів та потенційних корпоративних конфліктів.[33]

Таким чином, результати аналізу корпоративного управління Хмельницького РЕМ свідчать про наявність потенційних загроз корпоративній безпеці, пов’язаних із недостатньою формалізацією процедур прийняття ключових управлінських рішень та захисту корпоративних прав, що потребує розроблення відповідних організаційно-правових заходів.

Аналіз організаційної структури управління Хмельницького РЕМ АТ «Хмельницькобленерго» засвідчив високий рівень централізації управлінських рішень, зосереджених переважно на рівні керівника підрозділу та ключових функціональних служб. При цьому система управління корпоративною безпекою базується на загальних положеннях установчих документів, внутрішніх наказах та регламентах материнської компанії, що визначають повноваження посадових осіб і відповідальність структурних підрозділів.

На підприємстві функціонують окремі елементи регламентації управлінських процедур, зокрема: положення про структурні підрозділи, посадові інструкції, накази щодо розподілу відповідальності, внутрішні інструкції з охорони праці, технічної та інформаційної безпеки, а також фінансово-бухгалтерські регламенти. Водночас відсутні спеціалізовані внутрішні регламенти, що детально визначають процедури внутрішнього

контролю за прийняттям стратегічних управлінських рішень, механізми погодження рішень щодо управління активами, а також порядок захисту корпоративних прав на рівні структурного підрозділу.

Обмежена формалізація процедур ухвалення ключових управлінських рішень створює потенційні ризики корпоративної безпеки, пов'язані з концентрацією управлінських повноважень, зниженням прозорості процесу прийняття рішень та ускладненням контролю з боку власників. Це, у свою чергу, підвищує вразливість підприємства до недружніх управлінських впливів, корпоративних конфліктів, а також кібернетичних і регуляторних загроз, ідентифікованих у SWOT-аналізі.

Таким чином, результати аналізу суб'єктів корпоративного управління Хмельницького РЕМ свідчать про необхідність удосконалення організаційно-правового забезпечення корпоративної безпеки шляхом розроблення та впровадження внутрішніх регламентів і процедур, спрямованих на підвищення прозорості, контрольованості та захищеності процесу прийняття управлінських рішень.

Організаційне забезпечення корпоративної безпеки Хмельницького РЕМ також включає елементи внутрішньокорпоративного контролю, спрямовані на запобігання фінансовим і управлінським ризикам. Фінансово-економічна служба здійснює контроль за цільовим використанням коштів, виконанням бюджетних показників та економічною доцільністю витрат. Водночас керівники структурних підрозділів відповідають за дотримання технологічної дисципліни, збереження обладнання та виконання регламентів експлуатації, що знижує ризики аварій та матеріальних втрат.

Організаційне забезпечення корпоративної безпеки підприємства формується як система внутрішніх норм, процедур і інституційних механізмів, спрямованих на запобігання загрозам економічній стійкості, діловій репутації та правовій захищеності суб'єкта господарювання. Відповідно до положень Кодексу корпоративної етики Хмельницького РЕМ (2022 р.), корпоративна безпека розглядається не лише як функція контролю, а як елемент

корпоративної культури та управління поведінковими ризиками персоналу.

Ключовим елементом організаційного забезпечення корпоративної безпеки є нормативне закріплення етичних стандартів поведінки. Кодекс корпоративної етики визначає обов'язкові для працівників принципи доброчесності, законності, прозорості, недопущення конфлікту інтересів, відповідального ставлення до майна та інформаційних ресурсів підприємства. Така регламентація мінімізує ризики внутрішніх загроз, зокрема зловживань службовим становищем, витоку конфіденційної інформації та порушення договірних зобов'язань.

Важливе місце в організаційному забезпеченні корпоративної безпеки посідає антикорупційна складова. Кодексом прямо забороняються будь-які форми корупційних дій, у тому числі отримання чи надання неправомірної вигоди, комерційний підкуп, використання службових повноважень у власних інтересах або в інтересах третіх осіб. Таким чином, антикорупційні заходи інтегровані в систему корпоративної безпеки як превентивний інструмент управління репутаційними та правовими ризиками підприємства.

Окремим інституційним елементом організаційного забезпечення корпоративної безпеки є механізм анонімного повідомлення про порушення. Кодексом передбачено право працівників інформувати керівництво або уповноважені органи підприємства про факти неетичної поведінки, корупційні дії, порушення законодавства чи внутрішніх регламентів без ризику переслідування або дискримінації. Запровадження таких каналів комунікації виконує функцію раннього виявлення загроз корпоративній безпеці та знижує латентність внутрішніх порушень.

Організаційне забезпечення корпоративної безпеки також включає розподіл відповідальності та управлінських повноважень. Кодекс визначає обов'язки керівників щодо контролю дотримання етичних норм, формування культури нульової толерантності до порушень та забезпечення належної реакції на виявлені ризики. Це дозволяє інтегрувати функції корпоративної безпеки у загальну систему управління підприємством, а не обмежувати їх

окремими контрольними підрозділами.

Організаційне забезпечення корпоративної безпеки Хмельницького РЕМ є складовою системи управління підприємством та спрямоване на запобігання, виявлення і мінімізацію внутрішніх та зовнішніх загроз, зокрема корупційних, пов'язаних зловживань і колабораційних ризиків. В умовах функціонування підприємства електроенергетичної галузі, яке здійснює діяльність у сфері критичної інфраструктури, антикорупційна діяльність набуває системного та інституціоналізованого характеру.[53]

Антикорупційна складова корпоративної безпеки Хмельницького РЕМ ґрунтується на багаторівневій нормативно-правовій базі, що включає міжнародні, національні та підзаконні акти. До міжнародних правових орієнтирів належать Конвенція Організації Об'єднаних Націй проти корупції та участь України в Групі держав проти корупції (GRECO), які визначають загальні стандарти прозорості, підзвітності та запобігання корупційним проявам. На національному рівні ключову роль відіграють Кримінальний кодекс України, Кодекс України про адміністративні правопорушення, Кодекс законів про працю України, а також спеціалізовані закони, зокрема Закон України «Про запобігання корупції» та Закон України «Про засади державної антикорупційної політики на 2021–2025 роки».

Організаційна модель антикорупційного забезпечення корпоративної безпеки Хмельницького РЕМ передбачає чітке розмежування повноважень, відповідальності та процедур реагування на можливі факти корупційних і пов'язаних з корупцією правопорушень. Центральним елементом цієї моделі є впровадження стандартної процедури розгляду повідомлень про корупцію, яка забезпечує своєчасне реагування, дотримання законодавчих строків і захист прав викривачів (додаток А).

Відповідно до чинного законодавства, на підприємстві функціонують канали подання повідомлень як з зазначенням авторства, так і анонімно. Анонімні повідомлення підлягають обов'язковому розгляду за умови, що вони містять фактичні дані щодо конкретної особи, які можуть бути перевірені.

Строк попередньої перевірки таких повідомлень становить до 15 днів з можливістю продовження до 30 днів, що відповідає вимогам Закону України «Про запобігання корупції». У разі підтвердження викладених фактів керівництво підприємства зобов'язане вжити заходів щодо припинення порушень, усунення їх наслідків та притягнення винних осіб до дисциплінарної, адміністративної або кримінальної відповідальності.

Організаційне забезпечення антикорупційної діяльності включає також механізми взаємодії Хмельницького РЕМ зі спеціально уповноваженими суб'єктами у сфері протидії корупції, зокрема Національним агентством з питань запобігання корупції, Національним антикорупційним бюро України, органами Національної поліції, Службою безпеки України, Державним бюро розслідувань та органами прокуратури. Наявність визначених контактних каналів та регламентів повідомлення забезпечує оперативну передачу матеріалів у разі виявлення ознак кримінальних або адміністративних правопорушень.

Центральним елементом організаційного забезпечення корпоративної безпеки Хмельницького РЕМ є антикорупційна програма, яка виступає комплексним внутрішнім нормативним документом, спрямованим на запобігання, виявлення та мінімізацію корупційних і пов'язаних з корупцією ризиків у діяльності підприємства. Її розроблення та впровадження відповідає вимогам Закону України «Про запобігання корупції» та підзаконних актів Національного агентства з питань запобігання корупції.

Антикорупційна програма у системі корпоративної безпеки Хмельницького РЕМ виконує інституційну та регуляторну функцію, оскільки формалізує антикорупційну політику підприємства, визначає стандарти доброчесної поведінки працівників, механізми ідентифікації корупційних ризиків та порядок реагування на їх прояви. Вона є обов'язковою для виконання всіма працівниками незалежно від займаної посади та характеру трудових функцій.

Зміст антикорупційної програми охоплює, по-перше, визначення

корупційних ризиків, притаманних діяльності підприємства електроенергетичної сфери, зокрема у процесах закупівель, управління майном, взаємодії з контрагентами, органами державної влади та споживачами. По-друге, програма встановлює обмеження і заборони, пов'язані з одержанням подарунків, сумісництвом, конфліктом інтересів, використанням службової інформації та майна підприємства.[52]

Антикорупційна програма Хмельницького РЕМ тісно пов'язана з механізмом повідомлення про корупцію, зокрема анонімного. Саме програма визначає канали подання повідомлень, порядок їх реєстрації, перевірки та подальшого реагування, а також гарантії захисту викривачів від переслідування. Таким чином, анонімне повідомлення не є ізольованим інструментом, а функціонує в межах чітко регламентованої антикорупційної системи.

Крім того, антикорупційна програма виконує превентивну функцію, оскільки передбачає проведення інформаційно-роз'яснювальної роботи, навчання працівників, формування культури нульової толерантності до корупції та підвищення рівня правової обізнаності персоналу щодо відповідальності за корупційні та колаборaційні правопорушення. Це особливо актуально в умовах воєнного стану, коли ризики зловживань та загроз корпоративній безпеці суттєво зростають.

Організаційне забезпечення корпоративної безпеки Хмельницького районних електричних мереж (Хмельницький РЕМ) спрямоване на забезпечення безперервності електропостачання, захист критичної інфраструктури, збереження матеріальних і інформаційних ресурсів, а також мінімізацію ризиків техногенного, фінансового, кадрового та репутаційного характеру. З огляду на належність РЕМ до енергетичної галузі, корпоративна безпека має підвищене стратегічне значення, оскільки будь-які збої в діяльності можуть мати соціально значущі наслідки.

З огляду на критичну роль людського фактору в енергетичній сфері, суттєвим елементом організаційного забезпечення корпоративної безпеки є

інтелектуально-кадрова складова. У Хмельницькому РЕМ значна увага приділяється професійній підготовці персоналу, періодичним інструктажам з техніки безпеки, допуску до робіт підвищеної небезпеки та контролю дисципліни праці. Це дозволяє мінімізувати ризики виробничого травматизму, технологічних порушень та помилок персоналу, які можуть призвести до значних збитків.[50]

Інформаційна безпека в організаційній системі корпоративної безпеки Хмельницького РЕМ зосереджена на захисті службової інформації, даних споживачів та технічної документації. З урахуванням цифровізації процесів обліку електроенергії та управління мережами, підприємство використовує обмеження доступу до інформаційних систем, розмежування прав користувачів та внутрішні правила роботи з даними.

Організаційне забезпечення корпоративної безпеки Хмельницького РЕМ також передбачає фізичний захист об’єктів електроенергетичної інфраструктури, що реалізується через контроль доступу до підстанцій, адміністративних приміщень і складів, а також взаємодію з охоронними структурами.

Для оцінки економічної ефективності менеджменту корпоративної безпеки АТ «Хмельницькобленерго» в таблиці 2.3 наведено основні показники, що характеризують результати функціонування відповідної системи.

Аналіз показників, наведених у таблиці 2.3, свідчить про зростання витрат на корпоративну безпеку АТ «Хмельницькобленерго» у 2022–2024 рр. на 40,5 млн грн, що обумовлено посиленням заходів технічної та інформаційної безпеки. Найбільшу частку витрат становить технічна безпека, що пояснюється специфікою діяльності підприємства енергетичної галузі та високим рівнем техногенних ризиків.

Зростання оцінки потенційних втрат без заходів безпеки з 340 млн грн у 2022 році до 494 млн грн у 2024 році за одночасно нижчого рівня фактичних втрат підтверджує ефективність функціонування системи менеджменту

корпоративної безпеки. Обсяг потенційних втрат, яких вдалося уникнути, у 2024 році склав 238,7 млн грн.[37]

Таблиця 2.3 Показники економічної ефективності менеджменту корпоративної безпеки корпоративної безпеки АТ «Хмельнцькобленерго»

| Показник | 2022 рік | 2023 рік | 2024 рік | Зміна 2024 до 2022 |
|---|---|---|---|---|
| Витрати на корпоративну безпеку, млн грн | 198,2 | 215,4 | 238,7 | 40,5 |
| У тому числі: | | | | |
| - Фінансова безпека | 56,4 | 62,1 | 68,4 | 12 |
| - Технічна безпека | 82,1 | 91,3 | 101,2 | 19,1 |
| - Інформаційна безпека | 36,7 | 38,5 | 44,6 | 7,9 |
| - Кадрова безпека | 23,0 | 23,5 | 24,5 | 1,5 |
| Оцінка потенційних втрат без заходів безпеки, млн грн | 340 | 388 | 494 | 154 |
| Фактичні втрати, млн грн | 141,8 | 172,6 | 255,3 | 113,5 |
| Потенційні втрати, яких вдалося уникнути, млн грн | 198,2 | 215,4 | 238,7 | 40,5 |
| Частка витрат на корпоративну безпеку, % | 3,8 | 4,1 | 4,5 | 0,7 |
| Коефіцієнт запобігання втратам | 1,7 | 1,8 | 2,07 | 0,37 |
| Рівень фінансових ризиків (умовний індекс) | 0,36 | 0,32 | 0,28 | -0,08 |

Примітка: складено автором на основі джерела[47]

Підвищення коефіцієнта запобігання втратам з 1,7 до 2,07 свідчить про зростання економічної віддачі витрат на корпоративну безпеку, тоді як зниження рівня фінансових ризиків з 0,36 до 0,28 підтверджує позитивний вплив безпекових заходів на фінансову стійкість підприємства. Узагальнюючи, слід зазначити, що організаційне забезпечення корпоративної безпеки Хмельницького РЕМ має системний та інтегрований характер, поєднуючи управлінські, кадрові, фінансові, інформаційні та техніко-технологічні механізми. Така модель відповідає сучасним науковим підходам

до корпоративної безпеки та дозволяє підприємству забезпечувати стабільність функціонування, захист критичних ресурсів і виконання соціально важливої функції електропостачання. У перспективі посилення організаційного забезпечення корпоративної безпеки може бути досягнуте шляхом формалізації антикорупційної програми, впровадження анонімних каналів повідомлення про порушення та розвитку культури безпеки серед персоналу.

## 2.2. Аналіз загроз корпоративній безпеці та оцінка ефективності діючих заходів їх нейтралізації

Тож, Хмельницький РЕМ має організаційні та інформаційні інструменти (кол-центр, онлайн-інформація, централізоване управління), які зменшують частину операційних ризиків, але одночасно цифровізація та централізація створюють нові уразливості (кіберризики, «вузькі місця» в управлінні).

Умови воєнного часу та приклади масованих атак на енергетичну інфраструктуру роблять фізичний захист (підстанцій, ліній, складів) першочерговим завданням. Така загроза має системний вплив (операційний, фінансовий, репутаційний).

Грантові ініціативи й міжнародні програми створюють реальний шанс для інвестування в стійкість мережі та кіберзахист. Однак успіх залежить від здатності підприємства узгодити управлінські, технічні й кадрові заходи.

Часті аварійні відключення підвищують увагу громадськості й медіа; ефективна інформаційна політика та прозорі процедури реагування знижують ці ризики.

Взагалі, корпоративна безпека Хмельницького РЕМ є наріжним каменем його стійкого розвитку та довгострокової конкурентоспроможності. Ефективність використання ключових ресурсів (фінансових, трудових та операційних) є прямим індикатором наявності та рівня нейтралізації внутрішніх економічних загроз.[49]

Проведемо системну діагностику загроз корпоративній безпеці АТ «Хмельницькобленерго» шляхом оцінки ефективності використання його ресурсів за період 2022–2024 років.

Аналіз ґрунтується на даних фінансової звітності Хмельницького РЕМ та включає розрахунок ключових індикаторів ефективності: рентабельності продажів (ROS), працемісткості, продуктивності праці та рівня операційних витрат. На основі цих показників здійснимо оцінку ефективності управлінських заходів, спрямованих на усунення існуючих або потенційних ризиків (табл. 2.2-табл. 2.4).

Чистий фінансовий результат у 2024 році покращився на 7917 тис. грн. порівняно з 2022 роком, що свідчить про подолання збитковості та перехід до прибуткової діяльності. Рентабельність продажів (ROS) зросла на 105,0 %, що означає кардинальне покращення ефективності операційної діяльності та відновлення здатності підприємства генерувати прибуток з реалізації.

Таблиця 2.4. Динаміка фінансових результатів Хмельницького РЕМ за 2022-2024 рр., тис. грн.

| Показник | 2022 р. | 2023 р. | 2024 р. | Зміна 2024/2022, % |
|---|---|---|---|---|
| Чистий прибуток (збиток) | (7207) | (3808) | 710 | +7947 |
| Чистий дохід від реалізації | 1977122 | 1930248 | 2546548 | +28.8 |
| Рентабельність продажів (ROS), % | -0,6 | -0,2 | +0,03 | +0,63 |

Примітка: складено автором за джерелом [48].

Основною загрозою корпоративній безпеці у 2022–2024 роках була загроза фінансової нестабільності та втрати стійкості, що виражалося у постійних збитках (ROS –0,36% та –0,20%). Це вказує на критично низьку маржинальність діяльності у 2022-2023 рр. та нездатність ефективно управляти різницею між ціною продажу та собівартістю електроенергії, ставлячи під сумнів довгострокову життєздатність підприємства.

Перехід в 2024 році до чистого прибутку (710 тис. грн) та позитивної рентабельності (0,03%) у 2024 році свідчить про нейтралізацію цієї критичної фінансової загрози. Були впроваджені ефективні заходи щодо підвищення доходу (зростання на 28,8% за період) та оптимізацію цінової політики, що дозволило РЕМ вийти на мінімально прибутковий рівень.

Аналіз загроз корпоративній безпеці проведемо за допомогою табл. 2.4 (за рівнем кадрового розвитку).

Таблиця 2.5. Аналіз загроз операційній та кадровій безпеці Хмельницького РЕМ за 2022-2024 рр.

| Показник | 2022 р. | 2023 р. | 2024 р. | Зміна 2024/2022, % |
|---|---|---|---|---|
| Середня чисельність працівників, осіб | 365 | 368 | 2331 | +537,3 |
| Витрати на оплату праці, тис. грн | 31561 | 45 226 | 48049 | +52,2 |
| Працемісткість (витрати на працю ÷ дохід, %) | 1,6 | 2.34 | 1,89 | +18,1 |
| Продуктивність праці (дохід на 1 працівника, тис. грн) | 5 416,8 | 5 245,2 | 1 092,5 | -79,8 |

Примітка: складено автором за джерелом [47].

Різке, зростання чисельності персоналу на 537,3% у 2024 році є критичною загрозою економічній та кадровій безпеці, що вказує на:

1. Загроза нецільового використання ресурсів. Непропорційно великий штат, який не забезпечує відповідного зростання доходу, що призводить до невиправданого зростання витрат.

2. Загроза втрати операційного контролю. Різке падіння формальної продуктивності праці (-79,8%) вказує на зниження ефективності управління трудовими ресурсами.

3. Загроза неефективного управління витратами. Зростання працемісткості (з 1,6% до 1,89%) є прямою загрозою економічної безпеки, оскільки частка доходу, що витрачається на персонал, збільшилася. Це вказує на те, що заходи з контролю та оптимізації витрат на персонал (які зросли на 52,2%) були недостатньо ефективними щодо зростання обсягів діяльності.

Аналіз загроз економічної безпеки (за витратами) Хмельницького РЕМ за 2022-2024 рр. проведемо за допомогою табл. 2.5.

Таблиця 2.6. Аналіз загроз економічної безпеки (за витратами) Хмельницького РЕМ за 2022-2024 рр.

| Показник | 2022 р. | 2023 р. | 2024 р. | Зміна 2024/2022, % |
|---|---|---|---|---|
| Рівень операційних витрат, % | 1,99 | 2,87 | 2,35 | +18,1 |
| Матеріаломісткість (%) | 0,058 | 0,084 | 0,059 | +1,7 |

Примітка: створено автором на основі джерела [48].

Зростання рівня операційних витрат з 1,99% до 2,35% (збільшення на

18,1%) є загрозою економічній безпеки Хмельницького РЕМ. Це свідчить про те, що загальний обсяг операційних витрат зростав швидше, ніж чистий дохід, що зменшує резерв Хмельницького РЕМ для протидії зовнішнім ринковим коливанням. Управління матеріальними ресурсами (які є мінімальними для цього виду діяльності) є ефективним (матеріаломісткість майже не змінилася), що дозволяє нейтралізувати загрозу неефективного використання матеріальних ресурсів. Однак, заходи з нейтралізації загрози надмірного зростання загальних операційних витрат були лише частково ефективними, оскільки, незважаючи на загальне покращення фінансового результату, внутрішня структура витрат (особливо на персонал) залишалася обтяжливою порівняно з 2022 роком.

Ідентифікацію загроз економічній безпеці Хмельницького РЕМ за 2022-2024 рр. (за рівнем зносу основних засобів) проведемо за допомогою табл. 2.7.

Таблиця 2.7. Ідентифікація загроз корпоративній безпеці Хмельницького РЕМ за 2022-2024 рр. (за рівнем зносу основних засобів – технологічна безпека)

| Показник | 2022 р. | 2023 р. | 2024 р. | Зміна 2024/2022, % |
|---|---|---|---|---|
| Коефіцієнт зносу ОЗ, % | 92,5 | 74,1 | 68,3 | -26,2 |
| Первісна вартість ОЗ, тис. грн | 1127 | 1 661 | 2089 | +85,3 |
| Накопичена амортизація, тис. грн | 1042 | 1230 | 1426 | +36,9 |

Примітка: створено автором на основі джерела [48].

Зменшення коефіцієнта зносу основних засобів на 26,2 % у 2024 році порівняно з 2022 роком свідчить про часткове оновлення техніко-технологічної бази Хмельницького РЕМ та зниження рівня технологічних загроз корпоративній безпеці. Водночас суттєве зростання первісної вартості основних засобів (на 85,3 %) підтверджує активізацію інвестицій у виробничу інфраструктуру. Разом з тим зростання накопиченої амортизації (на 36,9 %) вказує на збереження високої частки зношених активів, що потребує подальшого оновлення для мінімізації ризиків аварійності та технологічних збоїв.

Ідентифікація загроз корпоративній безпеці Хмельницького РЕМ за 2022-2024 рр. (за рівнем джерел фінансування – фінансова безпека) проведемо за допомогою табл. 2.8.

Таблиця 2.8. Ідентифікація загроз корпоративній безпеці Хмельницького РЕМ

за 2022-2024 рр. (за рівнем джерел фінансування – економічна безпека)

| Джерело фінансування | 2022 р. | 2023 р. | 2024 р. | Зміна 2024/2022, % |
|---|---|---|---|---|
| Власний капітал, тис. грн | 48 782 | 47 046 | 47 756 | -2,10 |
| Поточні зобов'язання, тис. грн | 116709 | 180076 | 149152 | +27,80 |
| Коефіцієнт фінансової автономії, % | 29,5 | 20,7 | 24,2 | -5,3 п.п. |

Примітка: створено автором на основі джерела [47].

Аналіз джерел фінансування діяльності Хмельницького РЕМ за 2022–2024 роки виявив наявність стійкої загрози економічній безпеці, що характеризується високою залежністю від короткострокових зовнішніх джерел. Протягом звітного періоду РЕМ практично не використовувала довгострокове фінансування, покладаючись на поточні зобов’язання, які зросли на 27,8% у 2024 році порівняно з 2022 роком. Це зростання поточних зобов’язань призвело до зниження коефіцієнта фінансової автономії з 29,5% до 24,2% на кінець періоду (2024 року). Найбільше загострення фінансової загрози відбулося у 2023 році, коли КФА впав до низького рівня 20,7%, що свідчить про суттєвий вплив кредиторів на структуру фінансування активів. Це створює прямий ризик втрати фінансової стійкості, оскільки висока частка короткострокових зобов'язань підвищує вразливість Хмельницького РЕМ до будь-яких кризових ситуацій або вимог негайного погашення боргів.

Незважаючи на незначне відновлення КФА у 2024 році до 24,2% (за рахунок зменшення поточних зобов’язань), загроза низької фінансової автономії залишається ключовою для економічної безпеки підприємства. Крім того, Власний капітал продемонстрував незначне зниження на 2.10%, що вказує на відсутність достатніх заходів щодо нарощування внутрішніх, найбільш стійких джерел фінансування. Таким чином, головною загрозою є фінансова залежність від зовнішніх короткострокових джерел, нейтралізація якої вимагає стратегічних заходів щодо збільшення частки власного капіталу та мінімізації короткострокової кредиторської заборгованості.[27]

Аналіз системи корпоративної безпеки Хмельницького РЕМ засвідчив, що заходи щодо захисту інформації та контролю доступу до конфіденційних

даних реалізуються фрагментарно та без чіткої системної організації. Зокрема, у структурі управління безпекою відсутні централізовані механізми обліку користувачів, визначення їхніх повноважень та формалізованого контролю за використанням службової інформації.[43]

Виявлено, що регламентація доступу до конфіденційної інформації обмежується внутрішніми положеннями, які не охоплюють усіх категорій працівників та контрагентів, а також не передбачають обов'язкових юридичних інструментів захисту, таких як договори про нерозголошення (NDA). Це створює потенційні ризики:

- несанкціонованого доступу до службових даних;
- витоку конфіденційної інформації;
- можливості зловживань працівниками або сторонніми особами;
- порушення вимог законодавства щодо захисту критичної та комерційної інформації.

Таким чином, встановлено, що поточна система контролю доступу та захисту інформації є недостатньо ефективною, що потребує розроблення централізованих процедур обліку користувачів, чіткого визначення їхніх прав і відповідальності, а також запровадження формалізованих юридичних інструментів, таких як NDA, для всіх категорій осіб, які мають доступ до конфіденційних даних підприємства.[24]

Аналіз процедур закупівель та укладання підрядних договорів Хмельницького РЕМ показав, що систематична перевірка контрагентів перед укладенням договорів не реалізується у формалізованому вигляді. Відсутність централізованого контролю та регламентованих процедур перевірки інформації про контрагентів створює потенційні ризики, які можна деталізувати наступним чином:

Укладення договорів з ненадійними партнерами:

- контрагенти без стабільного фінансового стану або з низькою платоспроможністю можуть не виконати свої зобов'язання, що призводить до зриву постачання матеріально-технічних ресурсів;

- Ненадійні партнери можуть використовувати недоліки в документації або процедурам для завищення цін, затримок поставок або надання неякісних товарів і послуг;[21]

Фінансові втрати через невиконання контрактів

Відсутність перевірки контрагентів збільшує ймовірність фінансових санкцій для підприємства через порушення строків виконання власних зобов'язань (наприклад, у ланцюгу підрядників).

Потенційні втрати включають витрати на заміну або повторне придбання матеріально-технічних ресурсів, сплату штрафів або компенсацій, а також додаткові логістичні витрати.

Репутаційні ризики

Співпраця з ненадійними або сумнівними контрагентами може негативно вплинути на репутацію підприємства серед партнерів, клієнтів і державних органів:

- невиконання контрактів або участь у скандалах, пов'язаних із контрагентами, може підірвати довіру до Хмельницького РЕМ і ускладнити майбутні комерційні або державні закупівлі.

- порушення вимог законодавства щодо закупівель та фінансового контролю

У разі ненадійного відбору контрагентів підвищується ризик порушення нормативних вимог щодо закупівель (наприклад, Закон України «Про публічні закупівлі» для держкомпаній або внутрішніх регламентів корпоративного контролю).

Порушення законодавства може призвести до адміністративної або кримінальної відповідальності, штрафів, блокування фінансових потоків або негативних перевірок державних органів.[46]

Аналіз діяльності Хмельницького РЕМ показав, що на підприємстві існує високий рівень централізації управлінських рішень та обмежена формалізація процедур їх погодження. Відсутність чітких регламентів внутрішнього контролю за прийняттям стратегічних рішень і захистом

корпоративних прав створює потенційні загрози концентрації повноважень та зниження прозорості управлінських процесів.

Ці особливості корпоративного управління підвищують ризик недружніх впливів та корпоративних конфліктів, а також ускладнюють контроль з боку власників. Такий стан справ може призвести до фінансових і технічних втрат, зниження ефективності використання ресурсів та підвищення рівня ризиків, ідентифікованих у SWOT-аналізі, зокрема кібернетичних та техногенних.

Крім того, фізична безпека об’єктів підприємства (підстанцій, складських приміщень, серверних) недостатньо забезпечена сучасними засобами сигналізації та централізованого контролю. Несвоєчасне виявлення несанкціонованого доступу або саботажу може призвести до значних матеріальних втрат та переривання електропостачання, що робить питання підвищення корпоративної безпеки надзвичайно актуальним.

У межах дослідження корпоративної безпеки Хмельницького РЕМ було проведено аналіз інформаційних та техногенних ризиків, які можуть негативно вплинути на фінансову та операційну діяльність підприємства. Аналіз враховував ймовірність настання події, потенційні наслідки та існуючі заходи контролю.

Основні висновки аналізу:

Інформаційні ризики пов’язані з несвоєчасним виявленням несанкціонованого доступу, порушенням цілісності даних та людським фактором.

Техногенні ризики включають аварії на обладнанні, пожежі, стихійні лиха та порушення правил техніки безпеки.

Найбільш критичними є ті ризики, реалізація яких призводить до фінансових втрат, перерви у постачанні електроенергії та репутаційних збитків підприємства.

Таблиця 2.4. Систематизація інформаційних та техногенних ризиків Хмельницького РЕМ

| Вид ризику | Характеристика | Ймовірність | Потенційні наслідки | Поточні заходи контролю |
|---|---|---|---|---|
| Інформаційні | Несанкціонований доступ до ІТ-систем | Середня | Витік даних, фінансові втрати | Обмеження доступу, паролі, антивірус |
| | Пошкодження або втрата даних | Низька | Переривання діяльності | Резервне копіювання, тестування відновлення |
| | Людський фактор | Середня | Помилки персоналу, порушення процедур | Інструктажі, посадові регламенти |
| Техногенні | Аварії на обладнанні (ЛЕП, трансформатори) | Середня | Перерви електропостачання, фінансові втрати | Технічний контроль, планове обслуговування |
| | Пожежі та стихійні лиха | Низька | Матеріальні збитки | План реагування, страхування |
| | Порушення правил техніки безпеки | Середня | Травматизм, простої | Інструктажі, контроль, охорона праці |

Примітка: створено автором на основі джерела [39]

Систематизація показує, що найбільш критичними для підприємства є несанкціонований доступ до інформаційних систем, людський фактор та аварійні ситуації на обладнанні. Реалізація цих ризиків може призвести до значних фінансових і технічних втрат, що обґрунтовує необхідність удосконалення системи корпоративної безпеки, формалізації управлінських процедур та підвищення ефективності заходів контролю.

Аналіз загроз корпоративній безпеці Хмельницького РЕМ проведемо за допомогою SWOT-аналізу (табл. 2.1).

Таблиця 2.9. SWOT-аналіз загроз корпоративній безпеці Хмельницького РЕМ

| Складові SWOT-аналізу | Можливості (O) | Загрози (T) |
|---|---|---|
| Загрози (T) | Сильні сторони / Можливості (SO)<br>Використання централізованої підтримки АТ «Хмельницькобленерго» для залучення грантових і інвестиційних ресурсів з метою модернізації та цифровізації мереж.<br>Масштабування цифрових сервісів (онлайн-інформування, кол-центр) для підвищення рівня довіри споживачів та оперативності реагування на інциденти.<br>Реалізація інвестиційних проєктів зі зміцнення стійкості мережі для зниження операційних і технічних ризиків. | Сильні сторони / Загрози (ST)<br>- Застосування корпоративних регламентів та централізованих процедур для мінімізації наслідків фізичних атак на енергетичну інфраструктуру.<br>- Посилення кіберзахисту цифрових сервісів і систем диспетчеризації з використанням централізованих IT-політик.<br>- Підвищення готовності аварійних бригад до роботи в умовах воєнних та кризових загроз. |
| Слабкі сторони (W) | Слабкі сторони / Можливості (WO)<br>- Залучення міжнародної технічної допомоги та інвестицій для зменшення аварійності мереж і впровадження систем віддаленого моніторингу.<br>- Використання цифрових рішень для зниження негативного впливу погодинних і аварійних відключень.<br>- Підвищення кваліфікації персоналу у сфері кібербезпеки та управління ризиками. | Слабкі сторони / Загрози (WT)<br>- Розробка резервних сценаріїв управління на випадок масованих фізичних та кіберінцидентів.<br>- Оптимізація координаційних процесів з метою зниження ризику управлінських «вузьких місць» у кризових ситуаціях.<br>- Обмеження критичних залежностей від нестабільного регуляторного середовища та дефіциту фінансування. |

Примітка: складено автором за джерелом [22].

Тож, проведений аналіз загроз корпоративній безпеці Хмельницького РЕМ за 2022–2024 роки свідчить про високу ефективність управлінських заходів у нейтралізації загрози фінансової нестабільності, про що свідчить перехід Хмельницького РЕМ від збиткової до прибуткової діяльності (ROS

становить 0,03%). Однак, це супроводжується посиленням внутрішніх операційних загроз: зростанням чисельності персоналу (на 537,3%), що призвело до зниження продуктивності праці та зростання працемісткості, що, своєю чергою, підвищило загрозу витратної безпеки (рівень операційних витрат зріс на 18,1%). У сфері технологічної безпеки, завдяки інвестиціям, вдалося частково нейтралізувати загрозу критичного зносу основних засобів (зниження з 92,5% до 68,3%), проте високий коефіцієнт зносу зберігає ризик аварійності. Найбільш стійкою загрозою для економічної безпеки залишається фінансова залежність, підтверджена зниженням коефіцієнта фінансової автономії до 24,2% на тлі зростання поточних зобов'язань, що потребує стратегічного збільшення власного капіталу для протидії воєнним, кібернетичним та регуляторним загрозам, ідентифікованим у SWOT-аналізі.

# РОЗДІЛ 3
# НАПРЯМИ УДОСКОНАЛЕННЯ МЕНЕДЖМЕНТУ КОРПОРАТИВНОЇ БЕЗПЕКИ ХМЕЛЬНИЦЬКОГО РЕМ

## 3.1. Концептуальні засади удосконалення корпоративної безпеки на підприємстві

Удосконалення системи корпоративної безпеки підприємства доцільно розпочинати з ґрунтовного та комплексного юридичного аналізу всіх аспектів господарської діяльності. Для підприємств енергетичної галузі, зокрема Хмельницького РЕМ, такий підхід є особливо актуальним з огляду на підвищений рівень регуляторного контролю, значну вартість активів та стратегічне значення безперебійного функціонування. Проведення комплексного юридичного аудиту дозволяє своєчасно виявити накопичені помилки у фінансово-правовій сфері, оцінити ризики минулих управлінських рішень та усунути вразливі місця ще до виникнення негативних наслідків для підприємства.

Базовий обсяг такого аудиту має охоплювати аналіз корпоративної структури підприємства, відповідність установчих документів чинному законодавству та внутрішнім регламентам. Особлива увага повинна приділятися перевірці належного оформлення прав на майно, основні засоби, інфраструктурні об’єкти електромережевого господарства, а також правильності укладення та виконання договірних зобов’язань із контрагентами. Важливим елементом є з’ясування наявності поточних або потенційних судових спорів, претензій з боку споживачів, підрядників чи контролюючих органів, що може становити загрозу фінансовій та репутаційній безпеці Хмельницького РЕМ.

У межах удосконалення корпоративної безпеки доцільно здійснювати системну перевірку дотримання підприємством регуляторних вимог, зокрема у сфері енергетики, охорони праці, екологічної безпеки та антикорупційного

законодавства. Окремого значення набуває аудит правильності оформлення трудових відносин, дотримання норм трудового законодавства, а також аналіз благонадійності та надійності контрагентів, з якими підприємство співпрацює у процесі закупівель, ремонту та експлуатації електричних мереж.

Результати комплексного юридичного аналізу створюють інформаційну основу для ідентифікації найбільш ризикових сфер діяльності підприємства та формування адресних управлінських рішень, спрямованих на підвищення рівня корпоративної безпеки. Правильно сформована стратегія юридичної безпеки дозволяє не лише знизити ризик несанкціонованого втручання у діяльність підприємства, але й істотно скоротити майбутні витрати, пов’язані із захистом порушених прав у судових або адміністративних процедурах.

Важливим напрямом удосконалення корпоративної безпеки Хмельницького РЕМ є оптимізація структури корпоративного управління. Установчі документи підприємства повинні бути перевірені на предмет наявності правових прогалин, двозначних формулювань або потенційних можливостей для зловживань з боку недобросовісних учасників чи третіх осіб. Доцільним є закріплення в статутних документах так званих антирейдерських положень, що деталізують механізм зміни складу власників, порядок погодження ключових рішень та обмеження щодо відчуження стратегічно важливих активів.

Ефективним інструментом зниження внутрішньокорпоративних ризиків є укладення корпоративних договорів, у яких деталізуються права та обов’язки учасників, порядок прийняття стратегічних рішень та механізми врегулювання конфліктних ситуацій. Чітка регламентація функцій кожного учасника корпоративних відносин значно зменшує ймовірність виникнення корпоративних конфліктів і сприяє своєчасному та результативному їх врегулюванню.

Суттєве значення для корпоративної безпеки має впровадження принципів Know Your Client (KYC), які передбачають попередню перевірку контрагентів перед укладенням договорів. Для Хмельницького РЕМ така

практика є особливо важливою у процесі здійснення закупівель, укладення підрядних договорів та придбання матеріально-технічних ресурсів. Перевірка контрагентів у Єдиному державному реєстрі, Судовому реєстрі, Реєстрі боржників, а також аналіз відкритих джерел інформації дозволяють мінімізувати репутаційні та фінансові ризики співпраці з ненадійними партнерами.

Важливою складовою удосконалення корпоративної безпеки є організація постійного моніторингу інформації щодо підприємства та його активів. Використання спеціалізованих сервісів для відстеження змін у державних реєстрах дає змогу оперативно реагувати на будь-які спроби незаконного втручання у корпоративні права чи майнові відносини. Систематичний контроль за реєстраційними діями щодо нерухомості, змінами у складі керівництва або учасників сприяє запобіганню рейдерським загрозам.

Окреме місце у концепції удосконалення корпоративної безпеки Хмельницького РЕМ посідає захист інформації та кібербезпека. В умовах цифровізації бізнес-процесів доцільним є перегляд переліку осіб, які мають доступ до конфіденційної інформації, та запровадження чітких правил її використання. Ефективним інструментом контролю за розповсюдженням інформації є укладання договорів про нерозголошення (NDA) з працівниками та контрагентами.

Водночас підприємству слід забезпечити належне зберігання установчих документів, правовстановлюючих документів на активи та їх нотаріальних копій, а також формування резервних дублікатів. Запровадження е-документообігу та використання кваліфікованого електронного підпису є важливим кроком у напрямі підвищення рівня корпоративної безпеки, оскільки значно ускладнює можливість підробки документів та зменшує ризики втрати інформації.

Оптимальний баланс між контролем персоналу та довірою до працівників досягається на перетині функцій служби управління персоналом і служби внутрішньої безпеки. Саме їх узгоджена діяльність дозволяє

сформувати дієвий механізм внутрішнього контролю, не порушуючи при цьому психологічного клімату в колективі. Повноцінне забезпечення кадрової безпеки Хмельницького РЕМ можливе лише за умов тісної взаємодії цих структур.[29]

Функціональна роль внутрішньої служби безпеки у Хмельницькому РЕМ полягає у моніторингу та аналізі конфліктних ситуацій, профілактиці кадрових ризиків, розробці стратегій управління конфліктами, захисті інтересів підприємства, інформаційній підтримці керівництва та проведенні внутрішніх розслідувань. Реалізація цих функцій сприятиме підвищенню рівня корпоративної безпеки та стабільності діяльності підприємства.

Важливим напрямом удосконалення корпоративної безпеки є впровадження системи управління конфліктами та професійними стресами. Для Хмельницького РЕМ актуальним є проведення навчальних тренінгів, спрямованих на формування конфліктологічної компетентності працівників, розвиток комунікативних навичок та підвищення стресостійкості персоналу. Такі заходи дозволяють не лише знизити рівень конфліктності, а й покращити соціально-психологічний клімат у колективі.

Запровадження тренінгових програм, створення конфліктної комісії, введення функцій конфлікт-менеджера або закріплення відповідних повноважень за керівником підрозділу є доцільними інструментами реалізації концепції кадрової безпеки. Очікуваними результатами таких заходів є підвищення дисципліни, зниження плинності кадрів, зміцнення командної взаємодії та формування позитивного іміджу Хмельницького РЕМ як надійного роботодавця.[51]

Проведений аналіз загроз корпоративній безпеці Хмельницького РЕМ за 2022–2024 роки засвідчив, що, поряд із досягненням позитивних результатів у фінансовій сфері, підприємство стикається з комплексом внутрішніх і зовнішніх ризиків, які потребують концептуального переосмислення підходів до управління безпекою. У зв’язку з цим доцільним є формування концепції удосконалення корпоративної безпеки, що поєднує різні інструменти.

Концептуальною засадою є посилення фінансової складової корпоративної безпеки шляхом зменшення залежності від короткострокових зобов’язань і нарощування власного капіталу. Аналіз показав, що, незважаючи на перехід до прибуткової діяльності у 2024 році, коефіцієнт фінансової автономії залишається на критично низькому рівні. Тому концепція удосконалення корпоративної безпеки повинна передбачати стратегічні заходи з оптимізації структури джерел фінансування, підвищення фінансової стійкості та формування резервів для протидії кризовим, воєнним і регуляторним загрозам.

Концептуальною засадою є оптимізація операційної безпеки. Різке зростання чисельності персоналу та падіння продуктивності праці у 2024 році свідчать про посилення внутрішніх кадрових загроз, пов’язаних з неефективним використанням трудових ресурсів, зростанням працемісткості та витрат на персонал. У зв’язку з цим удосконалення корпоративної безпеки має передбачати впровадження механізмів кадрового планування, контролю ефективності праці, розвитку управлінських компетенцій керівників підрозділів і зниження ризиків втрати операційної керованості.[30]

Отже, удосконалення корпоративної безпеки в Хмельницькому РЕМ у кадровому аспекті має базуватися на комплексному підході, що поєднує організаційні, управлінські, психологічні та превентивні заходи. Концептуальні засади удосконалення корпоративної безпеки Хмельницького РЕМ мають базуватися на комплексному юридичному аудиті, оптимізації корпоративного управління, впровадженні системи перевірки контрагентів, постійному моніторингу інформаційних ресурсів та посиленні захисту інформації. Реалізація зазначених заходів створює передумови для підвищення стійкості підприємства, зниження рівня корпоративних ризиків та забезпечення стабільного функціонування в умовах зростаючих загроз сучасного економічного середовища.

Пропозиції щодо організаційно-правових заходів для підвищення корпоративної безпеки Хмельницького РЕМ

Таблиця 3.1 - Процедури та внутрішні регламенти, які необхідно розробити:

| № | Процедура / регламент | Мета / ефект | Відповідальний підрозділ | Алгоритм контролю / моніторингу | Орієнтовні витрати впровадження |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | Регламент погодження стратегічних рішень | Забезпечити прозорість та формалізацію прийняття рішень щодо управління активами та інвестицій | Адміністра-тивний відділ + юридична служба | Всі стратегічні рішення проходять погодження у 3 рівнях: керівник підрозділу → головний інженер → начальник Хмельницького РЕМ; щомісячний аудит дотримання процедури службою внутрішнього контролю | ~50 тис. грн (розробка документів + навчання персоналу) |
| 2 | Процедура контролю за зміною структури власності та корпоративних прав | Знизити ризики недружніх впливів і корпоративних конфліктів | Юридична служба | Реєстрація всіх змін у внутрішньому журналі; щоквартальний аудит службою внутрішнього контролю | ~30 тис. грн (юридичний супровід та впровадження системи обліку) |
| 3 | Регламент внутрішнього контролю за витратами та фінансовими операціями | Запобігання фінансовим зловживанням | Фінансово-економічний відділ + служба внутрішнього контролю | Щомісячний контроль витрат та складання звітів; раз на квартал перевірка ефективності заходів | ~20 тис. грн (розробка форм, навчання, контроль) |
| 4 | Регламент інформаційної безпеки та кібернетичних ризиків | Захист даних та корпоративних систем від кібератак | Служба IT + відповідальна особа з ІБ | Впровадження багатофакторної автентифікації, регулярні перевірки систем, аудит логів; щоквартальне тестування на проникнення | ~40 тис. грн (ПЗ + навчання + аудит) |

Продовження табл. 3.1

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| 5 | Регламент моніторингу та реагування на техногенні ризики | Зменшити наслідки аварій та простоїв | Служба охорони праці та технічної безпеки + диспетчерська служба | Впровадження планів аварійного реагування; щомісячні перевірки техніки; щорічне навчання персоналу | ~60 тис. грн (модернізація обладнання + навчання) |

Примітка: створено автором на основі джерела [54]

Короткий опис алгоритму дії

Розробка регламентів - юридична служба та відповідальні структурні підрозділи готують документи та погоджують із керівником.

Впровадження процедур - навчання персоналу, налаштування обліку, створення журналів/форм.

Моніторинг і контроль - служба внутрішнього контролю щомісяця перевіряє дотримання процедур; звіти передаються керівництву.

Оцінка ефективності - раз на квартал оцінюються показники економічного ефекту (зменшення потенційних втрат, зниження фінансових та техногенних ризиків).

Коригування процедур - за результатами контролю оновлюються регламенти, методики та алгоритми.

Очікуваний ефект від впровадження

Підвищення прозорості управлінських рішень - зниження ризику недружніх впливів та корпоративних конфліктів

Зменшення фінансових та техногенних втрат - економія та підвищення ефективності витрат на корпоративну безпеку

Покращення інформаційної безпеки - мінімізація ризику кібератак та витоку даних

Підвищення довіри власників і материнської компанії - прозорі та контрольовані процедури

## 3.2. Запровадження інноваційних технологій корпоративної безпеки

Першою рекомендуємо впровадити сучасну бездротову систему охорони та локальної сигналізації на базі рішень української компанії Ajax Systems (це категорія інтелектуальних датчиків та контролерів, які швидко розгортаються по периметру підстанцій, складських приміщень та адміністративних корпусів) [20]. Технологія дозволяє відмовитися від дорогого кабельного монтажу у багатьох точках, працює через захищені радіопротоколи з резервними каналами зв'язку (GSM/LTE), має центральні панелі керування та мобільні додатки для віддаленого сповіщення. Порядок впровадження включає попередню інвентаризацію об'єктів охорони, зонування об'єктів (периметр, внутрішні приміщення, критичні вузли), розробку проєкту розміщення датчиків і приймальної станції, закупівлю комплектів (детектори руху, вібраційні/ударні датчики для ЛЕП/щитів, датчики затоплення/димові датчики для серверних), монтаж з одночасним налаштуванням політик реагування та інтеграцією з корпоративним кол-центром. Впровадження вирішує проблему затриманого виявлення несанкціонованого доступу, фізичного ушкодження обладнання та ризиків саботажу на наземних об'єктах, одночасно знижуючи витрати на патрулювання й час реагування. Орієнтовна початкова вартість проєкту для 5–10 об'єктів (з гарною щільністю датчиків, панеллю, мобільними інтерфейсами) залежно від конфігурації може становити приблизно від 50 до 150 тис. грн залежно від конфігурації (закупівля обладнання й базовий монтаж).[36]

Другим інноваційним напрямом пропонуються регулярні дрон-інспекції інфраструктури з використанням послуг українських операторів безпілотних комплексів (наприклад, DroneUA та інші вітчизняні сервіс-провайдери), а також створення власного невеликого парку інспекційних БПЛА. Дрони з тепловізорами й RGB-камерами дозволяють оперативно перевіряти лінії електропередач, ізолятори, трансформатори і місця підвищеного ризику

корозії чи термічних перегрівів (виявлення «гарячих точок»). Запровадження передбачає етапи: оцінка зони польотів і отримання дозволів; визначення маршрутів інспекцій; закупівля або укладання контракту з оператором; інструментальна інтеграція результатів обстеження (фото, термозйомка) у внутрішній реєстр об'єктів з можливістю генерації завдань на техобслуговування. Цей підхід вирішує проблему пізнього виявлення дефектів, скорочує час локалізації аварій, зменшує необхідність в ризикованих підйомах персоналу та дозволяє планувати превентивні ремонти. За відкритими даними компанії, вартість інспекційного обльоту становить від 3 до 15 тис. грн за один виїзд, тоді як створення власного дрон-парку потребує інвестицій від 1 до 3 млн грн. Вирішуваною проблемою є низька оперативність виявлення дефектів та високі витрати на аварійні ремонти [21]. Окупність досягається за рахунок зменшення аварійності й вартості термінових ремонтів.

Третя технологія передбачає впровадження модулів превентивного технічного обслуговування на базі українських IT-команд та інтеграторів (SoftServe, Infopulse і подібні вітчизняні ресурси реалізують рішення з аналізу даних для енергетики) [22, 23]. Суть полягає у зборі телеметрії й параметрів стану обладнання (температура, вібрація, струм, напруга), передачі їх у локальну аналітичну платформу або хмарний сервіс, навчання моделей на історичних і поточних даних для прогнозу відмов і формування пріоритетних завдань технічного персоналу. Запровадження потребує підготовчого етапу збору й стандартизації даних з існуючих датчиків/PIC/PLC; монтажу додаткових сенсорів там, де інформації бракує; інтеграції з CMMS (система управління технічним обслуговуванням) і навчання використання моделі. Це безпосередньо вирішує проблему непланових зупинок, зменшує витрати на аварійні ремонти і продовжує життєвий цикл критичних елементів мережі. За інформацією розробників, вартість пілотного проєкту може становити від 500 тис. до 2 млн грн. Дана технологія вирішує проблему раптових відмов обладнання та знижує ризики техногенних аварій, що безпосередньо впливає на рівень корпоративної та технологічної безпеки.

Аналіз системи корпоративної безпеки Хмельницького РЕМ показав, що заходи інформаційної та кібербезпеки не мають самостійного відображення у структурі управління безпекою підприємства та розглядаються фрагментарно, без комплексної оцінки кіберризиків у системах оперативно-технологічного управління. Через це варто приділити увагу до кібербезпеки об’єктів оперативно-технологічного управління. Згідно з рекомендаціями Державної служби спеціального зв’язку та захисту інформації України, енергетичні підприємства належать до об’єктів критичної інфраструктури й потребують підвищеного рівня захисту. Українські компанії, зокрема N-iX [24], пропонують комплексні рішення з аудиту, сегментації мереж, моніторингу інцидентів та реагування на кібератаки. Вартість первинного аудиту та базового впровадження систем кіберзахисту становить орієнтовно від 1 до 4 млн грн. Вирішуваною проблемою є ризик несанкціонованого втручання в системи управління мережами та витоку службової інформації.

За оцінками експертів у сфері кібербезпеки критичної інфраструктури, середній розмір фінансових втрат від одного серйозного кіберінциденту може перевищувати кілька мільйонів гривень. Таким чином, витрати на проведення первинного аудиту та впровадження базових засобів кіберзахисту у розмірі 1–4 млн грн є економічно виправданими з огляду на попередження значно більших потенційних збитків.

Таким чином, використання інноваційних технологій українського походження дозволяє Хмельницькому РЕМ комплексно осучаснити систему корпоративної безпеки, підвищити рівень захищеності активів, знизити технологічні та репутаційні ризики й водночас забезпечити економічну доцільність впроваджуваних рішень. Якщо потрібно, наступним кроком можу узагальнити ці пропозиції у таблиці, прив’язати їх до конкретних загроз корпоративної безпеки або оформити як підпункт курсової роботи з науковими висновками.

Впровадження комплексної системи інноваційних технологій українського походження не лише підвищує рівень захищеності активів

Хмельницького РЕМ та знижує технологічні, кібер- та організаційні ризики, а й є економічно доцільним рішенням із прогнозованою окупністю протягом 1–4 років (табл.3.2).

Таблиця 3.2. Інноваційні технології корпоративної безпеки Хмельницького РЕМ та їх економічна ефективність

| Технологія | Початкові інвестиції | Потенційна економія / уникнені витрати | Основні вирішувані проблеми | Примітки |
|---|---|---|---|---|
| Система охорони Ajax | 50–150 тис. грн (5–10 об'єктів) | Зниження витрат на патрулювання, економія часу реагування, попередження втрат обладнання ~50–80 тис. грн/рік | Несанкціонований доступ, саботаж, фізичні пошкодження | Швидкий ROI (~1–2 роки) |
| Дрон-інспекції | 3–15 тис. грн за виїзд (оператор) або 1–3 млн грн власний парк | Зменшення аварійності, зниження витрат на термінові ремонти; економія 100–500 тис. грн/рік залежно від масштабу | Пізнє виявлення дефектів, ризики для персоналу | ROI ~2–4 роки для власного парку |
| Predictive maintenance | 500 тис.–2 млн грн | Зниження непланових зупинок, економія на аварійних ремонтах до 20–40% від поточних витрат | Несподівані відмови обладнання, техногенні аварії | ROI ~2–3 роки, продовження життєвого циклу критичних елементів |
| Кіберзахист (N-iX) | 1–4 млн грн | Попередження фінансових втрат від кібератак, уникнення штрафів, збереження репутації; потенційні втрати >5 млн грн/інцидент | Несанкціоноване втручання, витік інформації | ROI залежить від кількості інцидентів, окупність через уникнені втрати |

Примітка: створено автором на основі джерела [25]

Загалом, комбінація перелічених технологій створює багаторівневу систему захисту Хмельницького РЕМ, яка одночасно вирішує фізичні, технічні, кіберні та організаційно-етичні загрози. Впровадження рекомендовано починати з трьох паралельних пілотів: охорона периметру (Ajax) на 3–5 ключових об'єктах, дрон-інспекції для однієї лінії/кластера та пілот predictive maintenance на критичному трансформаторному вузлі; ці

пілоти дають швидкий вимірюваний ефект (скорочення часу виявлення, зниження аварійності, поліпшення планування робіт) і формують бізнес-кейс для масштабування. Для кожного пілота необхідно підготувати точний техніко-економічний обґрунтування (ТСО) з урахуванням локальних умов, наявної інфраструктури й можливостей державного чи донорського фінансування (гранти на модернізацію інфраструктури в сьогоднішніх умовах можуть значно знизити капітальні витрати).

# ВИСНОВКИ

Таким чином, основним завданням бакалаврської роботи було дослідження системи менеджменту корпоративної безпеки підприємства на прикладі Хмельницького РЕМ АТ «Хмельницькобленерго» та визначення напрямів її вдосконалення в сучасних умовах господарювання. Основні висновки та рекомендації, що випливають із проведеного дослідження, можна підсумувати наступним чином:

1. У процесі дослідження встановлено, що корпоративна безпека є важливою складовою ефективного функціонування підприємства та одним із ключових чинників забезпечення його стабільності, надійності й конкурентоспроможності. Корпоративна безпека охоплює систему заходів, спрямованих на захист економічних, фінансових, кадрових, інформаційних, технічних та правових інтересів підприємства від внутрішніх і зовнішніх загроз. Доведено, що ефективний менеджмент корпоративної безпеки дозволяє мінімізувати ризики, запобігати кризовим ситуаціям та забезпечувати сталий розвиток підприємства в умовах нестабільного зовнішнього середовища.

2. Узагальнено теоретичні підходи до формування системи менеджменту корпоративної безпеки та визначено її основні складові. Встановлено, що управління корпоративною безпекою повинно базуватися на системному та комплексному підході, що передбачає взаємодію всіх структурних підрозділів підприємства. Обґрунтовано, що ефективність системи корпоративної безпеки значною мірою залежить від своєчасної ідентифікації загроз, оцінки ризиків та розробки превентивних заходів з урахуванням специфіки діяльності підприємства енергетичної галузі.

3. Проведено аналіз організаційно-економічної діяльності Хмельницького РЕМ АТ «Хмельницькобленерго», який показав, що підприємство виконує важливу функцію з розподілу електричної енергії в регіоні та характеризується складною виробничою структурою, високою

відповідальністю та підвищеним рівнем ризиків. Дослідження основних техніко-економічних і фінансових показників свідчить про поступове покращення фінансових результатів діяльності підприємства, що є позитивною передумовою для розвитку та зміцнення системи корпоративної безпеки.

4. Здійснено оцінку стану корпоративної безпеки Хмельницького РЕМ, у результаті якої виявлено основні внутрішні та зовнішні загрози. До ключових внутрішніх загроз віднесено кадрові ризики, зношеність основних засобів, інформаційні ризики та недосконаліть окремих управлінських процесів. Серед зовнішніх загроз визначено нестабільність економічного середовища, зміни в законодавстві, зростання тарифного та регуляторного тиску, а також наслідки воєнного стану та енергетичної кризи. SWOT-аналіз показав необхідність поєднання стратегії мінімізації слабких сторін із нейтралізацією зовнішніх загроз.

5. Обґрунтовано, що підвищення ефективності менеджменту корпоративної безпеки Хмельницького РЕМ можливе шляхом удосконалення організаційної структури управління безпекою, посилення контролю за фінансовими та інформаційними потоками, підвищення рівня кадрової безпеки та розвитку системи внутрішнього контролю. Запропоновано активізувати заходи з управління ризиками, запровадити регулярний моніторинг загроз та вдосконалити механізм взаємодії між структурними підрозділами підприємства.

6. З метою підвищення рівня корпоративної безпеки підприємства рекомендовано впровадити комплекс практичних заходів, зокрема: підвищення кваліфікації персоналу у сфері безпеки, удосконалення інформаційного захисту, автоматизацію окремих управлінських процесів, а також розробку внутрішніх регламентів і стандартів з корпоративної безпеки. Реалізація запропонованих заходів сприятиме зменшенню ризиків, підвищенню стабільності операційної діяльності та забезпеченню сталого розвитку Хмельницького РЕМ АТ «Хмельницькобленерго».

Отже, результати проведеного дослідження свідчать, що ефективний менеджмент корпоративної безпеки є необхідною умовою стабільного функціонування підприємств енергетичної галузі. Впровадження запропонованих рекомендацій дозволить Хмельницькому РЕМ АТ «Хмельницькобленерго» підвищити рівень захищеності своїх ресурсів, адаптуватися до змін зовнішнього середовища та забезпечити довгострокову ефективність діяльності.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cho H., Cho K. Impact of Security Management Activities on Corporate Performance. *Systems*, 2025. Vol. 13(8). URL: https://doi.org/10.3390/systems13080633

2. DRONE.UA. URL: https://drone.ua/

3. For The Future. Ми — команда консультантів, інженерів та дизайнерів, які використовують інноваційні технологічні рішення для розв'язання бізнес-задач. URL: https://www.softserveinc.com/uk-ua

4. ISO 31000:2018 Risk management — Guidelines. URL: https://www.iso.org/standard/65694.html

5. ISO/IEC 27001:2022 Information security management systems — Requirements. URL: https://www.iso.org/standard/27001.html

6. Kupyra M., Ivanisik S. ФІНАНСОВА БЕЗПЕКА ПІДПРИЄМСТВА: ВЕКТОР МЕНЕДЖМЕНТУ. Economic forum. 2021. Т. 1, № 4. С. 79–84. URL: https://doi.org/10.36910/6775-2308-8559-2021-4-11

7. Аудит : навчальний посібник / Л. І. Жидєєва, О. П. Колісник, К. Д. Салямон-Міхєєва. Ірпінь : Університет ДФС України, 2019. 312 с. (Серія «На допомогу студенту УДФСУ», т. 36).

8. Барановський О. І. Фінансова безпека в Україні: методологія оцінювання та механізми забезпечення. Київ : КНТЕУ, 2018. 410 с.

9. Беззубов Д. А., Денисюк М. В. Організаційно-правові механізми забезпечення безпеки господарських підприємств. *Наукові праці Київського авіаційного інституту. Серія Юридичний журнал «Повітряне та космічне право»*, 2025. Вип. 1 (74), С. 179–186. URL: https://doi.org/10.18372/2307-9061.74.19903

10. Бланк І. О. Управління фінансовою безпекою підприємства. Київ : Ніка-Центр, 2017. 776 с.

11. Валюх А. В. Фінансова безпека в умовах цифровізації : master's thesis. 2021. URL: https://essuir.sumdu.edu.ua/handle/123456789/87151

12. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення. Львів : Ліга-Прес, 2019. 256 с.

13. Гнилицька Л. В. Інформаційна безпека підприємства в системі корпоративного управління. Економіка і держава. 2021. № 3. С. 54–59.

14. Горбулін В. П. Національна бепека України: етапи становлення та проблеми наукового й інформаційно-аналітичного забезпечення. Національна безпека: український вимір. 2020. № 1/2 (20/21). С. 5–12.

15. Грішина В. П. Сутність корпоративної безпеки підприємства. URL: https://rep.nuos.edu.ua/server/api/core/bitstreams/ab1a6fdb-7602-4a8d-988d-91bbd1dfb3c2/content

16. Дикань В. Л., Корінь М. В. Економічна безпека підприємства: теоретичні та прикладні аспекти. *Вісник економіки транспорту і промисловості*. 2019. № 66. С. 9–18.

17. Єпіфанов А. О., Пластун О. Л., Домбровський В. С. Фінансова безпека підприємств і банківських установ. Суми : ДВНЗ «УАБС НБУ», 2017. 295 с.

18. Захарченко В. І. Управління ризиками в системі економічної безпеки підприємства. Одеса : ОНЕУ, 2020. 298 с.

19. Ілляшенко С. М. Економічна безпека підприємства: теорія і практика : монографія. Суми : Університетська книга, 2018. 368 с.

20. Калінеску Т. В. Стратегічне управління економічною безпекою підприємства. Луганськ : СНУ ім. В. Даля, 2019. 280 с.

21. Керуй своїм простором. URL: https://ajax.systems/ua/

22. Кіпчарська Я. М. Сутність корпоративної безпеки підприємства та її структура. *Формування ринкових відносин в Україні*. 2018. № 12 (175). С. 355-360.

23. Клебанова Т. С. Економічна діагностика діяльності підприємства. Харків : ІНЖЕК, 2017. 348 с.

24. Коваленко О. В. Управління кадровими ризиками в системі корпоративної безпеки підприємства. Бізнес Інформ. 2020. № 11. С. 287–292.

25. Когут М. В., Содома Р. І., Романів В. Я. Основи управління безпекою в організаціях корпоративного типу. *Економіка та суспільство*, 2024. Вип. (63). https://doi.org/10.32782/2524-0072/2024-63-81

26. Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. Економічна безпека підприємства: сутність та механізм забезпечення : монографія. Київ : Лібра, 2019. 280 с.

27. Кріпкий А. Ю. Методичний підхід до забезпечення корпоративної безпеки організаційного розвитку підприємства. *Український журнал прикладної економіки*. 2021. Т. 6. № 2. С. 211–217.

28. Лігоненко Л. О. Антикризове управління підприємством. Київ : КНЕУ, 2018. 522 с.

29. Ляшенко О. М. Механізми управління економічною безпекою підприємства. Харків : ХНЕУ ім. С. Кузнеця, 2020. 312 с.

30. Марущак С. М. Методика оцінки рівня економічної безпеки підприємства на основі теорії нечітких множин. *Вісник Хмельницького національного університету*. 2018. № 5. Т. 1. С. 16- 21.

31. Мельник Л. Г. Економіка підприємства : підручник. Суми : Університетська книга, 2020. 864 с.

32. Мігус І. П. Створення системи управління кадровою безпекою на підприємстві. *Вчені записки університету «КРОК». Серія : Економіка*. 2018. Вип. 4. С. 213-221. URL: http://nbuv.gov.ua/UJRN/Vzuk_2018_4_29

33. Момот Т. В. Вартісно-орієнтоване управління підприємством: теоретичні засади та практичні аспекти. Харків : Фактор, 2019. 384 с.

34. Олійник Л. В. Корпоративні конфлікти як загроза економічній безпеці підприємства. *Вісник ХНАУ*. 2018. № 4. С. 214–220.

35. Пантелеєв В. П. *Внутрішньогосподарський контроль: методологія та організація*: монографія. Київ : ДП «Інформ-аналіт. агентство», 2024. 491 с.

36. Панчак В. Як вибудувати культуру корпоративної безпеки у компанії? URL: https://biz.ligazakon.net/analitycs/206649_yak-vibuduvati-kulturu-korporativno-bezpeki-u-kompan

37. Плєхова Г., Суханова Н., Левтеров А. Кібербезпека: загрози, рішення. *Theoretical Foundations in Economics and Management*. 2022. P. 681–692. URL: https://doi.org/10.46299/isg.2022.mono.econ.2.9.6

38. Погорєлов Ю. С. Управління розвитком підприємства. Київ : КНЕУ, 2016. 482 с.

39. Предборський В. А. Економічна безпека держави : Монографія. Київ : Кондор, 2021. 398 с.

40. Розвивайте свій бізнес за допомогою дизайнерських цифрових рішень від Tietoevry Create, вашого партнера для кращого майбутнього. URL: https://www.tietoevry.com/en/create/

41. Розширення можливостей бачення. Забезпечення цінності. N-iX. URL: https://www.n-ix.com/

42. Рудковський О. В. Структурні елементи системи корпоративної безпеки. *Університетські наукові записки*. 2019. № 1 (49). С. 355-360.

43. Савчук В. П. Діагностика фінансового стану підприємства. Київ : КНЕУ, 2019. 296 с.

44. Салоїд С. В. Механізм управління економічною безпекою підприємства: теоретичний аспект. *Економічний вісник НТУУ «Київський політехнічний інститут»*, 2017. Вип. (14), С. 160–165. https://doi.org/10.20535/2307-5651.14.2017.108778

45. Ситник Г. П. Корпоративне управління: теорія та практика. Київ : Центр учбової літератури, 2019. 360 с.

46. Соснін О. В. Корпоративне управління та безпека бізнесу в умовах глобалізації. Київ : Наукова думка, 2018. 320 с.

47. Хмельницький район електричних мереж АТ «Хмельницькобленерго». Opendatabot. URL: https://opendatabot.ua/c/22764703.

48. Хмельницький РЕМ ПАТ «Хмельницькобленерго». Mista.ua. URL: http://mista.ua/Інфраструктура/Держустанови/Енергетика/хмельницький-рем-пат-хмельницькобленерго/13269/.

49. Череп А. В., Северина А. С. Ризик-менеджмент у системі забезпечення економічної безпеки підприємства. *Економічний простір*. 2021. № 165. С. 102–108.

50. Чубаєвський, В. І. Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство*, 2022. Вип. (43), С. 1-8. https://doi.org/10.32782/2524-0072/2022-43-49

51. Шира Т. Б. Внутрішньокорпоративний контроль в системі управління корпоративною безпекою промислових підприємств. *Ефективна економіка*. 2020. № 1. URL: http://www.economy.nayka.com.ua/?op=1&z=7592

52. Шира Т. Б. Концептуальні засади забезпечення корпоративної безпеки підприємств. *Економічний часопис Східноєвропейського національного університету імені Лесі Українки*. 2019. № 18, Том 2. С. 51-56.

53. Шира Т. Б. Формування системи корпоративної безпеки підприємства: методологічні основи. *Причорноморські економічні студії*, 2019. Вип. 42, С. 117–120. URL: https://bses.in.ua/journals/2019/42_2019/24.pdf

54. Штангрет А. М. Антикризове управління та безпека розвитку підприємства. Львів : УАД, 2021. 242 с.

55. Що таке корпоративна безпека? Найкращі поради та рішення на 2024 рік. URL: https://hideez.bakotech.com/ua/what-is-corporate-security-top-tips-and-solutions-for-2024

56. Патик В.Р. Цифрові загрози та їх вплив на економічну безпеку сучасних підприємств. Матеріали Міжнародної науково-практичної конференції «SCIENCE AT THE FRONTIER OF PROGRESS» (27-29 січня 2026 року м. Париж, Франція). https://naukainfo.com/conference?id=93

# ДОДАТКИ

Додаток А

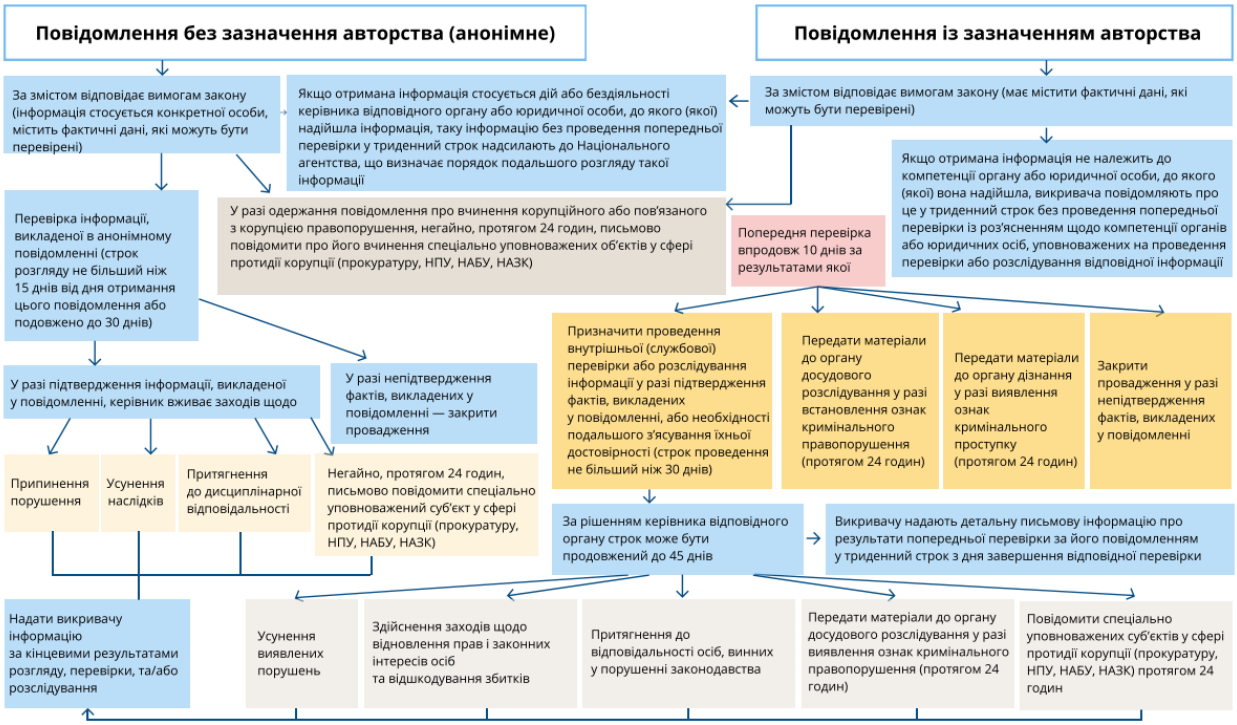


Рис. Схема стандартної процедури розгляду повідомлень про корупцію

Додаток Б

Таблиця 2.1. SWOT-аналіз загроз корпоративній безпеці Хмельницького РЕМ

| SWOT-компонент | Загрози / фактори | Пояснення (як це впливає на безпеку) |
|---|---|---|
| 1 | 2 | 3 |
| Сильні сторони | 1. Належність до АТ «Хмельницькобленерго» забезпечує централізовану організаційну підтримку, доступ до корпоративних ресурсів та сервісів (кол-центр, регламенти). | Централізовані служби дають доступ до оперативних процедур (реакція на аварії), корпоративних політик та контактів екстрених служб (зменшує час реагування на інциденти). |
| | 2. Існуючі цифрові сервіси: онлайн-інформація про відключення, централізований кол-центр – канали комунікації зі споживачами. | Прискорюють інформування споживачів і координацію ремонтних бригад; водночас вимагають захисту від кіберінцидентів. |
| | 3. Інвестиційні проєкти з модернізації та цифровізації (проєкт на зміцнення стійкості мережі) – ресурс для підвищення надійності. | Модернізація підстанцій і цифрові рішення зменшують технічні та операційні ризики, підвищують прогнозованість роботи мереж. |
| Слабкі сторони | 1. Вразливість до вимушених погодинних, аварійних відключень (оперативні обмеження інфраструктури та залежність від зовнішніх факторів). | Часті відключення підривають довіру споживачів, створюють репутаційні ризики та підвищують операційні навантаження на персонал. |
| | 2. Централізація РЕМів (злиття районів) короткостроково підвищує ризик перевантаження координаційних функцій; можливі «вузькі місця» в управлінні. | Скорочення числа РЕМів може підвищити ефективність, але збільшує навантаження на операторські центри й ризик затримок при кризах. |
| | 3. Підвищений ризик кіберзагроз у зв’язку з цифровізацією обліку й управління – потреба в сильній ІТ-захищеності. | Уразливі інформаційно-технологічні системи можуть стати каналами для втручання, маніпуляцій в обліку і порушення сервісів. |
| Можливості | 1. Грантові та інвестиційні проєкти для модернізації мережі (щоб підвищити стійкість та цифрові можливості). | Можна впровадити цифрові двійники, системи віддаленого моніторингу, превентивне технічне обслуговування (знизити аварійність і витрати). |
| | 2. Розвиток прозорих каналів комунікації (онлайн-інструменти, кол-центр, інформаційні сторінки) для підвищення довіри споживачів. | Посилення двосторонньої комунікації покращує репутацію та дозволяє оперативніше реагувати на інциденти. |
| | 3. Міжнародна підтримка/проєкти (енергетичні програми, донорські ініціативи), що забезпечить доступ до технологій та експертизи. | Можна отримати фінансування на підвищення кіберзахисту, інфраструктурну реконструкцію, підготовку персоналу. |
| Загрози | 1. Фізичні удари та саботаж (дрони, ракети, воєнні дії) уразливі для | Масовані удари можуть призвести до тривалих відключень, руйнувань |

| | | |
|---|---|---|
| | енергетичної інфраструктури – пряма загроза критичним об’єктам. | обладнання та серйозних репутаційних і фінансових збитків. |
| | 2. Кіберінциденти проти систем обліку та диспетчеризації (зростання складності атак у енергетиці). | Успішна кібератака може спричинити недостовірний облік, збої в подачі електроенергії, або компрометацію даних споживачів. |
| | 3. Регуляторні фактори (зміни тарифів, дефіцит фінансування, інфляційні витрати) впливають на спроможність модернізації. | Скорочує можливість швидкої модернізації мереж і реалізації програм підвищення безпеки. |

**Виконала** студентка 5 курсу
факультету управління та
економіки 073 Менеджмент
заочної форми навчання
«__» лютого 2026 р. _____ В. Р. Патик

**Науковий керівник**
доцентка кафедри
к.е.н., доцентка
«__» лютого 2026 р. _____ Д. А. Арзянцева

**Робота допущена до захисту:**
завідувачка кафедри
к.е.н., доцентка
«__» лютого 2026 р. _____ Н. П. Захаркевич