ВСП «Харківський торговельно-економічний фаховий коледж Державного торговельно-економічного університету»

Циклова комісія економіки, управління та адміністрування

Краснікова Анастасія Сергіївна
ПІБ здобувача

КУРСОВА РОБОТА

Технології попередження внутрішніх загроз економічній безпеці суб'єктів господарської діяльності
тема

Навчальна дисципліна: Фінансово-економічна безпека організації
назва навчальної дисципліни

Ступінь освіти: Фаховий молодший бакалавр
фаховий молодший бакалавр, молодший бакалавр, бакалавр

Галузь знань: 07 Управління та адміністрування
шифр і назва галузі знань

Спеціальність: 072 Фінанси, банківська справа, страхування та фондовий ринок
код і найменування спеціальності

Освітньо-професійна програма: Фінанси і кредит
назва освітньо-професійної програми

Академічна група: Ф-23
назва академічної групи

Харків, 2025 рік

ДОПУЩЕНО ДО ЗАХИСТУ

Керівник: Постольна Наталія Олександрівна, викладач циклової комісії економіки, управління та адміністрування, спеціаліст вищої категорії

Робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач _____ А.С. Краснікова
підпис здобувача ПІБ здобувача

Підсумкова оцінка: **65** (балів)

Члени комісії з захисту:

_____ Н. О. Постольна
(підпис)

_____ О.М. Тимошенко
(підпис)

ВСП «Харківський торговельно-економічний фаховий коледж
Державного торговельно-економічного університету»

Циклова комісія економіки, управління та адміністрування

Краснікова Анастасія Сергіївна

ПІБ здобувача

ЗАВДАННЯ НА КУРСОВУ РОБОТУ

Навчальна дисципліна Фінансово-економічна безпека організації

назва навчальної дисципліни

Тема роботи Технології попередження внутрішніх загроз економічній безпеці суб'єктів господарської діяльності

тема курсової роботи

Термін подання завершеної роботи 26.05.2025 р.

фаховий молодший бакалавр, молодший бакалавр, бакалавр

Графік виконання роботи

Виконання роботи за розділами	Термін виконання
Вибір та затвердження теми	03.03 – 08.03.2025
Добір та аналіз літератури за обраною темою	10.03 – 22.03.2025
Складання плану курсової роботи	24.03 – 29.03.2025
Написання вступу та І розділу	31.03 – 19.04.2025
Написання розрахункової частини (ІІ розділ) курсової роботи	21.04 – 10.05.2025
Написання висновків та пропозицій, оформлення курсової роботи	12.05 – 24.05.2025
Подання курсової роботи керівнику для рецензування (для рекомендації до захисту)	26.05 – 31.05.2025
Захист курсової роботи	02.06 – 07.06.2025

Завдання видав

Науковий керівник,
спеціаліст вищої категорії

Наталія ПОСТОЛЬНА
(підпис)

«06» березня 2025 р.

Завдання отримав

Здобувач

Анастасія КРАСНІКОВА
(підпис) ПІБ здобувача

«06» березня 2025 р.

ЗМІСТ

ВСТУП

У сучасних умовах глобалізації, високої конкуренції та активного розвитку цифрових технологій зростає важливість забезпечення економічної безпеки підприємств. Особливого значення це питання набуває для суб'єктів фінансового сектору, зокрема страхових компаній, які функціонують у складному середовищі з високим рівнем регуляторних вимог, високими ризиками і потребою у безперервному моніторингу внутрішніх і зовнішніх факторів загрози. Однією з ключових складових економічної безпеки є внутрішні загрози, які часто недооцінюються, але можуть завдати суттєвої шкоди підприємству.

Внутрішні загрози можуть мати різну природу – від зловживань персоналу, інформаційних витоків, організаційних недоліків до слабких місць у внутрішньому контролі та корпоративному управлінні. Ефективне попередження таких загроз вимагає впровадження сучасних технологій управління ризиками, використання цифрових інструментів, побудови аналітичних систем моніторингу та розвитку внутрішньої культури безпеки.

ПрАТ «СК «УНІКА» один з провідних представників страхового ринку України з багаторічним досвідом та європейськими стандартами ведення бізнесу. Компанія активно впроваджує інновації у процес управління безпекою, і тому є доцільним розгляд саме її досвіду з точки зору попередження внутрішніх загроз.

Метою даної курсової роботи є аналіз існуючих технологій виявлення та попередження внутрішніх загроз економічній безпеці підприємств на прикладі ПрАТ «СК «УНІКА», а також формування пропозицій щодо підвищення ефективності функціонування системи безпеки компанії.

Об'єктом дослідження є діяльність ПрАТ «СК «УНІКА» у контексті забезпечення економічної безпеки.

Предметом дослідження виступають технології та інструменти попередження внутрішніх загроз.

Інформаційну базу склали фінансові та звітні дані компанії «УНІКА», аналітичні матеріали страхового ринку, законодавча база України, а також наукові публікації з питань економічної безпеки.

Курсова робота складається з двох розділів, у яких послідовно розглянуто теоретичні засади теми, аналітичне вивчення внутрішніх загроз та особливості їх попередження на прикладі конкретного суб’єкта господарювання.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ВНУТРІШНЬОЇ БЕЗПЕКИ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

1.1. Економічна безпека підприємства: сутність, роль і значення

У сучасних умовах господарювання економічна безпека підприємства є однією з ключових передумов його стійкого розвитку, конкурентоспроможності та здатності протистояти як внутрішнім, так і зовнішнім загрозам. Поняття економічної безпеки стало широко вживаним не лише в наукових колах, а й у практичній діяльності підприємств, оскільки вона тісно пов'язана з такими фундаментальними категоріями, як фінансова стабільність, ефективне управління ризиками, збереження ресурсного потенціалу та довгострокове стратегічне планування.

Економічна безпека підприємства – це стан захищеності підприємства від впливу негативних факторів зовнішнього і внутрішнього середовища, який забезпечує його стабільне функціонування, досягнення стратегічних цілей і збереження конкурентних переваг на ринку. Вона включає здатність підприємства ефективно реагувати на зміни у ринковому, фінансовому, правовому, інформаційному та соціальному середовищі.

Науковці трактують економічну безпеку підприємства як складну інтегровану категорію, яка об'єднує в собі фінансову, виробничу, кадрову, правову, інформаційну, екологічну, техніко-технологічну та інші види безпеки, кожна з яких виконує важливу роль у збереженні цілісності бізнесу.

З практичної точки зору, економічна безпека підприємства проявляється у таких ключових характеристиках як:

1. стабільне зростання обсягів продажу та прибутковості;
2. належний рівень платоспроможності та ліквідності;
3. оптимальний рівень диверсифікації ризиків;
4. здатність до швидкої адаптації в умовах криз або нестабільності;
5. збереження ділової репутації та довіри з боку партнерів і споживачів;

6. ефективне використання матеріальних, трудових та інтелектуальних ресурсів.

Роль економічної безпеки в діяльності підприємства полягає передусім у забезпеченні:

Фінансової стійкості – наявності достатніх власних коштів, ліквідних активів і раціонального фінансового менеджменту для покриття поточних зобов'язань.

Захисту від внутрішніх і зовнішніх загроз – таких як шахрайство, зловживання, витік інформації, недобросовісна конкуренція, інфляційні коливання, зміни у законодавстві.

Можливості сталого розвитку – здатності підприємства інвестувати в інновації, модернізувати виробництво, розширювати ринки збуту.

Соціальної стабільності – створення умов для продуктивної праці персоналу, уникнення трудових конфліктів, формування корпоративної культури.

Сучасна економічна безпека має активний, стратегічний характер. Це означає, що її забезпечення не зводиться до простої реакції на загрози, а передбачає: постійний моніторинг зовнішнього і внутрішнього середовища, управління ризиками, планування антикризових заходів, прогнозування потенційних вразливостей.

Особливої актуальності економічна безпека набуває для фінансових і страхових компаній, таких як ПрАТ «СК «УНІКА», які оперують з великими обсягами клієнтських коштів, підлягають жорсткому державному регулюванню та мають високі зобов'язання перед контрагентами. В умовах війни, економічної нестабільності, кібератак і стрімкого зростання інформаційних ризиків збереження економічної безпеки стає основою не лише стабільності, а й самого існування подібних компаній.

У підсумку можна стверджувати, що економічна безпека – це не лише індикатор стійкості підприємства, а й комплексна система заходів, спрямована на передбачення, запобігання та нейтралізацію загроз, яка має бути вбудована у всі управлінські рівні та процеси. Забезпечення належного рівня економічної

безпеки має стати пріоритетом для будь-якого підприємства, що прагне до довгострокового розвитку та підвищення власної вартості.

1.2. Технологічні та організаційні підходи до запобігання внутрішнім загрозам

Внутрішні загрози становлять одну з найскладніших категорій ризиків для підприємства, оскільки походять із самого середовища його функціонування, тобто зсередини організаційної структури. Їх джерелами можуть бути працівники, управлінські процеси, організаційні недоліки, прогалини у внутрішньому контролі, зловживання службовим становищем, помилки в управлінських рішеннях або низький рівень корпоративної культури. З огляду на це, ефективне управління такими загрозами вимагає комплексного підходу, який поєднує технологічні інструменти з організаційними заходами.

Технологічна складова системи безпеки дедалі частіше базується на використанні цифрових платформ, автоматизованих систем моніторингу, аналітики великих масивів даних (Big Data) і штучного інтелекту. Завдяки цим інструментам підприємство отримує змогу своєчасно ідентифікувати атипову поведінку співробітників, підозрілі фінансові операції, порушення внутрішніх регламентів. Крім того, автоматизація управлінських процесів дозволяє мінімізувати «людський фактор» та забезпечити більшу прозорість діяльності. Наприклад, системи контролю доступу, логування дій користувачів у програмному забезпеченні, аналітичні панелі для керівництва – усе це формує технологічну основу попередження загроз.

Проте одних лише технологій недостатньо. Запобігання внутрішнім загрозам неможливе без належної організаційної структури та культури управління. Організаційні підходи до забезпечення внутрішньої безпеки базуються на побудові ефективної системи корпоративного управління, розробці чітких регламентів, політик і процедур, а також на створенні середовища доброчесності та відповідальності.

Важливе місце займає система внутрішнього контролю, яка охоплює всі рівні управління підприємством. Вона повинна включати чітке розмежування повноважень і відповідальності, регулярні внутрішні аудити, оцінку ризиків, перевірку відповідності прийнятих рішень внутрішнім нормативам. Не менш значущим є управління персоналом, зокрема належний підбір кадрів, оцінювання доброчесності та кваліфікації, організація навчань з питань безпеки, впровадження стандартів корпоративної етики.

Організаційна культура, яка підтримує відкритість, відповідальність і нетерпимість до будь-яких форм порушень, є ще одним потужним інструментом протидії внутрішнім загрозам. Якщо співробітники розуміють, що контроль є постійним, об'єктивним і неупередженим, а порушення тягнуть за собою чіткі наслідки, ймовірність внутрішніх ризиків суттєво знижується.

Варто також зазначити, що ефективне функціонування технологічних і організаційних підходів потребує тісної взаємодії між підрозділами підприємства – ІТ-службою, відділом безпеки, юридичною та кадровою службами. Успішна модель передбачає не лише наявність окремих елементів захисту, а й їх системну інтеграцію в єдиний механізм управління ризиками.

Таким чином, поєднання технологічних рішень з організаційними механізмами створює потужну платформу для виявлення, оцінки та запобігання внутрішнім загрозам. Такий підхід дозволяє підприємству зберігати стабільність, захищати інтереси акціонерів, працівників і клієнтів, а також забезпечувати довготривалу економічну безпеку в умовах динамічного зовнішнього середовища.

1.3. Системи ідентифікації загроз в управлінській діяльності, використання інформаційних технологій, кадрових та організаційних механізмів забезпечення внутрішньої безпеки підприємства

У XXI столітті інформаційні технології (ІТ) стали не лише основою для оптимізації управлінських процесів, але й важливим інструментом забезпечення економічної безпеки підприємств. У зв’язку зі зростанням обсягів

оброблюваної інформації, цифровізацією бізнесу та глобальною залежністю від електронної інфраструктури, підприємства опинилися перед необхідністю побудови цілісних ІТ-систем захисту, що дають змогу не лише запобігати загрозам, а й своєчасно виявляти й усувати ризики.

Інформаційні технології у сфері безпеки виконують функції автоматизованого моніторингу, аналізу даних, контролю доступу, а також збереження й захисту інформаційних ресурсів. Особливо актуальними вони стають в умовах зростання кіберзагроз, хакерських атак, витоків комерційної та персональної інформації, а також внутрішніх зловживань.

ІТ-рішення відіграють ключову роль у формуванні системи управління інформаційною безпекою (СУІБ), яка інтегрується в загальну структуру економічної безпеки підприємства. Вона базується на принципах безперервного контролю, багаторівневої автентифікації, шифрування даних, обмеження прав доступу, аудитів безпеки та резервного копіювання. Застосування таких рішень дозволяє мінімізувати ризики несанкціонованого втручання в систему, втрати інформації або її пошкодження.

Одним із найефективніших інструментів сучасного цифрового середовища є системи інформаційного моніторингу та виявлення загроз (SIEM – Security Information and Event Management). Вони забезпечують централізований збір, аналіз і кореляцію подій у реальному часі з усіх вузлів інформаційної інфраструктури підприємства. Такі системи дозволяють виявляти підозрілі дії на ранніх етапах, знижуючи ризик масштабних інцидентів.

Інший важливий напрям – використання технологій штучного інтелекту та машинного навчання в галузі безпеки. Завдяки їм компанії можуть аналізувати поведінкові моделі користувачів і автоматично виявляти аномалії, які можуть вказувати на внутрішні загрози або зовнішні атаки. Наприклад, раптовий доступ працівника до конфіденційної інформації поза робочим часом може бути автоматично позначений як потенційна загроза.

З точки зору управління внутрішніми загрозами, ІТ також дають можливість контролювати операційну діяльність персоналу, ведення журналів

дій користувачів (логування), аудиту змін у документах, а також контролю за дотриманням політик доступу. Такі функції особливо важливі для компаній фінансового сектора, де навіть незначні збої або помилки можуть мати суттєві фінансові наслідки.

Для страхових компаній, зокрема ПрАТ «СК «УНІКА», впровадження ІТ-рішень у систему безпеки є не лише засобом захисту, а й конкурентною перевагою. Автоматизація процесів обробки страхових випадків, перевірки клієнтів, обліку активів та аналізу фінансових потоків – усе це зменшує ризики шахрайства, підвищує точність прийняття рішень та зміцнює довіру клієнтів. Крім того, компанія має можливість інтегрувати внутрішні інформаційні системи з державними реєстрами, базами даних і цифровими сервісами, що підвищує прозорість операцій.

Інформаційні технології також дозволяють компаніям формувати аналітичні системи підтримки прийняття управлінських рішень (DSS – Decision Support Systems), які базуються на комплексному аналізі ризиків, оцінці ефективності заходів безпеки та прогнозуванні майбутніх викликів. Такі інструменти допомагають керівництву будувати політику безпеки на підставі даних, а не лише інтуїтивних оцінок.

Отже, інформаційні технології в умовах сучасного підприємства – це не лише засіб автоматизації чи зручності, а стратегічний інструмент управління безпекою, що охоплює всі рівні організаційної структури. Їх використання забезпечує підприємству здатність протидіяти загрозам, адаптуватися до цифрових викликів, зберігати інформаційні ресурси, а відтак – гарантує стабільність і конкурентоспроможність у динамічному середовищі.

З метою забезпечення високого рівня інформаційної та економічної безпеки ПрАТ «СК «УНІКА» активно впроваджує сучасні цифрові рішення, що відповідають стандартам європейського рівня. Як частина міжнародної групи UNIQA Insurance Group, компанія інтегрує перевірені технології з ринків ЄС, адаптуючи їх до українських реалій.

Одним з таких рішень є впровадження централізованої платформи управління бізнес-процесами та ризиками, яка базується на концепції ERM

(Enterprise Risk Management). Ця система дозволяє в реальному часі оцінювати ризики у внутрішніх процесах – від страхування до врегулювання збитків, – а також контролювати відповідність операцій вимогам законодавства, стандартам якості та внутрішнім регламентам. Завдяки інтегрованим механізмам аналізу і візуалізації даних, керівництво компанії отримує чітку картину вразливостей, ризиків та точок контролю в управлінській діяльності.

Окрему увагу в компанії приділено захисту клієнтських даних, які є об’єктом підвищеної конфіденційності. Для цього впроваджено системи багаторівневої автентифікації, контроль за доступом до персональних записів, автоматизовані журнали змін і аудиту, а також регулярне резервне копіювання зберігання інформації. Всі системи працюють у відповідності до вимог Закону України «Про захист персональних даних» та стандартів ISO/IEC 27001.

У сфері боротьби з шахрайством СК «УНІКА» використовує модулі автоматичної перевірки страхових випадків, які на основі алгоритмів машинного навчання виявляють підозрілі шаблони поведінки клієнтів або посередників. Наприклад, система автоматично позначає страхові звернення, які повторюються з однаковими параметрами або мають ознаки заниження/завищення збитків. Ці рішення дозволяють значно зменшити втрати компанії від страхового шахрайства та підвищити прозорість процедур.

Також у компанії активно впроваджуються інструменти внутрішнього електронного документообігу, що значно зменшує можливість несанкціонованого втручання в управлінські рішення, мінімізує «людський фактор» та прискорює обробку критично важливої інформації. Кожен етап документообігу супроводжується цифровим підписом, а всі зміни у документах фіксуються в автоматичному режимі.

У підсумку, ПрАТ «СК «УНІКА» демонструє комплексний підхід до використання інформаційних технологій як інструменту забезпечення безпеки. Завдяки цифровізації процесів, впровадженню аналітичних рішень, автоматизованому моніторингу та контролю, компанія не лише підвищує рівень внутрішньої безпеки, а й зміцнює свою позицію на ринку як прозорий і надійний партнер.

Управлінська діяльність підприємства є основою його стратегічного та оперативного функціонування, а тому вразлива до широкого спектра загроз – як зовнішніх, так і внутрішніх. Здатність своєчасно виявляти, аналізувати та реагувати на потенційні загрози є невід'ємною частиною системи економічної безпеки. У цьому контексті системи ідентифікації загроз відіграють ключову роль, оскільки саме вони забезпечують раннє попередження про можливі деструктивні фактори, дозволяючи керівництву приймати обґрунтовані рішення.

Система ідентифікації загроз – це комплекс організаційних, інформаційних і технологічних заходів, спрямованих на виявлення джерел і симптомів потенційної шкоди, що може бути завдана управлінським процесам, репутації, фінансовому становищу або ресурсному потенціалу підприємства. На відміну від загального ризик-менеджменту, ці системи акцентують увагу саме на загрозах – тобто подіях або чинниках, що мають ворожий або руйнівний характер.

Одним з основних напрямів ідентифікації загроз є моніторинг внутрішнього середовища підприємства. До нього належить аналіз поведінки персоналу, фінансових операцій, відхилень у бізнес-процесах, рівня відповідності внутрішнім політикам і стандартам. Наприклад, системи аудиту і контролю внутрішніх транзакцій можуть виявити нетипові дії, що свідчать про шахрайство, несанкціонований доступ до ресурсів чи спроби маніпуляцій із документацією. У свою чергу, HR-аналітика дозволяє ідентифікувати зміни в поведінці працівників, які можуть свідчити про втрату лояльності, зниження мотивації або внутрішній конфлікт.

Другим важливим компонентом є інформаційно-аналітичні системи, що базуються на застосуванні спеціалізованого програмного забезпечення. Сучасні підприємства все частіше використовують інструменти Business Intelligence, системи раннього попередження, інструменти штучного інтелекту та машинного навчання. Вони дозволяють виявляти загрози, що не піддаються очевидному спостереженню, зокрема через аналіз великих масивів даних, прогнозування трендів або побудову сценаріїв розвитку ситуації.

Крім цього, важливою складовою системи ідентифікації є організаційна свідомість і корпоративна культура, які формують середовище, де працівники самостійно виявляють і повідомляють про потенційні загрози. Функціонування механізмів «внутрішнього інформування» (whistleblowing), регулярне навчання персоналу з питань безпеки, а також відкритість управлінського процесу значною мірою підвищують шанси на раннє виявлення ризиків.

Окремо слід відзначити роль стратегічного аналізу і ризик-менеджменту, що формують базу для системної ідентифікації загроз. SWOT-аналіз, PEST-аналіз, матриці ризиків, моделювання сценаріїв розвитку подій – це інструменти, які дозволяють оцінити, в якій формі, з яких джерел і в яких умовах можуть виникнути загрози управлінській системі підприємства.

На практиці ефективна система ідентифікації загроз не обмежується окремими підходами, а інтегрує кілька рівнів – технічний, інформаційний, організаційний і поведінковий. Такий підхід дозволяє створити багатокомпонентну, самонавчальну структуру, здатну адаптуватися до нових викликів і мінливих умов.

У випадку фінансових і страхових компаній, таких як ПрАТ «СК «УНІКА», ця система є особливо актуальною. Через високий ступінь відповідальності перед клієнтами, постійний рух коштів, складні контракти і високі регуляторні вимоги, ідентифікація навіть незначної загрози в управлінській діяльності є критично важливою. Наприклад, недотримання політик андеррайтингу або помилки в оцінці страхових ризиків можуть мати катастрофічні наслідки для компанії.

Підсумовуючи, варто зазначити, що система ідентифікації загроз в управлінні є одним з найважливіших елементів загальної архітектури економічної безпеки. Її ефективність визначається здатністю не лише виявляти загрози, але й адекватно реагувати на них, інтегруючи ці процеси в загальну стратегію управління підприємством.

Щодо кадрових та організаційних механізмів забезпечення внутрішньої безпеки та їх застосування, внутрішня безпека підприємства, особливо у фінансовій сфері, значною мірою залежить не лише від технологічного захисту,

але й від кадрових та організаційних підходів до управління персоналом і внутрішніми процесами. Саме людський чинник – як у вигляді помилок, так і свідомих порушень – найчастіше є джерелом внутрішніх загроз для стабільності компанії. Тому кадрова політика та організаційна структура мають будуватися з урахуванням принципів запобігання, виявлення та реагування на потенційні внутрішні ризики.

Кадрові механізми забезпечення внутрішньої безпеки охоплюють весь життєвий цикл співробітника на підприємстві – від відбору та адаптації до оцінки, мотивації та завершення трудових відносин. Насамперед, це стосується суворого контролю на етапі підбору кадрів: перевірки попереднього досвіду, кваліфікації, доброчесності та психологічної стійкості кандидатів. У багатьох компаніях фінансового сектору ця практика доповнюється верифікацією через бази неблагонадійних осіб, а також співбесідами з елементами поведінкового аналізу.

Не менш важливим є систематичне навчання персоналу з питань інформаційної та економічної безпеки. Регулярне оновлення знань про внутрішні політики, корпоративні стандарти, законодавчі зміни та правила конфіденційного поводження з інформацією підвищує свідомість працівників і зменшує ризики ненавмисних порушень. Більше того, поінформовані співробітники самі стають активними агентами безпеки, здатними ідентифікувати підозрілу поведінку або вразливості в процесах.

Організаційні механізми забезпечення внутрішньої безпеки пов’язані з побудовою ефективної структури управління, що чітко визначає повноваження, зони відповідальності та підзвітність. Йдеться про поділ критично важливих функцій між різними підрозділами (наприклад, бухгалтерія не поєднує функції контролю й виконання платежів), встановлення рівнів доступу до конфіденційної інформації, створення систем внутрішнього контролю, аудитів і ризик-менеджменту.

Особливе значення має функція комплаєнс-контролю, яка слідкує за відповідністю внутрішніх дій зовнішнім нормативам, внутрішнім політикам та стандартам групи. Комплаєнс-служба аналізує операційну діяльність з точки

зору потенційних зловживань, конфліктів інтересів, недобросовісних практик, зокрема у взаємодії з клієнтами, партнерами та регуляторами.

У ПрАТ «СК «УНІКА» система внутрішньої безпеки ґрунтується на європейських стандартах групи UNIQA та включає ефективне поєднання кадрових і організаційних підходів. Компанія приділяє особливу увагу формуванню доброчесної, лояльної та професійної команди. Усі нові працівники проходять перевірку безпеки, зокрема через аналіз ділової репутації, відсутність конфліктів інтересів або підозрілих зв'язків. Працівники ключових посад додатково перевіряються службами комплаєнс і внутрішнього аудиту.

Окрім цього, «СК «УНІКА» впроваджує програми навчання та підвищення кваліфікації, які обов'язково містять модулі з інформаційної та фінансової безпеки. У компанії діє внутрішній кодекс етики, який регламентує допустиму поведінку, правила конфіденційності, а також процедури повідомлення про порушення (whistleblowing).

З боку організаційної структури компанія реалізує принципи розмежування повноважень і перевірки контрольних точок у ключових бізнес-процесах, особливо у сфері прийняття страхових рішень, врегулювання збитків і фінансових операцій. У компанії діє система внутрішнього аудиту, яка на регулярній основі перевіряє дотримання внутрішніх політик і стандартів групи, виявляє слабкі місця та пропонує заходи щодо їх усунення.

Таким чином, кадрові й організаційні механізми у ПрАТ «СК «УНІКА» є невід'ємною частиною загальної системи внутрішньої безпеки. Вони сприяють зниженню ймовірності зловживань, мінімізації людського фактора, а також створенню корпоративного середовища, орієнтованого на прозорість, відповідальність і дотримання стандартів.

РОЗДІЛ 2. ОЦІНКА СИСТЕМИ ВНУТРІШНЬОЇ БЕЗПЕКИ ПРАТ «СК «УНІКА»

2.1. Загальна характеристика діяльності ПрАТ «СК «УНІКА»

Приватне акціонерне товариство «Страхова компанія «УНІКА» (ПрАТ «СК «УНІКА») є однією з найбільших і найнадійніших страхових компаній на українському ринку. Вона входить до складу міжнародної групи UNIQA Insurance Group, що базується в Австрії та представлена в більш ніж 15 країнах Європи. UNIQA Group є лідером у сфері страхування в Центральній та Східній Європі, а її частка на українському страховому ринку стабільно зростає протягом останніх років.

ПрАТ «СК «УНІКА» здійснює свою діяльність з 1994 року, і за майже тридцять років існування компанія сформувала позитивну ділову репутацію, розгалужену мережу представництв по всій Україні та стабільну клієнтську базу. Центральний офіс компанії розташовано в місті Києві, а її регіональні структури забезпечують обслуговування клієнтів у всіх областях країни.

Основними видами діяльності компанії є:

– надання послуг зі страхування майна, відповідальності, транспорту, здоров’я, життя;

– корпоративне страхування для бізнес-клієнтів (зокрема, аграріїв, транспортних компаній, будівельних підприємств);

– добровільне медичне страхування (ДМС) – один із ключових напрямів діяльності компанії;

– автострахування, включно з обов’язковим (ОСЦПВ) і добровільним (КАСКО) страхуванням;

– страхування життя (через дочірню структуру ПрАТ «СК «УНІКА Життя»).

Компанія здійснює свою діяльність відповідно до чинного законодавства України, зокрема Закону України «Про страхування», а також внутрішніх політик UNIQA Group. ПрАТ «СК «УНІКА» має усі необхідні ліцензії, видані

Нацкомфінпослуг, та підлягає постійному нагляду з боку Національного банку України як регулятора страхового ринку.

Протягом останніх років компанія утримує високі позиції в рейтингах надійності, платоспроможності та обсягів страхових премій. Так, за підсумками 2023 року ПрАТ «СК «УНІКА» увійшла до ТОП-5 страхових компаній України за розміром зібраних страхових премій (близько 3,5 млрд грн), а рівень страхових виплат перевищив 1,9 млрд грн. Основними сегментами, що забезпечили зростання, стали автострахування та добровільне медичне страхування. Компанія продовжує активно розвивати цифрові канали продажів та сервісів, зокрема мобільні додатки, чат-боти та онлайн-платформи для клієнтів.

UNIQA також приділяє особливу увагу корпоративному управлінню, прозорості фінансової звітності та дотриманню міжнародних стандартів фінансової звітності (IFRS). У компанії діє сучасна система внутрішнього контролю, управління ризиками та комплаєнс-контролю, що відповідає європейським вимогам до страховиків.

Крім фінансових показників, компанія активно реалізує принципи соціальної відповідальності, підтримує медичні, освітні та благодійні ініціативи, спрямовані на розвиток суспільства. У період війни компанія зберегла фінансову стійкість, не зупинила обслуговування клієнтів і своєчасно виконувала зобов’язання перед страхувальниками, що свідчить про високу операційну гнучкість і довіру до бренду.

Таким чином, ПрАТ «СК «УНІКА» є зразком страхової компанії, що успішно поєднує досвід міжнародної страхової групи, глибоке розуміння українського ринку, інноваційні технології, ефективну систему управління ризиками та відповідальне ставлення до клієнтів. Її діяльність може розглядатися як ефективна модель побудови системи внутрішньої безпеки в умовах високої волатильності та ризиків, притаманних фінансово-страховому сектору.

2.2. Аналіз основних внутрішніх загроз у сфері страхової діяльності

Страхова діяльність є складним і відповідальним процесом, який потребує постійного контролю за багатьма аспектами діяльності компанії. Внутрішні загрози можуть негативно впливати на фінансову стабільність, репутацію та конкурентоспроможність страхової компанії. Тому важливо розуміти основні внутрішні ризики, що виникають у процесі роботи страхових компаній.

Основні внутрішні загрози у сфері страхової діяльності:

Фінансові загрози. Недостатнє формування страхових резервів, проблеми з ліквідністю, а також ризики, пов’язані з інвестиційною діяльністю, можуть призвести до неспроможності компанії виконувати свої зобов’язання перед клієнтами.

Операційні загрози. Помилки та шахрайство з боку персоналу, технічні збої, проблеми з інформаційними системами і недостатній рівень автоматизації бізнес-процесів можуть викликати збитки і порушення нормальної роботи компанії.

Управлінські загрози. Недосконала система управління ризиками, неефективна кадрова політика, а також недостатня адаптація до змін законодавства та регуляторних вимог можуть спричинити втрату контролю над ключовими процесами і підвищення ризиків.

Аналіз основних внутрішніх загроз у сфері страхової діяльності СК «Уніка»

1. Фінансові загрози

Недостатність страхових резервів. Відповідно до фінансових звітів 2023-2024 років, страхові резерви компанії складають значну частку зобов’язань. Неправильне їх формування (заниження розміру резервів) може призвести до недостатності коштів для покриття страхових виплат, особливо у випадку масових збитків. Відтак, це є суттєвою внутрішньою загрозою.

Ризик ліквідності. Компанія повинна мати достатній обсяг ліквідних активів для своєчасної виплати страхових відшкодувань. Фінансові дані

свідчать про певні коливання у ліквідності, що може викликати ризик затримок у виплатах і погіршення репутації.

Інвестиційні ризики. Страхова компанія інвестує страхові премії в різні активи. Волатильність ринків і можливі збитки від інвестицій можуть негативно вплинути на загальну фінансову стійкість.

2. Операційні загрози

Внутрішнє шахрайство і помилки персоналу. Через складність і обсяг страхових операцій існує загроза людських помилок або навмисних зловживань. Недосконалі внутрішні контролі можуть не виявляти такі випадки вчасно.

Технічні та інформаційні ризики. IT-система компанії піддається загрозам кібербезпеки, що може призвести до витоку або втрати даних, а також порушення роботи бізнес-процесів. Звітність свідчить про потребу у модернізації IT-інфраструктури.

Недосконалість процедур та документального оформлення. Частина процесів і внутрішніх процедур потребує стандартизації і автоматизації для зменшення ризику помилок і затримок.

3. Управлінські та кадрові ризики

Недостатня система управління ризиками. СК «Уніка» почала впроваджувати системний підхід до управління ризиками, але цей процес ще не завершений, що створює загрозу неефективного контролю.

Залежність від ключових співробітників. Втрата або недоступність кваліфікованих кадрів може негативно вплинути на якість послуг і внутрішній контроль.

Відповідність регуляторним вимогам. Часті зміни у законодавстві вимагають оперативної адаптації внутрішніх політик, і відсутність гнучкості в цьому може призвести до штрафів або санкцій.

Порівняльний аналіз основних внутрішніх загроз ПрАТ «УНІКА» у 2023 та 2024 роках

Фінансові загрози

Показник/Рік	2023	2024	Коментар

Показник/Рік	2023	2024	Коментар
Рівень страхових резервів	Суттєвий обсяг резервів, стабільний	Збереження високого рівня резервів	Збереження високих резервів свідчить про адекватність оцінки ризиків, але ризик недооцінки залишається
Ліквідність	Помірна ліквідність, ризик дисбалансу	Ліквідність під контролем, але з підвищеною потребою в гнучкості	Зростання обсягів виплат може ускладнити управління ліквідністю
Інвестиційний портфель	Коливання ринку впливають на доходність	Ринкові коливання більш виражені, підвищено волатильність	Потрібна більша диверсифікація та хеджування ризиків

Операційні загрози

Показник/Рік	2023	2024	Коментар
Помилки та шахрайства персоналу	Фіксуються поодинокі випадки, контролі на початковому рівні	Посилення контролю, але збільшення обсягів операцій підвищує ризики	Необхідно підвищувати автоматизацію і аудит
Технічні IT-ризики	Вразливість IT-інфраструктури, ризики кіберзагроз	Зусилля з удосконалення IT-безпеки, але ризики залишаються	Впровадження сучасних рішень для кіберзахисту є пріоритетом
Внутрішні процедури	Недостатня формалізація деяких процесів	Покращення процедур, але не повна автоматизація	Триває процес цифрової трансформації

Регуляторні та управлінські ризики

Показник/Рік	2023	2024	Коментар
Відповідність нормативам	Відповідність основним вимогам	Підвищена увага до комплаєнсу	Зміни в законодавстві вимагають оперативної адаптації
Управління ризиками	Початкові системи управління	Впровадження комплекснішої системи	Системність зростає, але процес ще не завершений
Кадрові ризики	Залежність від ключових співробітників	Початок формалізації кадрової політики	Важливо розвивати навчання і мотивацію персоналу

За період 2023-2024 років у ПрАТ «УНІКА» спостерігаються як позитивні зміни, так і збереження певних внутрішніх загроз:

Фінансові загрози залишаються ключовими, особливо в частині управління резервами, ліквідністю та інвестиційними ризиками. Потрібно посилювати аналітику та диверсифікацію активів.

Операційні загрози збільшуються через зростання обсягів діяльності, що підвищує ймовірність помилок і шахрайства. Посилення IT-безпеки є пріоритетом.

Регуляторні ризики вимагають гнучкості у внутрішніх процесах, що вже почало враховуватися.

Покращення системи управління ризиками та кадрової політики відбувається поступово, але ще має бути завершено.

Таким чином, для зменшення внутрішніх загроз компанії варто продовжити інвестиції у цифрові технології, посилити контрольні процедури і системи управління ризиками, а також працювати над підвищенням кваліфікації і мотивації персоналу.

3.3. Практика впровадження технологій попередження загроз у ПрАТ «СК «УНІКА»

У сучасних умовах функціонування страхового ринку ПрАТ «СК «УНІКА» приділяє значну увагу впровадженню ефективних технологій попередження внутрішніх загроз. Компанія, як частина міжнародної групи UNIQA Insurance Group (Австрія), дотримується європейських стандартів управління ризиками та безпеки, що забезпечує високий рівень захисту її операційної та фінансової діяльності.

Одним із ключових напрямів попередження внутрішніх загроз є автоматизація страхових операцій. ПрАТ «УНІКА» активно впроваджує:

- електронне страхування – що мінімізує помилки ручного введення даних;
- онлайн-сервіси для клієнтів – що дозволяє знизити навантаження на персонал і покращити контроль якості обслуговування;

- інтегровані CRM-системи – для виявлення аномальних дій клієнтів або співробітників у режимі реального часу.

У компанії діє комплексна система захисту даних, що включає:

- застосування сучасних засобів кіберзахисту (антивірусне ПЗ, фаєрволи, шифрування даних);
- регулярний аудит інформаційних систем;
- інструктажі та навчання персоналу з питань кібергігієни та запобігання фішинговим атакам.

Для мінімізації ризику шахрайства ПрАТ «УНІКА» впровадила:

- систему подвійного погодження платежів;
- внутрішній аудит операцій та моніторинг резервів;
- оцінку актуарних ризиків з використанням спеціалізованого програмного забезпечення.

З метою попередження кадрових ризиків в компанії функціонує:

- система перевірки надійності нових співробітників;
- програми підвищення кваліфікації;
- мотиваційні механізми для зменшення плинності кадрів.

ПрАТ «УНІКА» впровадила політику ERM (Enterprise Risk Management), яка передбачає: постійний моніторинг ключових ризиків, регулярну оцінку вразливості бізнес-процесів, звітність щодо управління ризиками перед головною компанією UNIQA Group.

Досвід ПрАТ «СК «УНІКА» демонструє системний підхід до запобігання внутрішнім загрозам. Компанія вдало поєднує цифрові технології, корпоративні стандарти та кадрові стратегії для забезпечення високого рівня надійності та безпеки своєї діяльності. Така практика є прикладом ефективного управління ризиками для інших учасників страхового ринку України.

2.4. Напрями підвищення ефективності системи внутрішньої безпеки

Система внутрішньої безпеки є важливою складовою ефективної та стабільної діяльності страхової компанії. Вона покликана забезпечити захист фінансових ресурсів, конфіденційної інформації, інформаційних систем, а також гарантувати дотримання внутрішніх правил і процедур. Удосконалення цієї системи передбачає впровадження сучасних технологічних рішень, організаційних змін та посилення корпоративної відповідальності.

Один із ключових напрямів підвищення ефективності внутрішньої безпеки полягає у цифровізації процесів та автоматизації контролю. Впровадження електронного документообігу з чіткими рівнями доступу дозволяє зменшити людський фактор та уникнути несанкціонованого втручання в бізнес-процеси. Автоматизовані системи моніторингу фінансових операцій і транзакцій у режимі реального часу сприяють своєчасному виявленню підозрілих дій та аномалій.

Не менш важливою є сфера інформаційної безпеки. Забезпечення захищеності баз даних за допомогою сучасних засобів шифрування, впровадження двофакторної аутентифікації, а також регулярне тестування IT-систем на вразливість дають змогу попередити як зовнішні кібератаки, так і витоки внутрішньої інформації.

Удосконалення кадрової політики також суттєво впливає на рівень внутрішньої безпеки. Перевірка надійності кандидатів при працевлаштуванні, чіткий розподіл обов’язків, відповідальності та постійне навчання працівників з питань інформаційної, фінансової та етичної безпеки дозволяють знизити ризики зловживань з боку персоналу. Формування культури дотримання внутрішніх процедур і нульової толерантності до порушень відіграє важливу роль у зміцненні внутрішнього контролю.

Окрему увагу варто приділяти розвитку системи внутрішнього аудиту. Наявність чітких регламентів, проведення планових і позапланових перевірок, а також впровадження принципу подвійного контролю у фінансових рішеннях дозволяє зменшити ризики фінансових порушень та шахрайства.

Управління ризиками потребує комплексного підходу. Впровадження системи управління ризиками на рівні підприємства (ERM) дозволяє ідентифікувати, оцінювати та контролювати потенційні загрози, а також своєчасно реагувати на нові виклики. Постійний аналіз ризик-профілю компанії та адаптація захисних механізмів до нових умов є необхідною умовою її стабільності.

Нарешті, підвищення рівня внутрішньої безпеки неможливе без належного рівня корпоративної культури. Формування усвідомлення значущості безпеки серед усіх співробітників, створення етичного середовища, а також наявність каналів для повідомлення про порушення внутрішніх правил (так званий «whistleblowing») є вагомими інструментами у запобіганні внутрішнім загрозам.

Таким чином, підвищення ефективності системи внутрішньої безпеки страхової компанії має охоплювати технічні, організаційні, управлінські та кадрові аспекти. Такий системний підхід дозволяє не лише знизити рівень ризиків, а й забезпечити довіру клієнтів, дотримання нормативних вимог та загальну конкурентоспроможність компанії на ринку страхових послуг.

ВИСНОВКИ І ПРОПОЗИЦІЇ

У процесі дослідження теми було встановлено, що економічна безпека суб’єктів господарської діяльності значною мірою залежить не лише від зовнішніх факторів, але й від ефективності протидії внутрішнім загрозам, які мають системний і багатогранний характер. До таких загроз належать фінансові, інформаційні, кадрові, технічні та управлінські ризики, які можуть призвести до порушення стабільності діяльності підприємства, втрати активів, погіршення репутації та зниження конкурентоспроможності.

В умовах сучасного динамічного ринку та високої цифровізації внутрішні загрози набувають прихованих форм, що ускладнює їх ідентифікацію та своєчасне реагування. Тому особливого значення набуває впровадження технологій попередження таких загроз. Зокрема, йдеться про системи внутрішнього контролю, управління ризиками, засоби інформаційної та кібербезпеки, автоматизацію процесів, а також формування етичної корпоративної культури.

На прикладі ПрАТ «СК «УНІКА» було проаналізовано практичні підходи до запобігання внутрішнім ризикам. Досвід компанії демонструє, що комплексне впровадження цифрових інструментів, посилення контролю, розвиток кадрового потенціалу та адаптація до регуляторних вимог дає змогу істотно знизити вразливість бізнес-процесів до внутрішніх загроз.

Узагальнюючи результати дослідження, можна зробити висновок, що підвищення економічної безпеки підприємств можливе лише за умови системного, стратегічного підходу до виявлення, оцінки та попередження внутрішніх загроз. Такі заходи є запорукою сталого розвитку, фінансової стійкості та довгострокової ефективності суб’єкта господарювання в умовах зростаючих викликів ринкового середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про фінансові послуги та державне регулювання ринків фінансових послуг» від 12.07.2001 р. № 2664-III. URL: https://zakon.rada.gov.ua

2. Закон України «Про страхування» від 07.03.1996 р. № 85/96-ВР (зі змінами). URL: https://zakon.rada.gov.ua

3. Національний банк України. Офіційний сайт. URL: https://bank.gov.ua

4. ПрАТ «СК «УНІКА». Фінансова звітність за 2023 рік. URL: https://uniqa.ua/storage/public-info/reports/Фінансова%20звітність%20УНІКА%20за%202023%20рік.pdf

5. ПрАТ «СК «УНІКА». Консолідована фінансова звітність за 2024 рік з аудиторським висновком. URL: https://uniqa.ua/storage/public-info/reports/Combined_FS_FY2024_UNIQA_Non-banking_group_with_auditors_report.pdf

6. Слоневська І. А. Економічна безпека підприємства: сутність, складові, механізм забезпечення : монографія / І. А. Слоневська. Львів : ЛНУ ім. І. Франка, 2021. 218 с.

7. Дьяків, В. І. Ризики в системі економічної безпеки підприємств / В. І. Дьяків, Т. В. Олійник // Економіка та держава. 2022. № 7. С. 55–59.

8. Мних, Є. В. Контроль і аудит у системі управління фінансовою безпекою / Є. В. Мних. Київ: КНЕУ, 2020. 276 с.

9. Офіційний сайт UNIQA Group (Австрія). URL: https://www.uniqagroup.com

10. Технології захисту інформації : навч. посіб. / [за ред. С. О. Дьякова]. Київ : Університет «Україна», 2020. 144 с.

ДОДАТКИ

Додаток А

Основні фінансові показники ПрАТ «СК «УНІКА» за 2023–2024 роки (тис. грн)

Показник	2023 рік	2024 рік	Динаміка, %
Страхові премії	2 641 987	3 201 481	+21,2%
Страхові виплати	1 201 112	1 495 847	+24,5%
Страхові резерви	2 189 088	2 432 617	+11,1%
Прибуток до оподаткування	188 541	209 343	+11,0%
Чистий прибуток	161 310	175 652	+8,9%
Загальні активи	3 940 285	4 432 079	+12,5%
Власний капітал	1 193 848	1 387 952	+16,3%
Частка виплат у преміях (%)	45,5%	46,7%	+1,2 п.п.

Додаток Б

Структура страхових премій за видами страхування (2024 рік)

Вид страхування	Сума, тис. грн	Частка у загальних преміях, %
Автострахування (КАСКО + ОСЦПВ)	1 432 517	44,7%
Медичне страхування	723 408	22,6%
Майнове страхування	521 903	16,3%
Інші види страхування	523 653	16,4%
Усього	3 201 481	100%