МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Бичков Олег Леонідович
(прізвище, ім'я, по батькові здобувача освіти)

УДК 004

КВАЛІФІКАЦІЙНА РОБОТА

Інформаційна система оцінки ризиків інформаційної безпеки підприємства

126 «Інформаційні системи та технології»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня бакалавр кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
Николюк Ольга Миколаївна
(прізвище, ім'я, по батькові)
професор, доктор економічних наук
(науковий ступінь, вчене звання)

Житомир – 2023

Висновок кафедри _____
за результатами попереднього захисту: _____

Протокол засідання кафедри _____
№ ____ від «_____» _____ 20____ р.

Завідувач кафедри _____

_____ _____ _____
(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)
«_____» _____ 20____ р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти _____ захистив (ла)
(прізвище ,ім'я, по батькові)
кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____
за шкалою ECTS _____
за національною шкалою _____

Секретар ЕК

_____ _____ _____
(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)

АНОТАЦІЯ

Бичков Олег Леонідович. Інформаційна система оцінки ризиків інформаційної безпеки підприємства. - *Кваліфікаційна робота на правах рукопису.*

Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 126 «Інформаційні системи та технології». – Поліський національний університет, Житомир, 2023.

В кваліфікаційній роботі продемонстровано етапи розробки та впровадження інформаційної системи оцінки ризиків інформаційної безпеки підприємства.

В результаті дослідження стану інформаційної безпеки підприємства було виявлено потребу у розробці та впроваджені автоматизованої системи обліку щодо захисту інформаційної безпеки та виявлення вразливостей за допомогою розрахунків та рекомендаціями щодо покращення захисту інформації підприємства.

В процесі виконання курсової роботи було виконано : аналіз існуючих методів та підходів до оцінки ризиків інформаційної безпеки на підприємстві., розробка вимог до інформаційної системи оцінки ризиків інформаційної безпеки підприємства, розробка структури та функціональності інформаційної системи оцінки ризиків інформаційної безпеки підприємства, розробка та впровадження інформаційної системи оцінки ризиків інформаційної безпеки на підприємстві, аналіз результатів впровадження інформаційної системи оцінки ризиків інформаційної безпеки на підприємстві, формулювання рекомендацій щодо подальшого розвитку інформаційної системи оцінки ризиків інформаційної безпеки підприємства.

Ключові слова: інформаційна система, оцінка ризиків, підприємство, додаток.

ANNOTATION

Oleg Leonidovych Bychkov. Information system for assessing the risks of information security of the enterprise. - Qualification work on manuscript rights.

Qualification work for obtaining a bachelor's degree in specialty 126 "Information systems and technologies". – Polissia National University, Zhytomyr, 2022.

In the qualification work, the stages of development and implementation of the information system for assessing the risks of information security of the enterprise are demonstrated.

As a result of the study of the state of the information security of the enterprise, the need for the development and implementation of an automated accounting system for the protection of information security and the detection of vulnerabilities with the help of calculations and recommendations for improving the protection of the information of the enterprise was identified.

In the course of the course work, the following was performed: analysis of existing methods and approaches to the assessment of information security risks at the enterprise, development of requirements for the information system for assessing the risks of information security of the enterprise, development of the structure and functionality of the information system for assessing the risks of information security of the enterprise, development and implementation of the information system assessment of information security risks at the enterprise, analysis of the results of the implementation of the information system for assessing information security risks at the enterprise, formulation of recommendations for the further development of the information system for assessing the risks of information security of the enterprise.

Keywords: information system, risk assessment, enterprise, application.

ЗМІСТ

ВСТУП

Сучасні технології та інформаційні ресурси дозволяють підприємствам значно розширити свої можливості та забезпечити ефективну діяльність. Однак, разом з цим, зростає ризик втрати інформації, який може викликати значні фінансові втрати та негативний вплив на репутацію підприємства.

Метою даної курсової роботи є дослідження питань створення інформаційної системи оцінки ризиків інформаційної безпеки підприємства та її впровадження для забезпечення ефективної захисту інформаційних ресурсів.

Об'єктом дослідження є процес захисту інформації на підприємстві.

Предметом дослідження є інформаційна система оцінки ризиків інформаційної безпеки підприємства, яка забезпечує процес ідентифікації потенційних загроз, визначення рівня ризику та прийняття необхідних заходів для запобігання втрати інформації.

У зв'язку з тим, що збільшення кількості інформації, яка обробляється на підприємстві, зробило її уразливою до кібератак та зломів, виникає потреба в розробці ефективних систем захисту інформації та оцінки ризиків її втрати. Відповідно, розробка інформаційної системи оцінки ризиків інформаційної безпеки підприємства є актуальною проблемою, яка вимагає дослідження.

У результаті проведеного дослідження будуть визначені переваги та недоліки використовуваних методів та підходів до оцінки ризиків інформаційної безпеки, а також буде розроблена та впроваджена інформаційна система оцінки ризиків інформаційної безпеки підприємства, що дозволить підприємству знизити ризики втрати інформації та забезпечити її надійний захист.

Завданням на курсову роботу є:

1. Аналіз існуючих методів та підходів до оцінки ризиків інформаційної безпеки на підприємстві.
2. Розробка вимог до інформаційної системи оцінки ризиків інформаційної безпеки підприємства.

3. Розробка структури та функціональності інформаційної системи оцінки ризиків інформаційної безпеки підприємства.

4. Розробка та впровадження інформаційної системи оцінки ризиків інформаційної безпеки на підприємстві.

5. Аналіз результатів впровадження інформаційної системи оцінки ризиків інформаційної безпеки на підприємстві.

6. Формулювання рекомендацій щодо подальшого розвитку інформаційної системи оцінки ризиків інформаційної безпеки підприємства.

Отже, далі буде розглянуто актуальну проблему розробки інформаційної системи оцінки ризиків інформаційної безпеки підприємства, визначено переваги та недоліки існуючих методів та підходів до оцінки ризиків інформаційної безпеки, а також розроблено відповідну інформаційну систему та протестовано її на підприємстві з метою забезпечення надійного захисту інформації від зловмисників. Виконання поставлених завдань дозволить підприємству виявити, оцінити та зменшити ризики втрати інформації, забезпечивши тим самим його стійкість та безпеку.

Дана курсова робота є важливим дослідженням, що може сприяти поліпшенню безпеки та захисту інформації на підприємствах та в інших сферах діяльності, де інформація є важливим ресурсом.

Розділ 1. СИСТЕМНИЙ АНАЛІЗ ОСОБЛИВОСТЕЙ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Розділ 1.1: Аналіз інформаційних потреб і визначення предметної області дослідження стосовно даної теми

Інформаційна безпека є однією з найважливіших складових безпеки підприємства. В сучасному світі, де кількість інформації, що обробляється та зберігається в електронному вигляді,забезпечення інформаційної безпеки стає все важливішою проблемою для бізнесу. З цієї причини виникає необхідність у створенні систем оцінки ризиків, що дозволяють виявляти потенційні загрози для інфо

Інформаційна безпека — стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного чи техногенного характеру, які можуть завдати шкоди суб'єктам інформаційних відносин, особливо власникам і користувачам інформації.рмаційної безпеки та приймати належні заходи щодо їх запобігання[1].

«Основними завданнями інформаційної безпеки є[3]:

- забезпечення доступності інформації;
- забезпечення цілісності інформації;
- забезпечення конфіденційності інформації;
- забезпечення вірогідності інформації;
- забезпечення юридичної значимості інформації, представленої у вигляді електронного документа;
- забезпечення невідстежуваності дій користувача.

Інформаційна безпека в рамках забезпечення працездатності ІС повинна забезпечувати захист від[3]:

- порушення функціонування інформаційної системи шляхом впливу на інформаційні канали, канали сигналізації, керування і віддаленого завантаження баз даних, комутаційного устаткування, системне і

прикладне програмне забезпечення;

- несанкціонованого доступу до інформаційних ресур¬сів і від намагань використання ресурсів мережі, що призводять до витоку даних, порушення цілісності мережі й інформації, зміни функціонування під¬систем розподілу інформації, доступності баз даних;
- руйнування засобів захисту, що вбудовуються, і зовнішніх засобів;
- неправомірних дій користувачів і обслуговуючого персоналу мережі.»

Підприємства зіштовхуються з різними видами загроз інформаційної безпеки, такими як шпигунство, віруси, хакерські атаки, фішинг, крадіжка даних тощо. Оцінка ризиків полягає в ідентифікації потенційних загроз та визначенні їх впливу на підприємство.

Захист інформації здійснюється шляхом застосування заходів для обмеження доступу до захищеної інформації і створення умов, що суттєво ускладнюють або повністю забороняють несанкціонований, незаконний доступ до інформації, що не знаходиться у вільному доступі[5].

Розробка інформаційної системи оцінки ризиків інформаційної безпеки підприємства є актуальною проблемою в сучасному світі. По-перше, це пов'язано зі зростанням кількості кібератак на підприємства та організації, які використовують інформаційні технології. По-друге, інформаційні системи стають все складнішими, тому необхідно мати ефективні інструменти для їх захисту.

1.2 Аналіз відомих технологічних рішень

На сьогоднішньому етапі розвитку підприємництва в Україні дедалі більше дослідників і експертів звертають увагу на питання, пов'язані з комерційною таємницею та її захистом, а також інформаційною безпекою інфраструктури. Інформаційна безпека підприємства стала необхідною складовою національної інформаційної безпеки.

Інформаційна безпека — це стан захищеності інформаційних ресурсів і потоків, технологічних процесів їх формування і застосування, а також прав суб’єктів інформаційної діяльності[6].

Забезпечення інформаційної безпеки підприємництва — це сукупність методів і засобів, спрямованих на всебічне системне підтримання необхідного рівня захисту інформаційних ресурсів шляхом виконання відповідними підрозділами системи безпеки господарюючого суб’єкта завдань щодо[6]:

- захисту інтелектуальної власності та комерційних секретів;
- захисту від незаконного проникнення в комп’ютерні системи і мережі, автоматизовані системи;
- захисту права суб’єктів господарювання на інформацію;
- розробки організаційних механізмів з технічного захисту

інформації від зовнішніх і внутрішніх загроз і для перекриття можливих каналів відтоку інформації в процесі використання засобів зв’язку, передачі та обробки інформації;

- захисту інформації шляхом збереження важливої інформації через шифрування невеликих за обсягом відомостей, що містять друковані документи, або перетворення повідомлень, які надсилають за допомогою засобів телефонування.

Інформаційна безпека користувачів інформаційних ресурсів підприємства забезпечує захищеність їх прав на доступ до інформації на матеріальних носіях (документи, технічна документація, бази даних і т. д.).

Основні напрямки захисту комп'ютерної системи підприємства включають:

- заходи зі забезпечення безпеки апаратних засобів та носіїв інформації;
- захисту мереж зв'язку та комутаційних вузлів,
- захисту інформаційних ресурсів від несанкціонованого доступу та забезпечення юридичної значущості електронних документів.

Метою таких заходів є забезпечення надійного захисту важливої інформації від різноманітних загроз, включаючи пошкодження, втрату, крадіжку, несанк

Аналіз відомих технічних рішень, пов'язаних з інформаційною безпекою підприємства, включає вивчення та порівняння доступних засобів і методів для забезпечення захисту даних, систем і мереж. Для ефективного впровадження інформаційної безпеки на підприємстві в основному розглядаються наступні основні технічні рішення:

- GRC – платформи (Governance, Risk and Compliance)- за допомогою даних платформ є можливіть поєднати в підприємстві такі вітки як стратегія розвитку, управління бізнесом та захист інформації. Будь-яка компанія на визначеному етапі розвитку вимагає вирішення завдань, таких як планування розвитку, оцінка ризиків і відповідність законодавству. Використання методів GRC є не просто показником продуктивності бізнесу, але й ефективним інструментом, що дозволяє зберегти або навіть збільшити темпи розвитку. У той же час впровадження та використання таких інструментів повинно бути простим і зрозумілим, щоб освоєння технологій, спрямованих на підвищення показників бізнесу не було проблемою(табл.1.1).

- Рішення для проведення вразливості сканування та оцінки ризиків відіграють одну з основних ролей в забезпеченні інформаційної безпеки підприємства. Саме вони допомагають визначити рівень вразливості системи, оцінюють рівень ризику та рекомндують відповідні заходи стосовно зменшення ризиків(табл.1.1).

- Рішення для аналізу та кореляції журналів безпеки (SIEM) – ці рішення поєднують у собі управління інформаційною безпекою та управління подіями безпеки(табл.1.1).

Таблиця 1.1- Порівняльна таблиця технологічних рішень

	GRC-платформи	Рішення для проведення вразливості сканування та оцінки ризиків	Рішення для аналізу та кореляції журналів безпеки (SIEM)
Переваги:	• Інтеграція управління ризиками, корпоративного управління та дотримання вимог законодавства. • Автоматизація процесів оцінки ризиків та контролю їх управління. • Гнучкість в адаптації під специфіку підприємства та його бізнес-процесів.	• Автоматичне виявлення вразливостей у мережевій інфраструктурі та додатках. • Оцінка рівня ризиків, пов'язаних з виявленими вразливостями. • Швидкість та ефективність сканування.	• Централізований збір та аналіз даних про події безпеки. • Автоматичне виявлення аномалій та інцидентів безпеки. • Забезпечення відповідності вимогам законодавства та стандартів безпеки.
Недоліки:	• Висока вартість впровадження та підтримки. • Складність впровадження та налаштування для менших підприємств.	• Можливість виявлення "фальшивих спрацьовувань" або пропуск деяких вразливостей. • Відсутність кастомізації для специфічних потреб підприємства.	• Висока вартість та складність впровадження та налаштування. • Можливість виявлення "фальшивих спрацьовувань" або пропуск деяких інцидентів безпеки.

Таким чином, після аналізу відомих технічних рішень виявлено, що вони мають багато переваг, оскільки можуть допомогти підприємствам управляти різними видами ризиків, контролювати дотримання нормативів і правил, знаходити слабкі місця та швидко виявляти проблемні місця. Ці рішення створюють комплексний підхід до інформаційної безпеки, який забезпечує захист корпоративних даних і систем.

Висновки до Розділу 1

В першому розділі було зроблено аналіз інформаційних потреб та визначено предметну область стосовно інформаційної системи оцінки ризиків інформаційної безпеки підприємства. Після чого був здійснений аналіз відомих технологічних рішень, якими є : GRC платформи, рішення для проведення вразливості сканування та оцінки ризиків, рішення для аналізу та кореляції журналів безпеки (SIEM).

Розділ 2. ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1 Функціональне моделювання інформаційної системи оцінки ризиків інформаційної безпеки підприємства

Одним із головних завдань на підприємстві є формування програми управління інформаційною безпекою підприємства. Однією з можливостей формування вище зазначеної програми є побудова контекстної IDEF0-моделі та її декомпозиції. Метою побудови IDEF0-моделі є формування та розробка програми управління інформаційною безпекою підприємства; предметом – інформаційна безпека; суб'єктом – процес управління інформацйною безпекою підприємства. На контекстній діаграмі IDEF0 функцією є – оцінювання інформаційної безпеки підприємства, вхідними даними: ресурсне забезпечення, виробниче та збут продукції, механізмом є системний адміністратор, розробник програмного забезпечення, експерти з інформаційної безпеки та інструментами керування виступає внутрішні регламенти підприємства, стандарти інформаційної безпеки та нормативно-правове забезпечення. На рисунку 2.1 зображено контексту діаграму IDEF0 – «Оцінювання ризиків інформаційної безпеки підприємства».

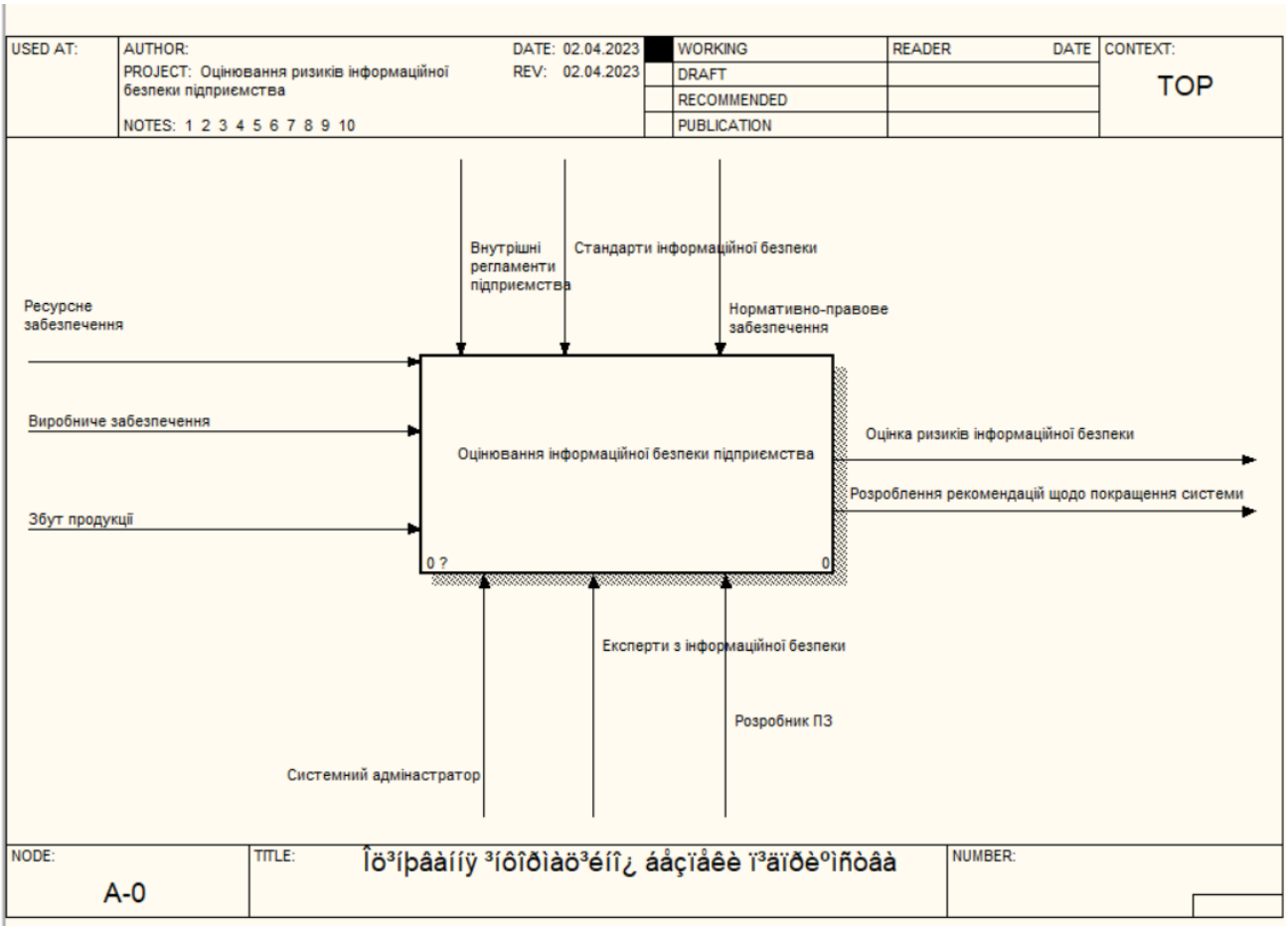

Рисунок 2.1 - Контекстна діаграма IDEF0 – «Оцінювання ризиків інформаційної безпеки підприємства

Надалі було розглянуто її декомпозицію (рис.2.2), що включає 5 блоків: аналіз ресурсного виробничого забезпечення та збуту продукції, виявлення загроз та вразливостей, оцінка ризиків, розробка стратегій управління ризиками, моніторинг і звітування про стан інформаційної безпеки. Результатом даних етапів на виході є оцінка ризиків інформаційної безпеки підприємства та рекомендації щодо розроблення та покращення системи.

Значимість розробки програми полягає в тому, що у сучасних умовах загроза щодо ризиків інформаційної безпеки постійно зростає, саме тому все більш необхідним стає формування спеціалізованої програми управління.

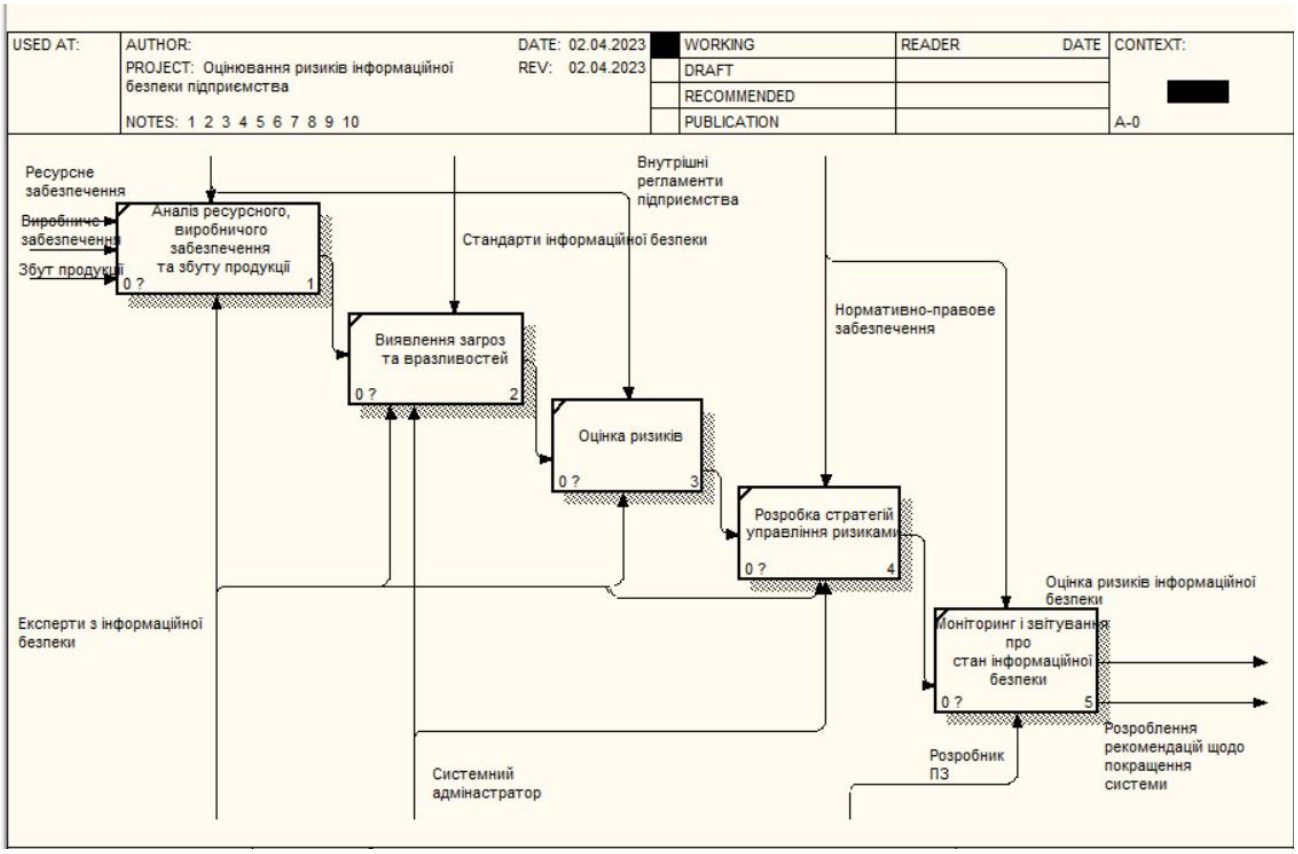

Рисунок 2.2 – Декомпозиція діаграми IDEF0 – «Оцінювання ризиків інформаційної безпеки підприємства

2.2. Формалізація моделі інформаційної системи оцінки ризиків інформаційної безпеки підприємства

Оцінка ризиків інформаційної безпеки є невід'ємною частиною практик управління підприємствами, яка забезпечує ідентифікацію, кількісну оцінку та визначення пріоритетів ризиків щодо елемента прийняття ризику та цілей, пов'язаних з організацією.

Управління ризиками визначає процес, який включає ідентифікацію, управління та усунення або зменшення ймовірності подій, які можуть негативно вплинути на ресурси інформаційної системи, щоб зменшити ризики безпеки, які потенційно можуть вплинути на інформаційну систему, за умови прийнятного значення захисту визначає аналіз ризиків, аналіз параметра «витрати-

ефективність», а також вибір, побудова та тестування підсистеми безпеки та дослідження всіх елементів безпеки.

Оцінка ризиків безпеки — це оцінка, яка включає визнання ризиків у компанії, технології та процесів для перевірки наявності засобів контролю для захисту від загроз безпеці.

Оцінка ризиків безпеки здійснюється спеціалістом з оцінки безпеки, який обчислює всі елементи систем компанії, щоб розпізнавати зони ризику. Це можуть бути як прості, як система, яка вмикає слабкі паролі, так і складніші проблеми, зокрема незахищені бізнес-процеси. Експерт, як правило, перевіряє все, починаючи від кадрової політики й закінчуючи конфігураціями брандмауера, працюючи над виявленням потенційних ризиків.

У процесі оцінювання необхідно переглядати та тестувати системи, рівень доступу та безпеки, шукаючи слабкі місця. Коли їх виявляють, вони класифікуються залежно від того, наскільки великий ризик вони становлять для компанії.

Як приклад на рис. 2.3 зображено алгоритм тестування.

Рис.2.3 – Алгоритм тестування системи

Розрахунок оцінок ризику інформаційної безпеки підприємства включає ідентифікацію потенційних загроз, вразливостей та наслідків, що можуть

виникнути внаслідок їх реалізації. Нижче наведено деякі основні формули для розрахунку оцінок ризику інформаційної безпеки:

Рівень ризику (R) можна розрахувати за формулою:

$$R = P \times \mathrm{I}$$

де: R - рівень ризику, P - ймовірність виникнення загрози ($0 \leq P \leq 1$),

I - потенційний збиток від реалізації загрози

Ймовірність виникнення загрози (P) можна розрахувати за формулою:

$$P = T \times V$$

де: P - ймовірність виникнення загрози ($0 \leq P \leq 1$), T - ймовірність виникнення джерела загрози ($0 \leq T \leq 1$), V - ймовірність вразливості системи до загрози ($0 \leq V \leq 1$).

Співвідношення ризиків (RR) можна розрахувати за формулою:

$$RR = (R1 - R2) / R1$$

де: RR - співвідношення ризиків, R1 - рівень ризику до впровадження контрольних заходів, R2 - рівень ризику після впровадження контрольних заходів.

Ці формули можна використовувати як основу для розрахунку оцінок ризику інформаційної безпеки підприємства.

Формалізована модель співвіднощення ризиків зображена на рис 2.4.

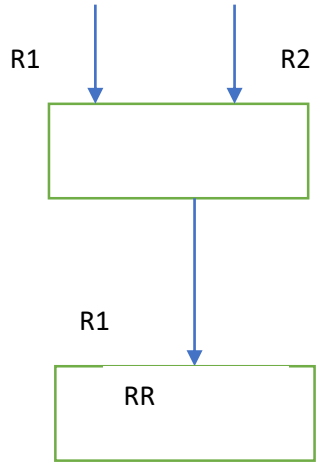

Рисунок 2.4 – Формалізація моделі співідношення ризиків

Для створення бази даних було обрано систему керування базами даних MySQL, в якості середовища розробки було обрано Visual Studio 2022.

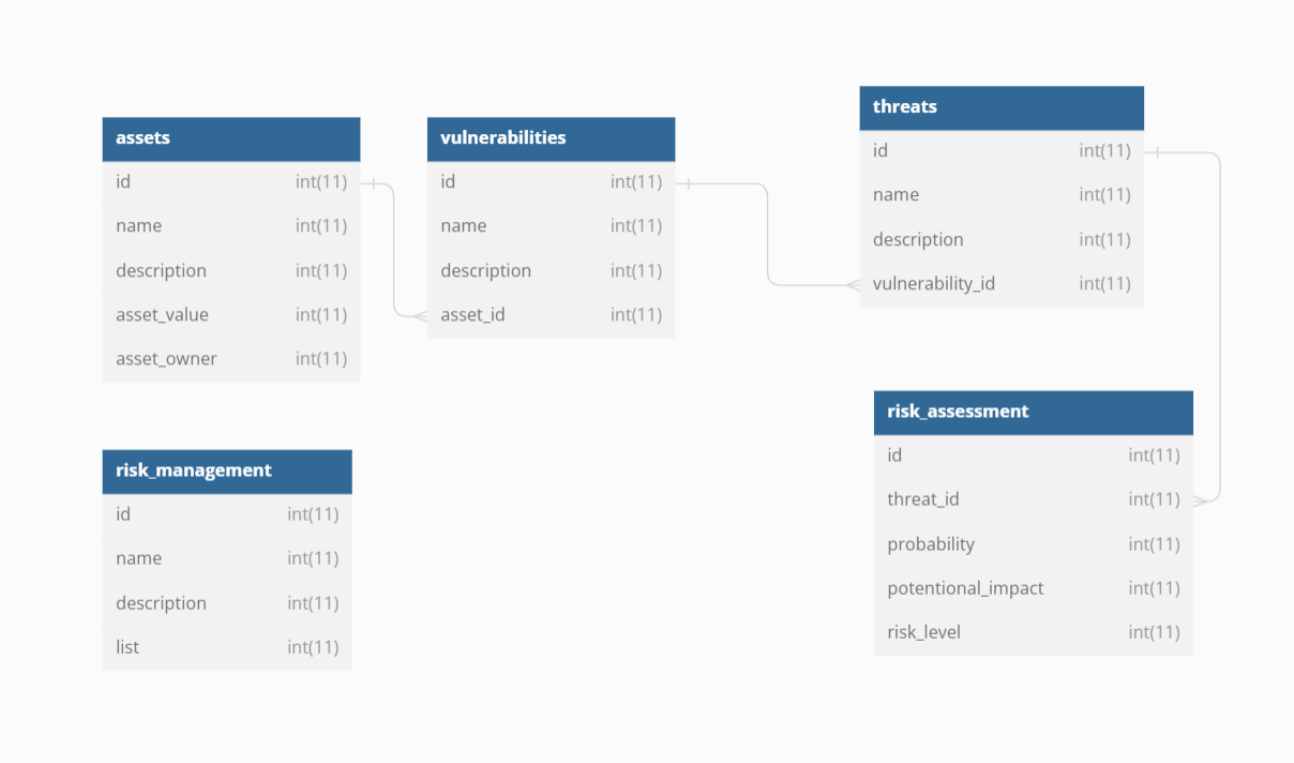

Рис.2.5 – База даних інформаційної системи

База даних складається з таких таблиць:

```
Table follows {
  following_user_id integer
  followed_user_id integer
  created_at timestamp
}

Table users {
  id integer [primary key]
  username varchar
  role varchar
  created_at timestamp
}

Table posts {
  id integer [primary key]
  title varchar
  body text [note: 'Content of the post']
  user_id integer
  status varchar
  created_at timestamp
}

Ref: posts.user_id > users.id // many-to-one

Ref: users.id < follows.following_user_id

Ref: users.id < follows.followed_user_id
```

Висновки до Розділу 2

У розділі було створено контекстну діаграму IDEF0 та її декомпозицію, розглянуто формули для розрахунку оцінки ризиків підприємства та створено формалізовану модель розрахунок співвідношення ризиків. Створено базу даних, вказано взаємозв’язки таблиць в ній.

РОЗДІЛ 3. ПРОГРАМНА РЕАЛІЗАЦІЯ ІНФОРМАЦЙНОЇ СИСТЕМИ ОЦІНКИ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1 Реалізація програмного застосунку

Для реалізації програми було обрано мову програмування C# та систему керування базами даних MySQL, в якості середовища розробки було обрано Visual Studio 2022. C# - це сучасна, об'єктно-орієнтована мова програмування, розроблена компанією Microsoft в 2000 році як частина платформи .NET. Вона була створена як пряма конкурентка Java і інтегрована з багатьма технологіями Microsoft, зокрема з Windows. C# дозволяє розробникам створювати широкий спектр застосунків, включаючи веб-застосунки, мобільні програми, додатки для робочого столу, відеоігри (через рушій Unity), і навіть програмне забезпечення для вбудованих систем[7].

Додаток має 5 модулів (вкладок): модуль аналізу ресурсного забезпечення, модуль аналізу виробничого забезпечення, модуль аналізу збуту продукції, модуль виявлення загроз та вразливостей.

Інтерфейс додатку реалізований за допомогою WindowsForms. Вигляд сторінки входу (рис. 3.1):

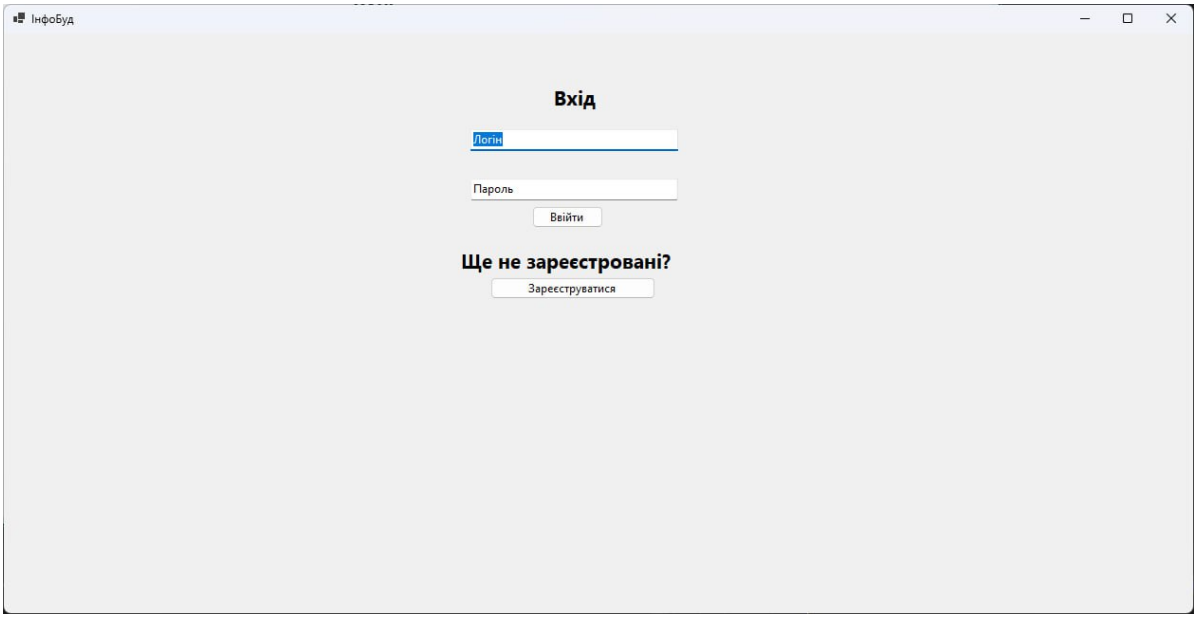

Рисунок 3.1 – Головна сторінка входу

На рис. 3.2 зображено модуль виявлення загроз та вразливостей. Він містить: назву загрози, її критичність та рекомендації щодо покращення роботи системи і зниження рівня загрози.

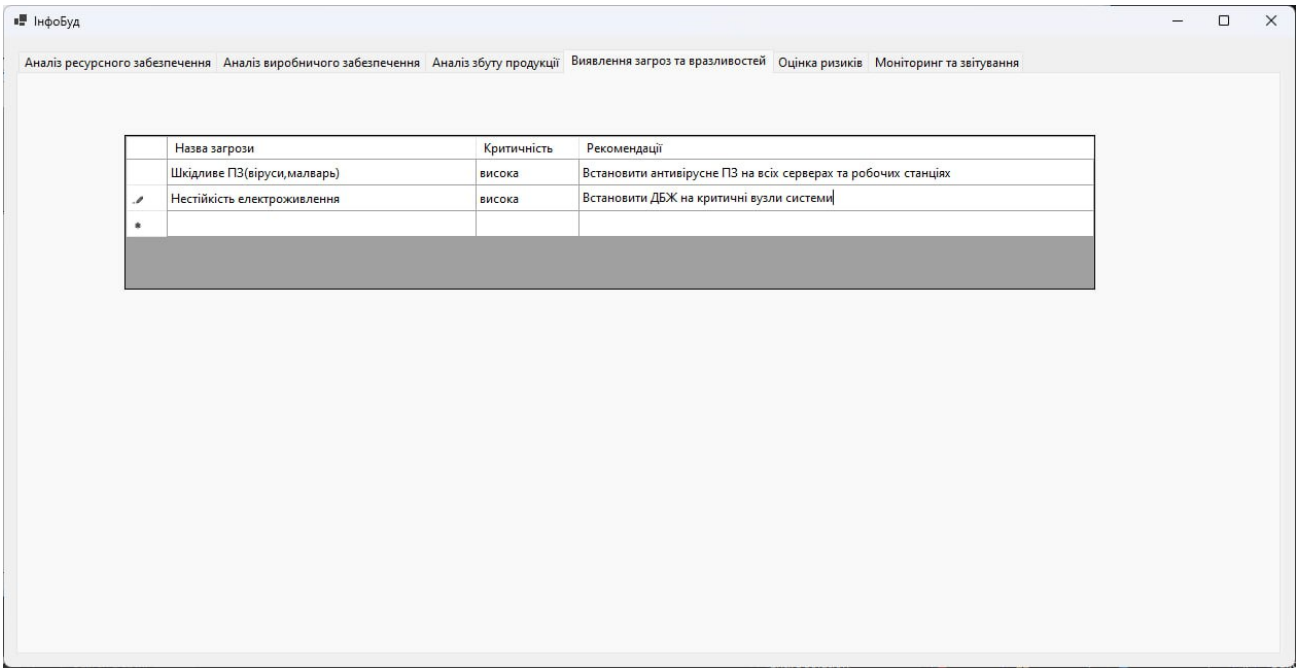

Рисунок 3.2 – Модуль виявлення загроз та вразливостей

На рис. 3.3 зображено модуль оцінки ризиків. Вона містить назву, рівень ризику, ймовірність виникнення загрози, потенційний збиток,який може понести компанія при неприйнятті рішень для захисту системи, ймовірність винекнення джерела ризику та ймовірність вразливості системи.

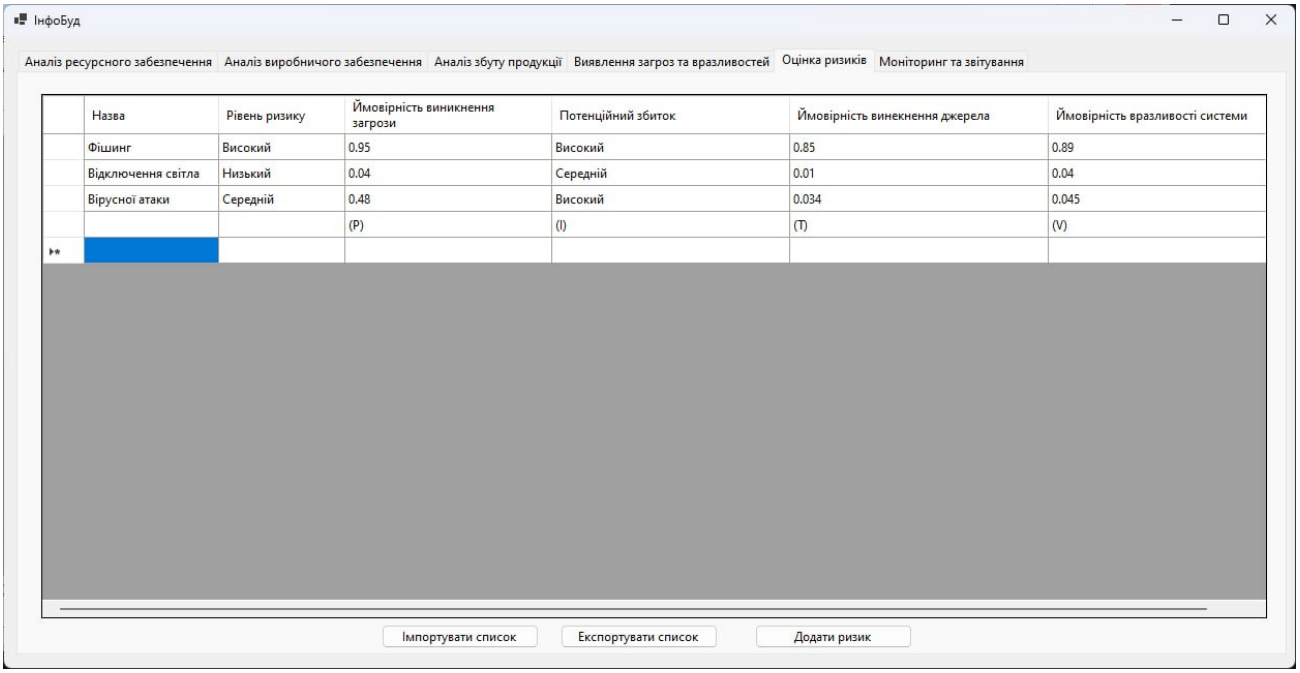

Рисунок 3.3 – Модуль оцінка ризиків

У модулі оцінка ризиків були застосованні формули для обчислення даних, що вказані у розділі 2.

Отже, розроблено додаток для компанії, що проводить аналіз ресурсного, виробничого забезпечення та аналіз збуту продукції. Після чого відбувається аналіз ймовірності виникнення загрози, оцінка можливих ризиків та надаються рекомендації щодо їх знищення.

3.2 Інструкція користувача щодо управління додатком

Інструкція користувача для управління додатком:

Реєстрація та вхід

Перед початком роботи з додатком потрібно зареєструватися, вказавши своє, ім'я, прізвище та пароль. Після підтвердження реєстрації, увійдіть в додаток, використовуючи свій логін та пароль.

Навігація

Основні модулі додатку розташовані у меню. Ви можете переходити між модулями, вибираючи відповідний пункт меню.

Модуль аналізу ресурсного забезпечення

Для додавання нових ресурсів, перейдіть в модуль "Ресурсне забезпечення" та натисніть кнопку "Додати ресурс".

Введіть дані про ресурс, такі як назва, тип, кількість, вартість та інші параметри, а потім натисніть "Зберегти".

Ви можете редагувати чи видаляти ресурси, натискаючи на відповідні кнопки поряд з кожним ресурсом.

Модуль аналізу виробничого забезпечення

Відкрийте модуль "Виробниче забезпечення" та додайте новий виробничий процес, натиснувши кнопку "Додати процес".

Введіть дані про виробничий процес, такі як назва, тривалість, витрати на ресурси, а також параметри якості продукції.

Ви можете вносити зміни в існуючі виробничі процеси, натискаючи на кнопки "Редагувати" чи "Видалити" поряд з кожним процесом.

Модуль аналізу збуту продукції

Перейдіть в модуль "Збут продукції" та натисніть кнопку "Додати кампанію" для створення нової маркетингової кампанії.

Введіть інформацію про кампанію, таку як назва, цільова аудиторія, бюджет, планувані дати початку та завершення, а також метрики успіху.

Ви можете редагувати або видалити існуючі кампанії, натискаючи на кнопки "Редагувати" або "Видалити" поряд з кожною кампанією.

Модуль виявлення загроз та вразливостей

Відкрийте модуль "Загрози та вразливості" та перегляньте список автоматично виявлених загроз та вразливостей і рекомендації до них.

Ви можете додати власні загрози або вразливості, натиснувши кнопку "Додати загрозу/вразливість" та вказавши відповідні параметри.

Видаліть або редагуйте існуючі записи, використовуючи відповідні кнопки.

Модуль оцінки ризиків

Перейдіть в модуль "Оцінка ризиків" та перегляньте автоматично згенеровані ризики на основі виявлених загроз та вразливостей.

Ви можете додати власні оцінки ризиків, натиснувши кнопку "Додати ризик" та вказавши відповідні параметри.

Видаліть або редагуйте існуючі записи, використовуючи відповідні кнопки.

Модуль моніторингу та звітування про стан інформаційної безпеки

Відкрийте модуль "Моніторинг та звітування" та перегляньте автоматично згенеровані звіти про стан інформаційної безпеки вашого підприємства.

Ви можете експортувати звіти у різних форматах, таких як PDF, CSV або Excel, натиснувши кнопку "Експорт".

Висновки до Розділу 3

У даному розділі створено веб-додаток, описано кількість модулів веб-додатку та інструкцію користувача для користування додатком.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Saderdinov AA, Trinev VA, Fedulov AA Informational security of the enterprise:Textbook.-2-е изд.- M., Publishing-trading corporation "Dashkov and K °", 2005 .- 336 s.
2. Bjorn A.G. CORAS, A Platform for Risk Analysis on Security Critical Systems - Model-based Risk Analysis Analysis Targeting Security, 2002.
3. Krasnikova, TV, Nevezhin, V.P. Modeling the assessment in the audit of information systems security / T.B. Krasnikov, V.P. Nevezhin // VII International Student Electronic Scientific Conference "Student Scientific Forum 2015".
4. Комаха А. Організація служби економічної безпеки на підприємстві // Бізнес і безпека. 2002. № 3. С. 12–13.
5. Комаха А. Методи економічної безпеки бізнесу // Бізнес і безпека. — 2002. № 3. С. 5–7.
6. Комаха А. Мета економічної безпеки бізнесу // Бізнес і безпека. — 2002. № 2. С. 23–26.
7. Арапова А. Система управління ризиками як необхідна складова забезпечення кібербезпеки. URL:http://repository.mdu.in.ua/jspui/bitstream/123456789/658/1/kiberbezpeka_2018.pdf
8. Архипов О. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Архипов, А. Скиба // Захист інформації. 2013. Т. 15, № 4. С. 366–375.
9. Богуш В. М., Кривуца В. Г., Кудін А. М., Інформаційна безпека: Термінологічний навчальний довідник/ За ред. Кривуци В. Г. К., 2004. 508 с.
10. Вадим Гребенніков, Модель порушника безпеки інформації в ІТС / Комплексні системи захисту інформації. Проектування, впровадження, супровід // URL: https://it.wikireading.ru/1000009747

11. Василенко М. Підвищення стану кібербезпеки інформаційно комунікаційних систем: якість у контексті вдосконалення інформаційного законодавства / М. Василенко // Юридичний вісник. № 3. 2018. С. 17–24.

12. 4. Дубецька С. П. Економічна безпека підприємств України. Недержавна система безпеки підприємництва як суб'єкт національної безпеки України : зб. матеріалів наук.-практ. конф. (Київ, 16-17 травня 2001 р.). Київ : Вид-во Європ. ун-ту, 2003. С.146–171.

13. Parsons, K. et al. (2010) Human Factors and Information Security: Individual, Culture and Security Environment, Science And Technology. Edinburgh South Australia. Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf. Parsons, K. et al. (2014) 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', Computers and Security. Elsevier Ltd, 42, pp. 165–176.

14. Кравчук П. Я. Сутність та передумови виникнення поняття корпоративної безпеки підприємства. Науковий вісник Волинського держ. унту ім. Лесі Українки. № 1. С.165–170.