ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут кібербезпеки та захисту інформації
Кафедра управління кібербезпекою та захистом інформації

КВАЛІФІКАЦІЙНА РОБОТА

СИСТЕМНИЙ ПІДХІД ДО УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

СТУДЕНТКА: КОТЕЦЬКА Вікторія Ігорівна

КЕРІВНИК: к.н.ц. доцент ЩАВІНСЬКИЙ Юрій Віталійович

Актуальність

- **постійне зростання і ускладнення загроз інформаційній безпеці на підприємствах критичної інфраструктури;**
- **необхідність забезпечення безперервності та стабільності функціонування об'єктів критичної інфраструктури;**
- **необхідність системного та автоматизованого підходу.**

Об`єкт дослідження – процес забезпечення інформаційної безпеки підприємства критичної інфраструктури.

Предмет дослідження – методи, моделі та інструменти системного управління ризиками інформаційної безпеки об'єктів критичної інформаційної структури.

Мета роботи: розроблення системного підходу до управління ризиками інформаційної безпеки на підприємствах критичної інфраструктури, що дозволяє підвищити ефективність і передбачуваність заходів захисту.

Завдання:

- 1.Проаналізувати наукові джерела, міжнародні стандарти та нормативно-правову базу управління ризиками (ISO/IEC 27005, NIST SP 800-30, CIS Controls).
- 2.Визначити основні загрози та вразливості інформаційних систем критичної інфраструктури.
- 3.Дослідити сучасні методи і моделі управління ризиками (кількісні, якісні, системні).
- 4.Розробити модель системного управління ризиками інформаційної безпеки.
- 5.Побудувати матрицю ризиків та пріоритети заходів для їх зменшення.
- 6.Провести апробацію системного підходу на умовному або реальному підприємстві.
- 7.Сформувати практичні рекомендації щодо впровадження розробленого підходу.

Методи дослідження:

- теоретичний аналіз наукових джерел і стандартів.
- порівняльний аналіз моделей управління ризиками.
- розгляд кейсів підприємств критичної інфраструктури.
- моделювання матриць ризиків.
- кількісна оцінка ризиків та експертна оцінка.
- використання AI для прогнозування загроз.
- візуалізація результатів через схеми і матриці.

Робота складає:

-**Вступ**
-**РОЗДІЛ 1.** ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
-**РОЗДІЛ 2.** АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ІНСТРУМЕНТІВ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
-**РОЗДІЛ 3.** РОЗРОБКА СИСТЕМНОГО ПІДХОДУ ДО УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
-**ВИСНОВКИ**
-**ПЕРЕЛІК ПОСИЛАНЬ (62 джерела)**

У першому розділі

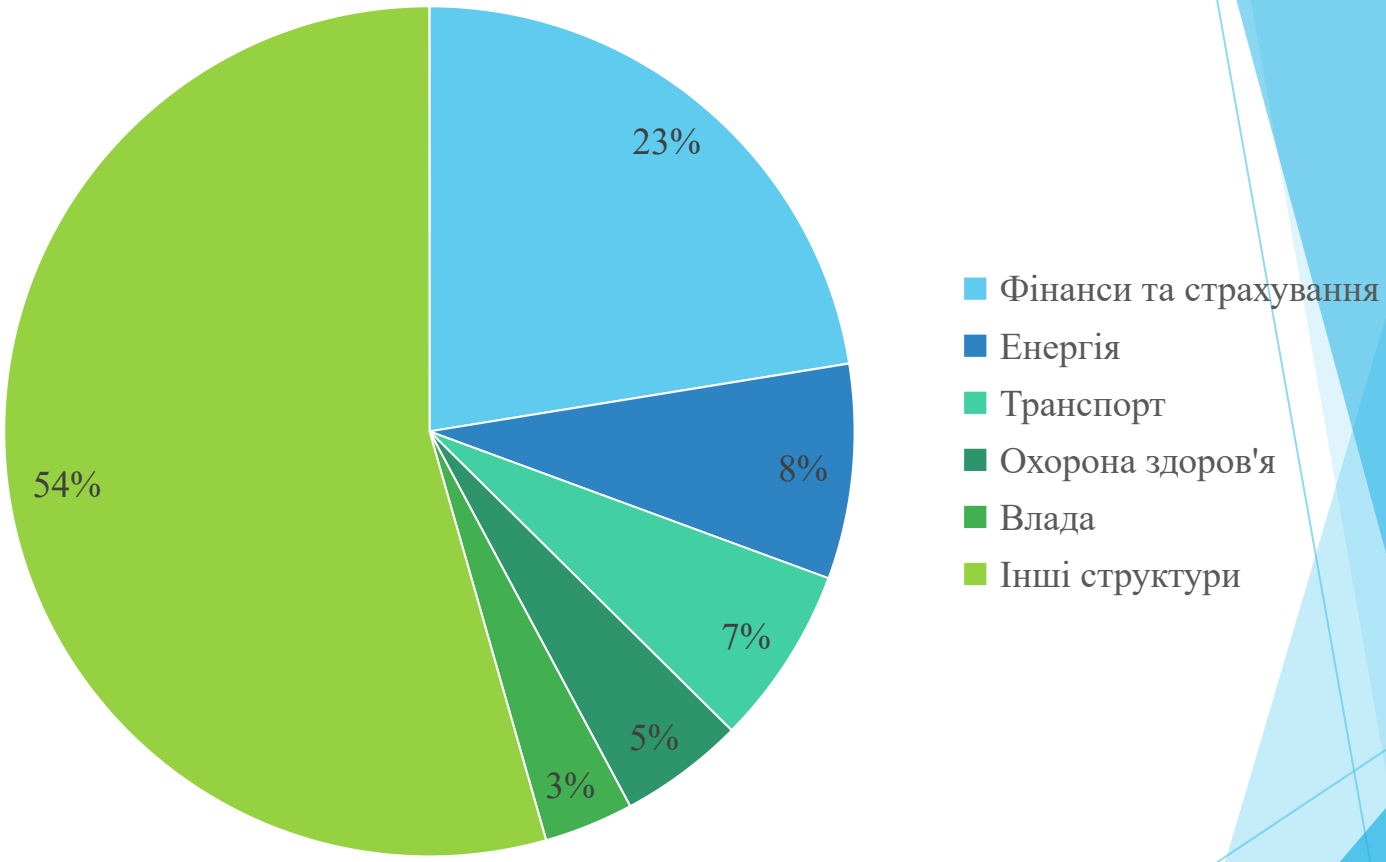

Рис. 1.4 - Відсоток кібератак з всього світу спрямований на КІ

У першому розділі

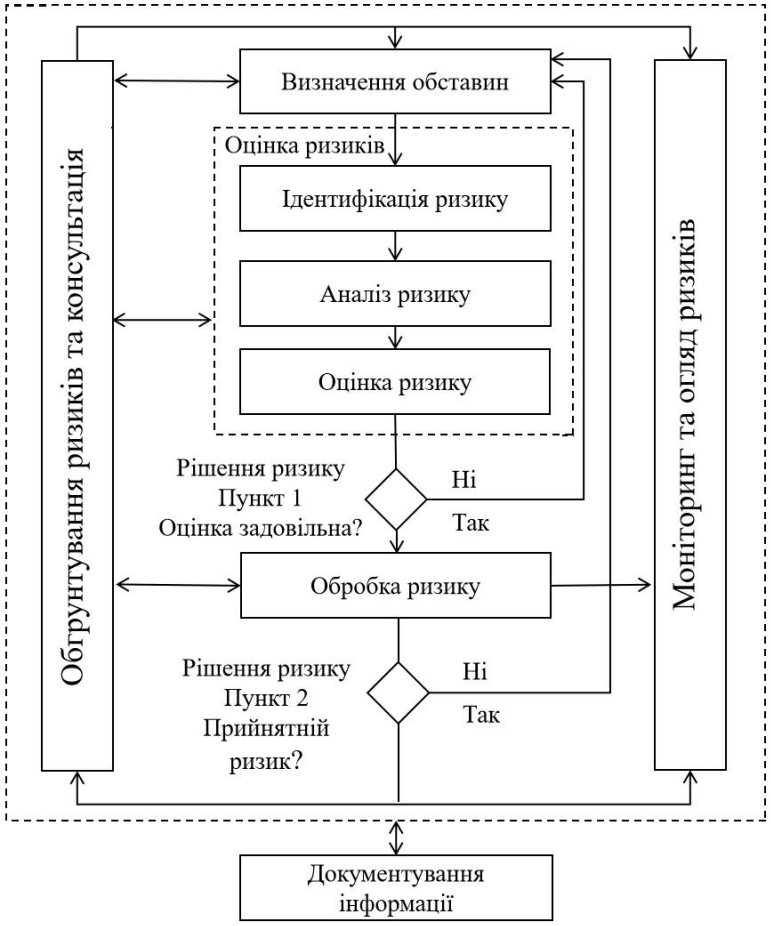

Рис. 1.2 Схема алгоритму дій з управління ризиками ІБ відповідно до ISO/IEC 27005

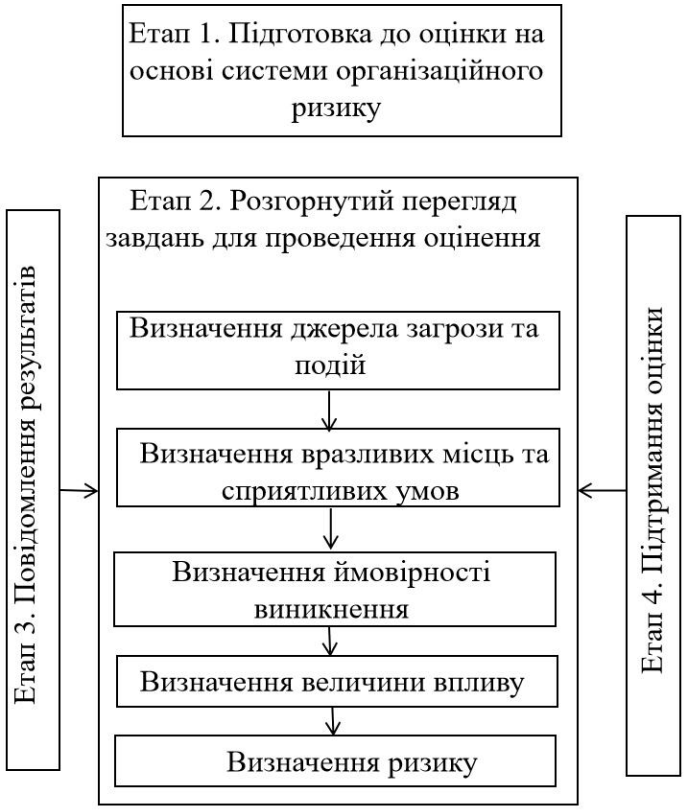

Рис. 1.3 Процес оцінювання ризиків NIST 800-30

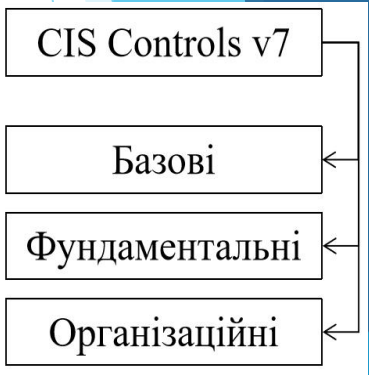

Рис. 1.4 Елементи керування CIS версії 7

У другому розділі

Рис. 2.1 Алгоритм ідентифікації ризиків

Рис. 2.3 Етапи автоматизації GRC

У другому розділі

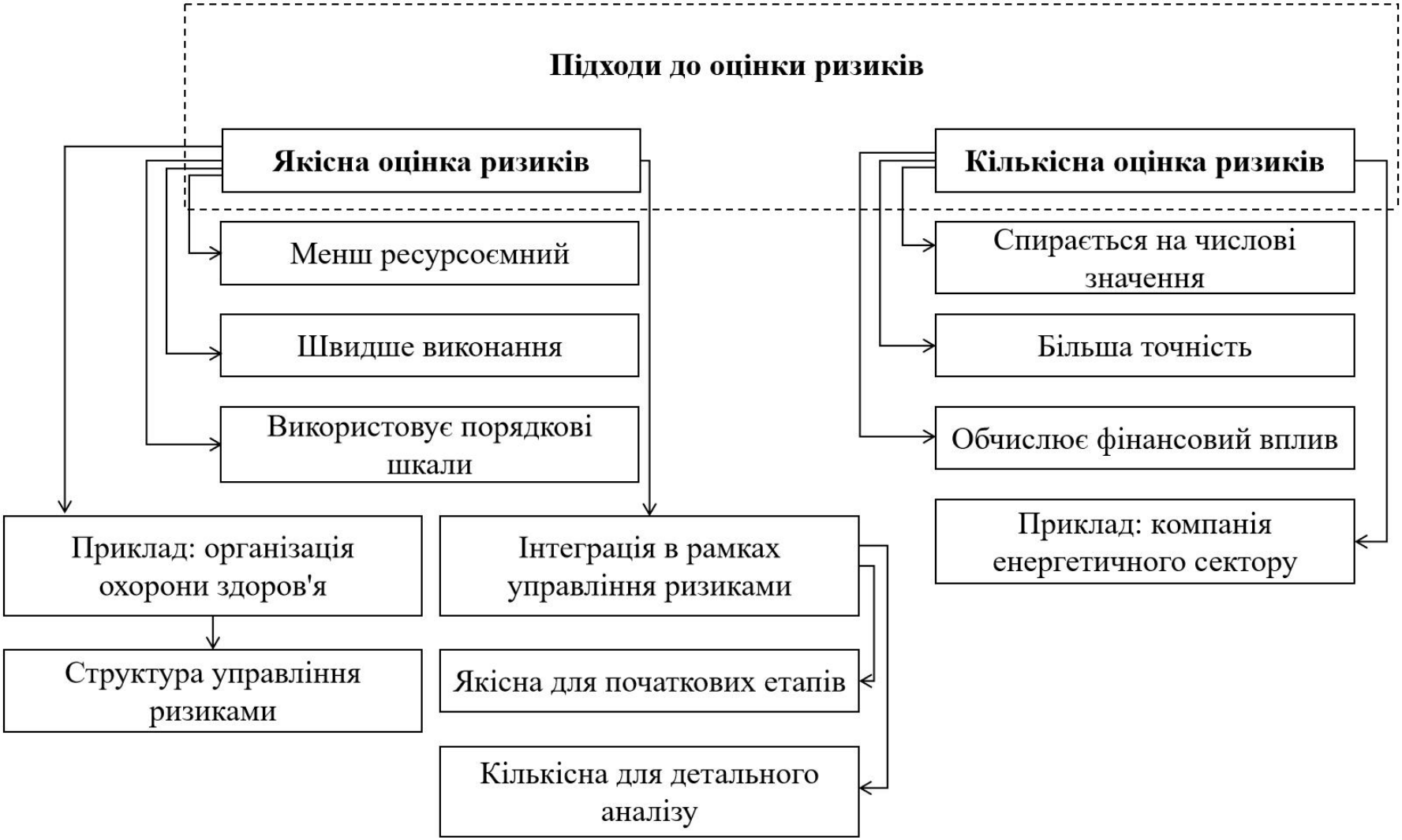

Рис. 2.2 Порівняння якісних і кількісних оцінок ризиків

У третьому розділі

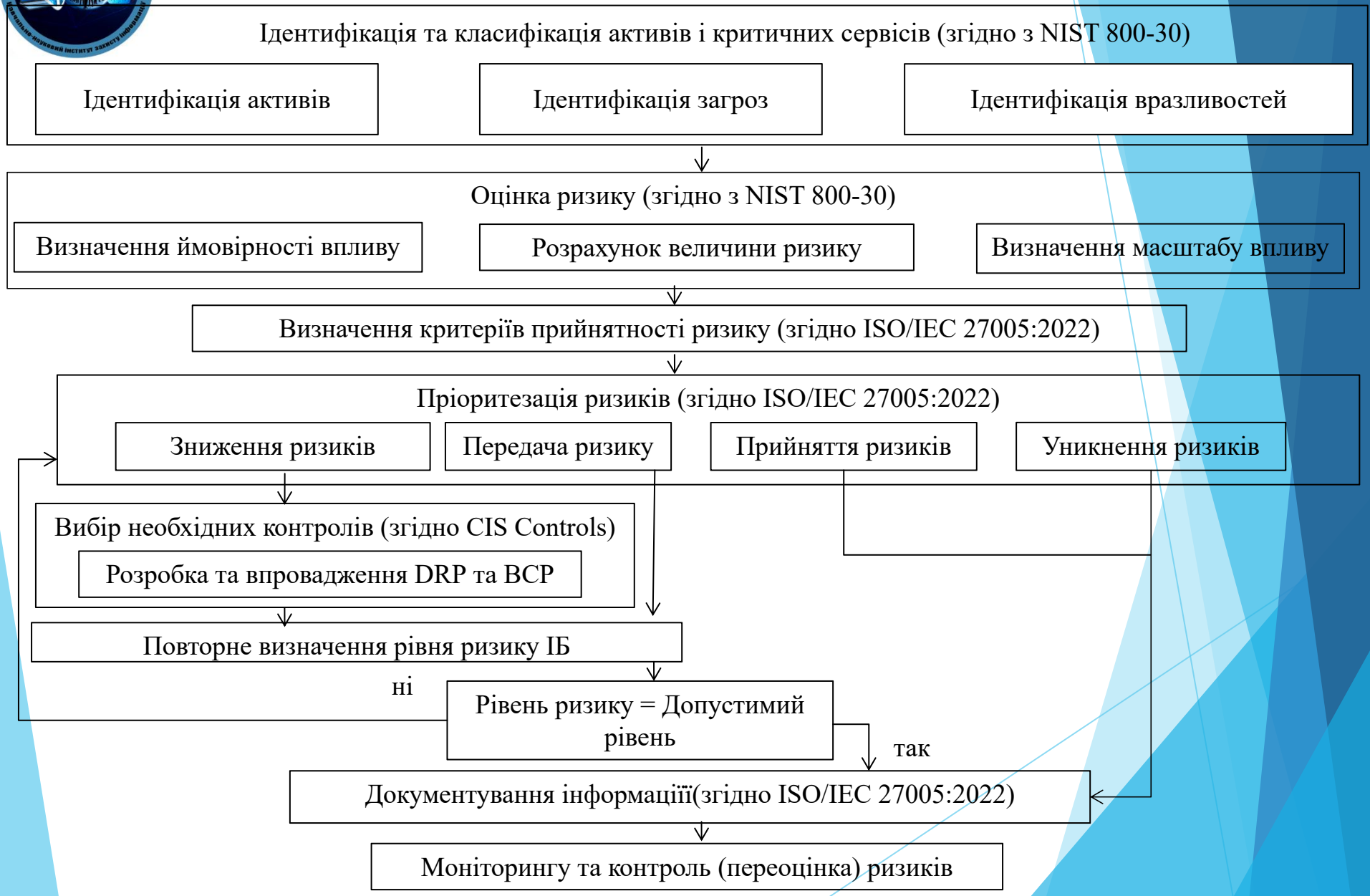

Рис. 3.1 - Модель управління ризиками для підприємств критичної інфраструктури

У третьому розділі

Серйозність \ Ймовірність	Дуже низька	Низька	Середня	Висока	Дуже висока
Мала	Низький ризик	Низький ризик	Низький ризик	Середній ризик	Середній ризик
Помірна	Низький ризик	Низький ризик	Середній ризик	Середній ризик	Високий ризик
Середня	Низький ризик	Середній ризик	Середній ризик	Високий ризик	Високий ризик
Велика	Середній ризик	Середній ризик	Високий ризик	Високий ризик	Високий ризик
Критична	Середній ризик	Високий ризик	Високий ризик	Високий ризик	Високий ризик

(3.2)

Рис. 3.2 Матриця ризику

1) $R = P \cdot I$ 2) $R = P \cdot A$ 3) $R = T \cdot V \cdot C$

У третьому розділі

Рекомендації щодо впровадження системного підходу до управління ризиками інформаційної безпеки на підприємствах критичної інфраструктури

Рекомендація	Очікувані перемоги	Очікуваний вплив на стійкість (%/час)
Впровадження системи моніторингу та раннього виявлення загроз	Швидке виявлення аномалій та потенційних атак	Зменшення часу реагування на інциденти, зниження ймовірності значних збитків, підвищення кіберстійкості критичної інфраструктури
Регулярне навчання персоналу та підвищення кіберобізнаності	Підвищення компетентності співробітників	Зниження ризику внутрішніх загроз, людських помилок та несанкціонованого доступу
Використання засобів шифрування та контролю доступу до критичних даних	Захист конфіденційної інформації від несанкціонованого доступу	Зменшення ризику витоку даних, відповідність законодавчим вимогам та підвищення довіри клієнтів
Регулярний аудит та тестування безпеки	Виявлення потенційних вразливостей до атак	Зниження ймовірності успішних кіберінцидентів, підвищення надійності систем
Впровадження системи резервного копіювання та відновлення	Збереження критично важливих даних та систем	Забезпечення швидкого відновлення після інцидентів, зниження ризику тривалого простою

Результати роботи оприлюднені на

Всеукраїнській науково-практичній конференції м. Київ, 27 лют. 2025 р., «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу»

Збірник тез. – К.: ДУІКТ, 2025 С. 58-60 (м. Київ, 27 лют. 2025 року)в Навчально-науковому інституті кібербезпеки та захисту інформації ДУІКТ.

Всеукраїнській науково-практичній конференції м. Київ, 29 жовт. 2025 р., «Актуальні проблеми кібербезпеки»

Збірник тез. – К.: ДУІКТ, 2025 С. 221-222 (м. Київ, 29 жовт. 2025 року) в Навчально-науковому інституті кібербезпеки та захисту інформації ДУІКТ.

Висновки

У кваліфікаційній роботі досліджено системний підхід до управління ризиками інформаційної безпеки критичної інфраструктури, розроблено й практично перевірено ефективну модель, що зменшує час реагування на інциденти та фінансові втрати, і надано рекомендації для підвищення кіберстійкості підприємств КІ.

ДЯКУЮ ЗА УВАГУ!