Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _Навчально-науковий центр заочної форми навчання_____
(повна назва)
Кафедра_економічної кібернетики та управління економічною безпекою____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти_____другий (магістерський)_____

____Організаційне забезпечення протидії ризикам у системі економічної____
_____безпеки підприємства_____
(тема)

Виконав:
студент _2_ курсу, групи УФЕБзм-20-1_____
_____Косінов А.Л._____
(прізвище, ініціали)

Спеціальність 073 Менеджмент_____
_____
(код і повна назва спеціальності)
Тип програми _освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма __Управління_____
фінансово-економічною безпекою_____
(повна назва освітньої програми)

Керівник __доц. Діденко Є.В._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ __Полозова Т. В.____
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет _Навчально-науковий центр заочної форми навчання_____
(повна назва)
Кафедра_економічної кібернетики та управління економічною безпекою____
(повна назва)
Рівень вищої освіти _другий (магістерський)_____
Спеціальність 073 Менеджмент_____
(код і повна назва)
Тип програми_освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма Управління фінансово-економічною безпекою_____
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«_____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові__Косінову Антону Леонідовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи_ Організаційне забезпечення протидії ризикам у системі економічної безпеки підприємства_____
_____
затверджена наказом по університету від 23 жовтня 2021 р. № _159 Стз_____
2. Термін подання студентом роботи до екзаменаційної комісії _14 грудня 2021 р._____
3. Вихідні дані до роботи Наукові інформаційні джерела, періодичні видання, теоретичні та методичні розробки вчених в області управління економічною безпекою підприємства, статистичні дані досліджуваного підприємства, інформаційні джерела_____
_____
_____
_____
_____
_____
4. Перелік питань, що потрібно опрацювати в роботі_____
Вступ. 1. Організаційні аспекти протидії ризикам у системі економічної безпеки підприємства. 2. Аналіз результатів господарської діяльності ТОВ «Ентерком». 3. Організаційне забезпечення протидії ризикам у системі економічної безпеки ТОВ «Ентерком». Висновки. Перелік джерел посилання. Додаток._____
_____
_____
_____
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій_____
1. Об'єкт, предмет, мета і завдання роботи. 2. Державне регулювання діяльності системи економічної безпеки макро- та мікрорівнів 3. Принципи функціонування системи економічної безпеки підприємства. 4. Класифікація небезпек, ризиків і загроз в економічній безпеці підприємства. 5. Зв'язок підприємства з загрозами. 6. Організаційна структура ТОВ «Ентерком». 7-8. Основні показники діяльності підприємства.9. Способи оцінки інформаційних ризиків. Заходи управління інформаційною безпекою. 10. Система вимог і правил управління інформаційною безпекою._____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Виконання першого розділу роботи	25.10.21-31.10.21	виконано
2	Виконання другого розділу роботи	01.11.21-15.11.21	виконано
3	Виконання третього розділу роботи	16.11.21-30.11.21	виконано
4	Оформлення роботи	01.12.21-05.12.21	виконано
5	Перевірка роботи на плагіат	06.12.21-08.12.21	виконано
6	Підготовка доповіді та ілюстративного матеріалу	09.12.21-10.12.21	виконано
7	Рецензування роботи	11.12.21-13.12.21	виконано
8	Подання роботи до екзаменаційної комісії	14.12.2021	

Дата видачі завдання _25 жовтня 2021 р._

Студент _____
(підпис)

Керівник роботи _____ __доц. Діденко Є.В._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота: 77 с., 15 табл., 8 рис., 54 джерела, 1 додаток.

ОРГАНІЗАЦІЯ, ПРОТИДІЯ РИЗИКАМ, КАДРОВІ РИЗИКИ, ІНФОРМАЦІЙНІ РИЗИКИ, ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКІ ЗАХОДИ.

Об’єктом дослідження є управління системою економічною безпекою підприємства.

Метою дослідження є теоретичне обґрунтування та розробка практичних рекомендацій з організаційного забезпечення протидії ризикам у системі економічної безпеки підприємства.

Розкрито зміст і принципи функціонування системи економічної безпеки підприємства. Класифіковано небезпеки, ризики і загрози в системі економічної безпеки підприємства. Проаналізовано можливі організаційні заходи протидії інформаційним і кадровим ризикам. Проаналізовано результати господарської діяльності ТОВ «Ентерком». Виявлено основні загрози та ризики підприємств ІТ-галузі. Запропоновано організаційно-методичне забезпечення оцінки інформаційних ризиків ТОВ «Ентерком». Розроблено організаційно-управлінські заходи щодо протидії інформаційним ризикам для досліджуваного підприємства.

ABSTRACT

Master thesis: 77 p., 15 tables, 8 fig., 54 sources, 1exhibit.

ORGANIZATION, COUNTER THE RISKS, PERSONNEL RISKS, INFORMATION RISK, INSTITUTIONAL AND MANAGEMENT ACTIVITIES.

The object of the research – management of the economic security system of the enterprise.

The purpose of the research – theoretical substantiation and development of practical recommendations for organizational support of risk management in the system of economic security of the enterprise.

The content and principles of functioning of the economic security system of the enterprise are revealed. Hazards, risks and threats in the system of economic security of the enterprise are classified. Possible organizational measures to counteract information and personnel risks are analyzed. The results of economic activity of «Entercom» LLC are analyzed. The main threats and risks of IT enterprises have been identified. Organizational and methodological support for information risk assessment of «Intercom» LLC is proposed. Organizational and managerial measures to counteract information risks for the researched enterprise have been developed.

ЗМІСТ

ВСТУП

У сучасних умовах розвитку економіки України загрози інтересам суб'єктів господарювання спричиняють реальні та потенційні умови, а також чинники внутрішніх та зовнішніх джерел небезпеки. Будь-яке підприємство, яке є частиною реальної економіки, буде вражено інфляцією, різким падінням валового внутрішнього продукту, падінням технологічного потенціалу країни, стагнацією в окремих галузях економіки, дефіцитом продовольчих ресурсів, а банківська система стане незбалансованою. Економічна криза та виклики світового рівня створили додаткове навантаження.

Значні ризики пов’язані з конфліктом інтересів суб’єктів господарювання та бізнес-середовищем, впливом деструктивних факторів на можливість реалізації цих переваг. Ці ризики зумовлені об’єктивними обмеженнями економічного середовища, але суб’єктивні інтерпретації їх можливих наслідків надають простір для прийняття рішень для управління корпоративною економічною діяльністю.

Дослідженню питань організаційного забезпечення протидії ризикам підприємства присвячено багато праць таких науковців, як О.Ф. Балацький, Т.В. Полозова, Л.В. Соколова, Є.В. Діденко, І.В. Колупаєва, І.А. Бланк, Т.В. Майорова, О.О. Ляхов, І.П. Мойсеєнко, А.А. Пересада та інших. Проте залишаються недостатньо вивченими процес і складові компоненти методів організації протидії ризикам, що обумовлює актуальність подальших досліджень.

Об’єктом дослідження є управління системою економічною безпекою підприємства.

Предметом дослідження є організаційне забезпечення протидії ризикам у системі економічної безпеки підприємства.

Метою дослідження є теоретичне обґрунтування та розробка практичних рекомендацій з організаційного забезпечення протидії ризикам у системі економічної безпеки підприємства.

Завдання дослідження:

– розкрити зміст і принципи функціонування системи економічної безпеки підприємства;

– класифікувати небезпеки, ризики і загрози в системі економічної безпеки підприємства;

– проаналізувати можливі організаційні заходи протидії інформаційним і кадровим ризикам;

– проаналізувати результати господарської діяльності ТОВ «Ентерком»;

– виявити основні загрози та ризики підприємств ІТ-галузі;

– запропонувати організаційно-методичне забезпечення оцінки інформаційних ризиків ТОВ «Ентерком»;

– розробити організаційно-управлінські заходи щодо протидії інформаційним ризикам для досліджуваного підприємства.

Інформаційною основою для проведення дослідження були наукові літературні джерела, періодичні наукові видання, законодавство України, фінансова звітність підприємства, що досліджується, відкриті джерела мережі Internet.

Під час виконання роботи були використані методи аналізу, синтезу, графічний, порівняння та узагальнювання, інтерпретація висновків.

Практична значущість отриманих результатів полягає у тому, що запропоновані практичні рекомендації можуть бути використані підприємствами ІТ-галузі для організації протидії ризикам.

Апробація результатів дослідження. Основні теоретичні положення і практичні результати проведених досліджень, висновки і рекомендації, які викладені в роботі, доповідались на ІІ Міжнародній науково-практичній конференції «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта» (Харків, 2021).

Публікації. Результати досліджень опубліковано у 2 наукових працях, у тому числі 1 стаття у колективній монографії, 1 тези конференції.

1 ОРГАНІЗАЦІЙНІ АСПЕКТИ ПРОТИДІЇ РИЗИКАМ У СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Зміст і принципи функціонування системи економічної безпеки підприємства

У сучасній науці існує кілька галузей в інтерпретації та побудові безпеки, а саме філософія, соціологія, право, математика тощо. Кожен із цих методів має свої специфічні обставини та логіку, що свідчить про значні розбіжності у думках. Для формування змісту методологічної основи екологічного комплексу вченими був обраний певний методологічний метод: системний, процесний або функціональний, що формує уявлення про опис системи та принципів, методів, технічних форм та засобів роботи, екологічний комплекс досліджень і концепцій.

Використання системних методів у дослідженнях є характеристикою сучасної економічної науки. У загальному розумінні система – це група взаємодіючих елементів. Більшість учених визначають системний метод ширше, а аналіз структури системи та форми її застосування значно складніші.

При визначенні поняття «система» пріоритет слід віддавати категорії взаємодії, яка розкриває взаємозалежність, взаємодію, взаємне проникнення, взаємозбагачення та заперечення елементів системи. Говорячи про структуру, доречніше говорити про взаємозв’язок між елементами системи та компонентами, що входять до складу елементів системи [1-5]. В умовах ринкової економіки суб’єкти господарювання, підприємства з різними системами власності та напрямами самостійно організовують власну виробничу, організаційну, операційну та фінансову діяльність, розробляють та впроваджують власні концепції виживання в ринковому середовищі, несуть відповідальність за організацію виробництва. діяльність. Робота

країни та чинне законодавство організовують процес забезпечення економічної безпеки бізнесу.

Система корпоративної економічної безпеки відноситься до організаційного комплексу, який складається з сукупності організацій, управління, технологій та законів, призначених для забезпечення корпоративної безпеки та захисту законних інтересів її керівництва та інвесторів та інші заходи для сприяння сталому розвитку. Як постійна наукова парадигма, система економічної безпеки підприємства має на меті виконання таких основних функцій: прогнозування, виявлення, попередження, пом'якшення небезпек і загроз, захист власності, створення сприятливого конкурентного середовища та усунення невідкладних втрат.

До загальної характеристики сучасної теорії системи економічної безпеки належать такі поняття: поняття економічної безпеки; стратегія системи економічної безпеки; комплексна система безпеки; власні ресурси; об'єкт системи економічної безпеки; основний орган системи економічної безпеки.

Вітчизняні вчені визначають зазначені поняття так: Концепція системи економічної безпеки є правдивим відображенням побудови, організації, управління та механізму економічної безпеки та розвитку підприємств.

Комплексна система економічної безпеки підприємства – це комплекс взаємопов’язаних організаційно-правових та матеріально-технічних заходів, призначених для захисту підприємства від реальних і потенційних загроз і ризиків, які можуть спричинити великі економічні збитки або затримати розвиток підприємства.

Ресурси підприємства – це сукупність усіх існуючих організаційних, матеріально-правових, фінансових, адміністративних, інтелектуальних та техніко-технічних можливостей підприємства, які покликані протистояти загрозам і ризикам, забезпечувати динамічний розвиток підприємства та досягати його цілей [6].

Іншими науковцями економічна безпека підприємства визначається як складність і неузгодженість процесів, що відбуваються у зовнішньому і внутрішньому середовищах підприємства, різноманітних загроз і ризиків, що супроводжують його ринкову діяльність, а також необхідність створення комплексної системи економічної безпеки [5-10].

Метою системи економічної безпеки підприємства є досягнення та підтримка такого стану об'єктів економічної безпеки, у якому підприємство може протистояти внутрішнім і зовнішнім загрозам і має здатність стабільно функціонувати та поступово розвиватися [5-10]. До основних цілей корпоративної економічної безпеки вчені та практики відносять визначення загроз, запобігання загрозам, нейтралізацію загроз, локалізацію загроз, знищення та виключення загроз.

У роботі [11] автори запропонували розглядати та вирішувати питання економічної безпеки підприємства на основі достовірності всієї інформації, системи зберігання, яка визначається рівнем безпеки найслабшої ланки. Вони дослідили, що метою комплексної системи економічної безпеки є стабільні економічні умови та розвиток підприємства зараз і в майбутньому.

Інвестиційна стратегія розглядається як система обраних довгострокових цілей і засобів досягнення цих цілей, які можуть бути реалізовані в інвестиційній діяльності підприємств. Початок створення нової системи економічної безпеки – це підготовка та складання концепції системи економічної безпеки підприємства.

Для вирішення мети та виконання завдання економічної безпеки підприємства необхідно визначити засоби безпеки. Отже, засіб забезпечення економічної безпеки – це комплекс заходів та організаційна система їх реалізації та контролю, за допомогою яких можна досягти найвищого значення рівня економічної безпеки підприємства.

Конкретні дії щодо створення та функціонування системи економічної безпеки підприємства включають кілька етапів, які дозволяють досягти

основної мети – комплексного захисту підприємства від різноманітних загроз.

На рис. 1.1 зображено державне регулювання системи економічної безпеки макро- та мікрорівнів [12-15].

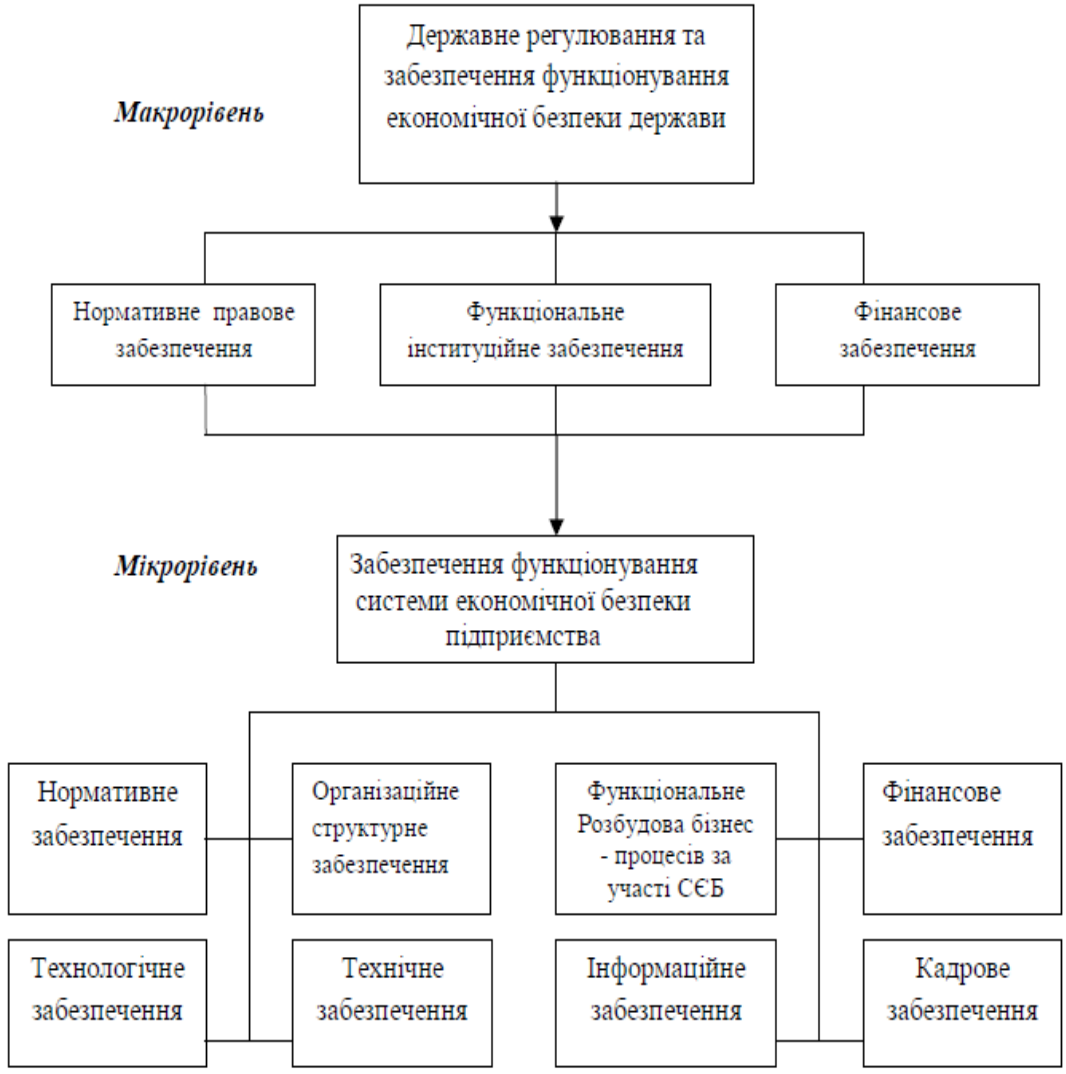

Рисунок 1.1 – Державне регулювання системи економічної безпеки на макро- та мікроівнях

Стратегічне планування та прогнозування економічної безпеки підприємства – це найважливішим етап забезпечення безпеки.

Комплексна система корпоративної безпеки – сукупність взаємозалежних організаційних, правових і технічних заходів, спрямованих

на зменшення та компенсацію реальних і потенційних, внутрішніх і зовнішніх корпоративних ризики та загрози спричиняють великі економічні збитки та перешкоджають або уповільнюють корпоративний розвиток [10].

Для реалізації своєї функції та виконання завдань, які ставить перед системою економічної безпеки, необхідно визначити спосіб її забезпечення. Засобом забезпечення економічної безпеки є комплекс заходів та системної організації та здійснення та контролю, за допомогою яких можна досягти найвищого значення рівня економічної безпеки підприємства. Ефективність і живучість економічної безпеки підприємства повністю залежать від злагодженості та системності механізму взаємодії різних елементів економічної безпеки підприємства.

На рис. 1.2 зображені принципи функціонування системи економічної безпеки підприємства [10-15].

Рисунок 1.2 – Принципи функціонування системи економічної безпеки підприємства

Інтеграція економічної безпеки підприємства в загальну систему підприємства та забезпечення безпеки функціонування та розвитку підприємства є важливим для концепції стабільності підприємства.

Якщо під впливом зовнішніх і внутрішніх факторів параметри системи не перевищують встановлену межу, тобто критичне значення, і забезпечують можливість компенсації впливу в межах конкретної межі, то система вважається стабільною. Цю ідею можна знайти в поясненні поняття «стабільність», пов'язаного з компанією – це здатність компанії підтримувати траєкторію розвитку, близьку до оптимальної (запланованої) в умовах постійних зовнішніх і внутрішніх негативних впливів.

На думку авторів у роботі [12], система економічної безпеки суб'єктів господарювання – це організована сукупність взаємопов'язаних елементів зовнішньої та внутрішньої безпеки суб'єктів господарювання, таких як спеціальні установи та служби, об'єкти, наукові методи, нормативно-правові бази, політики, стратегії, концепції, принципи, функції. Місія полягає у забезпеченні реалізації стратегічних і тактичних переваг суб'єктів господарювання та методах та інструментах захисту цих переваг від зовнішніх і внутрішніх загроз.

Аналіз способів виявлення змісту системи економічної безпеки суб'єктів господарювання свідчить про відсутність консенсусу щодо цього змісту, очевидні відмінності в суб'єкті, об'єкті системи та принципах формування. На практиці в системі економічної безпеки підрозділ, який інтегрує систему економічної безпеки в корпоративну структуру, має різні назви, організації та функціональні форми: служби безпеки, служби безпеки відповідно до покладених функцій, повноважень та матеріально-технічного забезпечення, відділ охорони, що обслуговує економічну безпеку.

Для формування успішної концепції економічної безпеки необхідно реалізувати стратегію економічної безпеки, що означає комплекс найважливіших рішень, покликаних забезпечити рівень безпеки

функціонування та розвитку комерційних суб’єктів [8]. Система корпоративної безпеки охоплює наукову теорію безпеки, стратегії та стратегії безпеки, методи та методи безпеки, концепції корпоративної безпеки [9]. Цілісність та ефективність економічної безпеки підприємства значною мірою залежить від існуючої законодавчої бази країни, матеріально-технічних і фінансових ресурсів, що виділяються особою, яка відповідає за підприємство, розуміння важливості безпеки підприємства кожного співробітника, а також знання та практичний досвід, що передбачають побудову та обслуговування самої системи [10].

Система безпеки підприємства – сукупність організованих спеціальних структур, засобів, методів і заходів для забезпечення безпеки діяльності підприємства від внутрішніх і зовнішніх загроз. Система корпоративної економічної безпеки – сукупність точок зору, ідей і цілей, спрямованих на забезпечення стабільної діяльності підприємств, включаючи заходи, методи та напрямки досягнення цілей, створення умов і умов для досягнення бізнес-цілей за невизначених обставин і запобігання (пом'якшення) внутрішніх і зовнішніх загроз [7].

Узагальнюючи погляди багатьох відомих вчених, сучасна стратегія економічної безпеки підприємства повинна включати: характеристики зовнішньої та внутрішньої загроз економічної безпеки; виявлення та моніторинг факторів короткострокової та довгострокової стабільності підприємства; визначення стандартів інтересів підприємства і показники вимог економічної безпеки і критичного значення, цілеспрямованість діяльності підприємств щодо реалізації стратегій економічної безпеки, розробка економічної політики та механізм взаємодії всіх компонентів системи підприємства для забезпечення економічної безпеки.

1.2 Класифікація небезпек, ризиків і загроз в системі економічної безпеки підприємства

Для будь-якої компанії, незалежно від її розміру чи сфери діяльності, завжди будуть загрози розвитку ззовні чи всередині компанії. Система економічної безпеки покликана захищати підприємство від зовнішніх і внутрішніх загроз, надійно захищати та ефективно використовувати його матеріально-фінансовий потенціал.

Тому необхідно розглянути природу основних визначень, що стосуються загроз економічній безпеці, і зазначити, що в широкому сенсі терміни «небезпека» та «загроза» можна розглядати як синоніми, а у вузькому – вони повинні бути обумовлені конкретними подіями, що поділяється на групу загроз для формування небезпеки.

У загальному розумінні небезпека – це об’єктивно існуюча можливість негативного впливу на соціальний організм, внаслідок чого соціальний організм може завдати будь-якої шкоди чи втрати, тим самим змінивши свій стан, або, як наслідок, його розвиток набуває негативних обертів чи параметри (характер, ритм, форма тощо) [12].

Джерела небезпека – це сукупність умов і факторів, які самі по собі містять і за певних умов самі або в будь-якій комбінації утворюють деструктивні (сукупність негативних впливів).

За тяжкістю можливих наслідків можна виділити наступні види небезпек:

– попередження – це набір ситуацій, які вимагають відповіді, не обов’язково загрозливих. Коли компанія або компанія не відповідає, попередження стає ризиком;

– ризик - це можливість того, що результат певного рішення або дії відхилиться від плану. Ці відхилення можуть бути пов’язані з їх додатковими

доходами та додатковими витратами. Ризики виникають принаймні в двох ситуаціях, які є двома чи більше можливими альтернативними результатами. Коли можливий лише один результат, ризику немає, тому що немає вибору [13]. Економічна безпека спрямована на усунення або зменшення ризику економічних втрат. Однак ніякі людські здібності не можуть усунути цей ризик. На практиці існують лише способи пом'якшити його вплив. Основним чинником господарської діяльності підприємства (компанії) є його вік. Чим довше існує компанія, тим менше ймовірність її збою;

– загрози – це навмисні або ненавмисні впливи, які дестабілізують компанію, завдають матеріальних і нематеріальних збитків і призводять до реальної можливості відхилення від стратегії.

У таблиці 1.1 наведена класифікація ризиків та загроз в економічній безпеці підприємства.

Таблиця 1.1 – Класифікація небезпек, ризиків та загроз в економічній безпеці компанії

Ознака	Вид
За можливістю прогнозування	Прогнозовані, що виникають за певних обставин, виявлені на підставі минулого досвіду, узагальнені галузевою наукою та закріплені в законах, стандартах, технічних умовах та іншій нормативній документації. Непередбачені – це форс-мажорні обставини, наукові технологічні досягнення й відкриття тощо
За джерелом походження	Об'єктивні, що виникають без участі суб'єктів системи (стан розвитку ринкової кон'юнктури, конкуренції, тощо). Суб'єктивні – навмисні або ненавмисні дії людей, органів влади або державних установ; конкурентна боротьба, злочинність тощо (що впливають на економічні відносини підприємства на ринку)
За можливістю запобігання	Форс-мажорні – відрізняються непереборністю впливу (природні катаклізми, техногенні катастрофи, війни, епідемії, які змушують вирішувати й діяти всупереч наміру) і представляють особливу складність запобігання бюджетними коштами. Передбачувані – можуть бути передбачені на стадії планування бізнесу для мінімізації або запобігання можливих збитків у випадку настання ризику

Продовження таблиці 1.1

За ймовірністю настання	Явні, очевидні, що обумовлені ринковими (економічними і юридичними) законами. Латентні – неявні, приховані, що важко виявляються.
За природою їх виникнення	Економічні - кон'юнктурні (ринкові) зміни. Політичні - зміна влади, введення ембарго. Правові – законодавче регулювання діяльності, ліцензування. Конкурентні – «чорний PR», недобросовісна конкуренція. Техногенні – аварії та катастрофи. Екологічні – виснаження ресурсів, кліматичні зміни; Контрагентські – невиконання зобов'язань, шахрайство
За значимістю або розміром збитку	Несуттєві – що не впливають на ринковий стан підприємства. Істотні – втрата значної частини матеріальних і фінансових ресурсів. Значні – втрата конкурентних переваг, можливе банкрутство. Катастрофічні – неможливе продовження господарської діяльності, неминуче банкрутство
За ступенем ймовірності	Неймовірні – при вкрай низькій ймовірності збігу обставин виникнення погрози. Малоймовірні – не вимагають планування превентивних заходів (як різновид форс-мажорних обставин). Імовірні – слабко прогнозовані (вимагають планування залежно від значимості збитку). Досить імовірні – прогнозовані, плановані й забезпечені бюджетом. Неминучі – легко прогнозовані, обумовлені природою виникнення, плановані й забезпечені бюджетом
За ознакою їх здійснення у часі	Безпосередні – з повною ймовірністю здійснення. Близькі (до 1 року) – прогнозовані та плановані. Далекі (понад 1 рік) – не передбачається поточним бюджетом.
За ознакою їх здійснення у просторі	На території підприємства. На території, що прилягає до підприємства. На території регіону. На території країни. На закордонній території.
За способами здійснення	Промислове шпигунство. Розкрадання. Вербування і підкуп персоналу. Психологічний вплив на персонал. Технологічний доступ тощо
За сферою виникнення	Внутрішні фактори, що пов'язані з господарською діяльністю підприємства і його персоналу. Зовнішні, що виникають за межами підприємства, пов'язані з кон'юнктурою ринку й середовищем функціонування підприємства

До найбільш небезпечних зовнішніх загроз, які можуть завдати шкоди компанії або перешкодити подальшій діяльності, належать [15-17]:

– нестабільне чинне законодавство. В Україні закони та нормативні акти часто суперечливі, часто змінюються та видаються заднім числом, що спричиняє суперечки між сторонами конфлікту з одного й того ж питання, що значно ускладнює стабільну роботу підприємства;

– недобросовісна конкуренція є очевидною формою корпоративної діяльності. Сюди входять: економічний шпигунство, підроблені конкуренти, шахрайство споживачів, шахрайство з бізнес-звітами, корупція тощо;

– зміни валютних курсів. Оскільки українська економіка доларизована, розрахунок здійснюється за такою схемою: долар-гривня-долар, то даному випадку обмінний курс впливає не тільки на імпортно-експортний бізнес компанії, але й визначає прибуток або збиток від їх імпорту. Зміна валютних курсів також впливає на експортний бізнес, діяльність якого зосереджена на внутрішньому ринку. Таким чином, бізнес-експортери виграють від зниження курсу національної валюти та його несприятливого зростання, а бізнес-імпортери виграють від підвищення курсу національної валюти та його несприятливого зниження;

– поява нових технологій (Інтернет), окрім своїх позитивних аспектів, це також джерело загроз для корпоративної економічної безпеки, зокрема: паролі доступу хакерів, крадіжка конфіденційної інформації, відмова в обслуговуванні, програми, керовані вірусами, та інші.

До типів внутрішніх загроз, які мають найбільший вплив на компанію, відносять:

– відсутність стабільних менеджерів середнього рівня. Рівень знань власника зазвичай нижчий, ніж у його підлеглих, а підлеглі в основному отримали професійну освіту;

– відсутність або поверхове ставлення до корпоративної маркетингової стратегії. Маркетинг – це системний механізм, що забезпечує довгострокову стратегічну стабільність і прибутковість компанії на ринку та покращує

економічну безпеку підприємства, а не засіб швидкого вирішення поточних проблем, на думку більшості керівників;

– забезпечення сировиною та комплектуючими. Ця проблема тісно пов'язана з такими проблемами, як недостатній попит на готову продукцію та збільшення взаємних непогашень за високою дебіторською заборгованістю.

– невизначеність цілей. Правильний вибір корпоративної місії – глобальна мета створення та функціонування компанії є запорукою успішного розвитку компанії;

– немотивована поведінка корпоративного персоналу, що в свою чергу призводить до зниження продуктивності.

На рисунку 1.3 зображено зв'язок підприємства з загрозами.

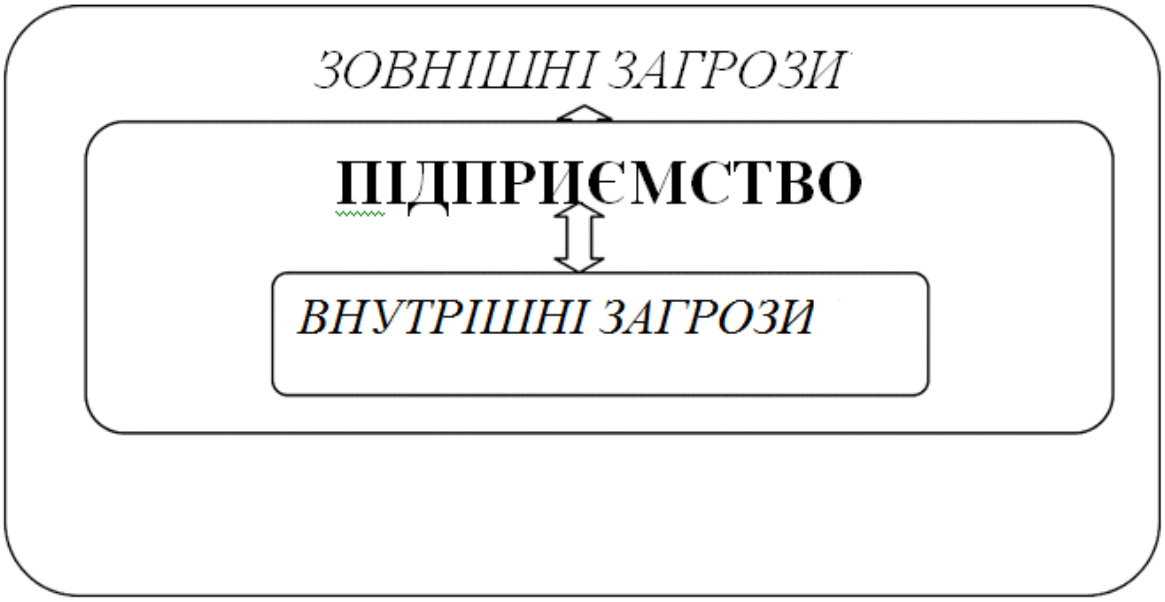

Рисунок 1.3 – Зв’язок підприємства з загрозами

Аналіз багатьох зовнішніх і внутрішніх загроз, напрямів і цілей їх дій, можливих наслідків для компанії доводить їх різноманітність. Вони різняться в залежності від виду корпоративної діяльності. Кожна компанія має власну систему загроз, характерну для цієї компанії. У зв’язку з цим основним

завданням керівників підприємств є виявлення найбільш небезпечних факторів відповідно до конкретної ситуації суб’єкта господарювання, формування системи заходів та своєчасного їх виявлення, запобігання чи пом’якшення.

1.3 Організаційні заходи протидії інформаційним і кадровим ризикам

Останнім часом у роботі успішних вітчизняних підприємств чітко простежується тенденція до широкого застосування сучасних технологій. Майже всі кадрові технології безпосередньо пов'язані із завданнями організації безпеки персоналу підприємства. Особливо – набір, тестування, моніторинг, дослідження думок команди, виявлення та співпраця з неформальними лідерами, звільнення.

Використовувана технологія відображається в реальній діяльності керівників, які приймають управлінські рішення щодо діяльності працівників та характеру організаційної роботи, що реалізує ці рішення.

Тому розроблення та впровадження певних процедур і заходів кадрових технологій є найбільш актуальним та ефективним засобом забезпечення безпеки персоналу підприємства.

На цьому етапі активно розвивається безпека персоналу, що також цікавить більшість підприємців, які впроваджують поступові, ефективні, наукові та розумні методи управління. Рівень впевненості відповідального за організацію у здібностях своїх співробітників залежить від безпеки персоналу, оскільки компанія не буде піддана ризику з вини співробітників.

Безпека персоналу є однією зі складових економічної безпеки бізнесу (та інших факторів – фінансів, влади, інформації, технологій і технологій, права, навколишнього середовища).

Відносно інших елементів системи безпеки компанії кадрова безпека є домінуючою, оскільки вона «працює» з працівниками, персоналом, а вони є в будь-якій головній складовій. Однак, визначаючи першість співробітників в організації, важливо відзначити, що саме співробітники становлять основну загрозу для компанії. За походженням ці загрози можна розділити на дві групи: внутрішні та зовнішні.

Класифікація внутрішніх загроз:

– недостатня кваліфікація персоналу;

– слабка організація системи управління персоналом;

– помилки в плануванні людських ресурсів;

– організація системи освіти слабка;

– неефективна система стимулювання;

– звільнення кваліфікованих робітників;

– відсутність політики компанії або «слабкість»;

– неякісні перевірки претендентів на роботу.

Зовнішні загрози включають:

– у конкурентів кращі умови заохочення;

– привести конкурентів до заманювання;

– тиск працівників ззовні;

– нехай співробітники потрапляють в різні види залежності;

– інфляційний процес (неможливо не враховувати при розрахунку заробітної плати та прогнозуванні її динаміки).

Важливим елементом безпеки персоналу на будь-якому підприємстві є ефективне управління персоналом.

Недостатність рівня системи управління персоналом може призвести до небажаних наслідків для підприємства, таких як:

– звільнення кваліфікованих працівників;

– недостатність або невідповідність кваліфікаційним вимогам працівників;

– знищення лояльності, що призводить до збільшення втрат, викликаних бездіяльністю і руйнуванням;

– зменшити кількість інноваційних пропозицій та ініціатив;

– співробітники позиціонуються для вирішення внутрішніх тактичних завдань, які не сприяють довгостроковому розвитку;

– захист власних інтересів співробітників і шкода загальним цілям підприємства [14].

Тому захист безпеки персоналу залежить від повноцінного використання функцій управління персоналом та формування та подальшої реалізації корпоративної кадрової політики. Безпосереднім засобом впливу на безпеку персоналу та її коригування є кадрова технологія управління персоналом.

Процес захисту компанії від небезпеки починається на етапі відбору працівників на наявні вакансії. І цей процес захисту продовжує існувати протягом усього періоду діяльності підприємства. Ефективність цього процесу забезпечується використанням різноманітних методів підбору персоналу.

При відборі кандидатів на вакантні посади ймовірність уникнути помилок становить: при використанні тесту – 45%. Лише персональні дані – 38%. Поведінкові інтерв'ю – 61%, неструктуровані інтерв'ю – 9%, центри оцінки – 87% [15].

Особливим видом перевірки є перевірка на поліграфі. Цей різновид тесту називається скринінгом (від англ. screening-просіювати), його суть

полягає у використанні складного технічного обладнання, призначеного для всебічної оцінки психологічних і фізіологічних особливостей досліджуваного для проведення комплексної процедури [16].

Основними причинами використання поліграфа є:

– підходить для будь-якого типу розслідування, дозволяючи швидко виявити брехню;

– надати додаткову інформацію, прямо чи опосередковано пов'язану з напрямком або метою розслідування;

– прискорити розслідування за відносно низьку вартість;

– об’єктивно та швидко оцінювати точність, потенційну достовірність та лояльність інформації, наданої кандидатами;

– дозволяє виявити приховані ознаки досконалості або загрозливих зловживань, а також інші фактори, які впливають на надійність співробітників.

Поліграф використовується для вирішення двох основних завдань: попередження та розкриття злочинів [17].

Сьогодні існує достатньо компаній, що спеціалізуються на діагностиці різноманітних якостей і особливостей людей за допомогою тестів. Слід зазначити, що цей тип тесту застосовний як до претендентів на конкретні посади, так і до тих, хто вже працює.

Серед багатьох таких компаній заслуговує на увагу MIDOT, яка розробила та постійно вдосконалювала інноваційні рішення для оцінки ризику порушення поведінки та зловживань співробітників на роботі.

Програма Midot System була створена командою ізраїльських психологів і поліграфів на основі 20-річних досліджень, її результати є найнадійнішими.

За допомогою системи Midot можна отримати відповіді на наступні питання:

– чи буде найнятий кандидат ефективним та успішним працівником?

– чи має працівник чи кандидат схильність до порушення дисципліни та зловживання владою, чи є ймовірність причетності до корупції та шахрайства на роботі?

Ядром рішення Midot System є алгоритм, який використовується для оцінки особистих моральних цінностей і моральних суджень, а не професійних оцінок, що забезпечує основу для прогнозування тенденцій поведінки. Система Midot може покращити якість оцінювання кандидата та значно скоротити час і вартість його навчання. Якщо кандидат чесний, порядний і надійний, має сенс продовжувати вивчати його професійні якості.

Технологія використання системи Midot для перевірки кандидатів така: кандидат «спілкується» з комп'ютерною програмою протягом 20 хвилин, а роботодавець в реальному часі отримає оцінку його чесності та надійності. Також надається рекомендація щодо професіональних здібностей кандидата та доцільність прийняти його на вакантну посаду. Результатом є відповідь на перше і дуже важливе запитання: чи є людина, яка претендує на вакансію, чесною та порядною, чи може вона працювати в одній команді з ним?

На відміну від поліграфа Midot дозволяє боротися з потенційними загрозами замість минулого досвіду.

Однак правильний підбір претендентів на роботу – це лише початок системи захисту персоналу компанії. Контроль необхідний, він дозволяє своєчасно отримувати інформацію та своєчасно проводити профілактичні заходи.

Періодична оцінка або атестація персоналу – це процедура, яка може використовувати сучасні технології контролю. Використовуючи методологію оцінки та сертифікації співробітників Midot, понад 600 компаній по всьому світу успішно вирішують питання безпеки персоналу та аналізу ризиків. Вони на 90% розуміють, де, що і чому це сталося.

Це системний підхід, який дозволяє вирішувати складні аналітичні завдання: відстежувати зміни в поведінці співробітників, виявляти структурні підрозділи, які є джерелом загроз, шукати помилки керівництва. З Midot роботодавець «покаже» брехуна, а лояльний співробітник просто підтвердить свою лояльність. [18].

Ефективно боротися з шахрайством та крадіжками співробітників допоможе запровадження підприємствами та компаніями технологій безпеки персоналу, таких як «гарячі лінії».

Організація «гарячої лінії» по боротьбі з шахрайством дозволить збирати інформацію про факти скоєних співробітниками компанії злочинів від колег та клієнтів. Це відкритий вихідний код. Це повністю конфіденційно і нейтрально – отримання та обробка інформації здійснюється фахівцями, які не працюють на компанію і не мають жодного відношення до своїх співробітників.

Заслуговує на увагу і розширена система управління персоналом Extended DISC. Це комп'ютерна програма, яка дозволяє визначити особистісні особливості співробітників для виконання конкретних завдань. Розширена система управління персоналом Extended DISC описує характер або поведінку природної реакції людини в різних ситуаціях, що дозволяє людині зрозуміти поведінку себе та інших, уникнути проблем у спілкуванні та досягти успіху в роботі та житті.

Розширена система управління персоналом Extended DISC може вирішити наступні кадрові проблеми:

– швидко і точно підбирати співробітників на конкретні роботи;

– урахування особистих особливостей працівників для їх мотивації;

– хто і чому повинен навчатися в інтересах компанії;

– створити злагоджену робочу пару або групу;

– сформувати хорошу психологічну атмосферу в колективі [19].

Використання цих технологій має враховувати фінансові можливості, культурні особливості та пріоритети розвитку підприємства.

Дослідження дозволило зробити висновок, що сучасна кадрова технологія є новим елементом організаційного менеджменту, якщо її не впровадити, то неможливо буде забезпечити досягнення рівня безпеки персоналу на підприємстві.

Ефективне використання кадрових технологій дозволяє вирішити багато важливих завдань безпеки персоналу підприємства:

– виявлення та запобігання загрозам, пов'язаним з персоналом: їх протиправною діяльністю, розголошенням «комерційної таємниці», змовою з конкурентами, нанесенням прямого збитку підприємству, створенням негативної морально-етичної та психологічної атмосфери в колективі;

– збирати та обробляти інформацію про майбутніх співробітників, щоб відповідальна особа могла прийняти рішення про прийняття на роботу чи відмову;

– збирати та обробляти інформацію про співробітників для подальшого прийняття рішення, чи приймати вони конфіденційну інформацію, чи брати участь в особливо важливих проектах компанії;

– розглянути соціально-психологічні чинники в процесі управління персоналом, вивчити психологічний клімат робочої сили та взаємовідносини між працівниками;

– проводити службові розслідування у справах, які виявляють факти діяльності працівників, що загрожують безпеці підприємства;

– виявити потенційні «зони ризику» серед співробітників і співробітників, які працюють у компанії-людей, які в деяких випадках можуть нашкодити компанії;

– отримати інформацію для проблемних управлінських рішень: оцінка кандидатів на вакансію, коригування політики стимулювання, розвиток та

утримання ключових співробітників, аналіз лояльності співробітників, оцінка корпоративної культури, структурні підрозділи для виявлення джерел загроз, помилок управління.

Забезпечення інформаційної безпеки є одним із головних завдань сучасних підприємств. Загрозою може бути не тільки технічний збій, а й невідповідність даних в різних системах обліку, таку ситуацію зустрічає практично кожна компанія, а також необмежений доступ співробітників до інформації.

Інформаційний ризик – це ризик втрати або пошкодження, спричинений використанням компанією інформаційних технологій. Іншими словами, IT-ризики пов’язані зі створенням, передачею, зберіганням та використанням інформації за допомогою електронних засобів масової інформації та інших методів комунікації.

Інформаційна безпека існує не для того, щоб обмежувати право користувачів на доступ до інформації та забороняти їм спілкуватися через ICQ. Безпека повинна допомогти організаціям уникнути деяких ризиків, пов’язаних із витоком важливої інформації, приймати неправильні управлінські рішення на основі спотворених даних та спричиняти часткову непрацездатність через збої інформаційної системи. З цієї причини необхідно визначити найбільш уразливі місця в операції обробки даних, повністю оцінити ризики та запропонувати методи мінімізації ризиків. При цьому запропоновані способи зазвичай не обмежуються конкретними засобами захисту.

Інформаційний ризик включає всі ризики, пов’язані з ризиком втрати або пошкодження, спричиненого використанням підприємством інформаційних технологій.

Не тільки технічні збої, але й невідповідність даних у різних системах, а також необмежений доступ співробітників до інформації можуть становити

загрозу. Отже, інформаційний ризик пов’язаний із створенням, передачею, зберіганням та використанням інформації в електронних носіях та інших способах комунікації.

ІТ-ризики можна розділити на дві категорії (рис. 1.4):

– ризики, викликані витоком інформації та використанням її конкурентами або співробітниками в цілях, які можуть зашкодити бізнесу;

– технічні збої програмного та апаратного забезпечення, каналів передачі інформації тощо можуть призвести до ризику втрати.

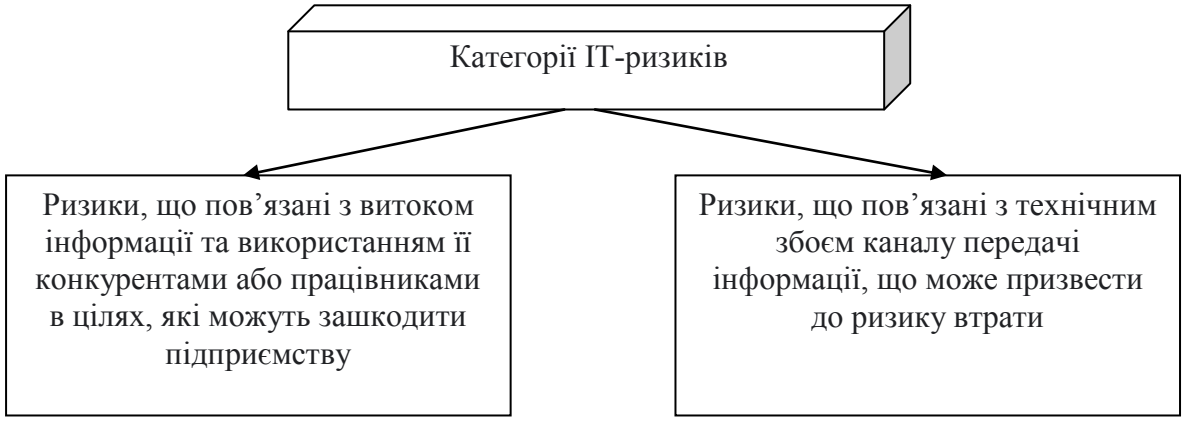

Рисунок 1.4 – Категорії ІТ-ризиків

Щоб оцінити ризик інформаційної системи організації, безпека кожного цінного ресурсу визначається шляхом аналізу загроз, які впливають на конкретні ресурси, і вразливостей, які можуть реалізувати ці загрози. Оцінити ймовірність реалізації загроз, пов'язаних з цінними ресурсами, та ступінь впливу реалізації загроз на ресурси, а також проаналізувати інформаційний ризик організаційних ресурсів. Для оцінки інформаційного ризику необхідно проаналізувати всі загрози, які впливають на інформаційну систему, та вразливості, які можуть бути реалізовані. На основі даних, внесених власником інформаційної системи, можна побудувати модель загроз і вразливостей, пов’язаних з інформаційною системою компанії. На

основі отриманої моделі аналізується ймовірність реалізації загроз інформаційної безпеки кожного ресурсу і на цій основі розраховується ризик, що підвищує рівень інформаційної безпеки комп'ютерної системи.

Завдання мінімізації IT-ризиків полягає в запобіганні несанкціонованого доступу до даних, а також аварій і збоїв устаткування та програмного забезпечення.

Процес мінімізації IT-ризиків слід повністю розглянути, відповівши на такі запитання:

– чи може підприємство контролювати доступ до інформаційних систем, які формують та зберігають фінансову звітність?

– чи отримали клієнти компанії необхідну інформаційну підтримку, тобто чи можуть вони зателефонувати в компанію або зв'язатися електронною поштою у відповідний час?

– чи може компанія інтегрувати існуючі технології для роботи за короткий проміжок часу, чи може вона отримувати інформацію з систем компанії та які з них є об'єктами злиттів і поглинань? Наприклад, компанія має одну або кілька систем обліку, за допомогою яких фінансисти отримують дані зведених звітів. При покупці нового бізнесу виявляється, що у нього інша система обліку. Тому компанія повинна мати чіткий план перетворення таких звітів у стандарти, прийняті материнською компанією. Інакше він може втратити оперативний контроль над ситуацією;

– чи дозволяє організація документообігу підприємства в існуючій системі продовжити його діяльність у попередньому режимі у разі звільнення ключового працівника? Це питання надзвичайно актуальне для українських компаній, адже навіть фінансова та бухгалтерська інформація часто вводиться та зберігається в будь-якій формі, не кажучи вже про інформацію про клієнтів. Це призводить до збільшення часу для нових співробітників для «введення» справи та збільшення ймовірності помилки;

– чи захищені права інтелектуальної власності компанії та її клієнтів?

– чи має компанія чіткий алгоритм дій у надзвичайних ситуаціях, таких як збої комп’ютерної мережі чи вірусні атаки?

– чи відповідає інформаційна система загальним цілям компанії? (Якщо завдання компанії – мати спільний центр управління грошовими потоками, а системи обліку, встановлені в різних філіях, не пов’язані між собою, це завдання не буде вирішено).

Це питання надзвичайно актуальне для компаній, адже навіть фінансово-бухгалтерська інформація часто вводиться і зберігається в будь-якій формі, не кажучи вже про клієнтську та іншу інформацію. Це призводить до того, що нові співробітники мають більше часу на «вхід» у справи та збільшують ймовірність помилок.

Важко визначити потенційні втрати більшості IT-ризиків, але їх можна приблизно оцінити.

Досвід багатьох компаній показав, що найуспішніші стратегії запобігання IT-ризикам базуються на трьох основних правилах:

– доступ співробітників до інформаційних систем і файлів компанії повинен відрізнятися залежно від важливості та конфіденційності вмісту файлів;

– компанія повинна контролювати доступ до інформації та забезпечувати захист вразливих місць в інформаційній системі;

– інформаційні системи, які безпосередньо впливають на діяльність компанії (канали зв'язку, файли документів, комп'ютерні мережі, що мають важливе стратегічне значення), повинні мати можливість безперебійно працювати навіть у кризових ситуаціях або швидко розгортатися в разі форс-мажорних обставин на інших об'єктах.

Для забезпечення необхідного захисту від IT-ризиків та контролю безпеки можна вжити таких заходів:

– визначити коло персоналу, відповідального за інформаційну безпеку;

– сформулювати положення, що описують дії співробітників компанії для запобігання IT-ризикам;

– забезпечити резервні можливості для роботи в надзвичайних ситуаціях;

– розробити стандарт єдиної інформаційної системи всередині організації, тобто перейти до єдиної форми звіту, і єдине правило розрахунку показників, які будуть використовуватися у всіх програмних продуктах компанії;

– класифікувати дані за ступенем конфіденційності та розрізняти права доступу до них;

– переконайтеся, що будь-які документи, що циркулюють в організації, створені за допомогою системи, централізовано встановленої на комп'ютері. Установка будь-якої іншої програми повинна бути авторизована, інакше ризик збою і вірусної атаки різко зросте;

– запровадити засоби контролю для моніторингу стану всіх систем компанії: якщо відбувається несанкціонований доступ, система повинна автоматично заборонити вхід або попередити про небезпеку, щоб співробітники могли вжити заходів;

– розробити та створити систему, яка дозволяє швидко відновити працездатність вашої IT-інфраструктури в разі технічного збою.

Крім цих заходів, необхідно також підготуватися до наслідків можливої кризи та описати дії, які компанія здійснила для подолання кризи.

Важливими кроками для аналізу інформаційних ризиків є:

– аналізувати сценарії, коли у внутрішню інформаційну мережу проникає третя сторона або особа, яка не має відповідних повноважень співробітника компанії, та проводити навчальні заходи для формування

моделі поведінки співробітників, відповідальних за інформаційну безпеку в кризових ситуаціях;

– розробити варіанти вирішення кадрових питань, включаючи турботу про ключових співробітників, наприклад, підготовку та ознайомлення співробітників з планом управління безперервністю компанії;

– підготувати запасні інформаційні потужності (сервери, комп'ютери) та резервні лінії зв'язку.

Якщо бізнес компанії значною мірою залежить від стану її інформаційної мережі (наприклад, компанія, яка займається розробкою комп’ютерних програм), необхідно призначити особу, відповідальну за формулювання, впровадження та моніторинг правил компанії, спрямованих на скорочення IT-ризиків.

Вважається, що найбільш об’єктивними людьми в організації діяльності з управління ризиками будуть працівники, які безпосередньо не задіяні в інформаційних технологіях. Його продуктивність слід оцінювати за допомогою вимірюваних показників, наприклад, час на усунення несправностей сервера не повинен перевищувати 30 хвилин або частота таких збоїв не повинна перевищувати двох разів на рік.

Передумовою успішного управління ризиками у сфері інформаційних технологій є його безперервність. Тому IT-ризики слід оцінювати на регулярній основі (наприклад, щоквартально), а плани слід розробляти та оновлювати, щоб мінімізувати їх. Регулярні перевірки (інформаційні аудити) системи управління інформацією незалежними експертами в подальшому допоможуть мінімізувати ризики.

Тому, якщо рекомендовані стандарти та правила зловживаються, наприклад, якщо співробітники не навчаються додаткам і не розуміють їх важливості, то розробка та впровадження політик, що мінімізують IT-ризики, не допоможуть. Тому робота із забезпечення IT-безпеки має бути комплексною та продуманою.

2 АНАЛІЗ РЕЗУЛЬТАТІВ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ ТОВ «ЕНТЕРКОМ»

2.1 Загальна характеристика діяльності підприємства

ТОВ «Ентерком» створено в 2011 році. Зараз у компанії працює 12 працівників, деякі з яких сертифіковані Google.

Діяльність компанії спрямована на 2 сегменти ринку, а саме на навчальні центри (консалтинг малого бізнесу та лідогенерація) та роздрібну торгівлю ювелірними виробами.

На рис. 2.1 наведена організаційна структура ТОВ «Ентерком»

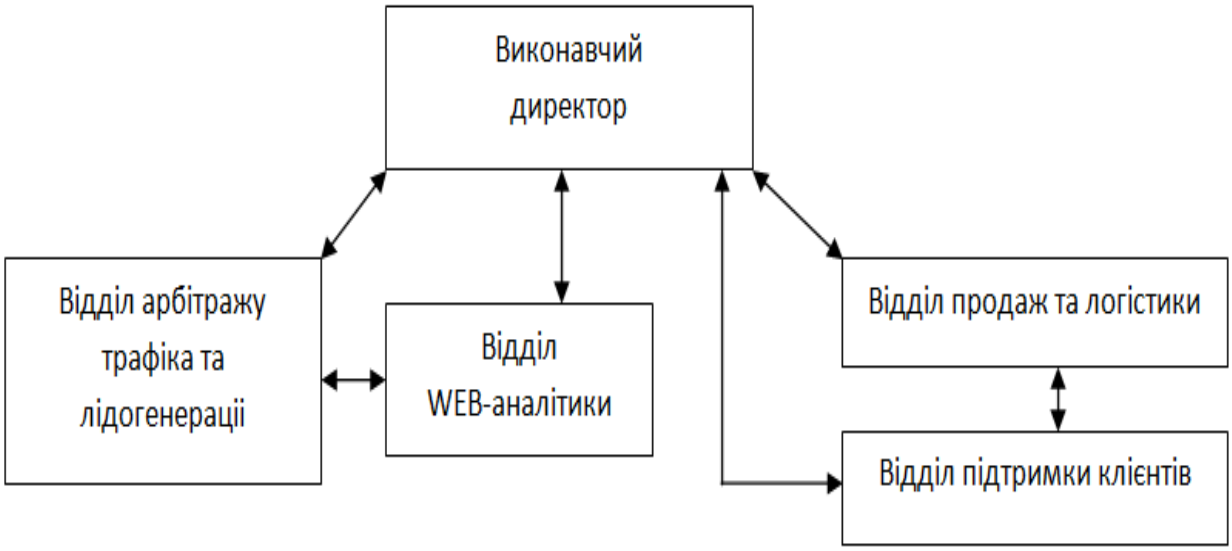

Рисунок 2.1 – Організаційна структура ТОВ «Ентерком»

Генеральний директор визначає, формулює, планує, реалізує та координує всю діяльність компанії.

Його завдання: визначати напрям розвитку компанії, спрямовувати діяльність співробітників на досягнення високих економічних і фінансових

результатів, представляти компанію в органах державної влади та відносинах з партнерами.

Відділ арбітражу трафіку та розвитку потенційних клієнтів регулярно генерує клієнтів і виконує процедури пошуку та тестування нових джерел трафіку. Цей відділ є ключовою ланкою в будь-якому Інтернет-бізнесі. Оскільки немає постійного покоління клієнтів, Інтернет-бізнес не може працювати та постійно розвиватися.

Відділ WEB-аналізу відповідає за вимірювання клієнтської привабливості та зручності (доступності) зовнішніх каналів для всіх ресурсів, що належать компанії. Усі ці точки контролюються, але щоб ними керувати, потрібно побудувати систему ключових індикаторів KRI для кожного каналу окремо та в цілому, адже потрібно знати, які з них ефективні, а які неефективні.

Відділ збуту та логістики займається такими питаннями:

– виклик «гарячих» клієнтів, тобто клієнтів, які входять у воронку продажів, що формується арбітражним відділом;

– існуючий номер телефону клієнта та пропозиція Ullsell;

– «холодні» мелодії для чужої клієнтської бази;

– надіслати фізичний об'єкт кінцевому покупцю через «НОВА ПОШТА»;

– викуп контролюється, дзвіночок не викупляє.

Завдання відділу підтримки:

– підтримка існуючих клієнтів;

– відкриті можливості навчання для клієнтів;

– надавати консультації з місцевих питань;

– консультація в онлайн-чаті.

2.2 Аналіз основних показників діяльності підприємства

Оскільки компанія має два напрямки (продаж інформаційних курсів/навчань; продаж матеріальних товарів), то техніко-економічні показники кожного напряму найкраще відображати окремо.

У таблиці 2.1 та таблиці 2.2 наведено основні показники корпоративної інформації про продажі (у двох частинах).

Таблиця 2.1 – Ключові показники ТОВ «Ентерком» (фрагмент 1)

Трафік, осіб	Підписники, осіб	Відписались, осіб	Дохід, грн	Повернення, грн	Ліди, осіб	Клієнти, осіб
20884	2076	595	328 457	23000	132	92
4105	1833	722	441 900	54000	139	75
8147	1031	338	297 932	13879	105	77
7493	1046	301	499 500	49987	135	75
3377	313	22	97150	-	32	22
2467	241	229	92856	-	27	13
7544	554	168	60353	-	38	22
4920	292	275	51191	14300	26	16

Таблиця 2.2 – Ключові показники ТОВ «Ентерком» (фрагмент 2)

Вартість, грн	Апсел, шт.	Відмова, шт.	Клієнти (нові), осіб	Вкладено в рекламу, грн	ROI, %
380,43	12	6	64	35000	
445,2	15	17	64	33444	
454,54	4	11	60	35000	751
466,66	8	25	57	35000	1327
273	3	10	4	6000	1519
769	6	14	5	10000	829
-	3	16	2	5250	1050
326	3	10	1	5210	608

З таблиці 2.1 видно, що одним із основних ключових показників є «трафік». Будь-який інтернет-бізнес побудований на цьому показнику, тому що без трафіку не буває клієнтів.

Важливим моментом є відстеження якості трафіку, адже цей етап економить більшу частину витрат на рекламу.

Крім того, важливим показником є кількість передплатників, адже це другий етап воронки продажів, де фільтрується трафік, а цільова аудиторія все ще існує.

Моніторинг кількості Upsell-лів (додаткових продажів) дуже важливий, адже запорукою успішного бізнесу є не продажі «чоло», а монетизація віддалених клієнтів.

Звичайно, найважливішим показником є ROI (рентабельність інвестицій), оскільки на основі цього показника ви повинні судити про прибутковість компанії на даному етапі.

Відстеження метрики типу «аналіз льоду» важливе, воно дозволяє відстежувати цикл клієнтів, точніше відстежувати, коли абонент стає клієнтом, і скільки з ним контактів.

У таблицях 2.3, 2.4 і 2.5 приведена метрика відстеження життєвого циклу ліда (таблиця складається з трьох фрагментів).

Таблиця 2.3 – Метрика відстеження життєвого циклу ліда (фрагмент 1)

№	ПІБ	Канал	e-mail
6905	Валерій	-	web-analiz-spb@ukr.net
6904	anatoliy	-	promotionpublik@gmail.com
6903	Галина Дичева	-	galdiva7gmail.com
6902	Захаров Валерій	-	GoldenGen@gmail.com
6901	Віктор	-	victor_bell@gmail.com
6900	Хромов Ігор	arweb2 (arweb-vk2)	sintegma@gmail.com
6899	Тимур	Відео-курс «Арбітраж трафіка на два млн»	ok52@gmail.com

Таблиця 2.4 – Метрика відстеження життєвого циклу ліда (фрагмент 2)

Дата підписки	Дата оплати	Ціна	Назва продукту	Новий	Канал
28.07.2020 14:06:22	04.12.2020 21:01:00	2469	«Google КМС на млн» BASE	ні	http://freedombiz.ru/odnostr3/
03.12.2020 21:05:09	04.12.2020 21:01:00	6663	«Google КМС на млн» PRO, «Таргет ВК на млн»	так	ibase2-arweb-auto
-	04.12.2020 21:00:00	2469	«Google КМС на млн» BASE	так	-
13.10.2020 17:56:21	04.12.2020 21:00:00	2469	«Google КМС на млн» BASE	ні	-
08.09.2020 14:25:45	04.12.2020 20:55:00	5382	«Google КМС на млн» PRO	ні	-
17.10.2020 13:49:20	04.12.2020 20:54:00	2469	«Google КМС на млн» BASE	ні	arkur_yandex_%D0%B0
08.07.2020 17:43:51	04.12.2020 20:29:00	130	Відправив лист, не відповідає	ні	Вигідна партнерська програма
13.10.2020 17:46:07	02.12.2020 21:26:00	5565	Швидка 1000$ в арбітражі 2.0 – PRO	-	-
08.07.2020 17:43:12	02.12.2020 21:25:00	2599	Швидка 1000$ в арбітражі 2.0 - BASE	-	arweb2
-	02.12.2020 21:18:00	5858	Швидка 1000$ в арбітражі 2.0 - PRO	-	-

Таблиця 2.5 – Метрика відстеження життєвого циклу ліда (фрагмент 3)

Взагалі відкрито листів	Кількість кліків у листах	Кількість пройдених каналів	Днів пройшло від підписки до купівлі	Остання листівка до факту купівлі продукту
45	65	3	22	*Менше Години До Старта «Швидка 1000$ В CPA і Арбітражі»
-	-	-	-	*Менше Години До Старта «Швидка 1000$ В CPA і Арбітражі»
72	23	1	129	
15	5	4	1	*Менше Години До Старта «Швидка 1000$ В CPA і Арбітражі»
23	1	1	52	2 Години До Старта Першого Вебінара По Google КМС!

За допомогою наведеної вище таблиці можна відстежити, з якого технічного каналу приходить абонент, і на основі отриманих даних збільшити трафік до каналу з найбільшою кількістю передплатників.

Також можна відстежувати кількість контактів клієнтів та їхню діяльність, а також середній час конверсії від передплатника до клієнта.

Одним із ключових моментів є відстеження аналізу вебінару для кожного курсу/тренінгу.

У таблиці 2.6 наведені основні вебінарні метрики на тренінг по лідогенерації.

Таблиця 2.6 – Основні вебінарні метрики на тренінг по лідогенерації

Дата проведення	06.09.2020	14.09.2020
Канал	Все	Все
Трафік	1707	1312
Із трафіка в підписники, %	10,13	5,72
Підписники	173	75
Підписники не активні	12,00	0,00
З підписника в учасника, %	40,46	81,58
Люди в ефірі	70	62
Старі	75	0
Нові	30	15
Ліди	2	5
Конверсія з ефіра в лід, %	2,86	4,84
ROI, %	1073.33	474.5
Грошей вкладено	1200	3600
Грошей від лідів	VIP 30 000	
Грошей отримано (по факту)	14080	20682
Середній чек		4134
Вартість кліка	0,70	2.84
Вартість підписника	6.94	48
Вартість ліда	600	720

В таблиці 2.7 і таблиці 2.8 приведені основні метрики товарних офферів (2 фрагменти).

Таблиця 2.7 – Основні метрики товарних офферів (фрагмент 1)

Період	Ліди	Клієнти	Хости	CR, %	%, клієнт/ лід	Витрати, грн.	Сума замовлень, грн.	Оплачено, шт.	Невикуп, шт.
Вересень	421	185	18751	2,25	43,94	4 745	29 497	185	45
Жовтень	698	295	71064	0,98	42,26	25 380	52 086	295	29
Листопад	604	312	90265	0,67	51,66	35 787	86 681	290	15
Грудень	536	355	57479	0,93	66,23	51 316	111 246	162	1

Таблиця 2.8 – Основні метрики товарних офферів (фрагмент 2)

Факт, грн	Прибуток, грн	Вартість ліда, грн	Прибуток з ліда, грн	Середній чек	Прибуток/клієнт, грн	% Викупу	ROI, %
29 497	6 437	11	70	159	159	100,00	105
52 086	23 151	36	75	177	177	100,00	126
80 973	43 011	59	134	278	260	92,95	117

У таблиці 2.8 відстежуються всі ключові економічні показники.

Відстеження клікабельності рекламних матеріалів (банерів, трейлерів) також дуже важливо.

У таблиці 2.9 наведено показники конверсії рекламних матеріалів Google KMC (07.12.2020).

Таблиця 2.9 – Метрики по конвертаційному рейтингу промо-матеріалів для Google KMC (07.12.2020)

1_300x250	3_300x250	500x200	butt_300x250	flag_728x90	hand_300x250	steel_728x90	yell_300x250	yello_728x90
-	-	-	-	-	-	-	1	-
-	-	-	1	-	-	1	1	-
-	-	6	-	-	1	1	-	-
-	-	-	-	-	-	1	1	-
2	6	-	-	1	1	1	-	2
-		-	-	-	-	-	1	-
2	6	6	1	1	2	4	4	2

За допомогою цієї таблиці можна зробити висновки про ефективність та розміри тих чи інших рекламних матеріалів.

У таблицях 2.10 та 2.11 наведено основні показники каналу генерації трафіку (2 сегменти).

Таблиця 2.10 – Основні метрики каналів генерації трафіка (фрагмент 1)

Назва каналу	Трафік, осіб	Ліди , шт	%, лідів	Клієнтів, осіб	% підтверджених лідів
cpawall	3430	76	2,22	28	36,84
kadam	8700	36	0,41	10	27,78
mgid	12335	73	0,59	28	38,36
Yottos	9406	75	0,80	45	60,00
noname	9700	43	0,44	21	48,84

Таблиця 2.11 – Основні метрики каналів генерації трафіка (фрагмент 2)

Вартість ліда, грн	Середній чек	Витрати на рекламу, грн	Очікуваний дохід, грн	Фактично надійшло, грн	ROI %
42,11	257	3200	7186	7186	125
30,58	129	1101	1289	1289	17
116,16	281	8480	7862	7065	-17
88,12	317	6609	14285	13986	112
0,02	297	1	6243	5700	569900

З таблиці 2.10 ви можете відстежити, скільки людей перебуває на цільовій сторінці за певний період часу, скільки з них стає потенційними клієнтами, відсоток глядачів, які перетворилися на потенційних клієнтів, і рентабельність інвестицій у певний канал. Після ознайомлення з такою інформацією зробіть висновки та коригування щодо перенаправлення глядачів (трафіку).

У таблиці 2.12-2.14 наведено основні економічні показники (3 сегменти) на щоденній основі.

Таблиця 2.12 – Основні економічні показники по дням (фрагмент 1)

Результат	Ліди, осіб	Клієнти, осіб	Хости, осіб	CR, %	%, клієнт/ лід	Витрати, грн	Сума підтверджених замовлень, грн	Очікуваний прибуток, грн
1	29	25	2971	0,98	86,2	2 699,0	7 882	4 945,4
2	24	19	1769	1,36	79,2	2 130,0	6 561	4 233,2
3	40	23	4740	0,84	57,5	3 898,0	7 455	3 332,2
4	61	46	6519	0,94	75,4	3 675,0	14 711	10 592,5
5	37	28	4269	0,87	75,7	4 256,0	8 442	3 931,5
6-7	90	50	9480	0,95	55,6	6 195,0	14 803	8 161,7
Разом	281	191	29748	0,94	68,0	22 853,0	59 854	35 196,4

Таблиця 2.13 – Основні економічні показники по дням (фрагмент 2)

Оплачено, шт.	Фактично надійшло, грн	Прибуток, грн
18	5611	1 578
33	11124	7 202
17	5253	870
32	9921	3 486
132	42914	19 071

Таблиця 2.14 – Основні економічні показники по дням (фрагмент 3)

Вартість ліда, грн	Прибуток з ліда, грн	Середній чек, грн	Прибуток з клієнта, грн	% Викупа
93	200	315	232	73,45
89	217	345	275	79,50
97	140	324	244	75,26
60	182	320	242	75,62
115	142	302	188	62,22
69	110	296	198	67,02
81	153	313	225	71,70

З наведеної вище таблиці можна щоденно відстежувати всі основні ключові показники.

Тривале зберігання таких форм дозволяє точно відстежувати приплив нових клієнтів, коливання середніх чеків клієнтів тощо.

2.3 Основні загрози та ризики підприємств IT-галузі

Кадровий ризик – цей вид ризику виникає з появою співробітників. Вони включають можливість виникнення трудових спорів, а також зловживання працівника (наприклад, крадіжка, переведення клієнтів тощо). Крім того, одним з основних ризиків у цій сфері є переміщення людей.

Податковий ризик – до цієї групи входять ризики, пов'язані з можливими помилками в податковому обліку, спричиненими умислом або недбалістю підприємця. Позов до нього може бути пов'язаний із зловмисністю контрагента, визначеною податковим органом. Втім, бувають випадки, коли інспектори самі помиляються, але й рясніють податковими претензіями підприємців.

Ризик контракту відноситься до ризику, що виникає в результаті господарської діяльності. Вони передусім включають можливе невиконання компанією та її підрядниками договірних зобов’язань. Вони проявляються у появі боргів, судових процесів, претензій.

Ризик порушення – в даному випадку це порушує законодавство сфери бізнесу, в якій працює фізична особа-підприємець. Цей набір ризиків може включати недотримання дозвільних вимог, правил експлуатації, гігієни та епідеміології, пожежі та інших вимог законодавства. Вони виражаються в

претензіях контролюючих органів до підприємців: прокуратури, інспекції праці, міліції та інших державних органів.

Ризики протиправних дій третіх осіб – до цієї групи входять ризики, пов'язані з незаконними діями шахраїв. Це також включає небезпеку рейдерських нападів на підприємницькі підприємства. Звісно, не можна ігнорувати й ризики конкуренції: вони можуть бути природними, а можуть випливати з незаконних дій підприємців та компаній, які займаються одним бізнесом.

Інформаційний ризик – до цієї групи входять ризики інформаційних технологій, а саме:

– втрата (часткова втрата бази клієнтів/потенційних клієнтів);

– сервер втрачено/зупинено;

– ризик втрати потенційних клієнтів при виключенні/відмові працювати в системі відносин «компанія/клієнт».

3 ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ РИЗИКАМ У СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТОВ «ЕНТЕРКОМ»

3.1 Організаційно-методичне забезпечення оцінки інформаційних ризиків

Сучасний етап суспільного розвитку характеризується підвищенням ролі інформаційного поля, що являє собою групу інформації, інформаційної інфраструктури, суб'єктів, що збирають, формують, поширюють та використовують інформацію, систем, що регулюють суспільні відносини. з'являтися.

За останні роки реалізовано низку заходів щодо покращення та забезпечення інформаційної безпеки. держава. Вживаються певні заходи щодо забезпечення захисту інформації органів державної влади, підприємств, установ та організацій власності.

Водночас аналіз ситуації з інформаційною безпекою України показує, що її рівень не може повністю задовольнити потреби суспільства та країни.

Сучасний політичний та соціально-економічний розвиток країни характеризується загостренням протиріччя між потребою суспільства у розширенні вільного обміну інформацією та необхідністю дотримання певних нормативних обмежень щодо її поширення. Суперечливість та нерозвиненість законодавчих та нормативних актів у сфері суспільних відносин в інформаційній сфері призвели до серйозних негативних наслідків.

Відсутня чітка національна політика щодо формування цілісного інформаційного простору, розвитку системи ЗМІ, організації міжнародного інформаційного обміну, інтеграції національного інформаційного простору у світовий інформаційній системі, що створює передумови для витіснення інформаційних організацій та ЗМІ з країна. Підтримка державою діяльності

інформаційних організацій щодо просування своєї продукції на зовнішніх інформаційних ринках є недостатньою.

Недостатній розвиток вітчизняних інформаційних технологій змушує органи державної влади та місцевого самоврядування створювати інформаційні системи шляхом закупівлі імпортного обладнання та залучення іноземних компаній, що збільшує можливість несанкціонованого доступу до інформації та посилює залежність України від іноземних виробників комп'ютерної та телекомунікаційної техніки та програмного забезпечення.

Через широкомасштабне впровадження іноземних інформаційних технологій у сфери особистості, суспільства та країни, а також широке використання відкритих інформаційно-телекомунікаційних систем, інтеграцію вітчизняних інформаційних систем та міжнародних інформаційних систем, загроза для збільшилося використання «інформаційної зброї» на тлі зростання інформаційної інфраструктури У разі недостатності коштів у корпоративному бюджеті та без належної координації проведено роботу з повного та комплексного реагування на ці загрози. Недостатньо уваги приділено розвиток розвідувальних та інформаційних контрзаходів.

Завдяки аналізу сформовано кращий напрямок вирішення цих протиріч, тобто на основі міжнародних стандартів ISO враховуються нові рішення, вимоги та правила безпеки інформаційних мереж для забезпечення безпеки комерційних та державних організацій. керувати.

Основні заходи щодо забезпечення безпеки інформаційно-комунікаційних систем.

Під забезпеченням безпеки інформаційної мережі слід розуміти попередження пошкодження та переривання інформаційних активів та операцій, пов'язаних із реалізацією безперервних бізнес-процесів.

Інформаційні ресурси та засоби обробки та розповсюдження інформації повинні бути піддані управлінню та фізично захищені.

Структура стандартів дає змогу обрати засоби управління, що мають відношення до конкретної організації або сфери відповідальності в межах організації.

Зміст стандарту включає наступні розділи:

– політика безпеки [security policy];

– організація захисту [organizational security];

– класифікація ресурсів та контроль [asset classification and control];

– безпека персоналу [personnel security];

– фізична безпека та безпека навколишнього середовища [physical and environmental security];

– адміністрування комп'ютерних систем та обчислювальних мереж [computer and network management];

– керування доступом до системи [system access control]; розробка та супроводження інформаційних систем [system development and maintenance];

– планування безперервної роботи організації [business continuing planning];

– виконання вимог (відповідність законодавству) [compliance].

Також важливо регулярно переглядати ризики безпеки та впроваджені інструменти управління для того, щоб:

– оцінювати та впроваджувати зміни, пов’язані з вимогами та пріоритетами бізнесу;

– розглянути нові загрози та вразливості систем і сервісів;

– підтвердити, що заходи контролю все ще ефективні та відповідні.

Перегляд політики безпеки має здійснюватися на різних рівнях глибини роботи компанії залежно від результатів попередньої оцінки та рівня можливих змін.

Оцінка ризику спочатку проводиться на більш високому загальному рівні, щоб визначити пріоритетність інвестування ресурсів високого ризику, а потім на більш детальному рівні розглядають конкретні ризики самої системи та її послуг.

Після визначення вимог безпеки слід вибрати та застосувати заходи управління, щоб забезпечити зниження ризику. Інструменти управління можуть бути обрані зі стандартів або різних інших документів і заходів управління, визначених для таких систем, або вони можуть бути розроблені відповідно до обраної стратегії безпеки для задоволення потреб компанії.

Заходи управління слід вибирати, виходячи з вартості надання послуг і впровадження систем безпеки, а також зниження ризиків і можливих втрат у разі порушення. Для підтримки конкурентоспроможності компанії слід також враховувати немонетарні фактори, такі як втрата репутації, суспільство тощо.

Деякі заходи управління в стандартах і правилах можна розглядати як керівні принципи управління інформаційною безпекою і застосовні до більшості організацій.

Оцінка ризику – це процес визначення значень наслідків, ймовірності настання та рівнів ризику. Це включає:

– оцінити можливість можливих загроз і вразливостей;

– розрахувати вплив, який може загрожувати кожному активу;

– визначте кількісну (вимірну) або якісну (описову) вартість ризику.

Слід пам’ятати, що ці три змінні рідко незалежні одна від одної. В інформаційній безпеці існує зв’язок між вартістю активів, впливом і ймовірністю. Наприклад, хакери з більшою ймовірністю експлуатують вразливості, які призводять до більшого впливу, ніж уразливості з низьким рівнем впливу. Крім того, цінні активи більш вразливі до пошкоджень, ніж непотрібні активи.

Тому в цьому відношенні слід розглядати більше, ніж просто випадкові дії. Слід пам’ятати, що за наявності достатньої кількості часу та рішучості у людей є можливість обійти майже всі заходи безпеки. Коли вони мотивовані, вони можуть бути дуже креативними. Тому в процесі оцінки безпеки інформаційних ризиків слід уважно враховувати мотивуючі фактори.

Тому існує три основні методи оцінки інформаційного ризику:

– метод;

– контрольні документи;

– інструмент.

На рис. 3.1 представлені способи оцінки інформаційних ризиків.

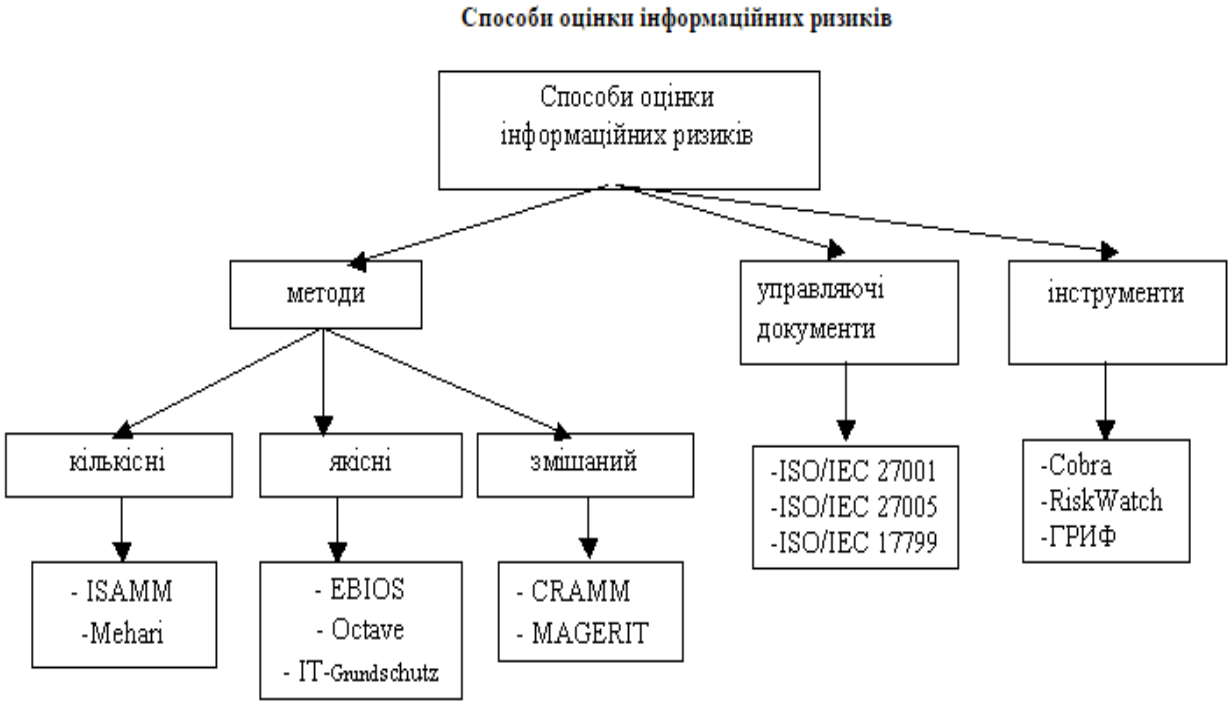

Рисунок 3.1 – Способи оцінки інформаційних ризиків

Під методом розуміють сукупність систематичних кроків, дій, які необхідно здійснити для вирішення проблеми або досягнення мети, в даному

випадку оцінки ризику. Іншими словами, метод відноситься до покрокового керівництва плюс інструменти (програмні продукти) для оцінки ризиків підприємства.

Усі методи оцінки ризику можна розділити на кількісні, якісні або комбінацію (змішані) кількісних та якісних методів.

Кількісні методи використовують вимірювані об'єктивні дані для визначення вартості активу, ймовірності збитку та пов'язаних з ним ризиків. Мета полягає в тому, щоб розрахувати вартість кожного компонента, зібраного під час оцінки ризику та аналізу витрат і вигод.

Якісні методи використовують відносний ризик або вартість активів на основі рейтингів або класифікацій низького, середнього, високого, неважливого, важливого, дуже важливого або від 1 до 10. Операції оцінки якісної моделі швидко визначають ризики та ймовірності економічно ефективним способом. Набір ризиків реєструється та аналізується під час якісної оцінки ризиків і може бути використаний як основа для цілеспрямованої кількісної оцінки.

У минулому частіше використовувалися кількісні методи. Однак останнім часом використання строгого кількісного управління ризиками зазвичай призводить до складної та тривалої роботи, а очевидних переваг порівняно з якісним методом оцінки ризику немає. Поєднання кількісних і якісних методів являє собою змішаний набір переваг і недоліків вищезазначених методів.

ISAMM-розроблено на базі Telindus. Це кількісний тип методу управління ризиками, при якому ризик оцінюється і виражається у річних очікуваних збитках у валютних одиницях.

ISAMM дозволяє візуалізувати та змоделювати зниження ризику кожного контролю покращення та порівняти його з вартістю впровадження. Ефективність цього методу дозволяє провести розумну оцінку ризику в

ньому з найменшими витратами часу та зусиль. Остання розробка методу ISAMM – це представлення активів. Це означає, що його можна використовувати для оцінки ризику активів або групування набору активів. Цей метод оцінки ризику складається з трьох основних частин: огляд, оцінка, розрахунок і звіт про результати.

Mehari – це модель управління ризиками з модульними компонентами та процесами. Крім інформаційної системи, модуль оцінки також охоплює всю організацію та її місцезнаходження, а також умови праці, правові та нормативні аспекти.

EBIOS – це повний набір посібників. Розроблені найкращі практики та документи для кінцевих користувачів у різних контекстах. Цей метод широко використовується в державному та приватному секторах. EBIOS стандартизує методи оцінки ризиків у сфері систем інформаційної безпеки. Цей метод розглядає всі технічні об'єкти (програмне та апаратне забезпечення, мережі) і нетехнічні об'єкти (організація, кадрові аспекти, фізична безпека).

OCTAVE – це незалежний метод, який вказує на те, що співробітники відповідають за встановлення політики безпеки організації. OCTAVE необхідно проаналізувати взаємозв’язок між ключовими активами, загрозами для цих активів та вразливими місцями (організація та технологія). Він визначає активи, пов’язані з інформацією, які є важливими для організації, і фокусується на цих активах, оскільки вони є найважливішими для організації (зосередьтеся на кількох важливих активах, не більше ніж на п’яти). Існує багато методів OCTAVE, заснованих на стандарті OCTAVE: OCTAVE, OCTAVE-S і OCTAVE Allegro.

IT-Grundschutz надає спосіб створення системи управління інформаційною безпекою. Він містить загальні рекомендації щодо IT-безпеки

та допоміжні технічні вказівки для досягнення рівня IT-безпеки, необхідного для конкретного домену. Метод IT-Grundschutz надає каталоги:

– модулі;

– каталоги загроз;

– захищені каталоги.

CRAMM – важко використовувати без інструментів CRAMM. Інструмент має ту ж назву, що й метод-CRAMM. Метод CRAMM заснований на комплексному підході до оцінки ризиків, що поєднує методи кількісного та якісного аналізу. Цей метод є універсальним і підходить для великих і малих організацій в державному та комерційному секторах. Правильне використання методу CRAMM дозволяє досягти дуже хороших результатів, найважливішим з яких є можливість економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та безперервності бізнесу. Економічно обґрунтована стратегія управління ризиками може в кінцевому підсумку заощадити гроші, уникаючи непотрібних витрат.

Magerit – це відкритий метод аналізу та управління ризиками, який є основою та керівництвом для забезпечення:

– забезпечити поінформованість персоналу, відповідального за інформаційну систему, про існування ризиків та своєчасного врахування цих ризиків;

– запропонувати системний підхід до аналізу цих ризиків;

– описати та спланувати відповідні заходи для контролю ризиків;

– підготувати організацію до процесу оцінки, аудиту, сертифікації та акредитації.

Крім методів оцінки ризиків, використовуються також контрольні документи. Який теоретично описує та дає рекомендації щодо процесу оцінки ризику, але не дає конкретних методик. Найвідоміші стандарти, які використовуються в Україні: ISO 27001, ISO 27005, ISO 17799.

Міжнародний стандарт ISO/IEC 27001 визначає процеси, які дозволяють компаніям створювати, застосовувати, переглядати, контролювати та підтримувати ефективні системи управління інформаційною безпекою. Цей стандарт визначає вимоги до розробки, впровадження, експлуатації, моніторингу, аналізу, підтримки та вдосконалення документованої системи управління інформаційною безпекою в контексті існуючих бізнес-ризиків організації.

Ці вимоги реалізуються в рамках документованого процесу управління інформаційною безпекою і побудовані за моделлю PDCA (Plan-Do-Chesk-Ast). Стандарт ISO/IEC 27001 – це чітка модель управління, яка дозволяє оцінювати ризики, проектувати та впроваджувати, керувати та переоцінювати системи інформаційної безпеки.

ISO/IEC 27005- цей стандарт має на меті визначити метод управління ризиками організації на основі сфери СМІБ, управління ризиками чи галузевої сфери тощо. Надавати поради щодо управління ризиками інформаційної безпеки, включаючи управління ризиками інформації та безпеки в телекомунікаційних технологіях. Стандарт підтримує загальні концепції, визначені в ISO/IEC 27001, і спрямований на сприяння адекватній інформаційній безпеці на основі методів управління ризиками. Він використовуються для різних організацій, які планують здійснювати управління ризиками (наприклад, комерційні підприємства, державні установи та некомерційні організації), щоб поставити під загрозу інформаційну безпеку організації.

Відповідно до ISO 17799 при створенні ефективної системи безпеки особливу увагу слід приділяти комплексному підходу до управління інформаційною безпекою. З цих причин елементи управління розглядаються не лише як технічні заходи, а й як організаційно-адміністративні заходи, спрямовані на забезпечення таких вимог до інформації:

– конфіденційність;

– цілісність;

– надійність;

– доступність.

Порушення кожного з цих пунктів може призвести до великих збитків у вигляді збитків і доходів не від праці.

Крім методів та управлінської документації, використовуються також інструменти оцінки ризиків. Ці інструменти є програмним забезпеченням із документацією правил використання. Найвідомішими інструментами без покрокового підходу є: Sobra, RiskWatch, GRIF 2006.

Cobra – це програмний інструмент, який дозволяє оцінити ризики безпеки. Він оцінює відносну важливість усіх загроз і вразливостей і генерує відповідні рішення та рекомендації. Це автоматично пов’язує виявлені ризики з потенційними наслідками діяльності підрозділу. Крім того, окремі сфери чи питання можна розглядати «самостійно» без будь-якого впливу на організацію.

RiskWatch – це серія програмних продуктів, вони побудовані на спільному програмному ядрі, призначених для управління різними типами ризиків і підтримки різних стандартів. RiskWatch використовує очікувані річні збиткові події (ALE – Annual Loss Expectancy) та рентабельність інвестицій (ROI – Return on Investment) як критерії для оцінки ризиків та управління ними. RiskWatch зосереджується на точній кількісній оцінці рівня втрат, спричинених загрозами безпеці, та вартості створення системи захисту.

GRIF 2006 є потужним і зручним інструментом для аналізу безпеки ресурсів інформаційної системи та ефективного управління ризиками. Дозволяє провести повний аналіз ризиків – всебічне розуміння всіх загроз, пов’язаних з інформаційною системою, оцінку серйозності вразливостей та

збитків, які вони можуть спричинити. Крім аналізу ризиків, існує також можливість управління ризиками. Алгоритм системи GRIF 2006 аналізує побудовану модель і формує звіт, що містить значення ризику кожного ресурсу. Конфігурація звіту може бути практично довільною, тому ви можете створювати короткі звіти для управління та докладні звіти для подальшої обробки результатів.

3.2 Організаційно-управлінські заходи щодо протидії інформаційним ризикам

Міжнародні стандарти ISO/IEC 17799 та ISO 27001 є основою галузі управління інформаційною безпекою. Це моделі систем управління, які визначають загальну організацію процесів, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризиків у контексті інформаційної безпеки.

Аналіз статус-кво нагляду та правового забезпечення інформаційної безпеки. Сучасний етап суспільного розвитку характеризується підвищенням ролі інформаційного поля, що являє собою групу інформації, інформаційної інфраструктури, суб’єктів, що збирають, формують, поширюють та використовують інформацію, систем, що регулюють суспільні відносини. з'являтися.

За останні роки реалізовано низку заходів щодо покращення та забезпечення інформаційної безпеки. держава. Вживаються певні заходи щодо забезпечення захисту інформації органів державної влади, підприємств, установ та організацій власності.

Водночас аналіз ситуації з інформаційною безпекою України показує, що її рівень не може повністю задовольнити потреби суспільства та країни.

Сучасний політичний та соціально-економічний розвиток країни характеризується загостренням протиріччя між потребою суспільства у розширенні вільного обміну інформацією та необхідністю дотримання певних нормативних обмежень щодо її поширення. Суперечливість та нерозвиненість законодавчих та нормативних актів у сфері суспільних відносин в інформаційній сфері призвели до серйозних негативних наслідків.

Відсутня чітка національна політика щодо формування цілісного інформаційного простору, розвитку системи ЗМІ, організації міжнародного інформаційного обміну, інтеграції національного інформаційного простору у світовий інформаційний простір, що створює передумови для витіснення інформаційних організацій та ЗМІ з країна. Інформаційний ринок обміну. Підтримка державою діяльності інформаційних організацій щодо просування своєї продукції на зовнішніх інформаційних ринках є недостатньою.

Відсталість вітчизняних інформаційних технологій змушує органи державної влади та місцевого самоврядування створювати інформаційні системи шляхом закупівлі імпортного обладнання та залучення іноземних компаній, що збільшує можливість несанкціонованого доступу до інформації та посилює залежність України від іноземних виробників комп'ютерної та телекомунікаційної техніки [27].

Через широкомасштабне впровадження іноземних інформаційних технологій у сфери особистості, суспільства та країни, а також широке використання відкритих інформаційно-телекомунікаційних систем, інтеграцію вітчизняних інформаційних систем та міжнародних інформаційних систем, загроза для збільшилося використання «інформаційної зброї» на тлі зростання інформаційної інфраструктури У разі недостатності коштів у корпоративному бюджеті та без належної координації

проведено роботу з повного та комплексного реагування на ці загрози. Недостатньо уваги приділено розвиток розвідувальних та інформаційних контрзаходів.

Завдяки аналізу сформовано кращий напрямок вирішення цих протиріч, тобто на основі міжнародних стандартів ISO враховуються нові рішення, вимоги та правила безпеки інформаційних мереж для забезпечення безпеки комерційних та державних організацій. керувати.

Основні заходи щодо забезпечення безпеки ІКС. Під захищеністю інформаційної мережі розумітиме попередження пошкодження інформаційних активів та переривання дій, пов’язаних із виконанням безперервних бізнес-процесів. Інформаційні ресурси та засоби обробки та розповсюдження інформації повинні бути піддані управлінню та фізично захищені.

У зв’язку з цим пропонується багато ключових елементів управління, які перераховані як основні елементи: політика інформаційної безпеки; розподіл відповідальності за інформаційну безпеку; навчання та навчання інформаційній безпеці; звітність про інциденти безпеки; захист від вірусів; забезпечення безперервності бізнесу; контроль копіювання ліцензійного програмного забезпечення ; захист архівів організації; захист персональних даних; реалізація політики інформаційної безпеки.

Як бачимо, окрім контролю систем автоматизації та мереж, велике значення надає також формуванню політики безпеки, співпраці з працівниками (підбір, навчання та звільнення), забезпеченню безперервності виробничого процесу, а також вимоги. Реалізація стратегії безпеки базується на оцінці ризиків і ретельно перевіряється.

Ризик визначається як добуток індексу можливих збитків та ймовірності збитку. Під втратою розуміють матеріальні збитки, пов'язані з

порушенням атрибутів інформаційного ресурсу: конфіденційності, цілісності, доступності.

Вимоги безпеки визначаються шляхом структурованої оцінки ризику безпеки. Витрати на управління повинні бути збалансовані з потенційними втратами бізнесу, які можуть бути спричинені порушенням безпеки.

Метод оцінки ризику може бути застосований до всієї організації чи її частини, або може бути застосований до окремих компонентів єдиної інформаційної системи, системи чи служби, якщо він практичний, реалістичний та корисний.

Визначимо оцінку ризику як можливі збитки бізнесу, спричинені порушенням безпеки, та врахуйте можливі наслідки: втрату конфіденційності, цілісності чи доступності інформації та інших активів; і реальну можливість таких порушень, що відображено у пріоритеті На фоні впровадження систем захисту від загроз та найважливіших ключових інструментів управління.

Результати цієї оцінки допоможуть спрямувати та визначити відповідні дії для загального керівництва компанії та пріоритетність впровадження управління ризиками інформаційної безпеки вибраних інструментів.

Важливо регулярно переглядати ризики безпеки та впроваджені інструменти управління, щоб:

– оцінювати та впроваджувати зміни, пов’язані з вимогами та пріоритетами бізнесу;

– розглянути нові загрози та вразливості систем і сервісів;

– підтвердьте, що заходи контролю все ще ефективні та відповідні.

Перегляд політики безпеки має здійснюватися на різних рівнях глибини роботи компанії залежно від результатів попередньої оцінки та рівня можливих змін. Оцінка ризику спочатку проводиться на більш високому загальному рівні, щоб визначити пріоритетність інвестування ресурсів

високого ризику, а потім на більш детальному рівні розглядають конкретні ризики самої системи та її послуг.

Після визначення вимог безпеки слід вибрати та застосувати заходи управління, щоб забезпечити зниження ризику. Інструменти управління можуть бути обрані зі стандартів або різних документів і заходів управління, визначених для таких систем, а також можуть бути розроблені відповідно до обраної стратегії безпеки для задоволення потреб компанії [20, 21].

Заходи управління слід вибирати, виходячи з вартості надання послуг і впровадження систем безпеки, а також зниження ризиків і можливих втрат у разі порушення. Для підтримки конкурентоспроможності компанії слід також враховувати немонетарні фактори, такі як втрата репутації, суспільство тощо.

Деякі заходи управління в стандартах і правилах можна розглядати як керівні принципи управління інформаційною безпекою і застосовні до більшості організацій. Більш детально це буде описано нижче.

Виходячи з цього, ми розглянемо заходи управління з точки зору законодавства, зокрема: захист даних та конфіденційність персональної інформації; захист інформаційних ресурсів організації; права інтелектуальної власності.

Наразі заходи з управління інформаційною безпекою включають (рис. 3.2):

– документи, пов’язані з політикою інформаційної безпеки;

– розподіл обов’язків, пов’язаних із інформаційною безпекою;

– відділи та навчальні структури, пов’язані з інформаційною безпекою;

– звіти про інциденти безпеки;

– управління безперервністю бізнесу.

На рис. 3.2 наведені заходи управління інформаційною безпекою.

Рисунок 3.2 – Заходи щодо управління інформаційною безпекою

Ці заходи управління застосовні до більшості організацій і більшості середовищ. Слід зазначити, що незважаючи на те, що всі заходи менеджменту в стандартах і правилах є важливими, доцільність (застосовність) будь-якого інструменту управління має визначатися на основі певних ризиків, з якими безпосередньо стикається організація. Тому, хоча вищезазначений метод і розглядається як вихідна точка інформаційної безпеки, він не є догмою і не може замінити вибір управлінських заходів на основі оцінки ризиків.

Однією з основних сфер інформаційної безпеки ІКС має бути система правил контролю доступу, повноваження кожного користувача чи групи користувачів, які мають бути чітко визначені при формулюванні політики доступу та безпеки.

На рис. 3.3 приведена система вимог і правил управління інформаційною безпекою.

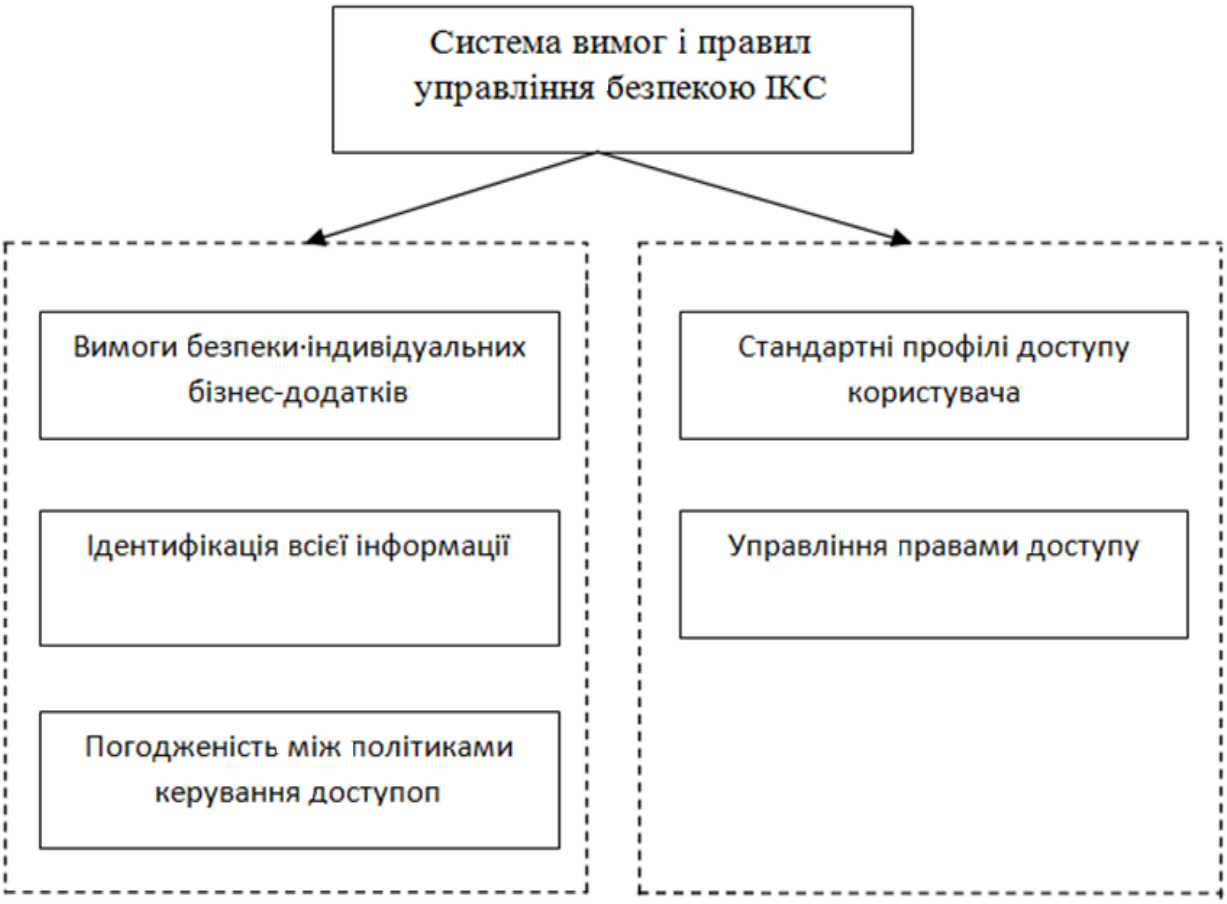

Рисунок 3.3 – Система вимог і правил управління інформаційною безпекою

Вимоги та система правил сучасного управління безпекою ІКСМ повинна включати:

– вимоги безпеки єдиного бізнес-додатка;

– ідентифікувати всю інформацію, пов'язану з бізнес-додатками, політику розповсюдження інформації та авторизації (необхідно зрозуміти принципи та рівні безпеки, а також класифікацію інформації, що поширюється та обробляється в системі);

– узгодженість між стратегіями контролю доступу та інформаційними класифікаціями різних кооперативних систем і мереж;

– відповідне законодавство та будь-які договірні зобов'язання щодо захисту доступу до системних даних або послуг;

– стандартні профілі доступу користувачів для загальних категорій роботи; керування повноваженнями доступу в розподіленому інформаційному середовищі мережі може ідентифікувати всі типи доступних з'єднань.

Ключовими факторами успішного впровадження інформаційної безпеки в організації є:

– політика безпеки, цілі та дії, що відображають цілі бізнесу;

– впроваджувати методи безпеки, які відповідають культурі організації та внутрішньої етики;

– підтримка та прихильність керівництва;

– правильно розуміти вимоги безпеки, оцінку ризиків та управління ризиками;

– ефективний маркетинг безпеки для всіх адміністраторів і співробітників;

– розподілити управління політикою та стандартами інформаційної безпеки між усіма співробітниками та підрядниками;

– забезпечити відповідну підготовку та освіту;

– комплексна та збалансована система вимірювання для оцінки ефективності управління інформаційною безпекою та пропозиції зворотного зв'язку для покращення бізнесу;

– оцінити інформаційні загрози, деструктивний вплив на інформацію, вразливість інформації та методів обробки та можливість їх виникнення.

– процес ідентифікації ризиків, управління ризиками (Risk management), а також зменшення або усунення ризиків безпеки, які можуть впливати на інформаційні системи в рамках кваліфікованих витрат.

ВИСНОВКИ

У першому розділі роботи розглянуто організаційні аспекти протидії ризикам у системі економічної безпеки підприємства.

Розкрито зміст і принципи функціонування системи економічної безпеки підприємства.

Використання системних методів у дослідженнях є характеристикою сучасної економічної науки. У загальному розумінні система – це група взаємодіючих елементів. Більшість учених визначають системний метод ширше, а аналіз структури системи та форми її застосування значно складніші.

При визначенні поняття «система» пріоритет слід віддавати категорії взаємодії, яка розкриває взаємозалежність, взаємодію, взаємне проникнення, взаємозбагачення та заперечення елементів системи

Комплексна система економічної безпеки підприємства – це комплекс взаємопов’язаних організаційно-правових та матеріально-технічних заходів, призначених для захисту підприємства від реальних і потенційних загроз і ризиків, які можуть спричинити великі економічні збитки або затримати розвиток підприємства.

Ресурси підприємства – це сукупність усіх існуючих організаційних, матеріально-правових, фінансових, адміністративних, інтелектуальних та техніко-технічних можливостей підприємства, які покликані протистояти загрозам і ризикам, забезпечувати динамічний розвиток підприємства та досягати його цілей.

Наведно напрями державного регулювання системи економічної безпеки макро- та мікрорівнів.

Систематизовано принципи функціонування системи економічної безпеки підприємства.

Для формування успішної концепції економічної безпеки необхідно реалізувати стратегію економічної безпеки, що означає комплекс найважливіших рішень, покликаних забезпечити рівень безпеки функціонування та розвитку комерційних суб'єктів.

Узагальнюючи погляди багатьох відомих вчених, сучасна стратегія економічної безпеки підприємства повинна включати: характеристики зовнішньої та внутрішньої загроз економічної безпеки; виявлення та моніторинг факторів короткострокової та довгострокової стабільності підприємства; визначення стандартів інтересів підприємства і показники вимог економічної безпеки і критичного значення, цілеспрямованість діяльності підприємств щодо реалізації стратегій економічної безпеки, розробка економічної політики та механізм взаємодії всіх компонентів системи підприємства для забезпечення економічної безпеки.

Наведено класифікацію небезпек, ризиків і загроз в системі економічної безпеки підприємства.

У загальному розумінні небезпека – це об'єктивно існуюча можливість негативного впливу на соціальний організм, внаслідок чого соціальний організм може завдати будь-якої шкоди чи втрати, тим самим змінивши свій стан, або, як наслідок, його розвиток набуває негативних обертів чи параметри (характер, ритм, форма тощо).

Джерела небезпека – це сукупність умов і факторів, які самі по собі містять і за певних умов самі або в будь-якій комбінації утворюють деструктивні (сукупність негативних впливів).

Під час аналізу виявлено, що до найбільш небезпечних зовнішніх загроз, які можуть завдати шкоди компанії або перешкодити подальшій діяльності, належать:

– нестабільне чинне законодавство. В Україні закони та нормативні акти часто суперечливі, часто змінюються та видаються заднім числом, що спричиняє суперечки між сторонами конфлікту з одного й того ж питання, що значно ускладнює стабільну роботу підприємства;

– недобросовісна конкуренція є очевидною формою корпоративної діяльності. Сюди входять: економічний шпигунство, підроблені конкуренти, шахрайство споживачів, шахрайство з бізнес-звітами, корупція тощо;

– зміни валютних курсів. Оскільки українська економіка доларизована, розрахунок здійснюється за такою схемою: долар-гривня-долар, то даному випадку обмінний курс впливає не тільки на імпортно-експортний бізнес компанії, але й визначає прибуток або збиток від їх імпорту. Зміна валютних курсів також впливає на експортний бізнес, діяльність якого зосереджена на внутрішньому ринку. Таким чином, бізнес-експортери виграють від зниження курсу національної валюти та його несприятливого зростання, а бізнес-імпортери виграють від підвищення курсу національної валюти та його несприятливого зниження;

– поява нових технологій (Інтернет), окрім своїх позитивних аспектів, це також джерело загроз для корпоративної економічної безпеки, зокрема: паролі доступу хакерів, крадіжка конфіденційної інформації, відмова в обслуговуванні, програми, керовані вірусами, та інші.

До типів внутрішніх загроз, які мають найбільший вплив на компанію, відносять:

– відсутність стабільних менеджерів середнього рівня. Рівень знань власника зазвичай нижчий, ніж у його підлеглих, а підлеглі в основному отримали професійну освіту;

– відсутність або поверхове ставлення до корпоративної маркетингової стратегії. Маркетинг – це системний механізм, що забезпечує довгострокову стратегічну стабільність і прибутковість компанії на ринку та покращує

економічну безпеку підприємства, а не засіб швидкого вирішення поточних проблем, на думку більшості керівників;

– забезпечення сировиною та комплектуючими. Ця проблема тісно пов'язана з такими проблемами, як недостатній попит на готову продукцію та збільшення взаємних непогашень за високою дебіторською заборгованістю.

– невизначеність цілей. Правильний вибір корпоративної місії – глобальна мета створення та функціонування компанії є запорукою успішного розвитку компанії;

– немотивована поведінка корпоративного персоналу, що в свою чергу призводить до зниження продуктивності.

Установлено та графічно представлено зв'язок підприємства з загрозами.

Розглянуто організаційні заходи протидії інформаційним і кадровим ризикам.

Розроблення та впровадження певних процедур і заходів кадрових технологій є найбільш актуальним та ефективним засобом забезпечення безпеки персоналу підприємства.

Безпека персоналу є однією зі складових економічної безпеки бізнесу (та інших факторів – фінансів, влади, інформації, технологій і технологій, права, навколишнього середовища).

За походженням загрози кадровій безпеці можна розділити на дві групи: внутрішні та зовнішні.

Класифікація внутрішніх загроз:

– недостатня кваліфікація персоналу;

– слабка організація системи управління персоналом;

– помилки в плануванні людських ресурсів;

– організація системи освіти слабка;

– неефективна система стимулювання;

– звільнення кваліфікованих робітників;

– відсутність політики компанії або «слабкість»;

– неякісні перевірки претендентів на роботу.

Зовнішні загрози кадровій безпеці:

– у конкурентів кращі умови заохочення;

– привести конкурентів до заманювання;

– тиск працівників ззовні;

– нехай співробітники потрапляють в різні види залежності;

– інфляційний процес (неможливо не враховувати при розрахунку заробітної плати та прогнозуванні її динаміки).

Важливим елементом безпеки персоналу на будь-якому підприємстві є ефективне управління персоналом.

Забезпечення інформаційної безпеки є одним із головних завдань сучасних підприємств. Загрозою може бути не тільки технічний збій, а й невідповідність даних в різних системах обліку, таку ситуацію зустрічає практично кожна компанія, а також необмежений доступ співробітників до інформації.

Інформаційний ризик – це ризик втрати або пошкодження, спричинений використанням компанією інформаційних технологій. Іншими словами, IT-ризики пов’язані зі створенням, передачею, зберіганням та використанням інформації за допомогою електронних засобів масової інформації та інших методів комунікації.

Інформаційний ризик включає всі ризики, пов’язані з ризиком втрати або пошкодження, спричиненого використанням підприємством інформаційних технологій.

У роботі систематизовано категорії IT-ризиків. Завдання мінімізації IT-ризиків полягає в запобіганні несанкціонованого доступу до даних, а також аварій і збоїв устаткування та програмного забезпечення.

У другому розділі роботи здійснено аналіз господарської діяльності ТОВ «Ентерком», яке було засновано у 2011 році. На даний момент в компанії працює 12 працівників, деякі з них мають сертифікати корпорації Google.

Проаналізована організаційна структура ТОВ «Ентерком».

Компанія спеціалізується в 2-х нішах, а саме – тренінговий центр (консалтинг дрібного бізнесу та лідогенерація), та ритейл біжутерії.

Виконавчий директор визначає, формулює, планує, здійснює й координує всі види діяльності компанії. Визначає напрями розвитку компанії, направляє діяльність персоналу на досягнення високих економічних та фінансових результатів, представляє компанію в органах державної влади і у взаємовідносинах з партнерами.

Відділ арбітражу трафіка та лідогенерації на постійній основі генерують клієнтів, виконують процедури пошуку та тестування нових джерел трафіка, даний відділ є ключовою ланкою в любому інтернет-бізнесі, оскільки інтернет-бізнес не може стабільно працювати та рости без постійної генерації клієнтів.

Відділ WEB-аналітики займається вимірами зовнішніх каналів залучення клієнтів і зручності (usability) всіх ресурсів, якими володіє компанія. Всі ці пункти керовані, але щоб ними управляти, необхідно побудувати систему ключових показників KPI для кожного каналу окремо і в цілому, тому що необхідно знати, що працює, а що ні.

Низкою цих питань і займається відділ WEB-аналітики.

Відділ продаж та логістики займається наступними питаннями:

– продзвін «гарячих» клієнтів, клієнтів, які були згенеровані відділом арбітражу і попали у воронку продаж;

– продзвін поточних клієнтів та запропонування Upsell-лу;

– «холодний» продзвін сторонніх баз клієнтів;

– відправкою фізичних товарів кінцевому покупцю через «НОВА ПОШТА»;

– контролем викупу, та продзвоном не викупів.

Відділ підтримки займається:

– підтримкою текучих клієнтів;

– відкриттям доступу до тренінгів клієнтам;

– консультуванням з приводу локальних питань;

– консультуванням в онлайн-чатах.

Наведені техніко-економічні показники діяльності компанії.

Виявлені основні загрози та ризики підприємств ІТ-галузі.

Інформаційні ризики – до цієї групи належать ризики, які носять інформаційно-технологічних характер, а саме:

– втрата (часткова втрата бази даних клієнтів/потенційних клієнтів);

– втрата/арешт серверів;

– ризик втрати потенційних клієнтів в разі виключення/відказу роботи в системі відношень «компанія/клієнт».

У третьому розділі роботи запропоновано напрями удосконалення організаційного забезпечення протидії ризикам у системі економічної безпеки підприємства.

Запропновано способи оцінки інформаційних ризиків:

– методи;

– управляючі документи;

– інструменти.

Всі методи оцінки ризику можна розділити на кількісні, якісні або комбінацію кількісних методів з якісними (змішаний).

Крім методів оцінки ризиків використовують управляючі документи. Де теоретично описуються і даються методичні вказівки процесу оцінки

ризиків, але не дається конкретних технологій. Найвідоміші стандарти, які використовуються на території України: ISO 27001, ISO 27005, ISO 17799.

Крім методів та управляючих документів використовують інструменти для оцінки ризиків. Інструменти являють собою програмне забезпечення з документацією про правила використання. Найвідомішими інструментами, існуючими без методики з покроковою інструкцією є: Cobra, RiskWatch, GRIF 2006.

Запропновано організаційно-управлінські заходи щодо протидії інформаційним ризикам.

Заходи управління слід вибирати, виходячи з вартості надання послуг і впровадження систем безпеки, а також зниження ризиків і можливих втрат у разі порушення. Для підтримки конкурентоспроможності компанії слід також враховувати немонетарні фактори, такі як втрата репутації, суспільство тощо.

Також розроблено заходи щодо управління інформаційною безпекою.

Ключовими факторами успішного впровадження інформаційної безпеки в організації є:

– політика безпеки, цілі та дії, що відображають цілі бізнесу;

– впроваджувати методи безпеки, які відповідають культурі організації та внутрішньої етики;

– підтримка та прихильність керівництва;

– правильно розуміти вимоги безпеки, оцінку ризиків та управління ризиками;

– ефективний маркетинг безпеки для всіх адміністраторів і співробітників;

– розподілити управління політикою та стандартами інформаційної безпеки між усіма співробітниками та підрядниками;

– забезпечити відповідну підготовку та освіту;

– комплексна та збалансована система вимірювання для оцінки ефективності управління інформаційною безпекою та пропозиції зворотного зв'язку для покращення бізнесу;

– оцінити інформаційні загрози, деструктивний вплив на інформацію, вразливість інформації та методів обробки та можливість їх виникнення.

– процес ідентифікації ризиків, управління ризиками (Risk management), а також зменшення або усунення ризиків безпеки, які можуть впливати на інформаційні системи в рамках кваліфікованих витрат.

Запропнован систему вимог і правил управління інформаційною безпекою.

Основні результати досліджень опубліковані в роботах [53, 54].

Копії опублікованих праць наведено в додатку А.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Мандзіновська Х. О. Управління фінансово-економічної безпекою: підручник / ред.Онищенко В. О. та ін. Полтава: ПолтНТУ, 2018. 530 с.

2. Козаченко Г. В., Рамазанов С. К., Ляшенко О. М., Погорелов Ю. С., Пшик Б. І. Система економічної безпеки: держава, регіон, підприємство: монографія [у 3 т.]. Т. 3. Луганськ: Промдрук, 2014. 336 с.

3. Комплексне забезпечення фінансово-економічної безпеки: навч. посіб. для студентів ВНЗ / ред. Г. Є. Павлова та ін. Дніпро: Акцент, 2018. 559 с.

4. Управління фінансовою безпекою економічних суб'єктів: навч. посіб. для студентів ВНЗ екон. і юрид. спец. усіх форм навчання / ДВНЗ «Укр. акад. банк. справи Нац. банку України», Каф. фінансів ; за заг. ред. д-ра екон. наук, проф. С. М. Фролова; [уклад.: С. М. Фролов та ін.]. Суми: ДВНЗ «УАБС НБУ», 2015. 331 с.

5. Єпіфанов А. О., Пластун О. Л., Домбровський В.С., Болгар Т. М., Ващенко О. М. Фінансова безпека підприємств і банківських установ: монографія; Ред.: А. О Єпіфанов. Суми: ДВНЗ «УАБС НБУ», 2009. 295 с.

6. Фінансово-економічна безпека: стратегічна аналітика та аудиторський супровід: монографія / ред.: Т. В. Момот; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків: ХНУМГ ім. О. М. Бекетова, 2015. 340 с.

7. Живко З. Б. Управління системою економічної безпеки підприємства: навч. посіб.; Львів. держ. ун-т внутр. справ. Львів, 2016. 211 с.

8. Онищенко С. В., Пугач О. А. Загрози економічній безпеці України: сутність, оцінювання та механізм упередження: монографія. Полтава: ПолтНТУ, 2015. 337 с.

9. Франчук В. І. Економічна безпека суб'єктів господарської діяльності: підручник; Львів. держ. ун-т внутр. справ. Львів, 2015. 235 с.

10. Майстро Р.Г., Полозова Т.В. Напрями вдосконалення державного регулювання економічної безпеки України. *Приазовський економічний вісник*. 2019. Випуск 1(12). С. 46-50.

11. Мазаракі А. А., Корольчук О. П., Мельник Т. М. Економічна безпека України в умовах глобалізаційних викликів: монографія; Ред.: А. А. Мазаракі; Київ. нац. торг.-екон. ун-т. К., 2010. 717 с.

12. Новик І. В. Проблеми та перспективи забезпечення економічної безпеки підприємства в Україні. *Інфраструктура ринку*. 2020. Вип. 43. С. 229-233.

13. Polozova T.V., Nicola Jennifer John Elia. Enterprise economic security system: theoretical aspects of formation. Економічні та безпекові виклики сучасного бізнес-середовища: колективна монографія / За заг. ред. д.е.н., проф. Т. В. Полозової. Харків: ХНУРЕ, 2020. С. 355-362.

14. Концептуальні засади формування фінансово-економічної безпеки: колект. монографія / [Абакуменко О. І. та ін.]; за заг. ред. д-ра екон. наук, проф. Шкарлета Сергія Миколайовича; Черніг. нац. технол. ун-т. Ніжин: Лук'яненко В.В.: Орхідея, 2015. 440 с.

15. Шмалій Л. В., Ількевич М. В. Управління економічною безпекою підприємства. *Економіка. Менеджмент. Бізнес*. 2020. № 4. С. 68-73.

16. Лук'янова В. В., Шутяк Ю. В. Діагностика економічної безпеки підприємства: монографія. Хмельницький: ХНУ, 2014. 165 с.

17. Тимошик М. М. Оцінювання ризиків промислових підприємств у різних умовах функціонування. *Вісник Одеського національного університету. Серія: Економіка.* 2018. Т. 23, Вип. 6. С. 94-99.

18. Швець Ю. О. Ризики в діяльності промислових підприємств: види, методи оцінки та заходи подолання ризику. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. 2018. Вип. 17(2). С. 131-135.

19. Смоляк В. А. Економічна оцінка ризику діяльності промислових підприємств: дис... канд. екон. наук: 08.07.01 / Харк. нац. екон. ун-т. Харків. 2005. 260 с.

20. Герасименко О. М. Порівняльний аналіз методів та програмних методик ідентифікації, аналізу та оцінки ризиків у забезпеченні економічної безпеки підприємства. *Економічний вісник Запорізької державної інженерної академії*. 2018. Вип. 6. С. 109-113.

21. Мороз О. В., Матвійчук А. В.. Оптимальне управління економічними системами в умовах невизначеності та ризику: монографія. Вінниця: УНІВЕРСУМ-Вінниця, 2003. 177 с.

22. Економічний ризик: практикум / З. Б. Артим-Дрогомирецька, І. Б. Романич; Львів. нац. ун-т ім. І. Франка. Л.: Вид-во Т. Сороки, 2008. 186 с.

23. Верченко П. І. Багатокритеріальність і динаміка економічного ризику (моделі та методи): монографія; Київ. нац. екон. ун-т ім. В.Гетьмана. Київ, 2006. 272 с.

24. Діагностика стану підприємства: теорія і практика: монографія / А.Е. Воронкова, Р.З. Вечерковські, Д.К. Воронков, Н.Г. Калюжна, Е.Н. Коренєв, І.В. Мажура; Харк. нац. екон. ун-т. – 2-ге вид., переробл. і доповн. Харків: ІНЖЕК, 2008. 520 с.

25. Герасименко Т. О., Мазуренко О. М. Аналіз господарської діяльності: навч. посіб.; Львів. комерц. акад. Львів, 2014. 319 с.

26. Божидарнік Т. В., Кривов'язюк І. В. Обґрунтування господарських рішень і діагностика промислового підприємства: сучасний формат: монографія; Луц. нац. техн. ун-т. Луцьк, 2014. 160 с.

27. Міщук Г. Ю., Джигар Т. М., Шишкіна О. О. Економічний аналіз: навч. посіб.; Нац. ун-т вод. госп-ва та природокористування. Рівне: НУВГП, 2017. 155 с.

28. Могилевська О. Ю., Уфімцева Т. М., Слободяник А. М. Економіка підприємства. Теорія і практика : навч. посіб.; Київ. міжнар. ун-т. Київ, 2017. 295 с.

29. Ковальчук І. В. Економіка підприємства: навч. посібник. Київ: Знання, 2014. 679 с.

30. Основи економічного аналізу: навч.-метод. посіб. для студентів екон. спец., магістрів, аспірантів, викл. / В. М. Микитюк та ін.; ред. В. М. Микитюк; Житомир. нац. агроекол. ун-т. Житомир: Рута, 2018. 439 с.

31. Шарко М. В., Мєшкова-Кравченко Н. В., Радкевич О. М. Економіка підприємства: навч. посіб. для студ. ВНЗ. Ч. 1; Херсон. нац. техн. ун-т. Херсон, 2014. 434 с.

32. Череп А. В., Ярмош В. В. Економіка підприємства: підручник; ДВНЗ «Запоріз. нац. ун-т». Запоріжжя: ЗНУ, 2014. 335 с.

33. Семенда Д. К., Бурляй О. Л., Коротєєв М. А., Семенда О. В. Економіка підприємства: підруч. для студентів ВНЗ; ред.: Д. К. Семенда; Уман. нац. ун-т садівництва. Умань: Сочінський, 2014. 477 с.

34. Стратегія та механізми забезпечення фінансово-економічної безпеки: колект. монографія / Чернігів. нац. технол. ун-т ; за заг. ред. д-ра екон. наук, проф. Ільчука Валерія Петровича. Чернігів: ЧНТУ, 2017. 349 с.

35. Ольшанський О. В., Крамчанінова М. Д. Вплив пандемії COVID-19 на проблеми забезпечення економічної безпеки малих та середніх підприємств. *Економічний вісник Донбасу*. 2021. № 2. С. 78-82.

36. Череп А. В., Худолєй Л. В. Використання інструментів забезпечення фінансово-економічної безпеки промислових підприємств: монографія; Запоріз. нац. ун-т. Запоріжжя: Запоріз. нац. ун-т, 2018. 221 с.

37. Єфдокимов В. В., Олійник О. В., Грицишен Д. О., Грищенко О. О. Концепція управління економічною безпекою суб'єктів господарювання в контексті теорії сталого розвитку: монографія; Житомир. держ. технол. ун-т. Житомир, 2013. 251 с.

38. Меліхова Т. О. Вдосконалення функцій та завдань забезпечення економічної безпеки підприємств. *Інвестиції: практика та досвід*. 2018. № 3. С. 70-73.

39. Штангрет А. М., Караїм М. М., Штангрет І. А. Інтенсифікація управління економічною поведінкою підприємства: безпекові засади. *Ефективна економіка*. 2020. № 5. URL: http://nbuv.gov.ua/UJRN/efek_2020_5_8.

40. Христофоров В. О., Андрющенко Є. Г. Формування механізмів забезпечення економічної безпеки підприємств. *Вісник ХНАУ. Серія: Економічні науки.* 2019. № 1. С. 328-336.

41. Polozova T., Musiienko V., Storozhenko O., Peresada O., Geseleva N. Modeling of energy-saving processes in the context of energy safety and security. *Journal of security and sustainability issues*. 2019. № 8 (3). С. 387-397.

42. Жадько К. С., Самойленко Д. М. Економічна безпека підприємств в умовах цифрових технологій і пандемії. *Центральноукраїнський науковий вісник . Економічні науки*. 2020. Вип. 5. С. 170-176.

43. Бакай В. Й. Забезпечення економічної безпеки підприємства на основі використання цифрових технологій. *Вісник Хмельницького національного університету. Економічні науки.* 2020. № 4(1). С. 32-35.

44. Герасименко О. М., Зачосова Н. В. Оцінка рівня зрілості управління ризиками в процесі забезпечення економічної безпеки підприємства: аналітичне дослідження. Вісник *Київського національного університету технологій та дизайну. Серія: Економічні науки*. 2019. № 3. С. 66-81.

45. Старенька О. М. Оцінка ризиків як компонент системи внутрішнього контролю підприємства. *Науковий вісник [Одеського національного економічного університету]*. 2019. № 9-10. С. 127-145.

46. Колесник Т. М., Колонтаєвський О. П. Оцінка ризиків на приватному підприємстві. *Комунальне господарство міст. Серія: Економічні науки.* 2018. Вип. 141. С. 17-21.

47. Чирва Г. М., Бовкун О. А. Оцінювання ризиків підприємницької діяльності та аналітичне забезпечення економічної стійкості підприємств у процесі захисту їх економічних інтересів. *Економічні горизонти*. 2018. № 1. С. 52-59.

48. Шегда А. В., Голованенко М. В. Ризики в підприємництві: оцінювання та управління. Київ: Знання, 2008. 271 с.

49. Старостіна А. О. Ризик-менеджмент: теорія та практика: навч. посіб. Київ: ТОВ «Кондор», 2009. 200 с.

50. Кондрашихін А.Б. Теорія та практика підприємницького ризику: навчальний посібник. Київ: ТОВ «Центр учбової літератури», 2009. 224 с.

51. Ілляшенко С. М. Економічний ризик: навчальний посібник. 2-ге вид., доп. перероб. Київ: Центр навчальної літератури, 2004. 220 с.

52. Stoian O., Polozova T., Didenko E., Storozhenko O., Moskvichova O. Strategies of interaction with a consumer within the marketing product policy). *Entrepreneurship and sustainability issues*. – 2018. – № 6 (2). – С. 1018-1027/.

53. Діденко Є. В., Косінов А. Л. Організація контролю рівня інформаційної безпеки підприємства. *Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта.* Матеріали II Міжнародної науково-практичної конференції (м. Харків, 2 листопада 2021 р.) / За заг. ред. Т. В. Полозової [та ін.]. Харків. ХНУРЕ. 2021. С. 85-86.

54. Діденко Є. В., Соломаха І. С., Косінов А. Л. Напрями протидії ІТ-ризикам у системі економічної безпеки підприємства. Сучасні економічні стратегії: інновації, безпека та сталий розвиток: колективна монографія / За заг. ред. д.е.н., проф. Т.В. Полозової, д.е.н., проф. І.В. Колупаєвої, к.е.н., доц. О.В. Мурзабулатової Харків: ХНУРЕ, 2021. С. 230-235.