МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«28» 12 2024 р.

Кваліфікаційна робота
на правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА

Розробка системи підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022

Ступінь вищої освіти: магістр
Галузь знань: 14 Електрична інженерія
Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконала: студентка 6 курсу групи 6367м
Іванюк Анастасія Олексіївна _____

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ А.О. Іванюк

Керівник:
к.т.н., доцент, доцент кафедри комп'ютерних технологій та інформаційної безпеки
Турти Марина Валентинівна _____

Миколаїв – 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми, к.т.н.,
доцент, доцент кафедри КТІБ
_____ Турти М.В.
«_4_» _11_____ 2024 р.

ЗАВДАННЯ
на кваліфікаційну роботу

Студентка: Іванюк Анастасія Олексіївна
Курс:6
Група: 6367м
Ступінь вищої освіти: магістр
Галузь знань: 14 Електрична інженерія
Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: Розробка системи підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022
затверджена наказом НУК від «_14__» жовтня 2024 р. № _1075 - уч___

2. Вихідні дані до роботи: ДСТУ ISO/IEC 27005:2022, теоретичні основи менеджменту інформаційної безпеки, побудови баз даних та прийняття рішень

3. Перелік питань, які необхідно розробити: провести аналіз відкритої нормативно-правової бази і визначити принципи та процедури ранжування загроз, критерії і правила прийняття рішень щодо рангів загроз; розробити основні алгоритми і структуру системи підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022.

4. Терміни виконання завдання:
термін видачі завдання: «_04_» вересня 2024 р.
термін подання роботи: «_19_» грудня 2024 р.

6. План-графік виконання кваліфікаційної роботи

№ п/п	Заходи	Дата		Готовність	Відмітка про виконання
		Навч. тиждень	Контрольна дата		
1.	Наукове стажування	1 - 8	25.10.2024	Звіт з наукового стажування	Виконано
2.	Організаційні збори	9	31.10.2024	Попередній варіант змісту КР	Виконано
3.	Рубіжний контроль	10	05.11.2024	Попередній варіант оглядових розділів	Виконано
4.	Рубіжний контроль	13	28-29.11.2024	1. Попередній варіант повної КР. 2. Попередній варіант презентації.	Виконано
5.	Рубіжний контроль	15	12.12.2024	Доповідь на 12-ій Всеукраїнській науково-технічній конференції з міжнародною участю «СПІБТ–2024»	Виконано
6.	Перевірка на плагіат	15	12-13.12.2024	Електронний варіант кваліфікаційної роботи	Виконано
7.	КЕ на рівень « магістра»	16	17-18.12.2024	Здавання державного екзамену зі спеціальності на ступінь бакалавра	Виконано
8.	Кафедральний захист	16	19.12.2024	1. Оформлена КР (в форматі pdf) (передається студентом на кафедрі для внутрішньої рецензії). У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).	Виконано
9.	Подання документів на захист	16	20.12.2024	1. Подання щодо захисту КР: тема, успішність, висновок керівника та висновок кафедри про КР. 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Електронний варіант та роздрукована презентація в кількості 5 примірників. 4. Електронний варіант КР на диску	Виконано
10.	Захист ДР	17	24,26,27, 28.12.2024	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.	Виконано

ПРИМІТКА: Завдання додається до виконаної роботи та подається до атестаційної комісії.

Керівник
доцент кафедри комп'ютерних технологій
та інформаційної безпеки, к.т.н., доцент _____М.В. Турти
Студентка _____А.О. Іванюк

АННОТАЦІЯ

Іванюк А.О. Розробка системи підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022

Кваліфікаційна робота на здобуття ступеня вищої освіти «магістр» за спеціальністю 141 «Електроенергетика, електротехніка та електромеханіка» галузі знань: 14 «Електрична інженерія» і освітньо-професійною програмою «Системи технічного захисту інформації, автоматизація її обробки». – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2024.

Пояснювальна записка: 114 с., 39 рис., 63 посилання.

Кваліфікаційна робота присвячена актуальній темі – розробці засобів підтримки прийняття ефективних рішень в галузі менеджменту інформаційної безпеки. Об'єктом дослідження в даній роботі є загрози безпеці інформації з обмеженим доступом. Предметом дослідження в даній роботі є методики оцінювання загроз безпеці інформації з обмеженим доступом. Метою даної кваліфікаційної роботи є розробка системи підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022. Методами дослідження є методи менеджменту інформаційної безпеки, методи теорії прийняття рішень і теоретичні основи баз даних. В роботі проведено аналіз відкритої нормативно-правової бази і визначені принципи та процедури ранжування загроз, критерії і правила прийняття рішень щодо рангів загроз; розроблено основні алгоритми і структура системи підтримки прийняття рішень щодо ранжування загроз за ISO/IEC 27005:2022

Результати роботи можуть бути використані при проектуванні та оцінюванні ефективності комплексних систем захисту інформації та в навчальному процесі за освітньою програмою «Системи технічного захисту інформації, автоматизація її обробки» зі спеціальностей 125 «Кібербезпека» та 141 «Електроенергетика, електротехніка та електромеханіка».

Ключові слова: міжнародний стандарт, кібербезпека, загрози інформації, ранг загрози, система підтримки прийняття рішень.

ANNOTATION

Ivanyuk A.O. Development of a decision support system for threat ranking according to ISO/IEC 27005:2022

Qualifying work on receiving degree of "Master" in the specialty 141 "Electrical energetics, Electrical Engineering and Electromechanics" in the field of knowledge 14 "Electrical Engineering" and educational and professional program "Systems of technical protection of information, automation of its processing." - Admiral Makarov National University of Shipbuilding, Mykolaiv, 2024.

Explanatory note: 114 p., 39 figures, 63 references.

The qualification work is devoted to a topical topic - the development of effective decision-making support tools in the field of information security management. The object of research in this work is threats to the security of information with limited access. The subject of research in this paper is methods of assessing threats to the security of information with limited access. The purpose of this qualification work is to develop a decision support system for threat ranking according to ISO/IEC 27005:2022. Research methods are methods of information security management, methods of decision-making theory, and theoretical foundations of databases. The analysis of the normative-legal base have been carried out, the principles and procedures of threat ranking, criteria and decision-making rules regarding threat ranks have been determined; the main algorithms and structure of the decision support system for threat ranking according to ISO/IEC 27005:2022 have been developed in this work

The results of the work can be used in the design and evaluation of the effectiveness of complex information protection systems and in the educational process under the educational program "Technical information protection systems, automation of its processing" in specialties 125 "Cybersecurity" and 141 "Electric power engineering, electrical engineering and electromechanics".

Keywords: international standard, cyber security, information threats, threat rank, decision support system.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

CERT-UA – Computer Emergency Response Team of Ukraine;

CIA − Confidentiality, Integrity, Availability;

CIAAN − Confidentiality, Integrity, Availability, Authentication, Non-repudiation;

DSECCT − Digital Security Classification of Threats;

ENISA − European Union Agency for Cybersecurity;

IoT − Internet of Things;

ISACA − Information Systems Audit and Control Association;

MITM − Man in the Middle;

OCTAVE − Operationally Critical Threat, Asset, and Vulnerability Evaluation methodology;

PDCA − Plan-Do-Check-Act;

АС − автоматизована система;

ДІР – державні інформаційні ресурси;

ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації ;

ДТ – державна таємниця;

ЄС – Євпропейський союз;

ІБ – інформаційна безпека;

ІзОД− інформація з обмеженим доступом;

ІКС − інформаційно-телекомунікаційна система;

ІКТ − інформаційно-комунікаційна технологія;

ІР − інформаційний ресурс;

КІ – критична інфраструктура;

КСЗІ – комплексна система захисту інформації;

МІБ – менеджмент інформаційної безпеки;

ОІД – об’єкт інформаційної діяльності;

ПЗ – програмні зазасоби;

РІБ – ризик и інформаційної безпеки;

СІ – службова інформація;

СМО – системи масового обслуговування;

СППР – система підтримки прийняття рішень;

СУІБ – система управління інформаційною безпекою;

ТЗІ − технічний захист інформації;

ШІ – штучний інтелект.

ВСТУП

Розвиток інформаційно-комунікаційних технологій (ІКТ) та інформаційно-комунікаційних систем (ІКС), цифровізація сучасного суспільства призволять до залежності економічної та національної безпеки держав, здатності людей задовольнити свої життєво необхідні потреби від безпеки ІКС, доступності та ефективності спільного використання інформаційних ресурсів (ІР).

Кіберпростір, який не так давно розглядався як просте середовище циркуляції інформації, на даний час має широкий спектр ролей: вимір геополітичного суперництва [17], середовище інформаційних воєн, засіб проведення оперативно-розшукової діяльності [30] тощо.

Захист кіберпростору, забезпечення його кіберстійкості і кіберготовності об’єктів інформаційної діяльності (ОІД) передбачає організацію ефективної системи виявлення загроз та протидії актуальним загрозам. Для визначення зактуальних загроз необхідними є заходи із створення ефективної системи індикаторів кіберзагроз, проведення моніторингу стану кіберпростору, оцінювання і управління кіберризиками, накопичення статистичних даних і виявлення ознак загроз, прогнозування появи новітніх загроз з пнвними очікуваними наслідками і асоційованими ризиками.

Організаційно-технічна модель кіберзахисту, затверджена Постановою Кабінету Міністрів України від 29 грудня 2021 р. №1426 [48], Стратегія кібербезпеки України [56] і плани її реалізації [46, 47] передбачають розвиток систем виявлення та реагування на кіберзагрози з метою ефективного управління ризиками інформаційної безпеки (ІБ) і забезпечення кіберготовності та кіберстійкості ОІД, особливо об’єктів критичної інфраструктури. Організаційно-технічна модель кіберзахисту [48] передбачає врахування досвіду держав - членів

Європейського Союзу (ЄС) та НАТО і розвиток систем реагування на кіберінциденти і управління ризиками інформаційної безпеки (РІБ).

На даний час прийнято проводити аналіз факторів РІБ і оцінювання РІБ шляхом використання евристичних експертних оцінок. При цьому можуть застосовуватися десятки методів оцінки ризиків [14], вибір серед яких складно здійснити [22]. Визначення РІБ проводиться на основі прийнятих дослідником класифікації загроз, моделі загроз і методів оцінки ризиків, які мають узгоджуватися з діючими нормативними документами. Цим питанням присвячені роботи багатьох науковців та практиків як в Україні, так за кордоном [1, 2, 5-12, 22-26, 28, 29, 32, 52-55, 59-63], однак залишається невирішеною задача автоматизації процесів визначення рангів загроз за їх критичністю згідно із відповідності з міжнародними стандартами.

Метою даної кваліфікаційної роботи є розробка системи підтримки прийняття рішень щодо ранжування загроз за *ISO/IEC* 27005:2022.

Для досягнення поставленої мети необхідно розв’язати наступні задачі:

– провести аналіз відкритої нормативно-правової бази і визначити принципи та процедури ранжування загроз;

– визначити критерії і правила прийняття рішень щодо рангів загроз;

– розробити основні алгоритми і структуру системи підтримки прийняття рішень щодо ранжування загроз за *ISO/IEC* 27005:2022.

Об’єктом дослідження в даній роботі є загрози безпеці інформації з обмеженим доступом (ІзОД).

Предметом дослідження в даній роботі є методики оцінювання загроз безпеці ІзОД.

Методами дослідження в даній кваліфікаційній роботі є методи менеджменту інформаційної безпеки (МІБ), методи теорії прийняття рішень і побудови систем підтримки прийняття рішень (СППР), теоретичні основи баз даних.

1 ПРОБЛЕМИ ОЦІНЮВАННЯ І КЛАСИФІКАЦІЇ ЗАГРОЗ

1.1 Актуальність задачі ранжування загроз

Актуальність задачі ранжування загроз викликана сучасними викликами кібербезпеці України. Такими викликами, згідно Стратегії кібербезпеки України (2021 рік) [57], є наступні фактори і тенденції:

– мілітаризація кіберпростору;

– поширення кіберборотьби на сферу міжнародної конкуренції;

– розвиток кіберзброї і змагальний характер розвитку засобів кіберборотьби в умовах впровадження новітніх інформаційно-комунікаційних технологій (ІКТ) (таких як хмарні обчисленння, 5G-мережі, засоби штучного інтелекту та Інтернету речей (англ. *Internet of Things, IoT*), обробки великих даних) та новітніх технологій електронної взаємодії громадян із державою;

– вплив пандемії *COVID*-19 на економіку України, в результаті якої відбулася трансформація суспільних відносин шляхом розширення сфер дистанційного використання електронних сервісів, ІКС та ІКТ.

Ефективна протидія кіберзагрозам у сучасному безпековому середовищі визначаються Стратегією національної безпеки України [58] (2020 рік) і Стратегією забезпечення державної безпеки (2022 рік) [56] як один з напрямів реалізації національної безпеки, разом із захистом водного, повітряного та територіального просторів країни.

Безпека сучасного кіберпростору суттєво залежить від тенденцій його розвитку, зокрема від:

– посилення міжнародної конкуренції в сфері політики та економіки, наприклад, загострення змагання за світове політичне лідерство між США і

Китаєм, конкуренція України і Російської Федерації на світових ринках зерна, що стало причиною (на думку заступниці голови транспортного комітету Верховної Ради України про Чорне море Юлії Клименко [33]) економічної блокади українських портів Росією, яка «не має нічого спільного з військовими діями»;

– поширення внаслідок глобалізації і анонімності Інтернету міжнародної злочинності і міжнародного тероризму, розширення спектру злочинів, скоюваних за допомогою глобальної мережі та дистанційних сервісів;

– застосування кіберзасобів в умовах гібридної війни Російською Федерацією (на час прийняття Стратегії національної безпеки України – 2020 рік) і під час активних військових дій;

– поширення кіберзагроз, спрямованих на порушення штатних режимів функціонування об’єктів критичної інфраструктури, і підвищення рівня критичності їх наслідків.

Таким чином, протидія кіберзагрозами, забезпечення кіберготовності і кіберстійкості стало одним напрямів діяльності держави на зовнішньополітичній та внутрішньополітичній арені.

Забезпечення здатності завдавати супротивнику таких втрат у кіберпросторі, які унеможливлять реалізацію його агресивних намірів не тільки у кіберпросторі, а й не землі, в повітрі і на морі є пріоритетним напрямом розвитку боєздатнихі Збройні Сили України, військового резерву, територіальної оборони та інших органів сектору безпеки і оборони [58].

Організація активної протидії кібератакам та підвищення її ефективності є пріоритетними завданнями також для «правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їх компетенції» [58].

В умовах цифрової трансформації розвиток методів і засобів забезпечення кібербезпеки має бути спрямованим на «гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури» [58] і мати системний

характер. В рамках системного підходу до захисту України від кіберзагроз, що впливають на стан національної безпеки, планується [47, 48] завершити створення національної системи кібербезпеки, сформувати і скоординувати адаптовні спроможності суб'єктів забезпечення кібербезпеки і кібероборони, що будуть адекватні сучасним загрозам і викликам.

Актуальні загрози кібербезпеці України за Стратегією кібербезпеки України [57] становлять кіберзлочинність, кібершпигунство, кібертероризм, які можуть бути ініційовані одиничним злочинцями, злочинними і терористичними угрупуваннями, а також урядами окремих країн.

Для сучасної кіберзлочинності і кібершпигунства характерним є використання прихованих, тривалих і складних кібератак, попередження, виявлення та нейтралізаця котрих є складною задачею.

Терористичні організації використовують кіберпростір не тільки для вчинення актів кібертероризму, а й для організації терористичної діяльності, наприклад для надання і отримання фінансової підтримки.

Гібридна агресія Російської Федерації у кіберпросторі України, що переросла у військову агресію, здійснювалася із застосуванням кіберзброї наступального призначення, арсенал якої невпинно нарощувався. Її цілями були і залишаються, насамперед, об'єкти критичної інформаційної інфраструктури, зокрема, ІКС державних органів України, ІКС систем енергозабезпечення та транспорту, в котрих неодноразово реєструвалися кіберінциденти, метою котрих були кібердиверсії. Кібератаки на об'єкти критичної інформаційної інфраструктури можуть використовуватися для організації спеціальних інформаційних операцій, зокрема, для «маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності» [57], отримання розвідданих, здійснення розвідувально-підривної діяльності, отримання прихованого доступу до інформаційних ресурсів обмеженого доступу, контролю над ними і процесами їх обробки тощо.

Чинниками, які формують кіберзагрози в Україні є:

– недоліки правового забезпечення: недосконаліть і застаріліть нормативно-правової бази з ІБ, повільна імплементація положень міжнародного і європейського законодавства, неврегульованість і складність процедур проведення розслідувань правопорушень у кіберпросторі, занизький рівень правової відповідальності за їх скоєння;

– недостатня захищеність об'єктів критичної інформаційної інфраструктури, ІКС суб'єктів господарювання, в яких обробляється ІзОД, державних ІР;

– недоліки організації робіт із кіберзахисту: фінансування за залишковим принципом, відсутність кадрового забезпечення необхідного рівня кваліфікації, відсутність жорстко заданих процедур підвищення кваліфікації кадрів до відповідного сучасним вимогам рівня, неефективні механізми стимулювання висококваліфікованих фахівців, відсутність належного контролю за станом кібербезпеки у значній частині державних органів, відсутність системи незалежного аудиту ІБ, відсутність механізмів оперативного аналізу стану кібербезпеки з метою своєчасного виявлення загроз і вразливостей ІКС та механізмів оперативного оповіщення зацікавлених сторін про виявлені загрози, вразливості та найліпші практики їх нейтралізації;

– недостатня спроможність України протидіяти кіберзагрозами внаслідок відсутності гарантій безпеки і наявності ризику присутності незадекларованих функцій в апаратних і програмних засобах (ПЗ) ІКТ закордонного виробництва, тобто залежність України від іноземних виробників ІКТ-продукції створює додаткові уразливості вітчизняної інформаційної інфраструктури;

– недостатній рівень обізнаності громадськості щодо кібергігієни, кіберзагроз, механізмів та практик кіберзахисту та відсутність системи заходів підвищення цього рівня.

З метою впровадження в життя проголошених у Стратегії кібербезпеки України [57] положень було розроблено і прийнято «План реалізації Стратегії кібербезпеки України» [47] і «План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України» [46], а також ряд нормативно-правових актів щодо захисту критичної інфраструктури і «Положення про організаційно-технічну модель кіберзахисту» [48]. В цих документах, крім іншого, розглядаються питання створення і впровадження ефективної системи індикаторів кіберзагроз, розробки механізмів сповіщень зацікавлених сторін про кіберзагрози та поширення найкращих практик їх виявлення і нейтралізації.

Моніторинг кіберпростору має на меті виявлення актуальних загроз, серед яких потім обираються ті загрози, з якими асоційовані РІБ, що мають пройти процедуру обробки у циклі менеджменту РІБ згідно міжнародному стандарту *ISO/IEC* 27005:2022 «*Information security, cybersecurity and privacy protection — Guidance on managing information security risks*» [4]. При цьому першочерговій обробці підлягають ризики, асоційовані із загрозами з максимальним рейтингом. Оскільки процедура менеджмену ризиків за *ISO/IEC* 27005:2022 є циклічною, то ранжування загроз багатократно повторюється і має займати якомога менше часу.

Таким чином, побудова СППР ражування загроз за за *ISO/IEC* 27005:2022 є актуальною задачею з точки зору національної безпеки України, кібербезпеки і з точки зору ефективного планування обробки ризиків.

1.2 Теоретичні засади ранжування загроз

За визначенням, наведеним у «Стратегії забезпечення державної безпеки», інформаційна безпека є станом «захищеності національних інтересів людини,

суспільства і держави в інформаційній сфері» [56] , і є складовою національної безпеки України.

Кібербезпека, згідно «Положенню про організаційно-технічну модель кіберзахисту» [48], є захищеністю «життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».

Об’єктами забезпечення державної безпеки згідно [56] є, крім іншого, державна таємниця (ДТ), службова інформація (СІ), ІБ та кібербезпека.

Безпека інформації, що є ДТ та СІ, забезпечується за рахунок «впровадження комплексу організаційно-правових, адміністративних, інженерно-технічних, оперативно-розшукових, контррозвідувальних, розвідувальних заходів, заходів із забезпечення технічного та криптографічного захисту секретної та службової інформації, спрямованих на запобігання її витоку» [56] .

Загрозу державній безпеці утворюють такі чинники і тенденції, які ускладнюють чи унеможливлюють захист життєво важливих національних інтересів або потенційно здатні спричинити такий ефект.

За НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу» [34] загрозою (англ. *threat*) є «будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків» автоматизованій системі (АС).

Закон України «Про основні засади забезпечення кібербезпеки України» [21] [21] визначає кіберзагрозу як «наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам

України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів».

Загроза може бути придушена засобами кібероборони або може бути успішно реалізована шляхом експлуатації наявної в системі обробки або в системі захисту інформації вразливості. За НД ТЗІ 1.1-003-99 [30] вразливість системи (англ. *system vulnerability*) визначається як «нездатність системи протистояти реалізації певної загрози або сукупності загроз».

Першим кроком на шляху адекватного і своєчасного реагування на кіберзагрози є їх виявлення. Виявлення загроз здійснюється за допомогою сигнатур, шаблонів поведінки, евристик. У IV кварталі 2024 року згідно «Плану реалізації Стратегії кібербезпеки України» [47] мала бути побудована система індикаторів кіберзагроз на підставі певних технічних даних, однак «План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України» [46] свідчить, що на поточний момент ця задача вирішена частково, що зумовлено швидкими темпами змін без пекового середовища у кіберпросторі.

З кожною загрозою пов'язаний (асоційований) певний ризик (англ. *risk*), який розглядається як ймовірний (потенційний) збиток в разі успішної реалізації загрози. Величина ризику визначається як функція від «ймовірності реалізації загрози, виду і величини завданих збитків» [30]. При цьому вид цієї функції визначається прийнятою моделлю загроз, а ймовірності і збитки можуть бути представлені у природних одиницях вимірювання або у вигляді бальних оцінок.

Поява і реалізація загрози розглядаються в МІБ як інцидент ІБ. Закон України «Про основні засади забезпечення кібербезпеки України» [21] визначає кіберінцидент як подію або низку несприятливих подій у кіберпросторі ненавмисного чи навмисного характеру. В останньому випадки говорять про події з ознаками потенційної кібератаки.

Кібератакою є навмисні дії в кіберпросторі, спрямовані на:

– порушення безпеки та штатного режиму функціонування ІКС та АС будь-якого технологічного призначення;

– отримання несанкціонованого доступу до ІР і здійснення негативного впливу на захищеність інформації (порушення конфіденційності, цілісності, доступності і спостереженості ІР);

– використання ІКС для здійснення кібератак на інші об’єкти у кіберпросторі.

Виявлені кіберінциденти і кібератаки мають бути ретельно проаналізовані. Аналізу підлягають всі доступні відомості про кіберінциденти: інформація про джерело загрози; тип зловмисника; його цілі, кваліфікацію і ресурси; алгоритм дій зловмисника і технологію атаки; використані зловмисником апаратні і програмні засоби для реалізації атаки; вразливості систем обробки і захисту інформації, через які може реалізуватися або успішно реалізувалася загроза; об’єкт атаки; стан середовища функціонування об’єкта атаки і зловмисника; наслідки; заходи щодо нейтралізації негативних наслідків і результати аналізу їх ефективності. Такий аналіз дозволяє визначити індикатори кіберзагроз і сформувати рекомендації щодо попередженя, нейтралізації і зниження критичності наслідків реалізації загроз.

Закон України «Про основні засади забезпечення кібербезпеки України» [21] класифікує діяльність зловмисників у кіберпросторі як кібершпигунство, кіберрозвідку, кібертероризм і кіберзлочинність, що є сукупністю кіберзлочинів. Кіберзлочином є суспільно небезпечні дії у кіберпросторі, які визначаються як злочин за міжнародними договорами України, або за які передбачена кримінальна відповідальність за законами України.

Для кіберзахисту ІКС та/або АС мають бути задіяні певні сили кіберзахисту. За «Положенням про організаційно-технічну модель кіберзахисту» [48] такими силами є організації будь-якої форми власності, які провадять діяльність у сфері кіберзахисту та/або надають послуги із забезпечення кіберзахисту. З цією метою в

різних країнах і на міжнародному рівні утворюються спеціальні групи фахівців з кібербезпеки - команди реагування на комп’ютерні надзвичайні події, в тому числі - урядова команда реагування на комп’ютерні надзвичайні події України *CERT-UA* (англ. *Computer Emergency Response Team of Ukraine*), що є спеціалізованим підрозділом Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ).

За Положенням [48] «організаційно-технічна модель кіберзахисту є комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем». До складу цієї моделі входять три організовані сукупності об’єктів і суб’єктів:

– технологічна інфраструктура кіберзахисту - сукупність «сил та засобів кіберзахисту, інфраструктурних об’єктів, що забезпечують функціонування сил кіберзахисту, інформаційно-телекомунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту» [48];

– організаційно-керуюча інфраструктура кіберзахисту - сукупність «суб’єктів забезпечення кібербезпеки, що формують та/або реалізують державну політику у сфері кібербезпеки, визначають процедури та механізми кіберзахисту, організаційно-правові засади взаємодії між силами кіберзахисту та іншими суб’єктами забезпечення кібербезпеки» [48];

– базисна інфраструктура кіберзахисту - сукупність об’єктів «критичної інформаційної інфраструктури, комунікаційних і технологічних систем підприємств, установ та організацій, що належать до об’єктів критичної інфраструктури, а також суб’єктів господарювання, громадян та їх об’єднань, інших осіб, які провадять діяльність та/або надають послуги у сферах електронних комунікацій, електронної комерції, розвитку національних електронних ресурсів, захисту інформації та кібербезпеки» [48];

Сукупність заходів криптографічного та технічного захисту інформації (ТЗІ), організаційних, наукових, політичних, соціальних, економічних та інших заходів може бути класифікована в залежності від її цілей як:

– кіберзахист, якщо метою сукупності заходів є «запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідація їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [21];

– кібероборона, якщо метою сукупності заходів є «забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії» [21];

– система активної протидії агресії у кіберпросторі, якщо метою сукупності заходів є «підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак» ([21], [48]).

У Положенні [48] підкреслюється важливість для забезпечення кібербезпеки активної протидії агресії у кіберпросторі та кібергігієни – уміння і навичок «здійснення заходів щодо своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз» [48].

1.3 Класифікація загроз

1.3.1 Узагальнений механізм атаки на інформаційні ресурси

Механізм атаки на IP в узагальненому вигляді, наведений на рис.1.1, відображає взаємодію джерела загроз і об’єкту захисту в процесі атаки. Загрози генеруються джерелом загроз, реалізуються через вразливості об’єкту захисту і

мають для нього певні наслідки. Загрози ІР за природою виникнення можуть бути антропогенного, техногенного або природного походження і генеруватися джерелами різних типів, наприклад, зовнішніми і внутрішніми зловмисниками, різним апаратним і програмним забезпеченям ІКС та ІКТ, природними явищами.

Рисунок 1.1 - Узагальнений механізм атаки на інформаційні ресурси

Загрози за своєю сутністю не можуть бути описані повністю для будь-якого об'єкта захисту, хоча б тому, що завжди існує ймовірність появи нових, невідомих на початку дослідження загроз і дуже малоймовірних загроз. Тому при аналізі загроз враховують тільки ті загрози, ймовірність виникнення котрих або асоційований з ними ризик перевищують задане мінімальне значення. При побудові систем захисту з цієї множини загроз враховують вибірку з тих загроз, які можуть бути реалізовані через наявні вразливості.

При аналізі загроз приймають певну модель загроз. Основою кожної моделі загроз є прийнята класифікація загроз. Загрози ІР можуть бути класифіковані різним чином, за різними ознаками. Найбільш універсальною і найпоширенішою

є класифікація загроз за результатом впливу на властивості інформації, що характеризують її захищеність (конфіденційність, цілісність, доступність, спостережуваність). Така класифікація загроз відповідає, наприклад, НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [37].

1.3.2 Моделі *CIA* та *CIAAN*

Конфіденційність, цілісність і доступність (англ. *Confidentiality, Integrity, Availability*) є властивостями захищеної інформації, порушення яких приймається до уваги в моделі *CIA*, яку часто називають тріадою *CIA*. Модель *CIA* є основою аналізу загроз і вибору засобів протидії загрозам в НД ТЗІ 2.5-004-99 і НД ТЗІ 2.5-005-99 [37, 38]. В цих нормативних документах за моделлю *CIA* здійснюється вибір стандартного функціонального профілю захищеності АС. Формування комплексу засобів захисту при цьому здійснюється згідно з вимогами профілю щодо забезпечення тетроди властивостей - конфіденційності, цілісності, доступності і спостережуваності. Однак, забезпечення спостеражуваності вважається обов'язковим для усіх АС незалежно від обраного профілю, тому комплекс засобів захисту формується фактично також за моделлю *CIA*. Тріада *CIA* визначає ключові елементи, які необхідно захищати, щоб забезпечити достатній рівень захищеності ІР, ІКС, ІКТ.

В іншій популярній моделі *CIAAN* враховується п'ять властивостей захищеної інформації: конфіденційність, цілісність, доступність, автентичність і незаперечність (англ. *Confidentiality, Integrity, Availability, Authentication, Non-repudiation*). Автентичність важлива для того, щоб інформація та повідомлення надходили з надійного джерела, а незаперечність - для того, щоб суб'єкт інформаційних відносин не міг заперечити, що надіслав або отримав повідомлення чи транзакцію.

Модель *CIA* є більш розповсюдженою, ніж модель *CIAAN*. Крім цих моделей існують й інші, які можуть враховувати важливі для конкретного дослідження властивості інформації, наприклад, неспростовність.

.

1.3.3 Модель *STRIDE*

Модель *STRIDE* – це модель загроз фірми *Microsoft*. Ця модель була розроблена у 2009 році і поділяє загрози на шість типів (табл.1.1), для кожного з яких *Microsoft* надає рекомендації з протидії. Назва моделі складається з перших літер назв типів загроз.

Таблиця 1.1 - Модель *STRIDE*

Загроза		Сутність загрози
S	*Spoofing identity* Підміна мережевих об'єктів	Зловмисник видає себе за лігітимного користувача, використовуючи чужі дані для автентифікації, або замінює справжній мережевий об’єкт, наприклад сервер, хибним чи підробним. В результаті можуть бути порушені конфіденційність, цілісність, доступність і спостережуваність інформації
T	*Tampering with data* Модифікація даних	Зловмисник несанкціоновано змінює дані в процесі їх обробки або передавання, або у місці зберігання, наприклад, в базі даних. В результаті порушується цілісність даних
R	*Repudiation* Відмова від авторства	Зловмисник, що є легітимним користувачем, використовує недоліки механізмів реєстрації дій користувача для того, щоб відмовитися від «авторства» виконаної операції. В результаті порушується спостережуваність інформації
I	*Information disclosure* Розголошення інформації	Зловмисник повідомляє ІзОД особам, які не мають на неї прав доступу. В результаті порушується конфіденційність інформації
D	*Denial of service* Відмова в обслуговуванні	Зловмисник перевантажує канали зв’язку або центральний процесор сервера, що робить мережеві ресурси тимчасово недоступними для легітимних користувачів і процесів. В результаті порушується доступність інформації
E	*Elevation of privilege* Підвищення рівня привілеїв	Зловмисник, який санкціоновано отримав доступ низького рівня, несанкціоновано дістає доступ високого рівня і, відповідно, можливість виконувати несанкціоновані дії, наприклад, зчитати ІзОД, встановити шкідливі ПЗ тощо. В результаті можуть бути порушені конфіденційність, цілісність, доступність і спостереженість інформації.

1.3.4 Модель *OCTAVE*

OCTAVE (англ. *Operationally Critical Threat, Asset, and Vulnerability Evaluation methodology*) – це методологія оперативної оцінки критичних загроз, активів і вразливостей, розроблена у 2003 році Університетом Карнегі-Меллона (США) та відділом *CERT* (англ. *Computer Emergency Response Team*) Інституту розробки програмного забезпечення (англ. *Software Engineering Institute, SEI*).

Методологія *OCTAVE* спирається на власні принципи побудови моделей загроз. Вона передбачає, що опис загроз і ризиків здійснюється з різним ступенем деталізації для:

– первинного аналізу загроз і ризиків та для наступних аналізів. Це дозволяє при первинному поверхневому аналізі швидко виявити загрози і ризики, які не є критичними, і виключити їх з подальшого детального розгляду;

– великого і малого бізнесу. Кількість даних, яка обробляється при описі і аналізі загроз та ризиків для малого бізнесу є суттєво меншою за кількість даних для великого бізнесу. Тому для малого бізнесу первинний аналіз загроз одразу є деталізованим, а для великого бізнесу спочатку проводиться первинний узагальнений аналіз, при якому визначаються загрози і вразливості, які на наступному етапі опису загроз і ризиків підлягають деталізації;

– критичних і некритичних для бізнес-процесів активів. Загрози і ризики, асоційовані із некритичними для бізнес-процесів активами, на першому етапі побудови моделі загроз описуються менш детально і підлягають деталізації тільки в тому випадку, якщо первинний аналіз виявить, що асоційовані з ними ризики перевищують рівень прийнятних для організації ризиків.

OCTAVE головну увагу приділяє оцінці організаційних, а не технологічних загроз, виходячи з того, що недоліки організаційного забезпечення ІБ, наприклад, некоректний розподіл прав доступу в компанії, спричиняють несанкціоновані дії з активами і негативно впливають на операційну діяльність бізнесу

1.3.5 Классификація загроз *DSECCT*

Классификація загроз *DSECCT* (англ. *Digital Security Classification of Threats*) була розроблена компанією *Digital Security* і застосована у її відомому продукті *Digital Security Office* 2006, який складався з двох компонентів – «Гриф» і «Кондор».

За класифікацією *DSECCT* [50] загрози поділяються на:

1) загрози технологічного характеру:

а) фізичні загрози, які класифікуються за джерелом загрози і об’єктом негативного впливу:

– дії порушника (людини), що впливають: на ресурс, на канал зв'язку;

– форс-мажорні обставини для ресурсу, для каналу зв'язку;

– відмова обладнання та внутрішніх систем життєзабезпечення, що впливають на ресурс, на канал зв'язку;

б) програмні (логічні) загрози, які також класифікуються за джерелом загрози і об’єктом негативного впливу:

– локальний порушник, який негативно впливає на ресурс, на операційну систему, на прикладне ПЗ, на інформацію;

– віддалений порушник, , який негативно впливає на ресурс (на операційну систему, на мережеві служби), на інформацію, на канал зв'язку (на мережеве обладнання, на протоколи зв'язку);

2) загрози організаційного характеру, серед які класифікуються за об’єктом негативного впливу:

а) загрози впливу на персонал, які класифікуються за способом і метою негативного впливу:

– загрози фізичного впливу з метою отримання інформації, порушення неперервності ведення бізнесу;

– загрози психологічного впливу з метою отримання інформації, порушення неперервності ведення бізнесу;

б) загрози, спричинені діями персоналу, які класифікуються за мотивацією скоєння дій і об’єктом негативного впливу:

– навмисні дії, які негативно впливають на інформацію, на безперервність ведення бізнесу;

– ненавмисні дії, які негативно впливають на інформацію, на безперервність ведення бізнесу;

Таким чином, класифікація *DSECCT* загроз ІБ здійснюється за наступними критеріями: характер загрози, джерело загрози, мотивація генерування загрози, об'єкт негативного впливу загрози, спосіб здійснення негативного впливу, мета негативного впливу,

1.3.6 Класифікація загроз безпеці інформації з врахуванням специфіки предметної галузі

При дослідженні захищеності інформації в певній предметній галузі загрози часто класифікацікують таким чином, щоб врахувати її особливості.

Прикладами таких класифікацій є:

1) класифікація загроз для державних інформаційних ресурсів (ДІР) [63], в якій інформаційно-аналітична модель базується на двох платформах: на властивостях інформації, що підлягають захисту і відповідають моделі *CIA,* та на методах і засобах реалізації системи захисту, що, як і модель *CIA,* мають три складові - нормативно-правову, організаційну та інженерно-технічну. Метод захисту на основі цієї моделі був названий авторами [63] «методом подвійної трійки захисту». На рис.1.2 наведені критерії класифікації загроз моделі подвійної трійки захисту і визначені авторами типи загроз ДІР. Специфіку предметної галузі в моделі віддзеркалюють наступні поняття, введені в [63]:

– загроза державним інформаційним ресурсам (англ. *threat to the state informative resources*);

– загрози нормативно-правового спрямування (англ. *threat of normatively legal aspiration*), спричинені навмисним або ненавмисним порушенням процесів створення та застосування нормативно-правових актів, що стстановлять правову основу дослідження;

– загрози організаційного спрямування (англ. *threat of organizational aspi ration*), спричинені навмисним або ненавмисним порушенням процесів організації виробничої діяльності та взаємодії виконавців, внаслідок чого стає складніще організувати протидію загрозам;

– загрози інженерно-технічного спрямування (англ. *threat of technical aspiration*), спричинені несанкціонованим втручанням зловмисників у роботу ІКС з використанням фізичних і апаратно-програмних засобів;

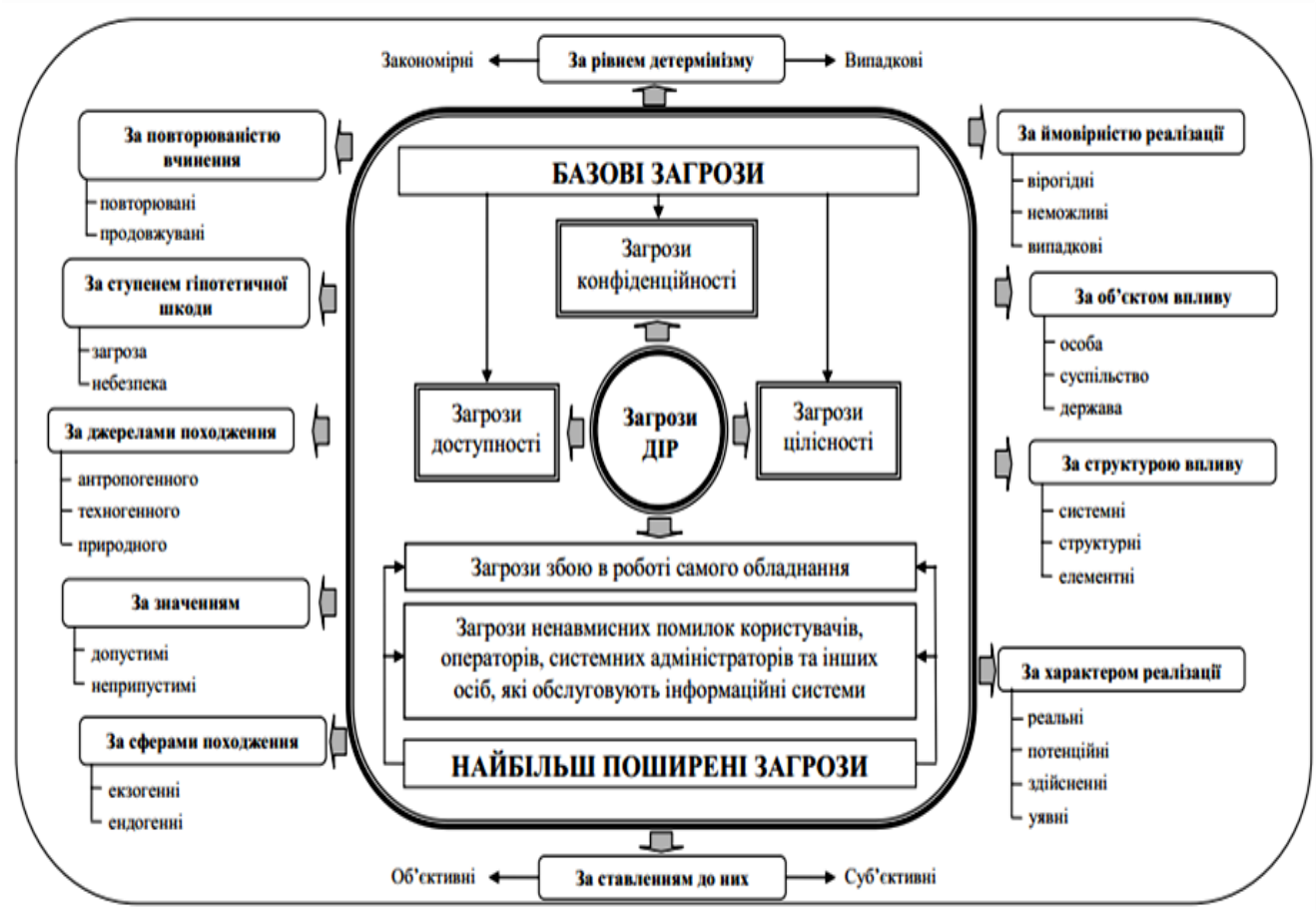

Рисунок 1.2 - Класифікація загроз для державних інформаційних ресурсів [63]

2) класифікація загроз для критичної інфраструктури (КІ), в якій автори [55] виділяють типові загрози за джерелом загроз і загрози функціонуванню КІ за спрямуванням загроз. Типові загрози поділяються зловмисні і незловмисні; природні, техногенні, антропогенні. Загрози функціонуванню поділяються на дві групи: кіберзагрози (порушують штатне функціонування виробничих АС, ПЗ, систем моніторингу і контролю тощо) і фізичні загрози (порушують штатне функціонування трубопроводів, підстанцій, складів, промислових заводів тощо). На 2022 рік автори класифікації [55] визначають як актуальні загрози КІ:

– недостатнє організаційне і технічне забезпечення захисту електронних ДІР та об'єктів КІ;

– несвоєчасне і нефективне реагування органів державної влади та силових структур на загрози пошкодження КІ та забезпечення її відновлення;

– недостатність спроможностей суб'єктів сектору захисту забезпечити стале функціонування об'єктів КІ, їх надійну охорону та кібербезпеку, зокрема, захист від кібершпигунства, кібертероризмому та кіберзлочинності;

3) класифікація загроз соціально-економічній безпеці в кіберпросторі [61], в якій кіберзагрози поділяються за цільовим призначенням (спрямування конкурентної та політичної боротьби, глобальні загрози для соціальних взаємодій індивідуумів, поглиблення соціальних суперечностей соціальних груп, формування певної соціальної позиції індивідуумів) і об'єктами впливу (глобальні загрози, загрози для окремих соціальних груп, загрози для індивідуумів).

Поява і поширення загроз соціально-економічній безпеці в кіберпросторі пов'язані із новими тенденціями в соціумі, розвитком кіберпростору і процесами глобалізації:

– класичні соціальні загрози (загрози терору; громадянські, екологічні і фінансові кризи; формування і спрямування міграційних потоків та антиглобалізаційного руху тощо) все частіше пов'язуються із кіберзагрозами;

– соціальні процеси і конфлікти втрачають територіальну прив'язку, нівелюється автентичність культур, відбувається універсалізація соціальних явищ та їх впливових факторів;

– зявляються нові суб'єкти впливу на соціум, які проводять свою діяльність у кіберпросторі (неурядові організації, провайдери мережевих послуг, мережі продажів товарів тощо), і нові платформи для організації їх діяльності та для безпосередньої анонімної комунікації індивідуумів (месенджери, чат-рулетка);

– змінюється сприймання громадянами суспільних явищ, які, внаслідок медіатизації, перетворюються у свідомості громадян на комплекс символічних відображень;

– незважаючи на загальний принцип ананонімності глобальної мережі, збільшується кількість ознак ідентифікації суб'єктів у кіберпросторі за рахунок поширення електронних документів особи (наприклад, *ID*-карток, водійських посвідчень, документів про освіту та інших документів в «Дії»), банківських електронних засобів (*MobileID, BankID*), цифрових підписів, електронних звернень, інформації із соціальних мереж;

– змінюються інформаційно-комунікаційні компетентності індивідуумів, зокрема, компетентності із уникання кіберзагроз.

Автори [61] поділяють кіберзагрози соціально-економічній безпеці на три типи і відносять:

– до загроз першого типу - ті загрози, які зумовлені цифровізацією і тенденцією до зростання кількості кіберзагроз: «тероризм, екстремізм, авторитарний режим, міграційні потоки, кібертероризм (інформаційні спецоперації, хакерські атаки, бойове використання соцмереж та інтернет-сервісів), цифрова нерівність, цифрова недбалість, втрата приватності та чистоти інформації» [61];

– до загроз другого типу - «глобальні фінансові кризи в умовах розвитку фінансових технологій (на тлі поширення цифровізації), що є наслідками

мегатрендів глобалізації, інформатизації та індивідуалізації споживчих потреб, посилені дією пандемій» [61];

– до загроз третього типу – загрози, зумовлені нестабільною безпековою ситуацією в інформаційній сфері.

Автори [61] підкреслюють, що глобальний характер кіберпростору підвищує рівень соціальних ризиків, оскільки дозволяє впливати індивідуалізовано на окремих осіб, на соціальні групи, на суб'єктів державного та приватного секторів.

4) класифікація загроз при створенні комплексної системи захисту інформації (КСЗІ). В навчальному посібнику [10] зазначається, що найкращий за критерієм ціна-якість варіант КСЗІ можна побудувати лише за результатами аналізу всіх можливих загроз ІБ для об'єкту захисту. При цьому підлягає аналізу інформація про загрози, яка включає в себе відомості про джерела загроз; про фактори, що зумовлюють можливість реалізації загроз; про способи реалізації загроз через різні вразливості об'єкта захисту і про наслідки реалізації загроз.

В якості критеріїв класифікації загроз в [10] використовуються:

– джерела загроз (їх класифікація наведена на рис.1.3);

– природа загроз (об'єктивні загрози, які створюються техногенними і стихійними джерелами, - природні загрози, і суб'єктивні загрози, які створюються антропогенними джерелами, - штучні загрози);

– розташування джерела загрози відносно контрольованої зони (внутрішні і зовнішні загрози);

– тип уразливості, яку експлуатують загрози при реалізації (загрози, які експлуатують наявні технічні канали витоку інформації, уразливості в апаратних чи програмних засобах, уразливості каналів передавання даних чи мережевих протоколів);

– порушувані властивості ІзОД (загрози конфіденційності, цілісності, доступності, спостережуваності, автентичності тощо);

– ступінь впливу на ІКС при реалізації загроз (пасивні і активні загрози, реалізація яких, відповідно, змінює/не змінює склад чи структуру ІКС, процеси її функціонування чи захисту).

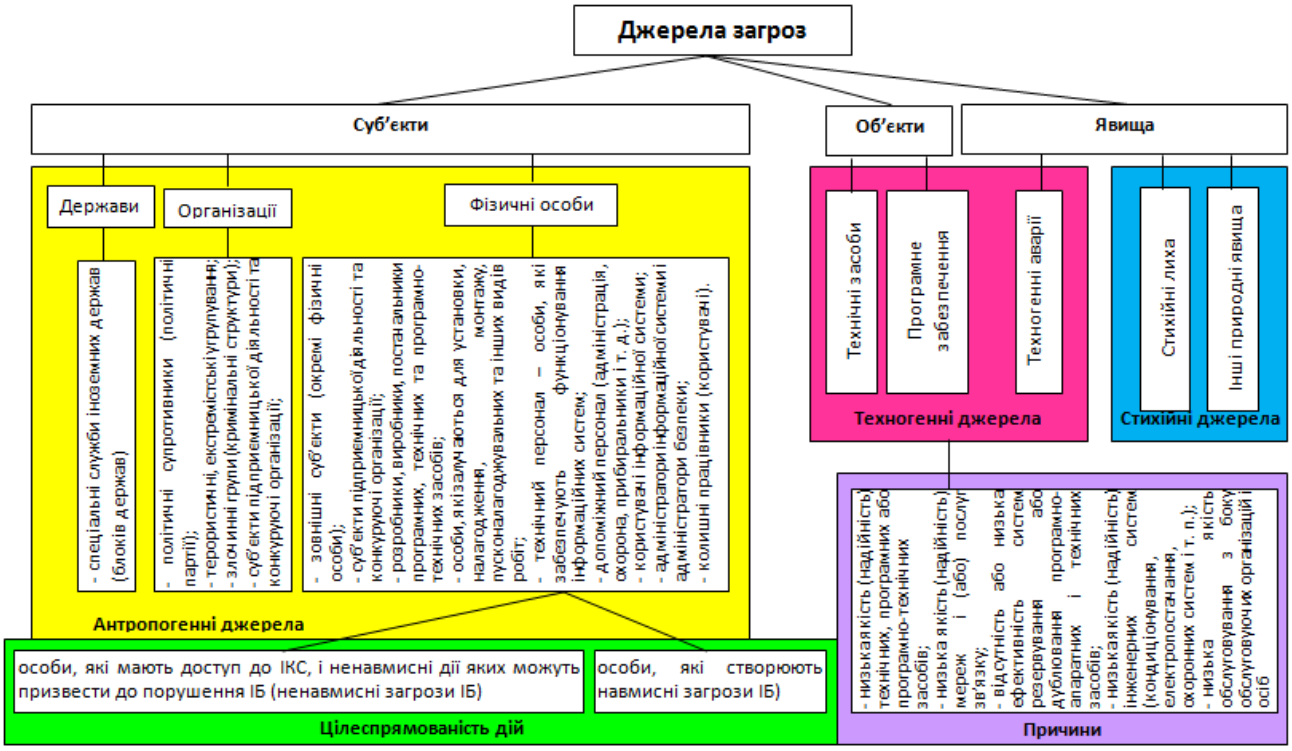

Рисунок 1.3 – Джерела загроз, що використовуються для класифікації загроз

1.3.7 Класифікація загроз за технологіями проведення атак

Зловмисник може використовувати для реалізації своїх злочинних намірів різні технології проведення атак, серед яких можна виділити мережеві технології і технології соціальної інженерії. Відповідно, загрози за технологіями проведення атак можуть бути класифіковані наступним чином:

1) за типом використовуваних мережевих технологій і засобів, серед яких для реалізації загроз найчастіше використовуються [9]:

а) сніфер пакетів для перехопення і аналізу трафіку, призначеного для інших вузлів, який дозволяє:

– адміністратору - виявляти паразитний, вірусний і закільцьований трафік, шкідливе та несанкціоноване ПЗ (мережні сканери, флудери, троянські програми тощо), помилки конфігурації мережних агентів і локалізувати несправності мережі;

– зловмиснику - аналізувати трафік користувача з метою отримання паролів та іншої інформації;

б) *DoS* і *DDoS* для понаднормованого завантаження процесора та/або каналів зв'язку і реалізації відмови в обслуговуванні лігітимних користувачів. Різняться за:

– технологією організації атаки - *DoS* і *DDoS*;

– об'єктом, що перевантажується - процесор, порти, канали зв'язку;

– технологіями і пакетами, що використовуються для «затоплення» і перевантаження: *Trinity, Trinco, Stacheldracht, Ping of Death, Tribe Flood Network, Identification flood, TCP SYN flood, ICMP flood;* для *DDoS*-атак – бот-нети, *Smurf, UDP flood* тощо;

– роллю у комбінованій атаці - порушення процесу «рукостискання», використання часу непрацездатності об'єкта атаки здійснення інших атак, створення передумов для *TFN, TFN2K, Stacheldracht*;

в) *IP*-спуфінг для приховування власних адрес зловмисників у комплексних атаках і розміщення ними шкідливого ПЗ за чужою *IP*-адресою;

г) атака на пароль, яка може бути проведена як простий перебір чи перебір за певнм алгоритмом (наприклад, з врахуванням частоти застосування певних паролів), крадіжка паролю (в тому числі з баз даних паролів) або складна атака із застосуванням методів соціальної інженерії для безпосереднього отримання зловмисником паролю або для отримання ним інформації, що може бути використана для підбору паролю;

д) *SQL Injection*, що дозволяє зловмиснику несанкціоновано отримувати інформацію з інфікованого об'єкта, який використовує *SQL*, наприклад, з сервера;

е) фішинг (англ. *fishing* - риболовля), який спонукає об’єкт атаки виконати певну дію або повідомити зловмиснику певну інформацію. Технології фішингу різняться за:

– способом комунікації зловмисника і об’єкта атаки (найчастіше – *e-mail*);

– за діями, до яких спонукають об’єкт атаки - перехід на сайт, відкриття або запуск файлу, надання певної інформації;

– за можливостями, які отримує зловмисник – впровадження шкідливого ПЗ, отримання інформації для подальшого розвитку комбінованої атаки або створення умов для її отримання (наприклад, зчитування паролів і номерів банківських карток на підробних сайтах);

є) атаки на рівні додатків типу троянів і логічних бомб. Різняться за типами додатків і видами шкідливого ПЗ;

ж) атаки типу *Explosion of Data*, при яких зловмисники використовують дані на мобільних пристроях для пошуку точки входу в мережу через них. Різняться за типом мобільних пристроїв (ноутбуки, мобільні телефони тощо), технологіями отримання доступу до даних на них і технологіями пошуку точок входу в мережу;

з) атаки, що використовують особливості технологій розумного дому та Інтернету речей (англ. *The Internet of Things*, *IoT*) для отримання зловмисниками:

– інформації про розпорядок дня і закономірності поведінки користувачів;

– доступу до медичних записів, банківських виписок, облікових даних і даних автентифікації користувачів *Wi-Fi;*

– отримання можливості впливати на поведінку користувачів шляхом керування режимами роботи пристроїв, які підключаються до Інтернету чи інших мереж, як точки доступу;

і) атаки типу *MITM* (англ. *Man In The Middle* - людина посередині), при яких зловмисник входить у двосторонню транзакцію між легітимним користувачем і мережею. Різняться за:

– способами і засобами вбудовування зловмисника у транзакцію;

– середовищем, в якому відбувається транзакція (найчастіше - це незахищений публічний *Wi-Fi*);

– можливостями, які отримує і використовує зловмисник – фільтрація та викрадання даних, впровадження шкідливого ПЗ, в тому числі такого, що дозволятиме надалі встановити інше ПЗ;

к) використання шкідливого ПЗ, яке різниться:

– за типом – шпигунське ПЗ, програми-вимагачі, віруси, черви тощо;

– за способом активації – безумовна активація чи активація після певної події, наприклад, після виконання певної дії користувачем - натискання шкідливого посилання або вкладення;

– за можливостями, які отримує і використовує зловмисник після активації ПЗ: блокування доступу до певних мережевих компонентів і сервісів (вимагачі); впровадження іншого шкідливого ПЗ; приховане передавання зловмиснику інформації (шпигунське ПЗ) з жорсткого диска жертви, її портів (за допомогою сканерів портів, наприклад, програми *Neo Trace*), клавіатури (за допомогою клавіатурних шпигунів, наприклад, програми *Hook Dump*); моніторів (за допомогою екранних шпигунів, наприклад, програми *Ghost spy*), модемів (за допомогою модемних шпигунів, наприклад програм *Modem spy, Mobile Spy, Flexispy, Mobistealth*); автоматичний запис телефонних розмов і програвання записів через звукову карту чи телефонну лінію, надсилання записів по *e-mail*; електронною поштою; визначення параметрів апаратного і програмного забезпечення жертви (версії встановленої операційної системи, обсягу пам’яті, типу процесора); відстеження активності жертви в мережі (мережні шпигуни) - моніторинг адрес *e-mail*, відвідуваних сайтів і їх тематики, потоків інформації в мережі, збирання інформації, що передається через певний порт тощо; виведення з ладу окремих частин системи.

2) за типом використовуваних технологій соціального інжинірингу, які, в свою чергу, класифікуються за наступними ознаками:

а) за типом використовуваних соціоінженером інформаційних джерел:

– соціальні мережі, в тому числі вікові та гендерні соцмережі, професійні соцмережі для розвитку ділових зв'язків;

– геосоціальні мережі з даними про геолокації користувачів;

– багатокористувальницькі мережні ігри з реєстрацією учасників;

– бази даних у певній галузі чи галузях науки;

– списки закладок чи *web*-сайтів для пошуку користувачів;

– мережі для пошуку роботи тощо;

б) за методами пошуку та збирання інформації:

– претекстинг, який реалізується у два етапи. Зловмисник встановлює попередній контакт з жертвою, наприклад телефоном, і, посилаючись на відомих жертві осіб (найчастіше – керівників його організації), звертається до неї за незначною і не підозрілою допомогою. На другому етапі зловмисник звертається до жертви вже з цільовим проханням. Претекстинг має великі шанси на успіх, якщо в ролі жертви виступають нетехнічні користувачі, які володіють цінною для зловмисника інформацією;

– фішинг - тип атаки, який був розглянутий вище в цьому розділі. При застосуванні у понад 70% фішингових атак є успішними;

– бейтинг – провокування жертви на запуск шкідливого ПЗ, наприклад троянської програми (бекдорів, руткітів, кейлогерів, клікерів, проксі-троянів) з інфікованого електронного листа або із змінного носія інформації (наприклад, з підкинутої флешки);

в) за інструментами нападу [9]:

– з використанням *e-mail*: фішинг, що використовується зловмисниками при реалізації атак з підміною *URL,* крос-сайтових сценаріїв, атак типу *MITM* та

інших; спіар-фішинг, що використовує для одержання важливих даних наперед отриману інформацію про компанію або особу і є вузько спрямованою атакою саме на цю компанію або на певного користувача; вішинг – атака з імітацією телефонних дзвінків від офіційних установ, при якій зловмисники вимагають від жертви повідомлення *PIN*-коду або пароля і найчастіше використовують *IP*-телефонію і автонабирач номера; фарминг – атака у чотири етапи, перший з яких полягає у створенні хибного сайту, скрипт-вірусу, який спрямовує жертву на цей сайт, і навігаційної структури та системи доменних імен, що викривлюють дійсну інформацію про хости, другий етап – надсилання жертві фішингового повідомлення або спонукання її до відвідування *web*-сервера, на якому виконується скрипт-вірус, третій етап - спрямування жертви на хибний сайт в результаті дії скрипт-вірусу, четвертий етап – виконання дій, передбачених хибним сайтом;

– з використанням телефонного зв’язку (англ. *phreaking*). Розрізняють атаки з використанням телефону для отримання інформації для подальших стадій комбінованих атак (наприклад, при спіар-фішингу) і безпосередні атаки на телефонний зв’язок за *IP*-протоколом, який здійснюється за наступним алгоритмом: зловмисник представляється жертві лігітимним користувачем (найчастіше - телефонним інженером) і просить надати певну інформацію, яка дозволяє порушнику на наступних етапах отримати доступ до «вільного» використання телефону і до системи комунікацій;

– з використанням аналізу сміття (носіїв інформації, в тому числі паперових, які з тих чи інших причин підлягають утилізації) для отриманням зловмисником інформації про організацію та її співробітників для посилання в подальших комбінованих атаках на реальних осіб і проекти, а в деяких випадках – для того, щоб видавати себе за співробітника компанії;

г) за методами соціальної інженерії:

– атаки з використанням особистісного підходу, що є основою шахрайських схем: зловмисник встановлює з жертвою контакт (особистий або віртуальний - за допомогою повідомлень *e-mail* або спливаючих повідомлень браузера), а потім, використовуючи різні способи особистісного підходу (залякування із посиланням на особисті повноваження і гарантуванням службових неприємностей, переконання з використанням лестощів, використання створених наперед довірливих стосунків, створення для жертви певної проблеми і гарантування їй допомоги у розв'язанні складної ситуації), змушує жертву розголосити необхідну зловмиснику інформацію;

– атаки із застосуванням реверсивної соціальної інженерії, які передбачають, що довірливі відносини із жертвою для отримання зловмисником необхідної інформації встановлюються після допомоги жертві (надання контактів «комп'ютерної швидкої допомоги», безоплатних тренінгів тощо) в усуненні проблем, що спровоковані самим зловмисником.

1.3.8 Класифікація загроз за *ISO/IEC* 27005:2022

Згідно *ISO/IEC* 27005 [3] загрози класифікуються за наступними критеріями:

1) за природою виникнення (враховують, що одна загроза може мати різну природу виникнення):

– *A* - антропогенні ненавмисні загрози, джерелом яких є користувачі або персонал ІКС;

– *D* - антропогенні навмисні загрози, джерелом яких є зловмисник;

– *E* - природні (екологічні) загрози, джерелом яких є всі випадкові негативні впливи зовнішнього середовища, що не пов'язані з діями людини.

2) за типом загроз:

а) фізичні пошкодження, які можуть мати будь-яку природу виникнення, тобто позначатися як *A,* або *D,* або *E*, наприклад - пошкодження носіїв інформації внаслідок впливу вогню, пилу тощо;

б) природні події, які відносяться тільки до категорії *E,* наприклад – гроза, повінь (будь-які кліматичні, метеорологічні, сейсмічні і вулканічні явища);

в) загрози, зумовлені втратою необхідних сервісів, включають загрози втрати електроживлення з будь-якої причини (категорії *A, D, E*) і можуть бути антропогенними цілеспрямованими і випадковими (категорії *A, D*) загрозами, наприклад - відмови систем кондиціонування чи водопостачання, відмови телекомунікаційного обладнання тощо;

г) несправності внаслідок негативного впливу випромінювання, які можуть мати будь-яку природу (можуть належати будь-якій з категорій *A, D, E*) і поділяються за природою випромінювання на загрози внаслідок:

– негативного впливу електромагнітних імпульсів;

– електромагнітного випромінювання;

– радіації;

– теплового випромінювання тощо;

д) загрози компрометації інформації, які включають антропогенні навмисні і ненавмисні загрози, частина з яких має тільки категорію *D* (наприклад - дистанційне шпигування, крадіжка носіїв інформації, втручання в роботу апаратних і програмних засобів тощо), а частина – може мати як навмисний, так і ненавмисний характер. Наприклад, загроза виявлення (розкриття) інформації і загроза отримання даних з ненадійних джерел можуть мати як категорію *A* так і категорію *D*:

е) загрози технічних відмови, які включають відмови і збої обладнання та ПЗ, спричинені випадковою (категорія *A*) чи цілеспрямованою (категорія *D*) людською діяльністю. Вихід обладнання з ладу внаслідок зношування, перенапруг тощо відноситься до природних загроз;

ж) загрози несанкціонованих дій, які є антропогенними загрозами, частина котрих має категорію *D*, наприклад - несанкціоноване використання обладнання, шахрайське копіювання ПЗ, несанкціонована обробка або викривлення даних, а частина – може бути двох категорій (*A, D*), наприклад - використання контрафактного або скопійованого ПЗ;

з) загрози компрометація функцій, які, залежно від виду загрози, можуть мати різні категорії. Наприклад, загроза помилки у використанні має категорію *A*, загроза фальсифікації прав і заперечення дій - категорію *D*, загрози ненавмисного і навмисного зловживання правами - категорії *A* і *D* відповідно, загрози порушення працездатності персоналу з певної причини можуть мати категорії *A, D* чи *E*.

Джерела антропогенних загроз (загроз категорій *A* і *D*) можуть бути різних типів, і мати різну мотивацію для злочинних дій, що визначає наслідки успішної реалізації загроз.За даними *ISO/IEC* 27005 складена таблиця 1.2.

Таблиця 1.2 – Характеристики зловмисників

Тип	Цілі (найбільш ймовірні)	Загрози (найбільш ймовірні)
Хакери і крекери	Отримання грошової вигоди Задоволення власного его Вираження протесту; Підтвердження кваліфікації	Несанкціонований доступ в систему (в тому числі – отриманий методами соціальної інженерії) Вторгнення в систему Злам програм і систем захисту
Комп'ютерні злочинці	Глобальні цілі: отримання грошової вигоди, в тому числі кредитної, приховування або розкриття інформації Підцілі: шахрайство, шантаж, кіберпереслідування; інформаційний підкуп	Імітація Вторгнення в систему Несанкціонований доступ до інформаційних ресурсів, перехоплення інформації, розголошення інформації, відтворення даних (порушення конфіденційності інформації) Несанкціоновані підробка, модифікація, руйнування даних (порушення цілісності інформації)
Кібертерористи	Отримання політичних переваг Організація терористичної діяльності	Системні атаки (наприклад, DDoS) Вторгнення в систему Втручанням в роботу системи

Продовження таблиці 1.2

Тип	Цілі (найбільш ймовірні)	Загрози (найбільш ймовірні)
	Помста Розвідка Шантаж Інформаційна війна	Несанкціонований доступ до інформаційних ресурсів Руйнування даних Розголошення ІзОД в засобах масової інформації
Промисловиі шпигуни	Отримання замовником (компанією, іноземним урядом) конкурентних переваг або економічного зиску Отримання нагороди виконавцем Економічна розвідка	Несанкціонований доступ до ІзОД (в тому числі до персональних даних, службової та технологічної інформації) Соціальний інженіринг (зокрема, порушення недоторканості особистого життя з метою отримання підстав для шантажу і вербування інсайдерів) Викрадання носіїв інформації;
Інсайдери: Співробітники недостатньої кваліфікації Недбалі співробітники Невдоволені співробітники Звільнені співробітники Нечесні співробітники Зловмисні співробітники, які спеціально впроваджені в компанії	Ненавмисні помилки Нехтування правилами безпеки Цікавість Помста Помста Отримання грошової винагороди Отримання грошової винагороди Шантаж Шахрайство Розвідка Помста Шантаж Шахрайство Отримання грошової винагороди	Впровадження шкідливого ПЗ Системні помилки Системний саботаж Несанкціонована модифікація даних (введення фальсифікованих даних, руйнування даних) Перевищення прав доступу Загрози соціального інжинірингу Фізичний напад на співробітника і/або шантаж Продаж чи розголошення персональних даних Ознайомлення з ноу-хау і фінансовими секретами фірми Нештатне використання апаратних і програмних засобів Інформаційний підкуп Крадіжка

Найширший спектр загроз асоціюється з інсайдерами різних типів. Статистикою підтверджується, що 80% витоків інформації пов’язані із діяльністю внутрішніх зловмисників.

1.4 Роль оцінок загроз в менеджменті інформаційної безпеки

МІБ передбачає проведення оцінювання загроз протягом всього життєвого циклу ІКС для всіх процесів і інструментів обробки та захисту інформації всіх цифрових активів.

Оцінка загроз кібербезпеці є важливою для:

– виявлення актуальних загроз і ризиків для бізнес-процесів;

– виявлення актуальних загроз і ризиків для всіх цифрових активів організації і її структурних підрозділів;

– виявлення актуальних загроз і ризиків для цифрових активів організації, що містять ІзОД, захищеність якої гарантується державою, та для процесів її обробки;

– визначення пріоритетів обробки загроз (ризиків), оскільки різноманіття загроз (див.п.1.3 даної кваліфікаційної роботи) зумовлює необхідність визначення найбільш небезпечних загроз і застосування до них засобів контролю, які можуть запобігти цим загрозам або пом’якшити їх наслідки. При цьому особливу увагу приділяють загрозам конфіденційності, оскільки несанкціонований доступ до інформації є передумовою порушення її цілісності, а іноді – й доступності;

– вибору адекватних до загроз засобів контролю;

– побудови КСЗІ та систем управління інформаційною безпекою (СУІБ) з найкращими показниками «ціна-якість»;

– планування діяльності організації, оскільки оцінки загроз надають інформацію про ймовірні втрати і є важливими для плануванняі витрат організації.

Оцінювання загроз кібербезпеці починається із складання переліку активів організації і максимально повного переліку загроз для них. Топ-менеджери організації визначають зв'язки кожного активу з бізнес-процесами і значимість

(критичність) кожного активу для бізнес-процесів організації, які, в свою чергу, також різняться за ступенем важливості для організації.

За методикою Національного інституту стандартів і технологій (англ. *The National Institute of Standards and Technology, NIST*) загрози визначаються як будь-які події чи обставини, котрі можуть порушити нормальні бізнес-процеси або цілісність активів організації, а кіберзагрози – як підмножина загроз безпеці інформації.

За методикою *NIST* спочатку при описі кіберзагроз вказують їх джерела і ймовірність виникнення. Як джерела загроз кібербезпеці методика *NIST* розглядає:

– прямі атаки на активи (приклад - програми-вимагачів);

– людські помилки через недостатню кваліфікацію або недбалість (приклад – порушення правил парольного захисту);

– системні збої засобів контролю ІБ (як обладнання, так і ПЗ);

– стихійні лиха (приклади – землетрус, блискавка).

Звгрози ІБ, в тому числі і кіберзагрози, можуть бути спричинені не тільки одним джерелом, а й комбінацією джерел загроз, тому при оцінюванні загроз ІБ вкрай важливо застосовувати комплексний підхід, щоб врахувати і мати можливість нейтралізувати потенційно всі можливі небезпечні загрози.

Загрози інформації ріалізуються шляхом експлуатації наявних в ОІД вразливостей безпеки, які визначаються *NIST* як прогалини в засобах безпеки. Наявність вразливостей зумовлюється відсутністю засобів контролю безпеки, їх відомими недоліками або природною появою вразливих місць через зміни в цілях організації, її бізнес-функціях, середовищі функціонування бізнесу, технологіях, які використовується у певній галузі. Вразливості можуть також виникати через організаційні недоліки системи управління компанією, наприклад, внаслідок:

– прийняття невірних і непослідовних рішень при оцінюванні важливих для бізнесу функцій;

– недоліки СУІБ: недоліки політики безпеки, недоліки управління ризиками і управління інфраструктурою кібербезпеки, що наражає активи на кіберзагрози;

– недоліки організації нагляду за дотриманням політики безпеки тощо.

При оцінюванні загроз важливо виявити їх потенційні можливості через вразливості стати повномасштабними атаками і спричинити певні збитки. Тому для виявлення вразливих місць кіберзахисту проводять аналіз якомога більшої кількості сценаріїв розвитку загроз.

Кожна організація має власні бізнес-процеси, ІКС та активи, власні вимоги до безпеки організації, бізнес-безпеки і кібербезпеки, тому певна організація можете бути більш або менш схильною до певних загроз, ніж інші, навіть в тій самій галузі діяльності. Тому при оцінювання загроз кібербезпеці і їх ранжуванні необхідно індивідуально для кожного ОІД визначити ймовірності векторів і сценаріїв атак, ймовірності виникнення і реалізації загрози через вразливості ОІД.

Імовірність виникнення певної загрози зазвичай визначається експертним шляхом або шляхом аналізу статистичних даних, зібраних в галузі і організаціїами, тобто є суб’єктивним чи об’єктивним прогнозом.

На величину ймовірності виникнення загрози впливають стан стан ІКС організації, стан СУІБ, типи засобів контролю, які застосовуються на поточний час і плануються до впровадження, наміри зловмисника (наприклад, розголошення конфіденційних даних), його можливості (наприклад, складність вектора атаки) і ймовірні цілі (наприклад, сервер, на якому міститься база з конфіденційними даними). При оцінюванні ймовірності загрози також враховуються :

– можливості ініціювання/виникнення загрози;

– ймовірність негативного впливу зарози (в разі її виникнення) на бізнес-процеси, активи організації, ІКС і пов’язану з нею інфраструктуру, інтереси зацікавлених сторін;

– наявність уразливостей, через які загроза може бути реалізована.

При цьому аналізуються всі можливі (відомі і потенційні) уразливості ОІД, і визначається, якими з них може скористатися конкретна загроза.

Аналізу підлягають також всі фактори, які впливають на можливість запобігти атаці, своєчасно ідентифікувати загрозу, усунути загрозу чи її наслідки, якщо вона вже сталася.

Після визначення кіберзагроз і ймовірностей їх виникнення для конкретного об’єкта захисту необхідно оцінити силу потенційного негативного впливу актуальних для ОІД загроз, що реалізуються через певні вразливості на бізнес-процеси, активи організації, ІКС і пов’язану з нею інфраструктуру, інтереси зацікавлених сторін, тобто, відповідно *NIST SP* 800-30, визначити наслідки реалізації загроз і оцінити їх критичність. Наприклад:

– якщо метою зловмисника є отримання і розголошення конфіденційної інформації, то з точки зору власника інформації це призводить до її викриття;

– якщо зловмисник модифікує дані, то порушується їх цілісність;

– якщо зловмисник видаляє дані, то власник втрачає дані.

Визначення і оцінка критичності потенційного впливу загроз на всіх стейкхолдерів, пов’язаних із певною організацією, потрібні для оцінювання кіберзагроз в довгостроковій перспективі і прийняття рішень не тільки щодо кіберзахисту організації, а й щодо ведення бізнесу. Стейкхолдерам має надаватися інформація про те, вплив загроз на які процеси був оцінений, які оцінки наслідків були отримані, якими методами і з якими припущеннями були оціннені негативні вплии загроз.

Оцінювання кіберзагроз має проводитися за методологією, яка на практиці довела свою ефективність в галузі МІБ. Часто провідні організації, що надають послуги з побудови СУІБ і аудиту ІБ, розробляють власні методи і методики оцінювання загроз ІБ. Існує практика прийняття найкращих з цих методик в якості

національних і міжнародних стандартів після тривалої практичної апробації. Зазвичай такі стандарти містять вказівки щодо найкращих практик МІБ, побудови СУІБ і аудиту ІБ з врахуванням попередніх і поточних оцінок загроз, гарантуючи безпеку всіх активів організації. В загальному випадку методологія оцінки кібербезпеки охоплює:

– процеси оцінки загроз із етапами розповсюдження результатів оцінювання і визначення поточних оцінок за результатами моніторингу;

– моделі ризику, які враховують фактори ризику, що діють протягом життєвого циклу загрози, і основою до призначення рейтингу ризику і загрози;

– підходи до оцінки загроз, які передбачають отримання кількісних, якісних або комбінованих оцінкок ризиків, асоційованих із загрозами;

– підходи до аналізу ризиків і загроз, що передбачають групування ризиків за їх зв'язком із певними вразливостями, певними активами, з інформацією певного рівня секретності, з певними активами або бізнес-процесами, певними негативними наслідками реалізації загроз чи із певними загрозами (найчастіше розглядається порушенняи конфіденційності, цілісності і доступності інформації).

Методологія оцінки загроз ІБ може бути спеціалізованою під певну галузь діяльності, наприклад – водний транспорт, і може бути універсальною. Згадана вище методологія *NIST* є універсальною і може бути адаптована для оцінки загроз будь-якої організації з врахуванням її специфічних вимог безпеки.

В СУІБ аналіз, оцінка загроз і асоційованих з ними ризиків здійснюється на всіх етапах циклу Демінга - модель *PCDA* (англ. *Plan-Do-Check-Act*).

– на етапі планування СУІБ здійснюються: встановлення контексту (визначаються критерії оцінки РІБ і критерії оцінювання наслідків, рівні прийнятних ризиків, сфери дії і структура СУІБ), розробляється план обробки ризиків за результатами попереднього обстеження ОІД та оцінювання ризиків і ефективності

СУІБ, ідентифікуються ризики, що передбачає проведення ідентифікації активів, засобів контролю, вразливостей, загроз та наслідків їх реалізації;.

– на етапі реалізації СУІБ впроваджуються засоби контролю та заходи згідно плану обробки ризиків;

– на етапі перевірки СУІБ проводиться моніторинг інцидентів ІБ, загроз та РІБ, оцінюються їх критичність та поточна ефективність засобів контролю, визначається необхідність зміни процедур обробки РІБ;

– на етапі покращення СУІБ здійснюється її адаптація до поточних актуальних загроз, включаючи повторне ініціювання процесу управління РІБ.

2 АНАЛІЗ МЕТОДІВ ВИЗНАЧЕННЯ РАНГІВ ЗАГРОЗ

2.1 Нормативно-правове забезпечення ранжування загроз

2.1.1 Зарубіжні нормативні документи щодо ранжування загроз

Зарубіжні нормативні документи щодо ранжування загроз можна умовно поділити на дві групи: національні і міжнародні документи.

Серед міжнародних документів можна виділити Конвенцію про кіберзлочинність стандартів [27] та низку міжнародних стандартів.

За Конвенцією про кіберзлочинність [27] кожна країна, що визнала цю Конвенцію, самостійно визначає і застосовує необхідні для встановлення кримінальної відповідальності за порушення ІБ законодавчі акти і заходи. Загрозам ІБ присвячені окремі статті Конвенції, зокрема, розглядаються незаконноий доступ, нелегальне перехоплення, втручання у дані та систему, зловживання пристроями, пов’язані із використанням ІКС підробки та шахрайства, правопорушенням щодо викривлення змісту інформації і порушення авторських та суміжних прав.

Серед міжнародних стандартів, які використовуються при ранжуванні загроз, можна виділити:

– стандарти, які визначають загальні принципи управління ризиками: *ISO Guide* 73:2009 “*Risk management – Vocabulary*”, *ISO* 31000:2018 «*Risk management – Guidelines*», *ISO/TR* 31004:2013 «*Guidance for the implementation of ISO* 31000»;

– стандарти, які визначають загальні принципи управління ІБ: *ISO/IEC* 15408 «*Common Criteria for Information Technology Security Evaluation*», *ISO/IEC* 27001:2022 «*Information Security Management System Standard*»;

– стандарти, які визначають технології управління ризиками ІБ: *ISO/IEC* 27005:2022 «*Information Technology – Security Techniques – Information Security*

Risk Management» [4]; *ISO/IEC* 31010:2019 «*Risk management – Risk assessment techniques*».

Серед зарубіжних національних стандартів, які можуть застосовуватися при ідентифікації загроз і ранжуванні загроз та ризиків, слід виділити ряд популярних стандартів, які де-факто стали міжнародними в окремих регіонах:

–стандарти, які визначають загальні принципи управління ризиками ІБ: *NIST* 800-30 «*Risk Management Guide for Information Technology Syste*ms» (США); *BSI-Standard* 100-3 «*Risk Analysis based on IT-Grundschutz*» (Германія); *ISO/FDIS* 31000 «*Risk management – Principles and guidelines*» (Швейцарія) *AS/NZS* 4360:2004 «*Risk management*» (Австралія і Нова Зеландія);

–стандарти, які визначають критерії оцінювання ризиків ІБ і якості комп'ютерних систем: «*Trusted Computer Systems Evaluation criteria*», «*Federal Criteria for Information Technology security*» (США); «*Canadian Tusted Computer Product Evaluation Criteria*» (Канада); «*Information Tecnhology Security Evaluation Criteria*» (Євросоюз).

2.1.2 Нормативні документи Україні щодо ранжування загроз інформаційної безпеки

Ідентифікація і аналіз загроз є першим етапом робіт з технічного захисту інформації (ТЗІ), на якому, згідно із нормативними документами з ТЗІ [35, 37, 45] необхідно:

– провести обстеження і аналіз об'єктів технічного захисту;

– визначити модель порушника і модель загроз;

– оцінити ймовірності появи загроз і успіху їх реалізації;

– оцінити потенційний негативний вплив загроз на активи організації.

Модель загроз містить опис загроз, шляхів їх реалізації і джерел загроз, тому вона органічно пов'язана із моделлю порушника. За НД ТЗІ 1.4-001-2000

«Типове положення про службу захисту інформації в автоматизованій системі» [35] служба захисту інформації для побудови цих моделей повинна обстежити ОІД, дослідити технології обробки інформації в АС, виявити вразливості ІКС і потенційні канали витоку інформації, ідентифікувати загрози ІБ та оцінити їх критичність. На підставі отиманих характеристик ОІД як об'єкту захисту розробляється політика безпеки, плани її реалізації, процедури обробки ризиків і правила їх застосування, процедури моніторингу та аудиту ІБ.

Проведення планових і позапланових періодичних аудитів ІБ та моніторинг стану кібербезпеки в ОІД дозволяють своєчасно виявляти недоліки системи захисту, визначати адекватність поточним вимогам політики безпеки і засобів контролю, виявляти і прогнозувати появу нових загроз, і, в разі потреби, вносити зміни в модель загроз.

Оцінювання захищеності інформації в АС вже тривалий час здійснюється як процедура оцінки відповідності системи захисту вимогам наступних нормативних документів з ТЗІ:

– НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [37];

– НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [38];

– НД ТЗІ 2.6-001-11 «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах»;

– НД ТЗІ 2.6-003-2015 «Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99»;

– НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу»;

– НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу»;

– НД ТЗІ 2.7-013-2016 «Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99»;

– НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу»;

– НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»;

– НД ТЗІ 3.7-002-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова)»;

– НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

В останні роки було прийнято ряд НД ТЗІ, призначених для регулювання процесів вибору, впровадження та моніторингу заходів захисту:

– НД ТЗІ 2.3-025-24 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [36];

– НД ТЗІ 2.6-004-21 «Порядок авторизації безпеки інформаційних систем» [39];

– НД ТЗІ 3.6-004-21 «Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в ІКС, в яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці» [40];

– НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації» [41];

– НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [42];

– НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» [43];

– НД ТЗІ 3.6-008-21 «Порядок моніторингу безпеки інформаційних систем» [44].

В цих документах використовуються поняття вимог безпеки, яким мають авдповідати засоби захисту, що протидіють загрозам безпеки і приватності [39-44]:

– вимоги безпеки – вимоги щодо безпеки інформації (активу) разом із супутніми обмеженнями та умовами, які випливають з нормативних документів і необхідні для виконання організацією її функцій;

– вимоги щодо приватності – підмножина вимог щодо захисту особистого життя приватних осіб, яка пов’язана із захистом персональних даних і відповідає ДСТУ 7731:2015 «Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD)»

– вимоги безпеки та приватності - підмножина вимог стосовно забезпечення конфіденційності, цілісності та доступності інформації;

Для оперативного реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем, в Україні у 2021 році було прийняте «Положення про організаційно-технічну модель кіберзахисту», що визначає відповідний комплекс заходів, сил і засобів кіберзахисту.

Нейтралізація реальних і потенційних кіберзагроз здійснюється у порядку, визначеному асоційованими з ними ризиками, що оцінюються і управляються згідно ряду міжнародних стандартів, імплементованих в Україні як ДСТУ:

– ДСТУ *ISO* 31000:2018 «Менеджмент ризиків. Принципи та настанови»;

– ДСТУ *ISO/TR* 31004:2018 «Менеджмент ризиків. Настанови з впровадження *ISO* 31000»;

– ДСТУ *EN IEC* 31010:2022 «Керування ризиками - методи оцінки ризиків» (*EN IEC* 31010:2019, *IDT; IEC* 31010:2019, *IDT*) прийнятий на заміну ДСТУ *ISO/IEC* 31010:2013 «Керування ризиком. Методи загального оцінювання ризику (*ISO/IEC* 31010:2009, *IDT*))»[14];

– ДСТУ *ISO/IEC* 27001:2015 «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги»;

– ДСТУ *ISO/IEC* 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки»;

– ДСТУ *ISO/IEC* 27005:2019 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки» [13] .

– ДСТУ 7731:2015 «Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя» (*ISO/IEC* 29100:2011, *MOD*).

Одним з останніх нормативних документів за тематикою кваліфікаційної роботи є Наказ Адміністрації ДССЗЗІ №354 від 10.07.2024.«Рекомендації з оцінки достатності заходів захисту інформації КСЗІ в інформаційних, електронних комунікаційних та ІКС, створених з використанням профілів безпеки інформації».

2.2 Способи і міри оцінювання загроз

Оцінювання загроз за *ISO/IEC* 27005 (передостання і остання версії [3, 4]) здійснюється за рівнем асоційованих з ними ризиків, який визначається на

окремому етапі менеджменту РІБ (рис.2.1) [3]. Величина ризику отримує якісну (наприклад, «високий», «середній», «низькиі») або кількісну оцінку.

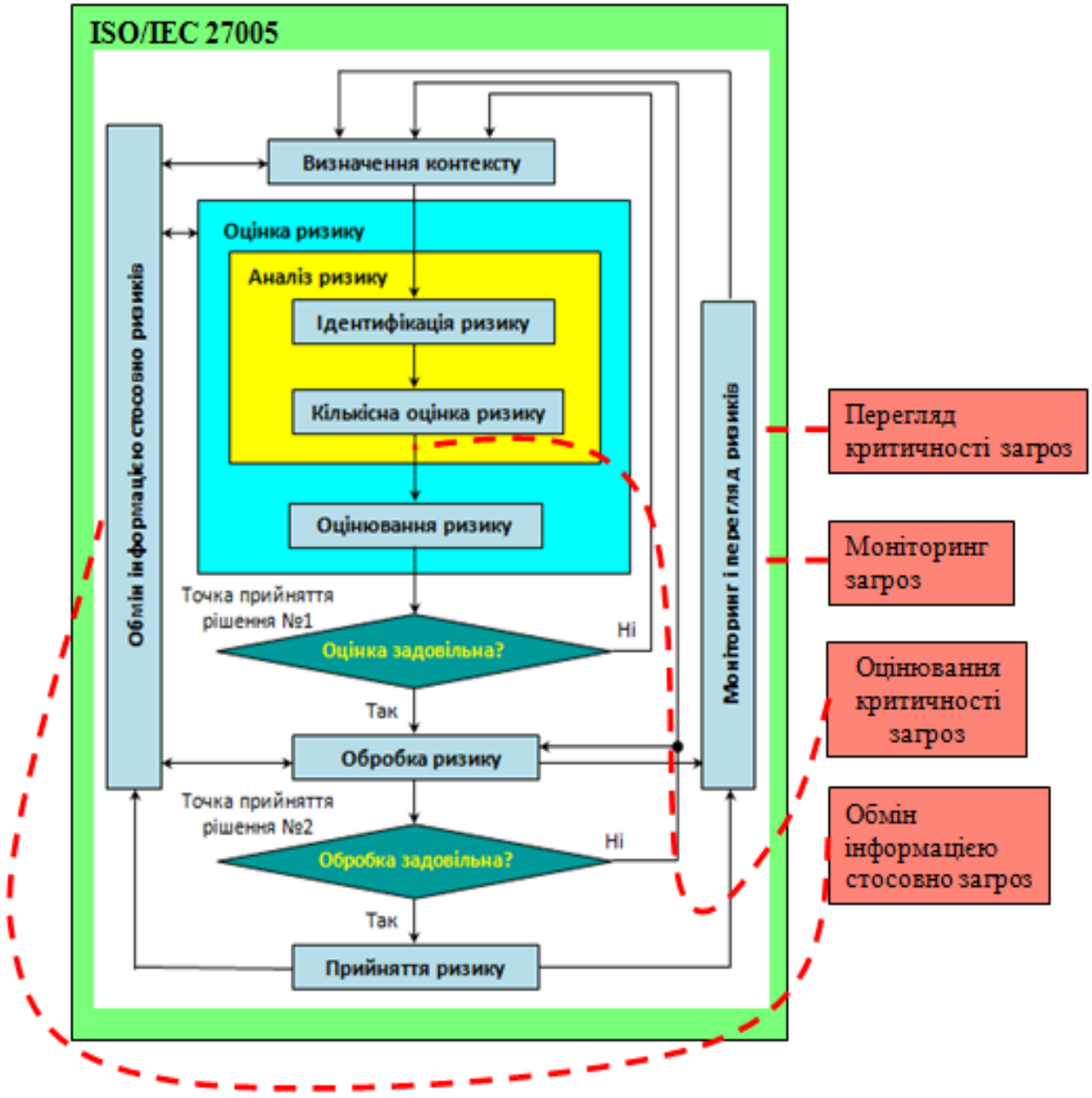

Рисунок 2.1 – Оцінювання загроз в ітераційному процесі менеджменту РІБ

Як випливає з рис.2.1, оцінка ризиків в циклах менеджменту РІБ проводиться після визначення контексту ризиків і передує реагуванню на ризики та їх

моніторингу. Оцінка та оцінювання ризиків і загроз в неперервному ітераційному процесі менеджменту РІБ дозволяє оцінити ефективність засобів контролю, виявити недоліки системи захисту і побудувати плани модернізації системи захисту та СУІБ.

Цілями ранжування загроз є:

–створення інформаційної бази для прийняття рішень щодо планування бюджету і впровадження засобів контролю, визначення порядку обробки ризиків;

–скорочення витрат на забезпечення ІБ, оскільки ранги загроз дозволяють визначити ризики, що підлягають першочерговій обробці, і оптимальним чином сформувати портфель інвестицій в ІБ.

На рис.2.2 наведена класифікація способів оцінки РІБ, серед яких можна виокремити три великі групи: методи; нормативні документи; програмні засоби.

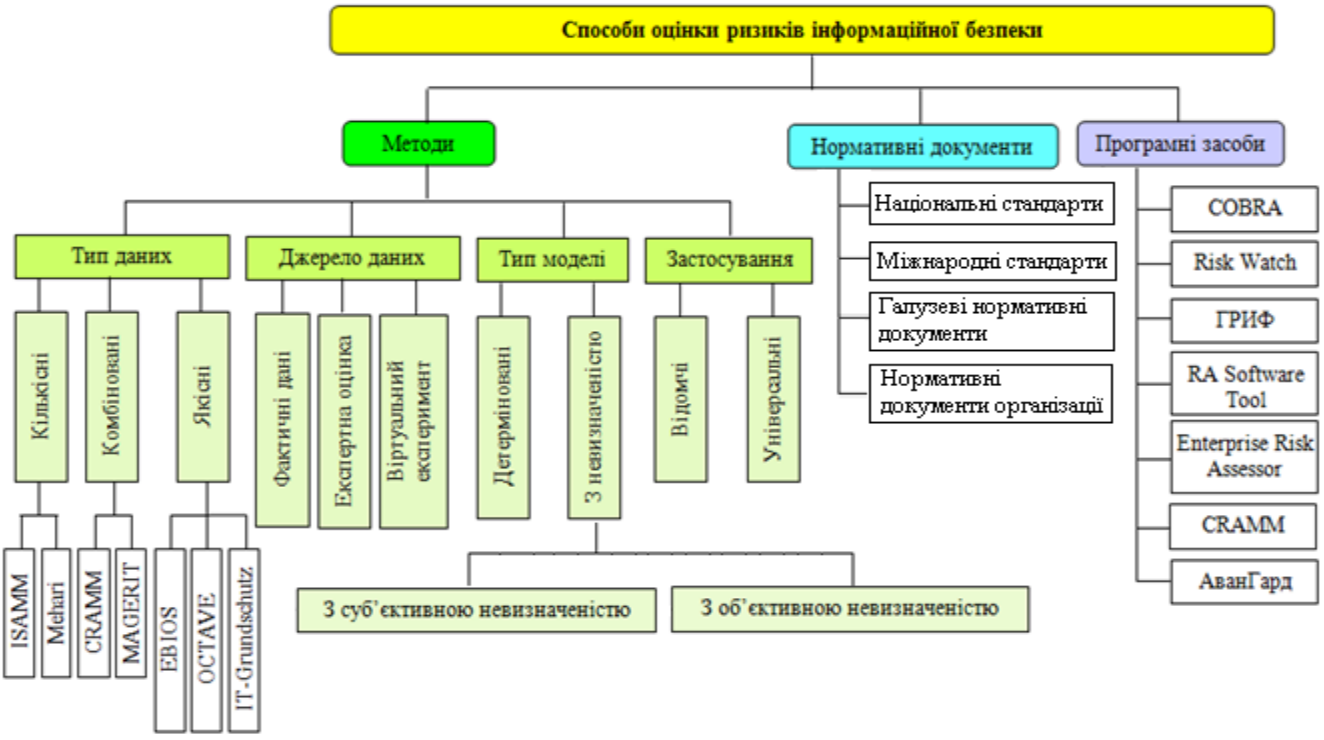

Рисунок 2.2 – Класифікація способів оцінки РІБ

Кількісна міра ризику *R* може бути обчислена за різними формулами, що враховують різні фактори, які впливають на ризик:

– за формулою, яка була рекомендована *NIST SP* 800-30 і враховує - ймовірність реалізації загрози *T* - P_T, ймовірність впливу загрози *T* на актив *I* – P_{IT}, вартість (критичність) наслідків впливу загрози *T* на актив *I* - *W*:

$$R = P_T \cdot P_{IT} \cdot W\,, \tag{2.1}$$

– за спрощеною формулою, в якій ймовірність виникнення і успішної реалізації загрози *P* за змістом дорівнює $P = P_T \cdot P_{IT}$

$$R = W \cdot P\,, \tag{2.2};$$

– за формулою, в якій враховуються оцінки ймовірностей виникнення загрози p_t та успішної експлуатації нею вразливості *v* - p_v, оцінки ефективності наявних заходів і засобів контролю, призначених для унеможливлення реалізації загрози шляхом експлуатації вразливості *v* - E_v, та заходів і засобів контролю, призначених для зниження критичності *q*-го наслідку реалізації загрози -E_q:

$$R = W \cdot p_t \cdot (1 - E_v) p_v (1 - E_q);\tag{2.3}$$

– за методикою *RiskWatch*, згідно з якою ризик визначається як прогнозовані річні втрати *R=ALE* (англ. *Annual Loss Expectancy*, *ALE*) з врахуванням очікуваної кількості реалізацій загрози на рік *ARO* і очікуваного збитку внаслідок однієї реалізації загрози *SLE* або з врахуванням вартості активу *AV*, коефіцієнт впливу *EF*, що визначає у відсотках долю вартості активу, що втрачається під впливом загрози, і частоти реалізації загрози *F* на рік:

$$ALE = ARO \cdot SLE;\tag{2.4}$$

$$ALE = AV \cdot EF \cdot F;\tag{2.5}$$

– за формулами, що враховують мотивацію зловмисників, яка може бути оцінена, в свою чергу, за відношенням необхідних витрат зловмисника на реалізацію атаки і очікуваного ним прибутку [28];

– за суб'єктивною експертною оцінкою в балах за прийнятою шкалою оцінювання, наприклад від 0 до 5 (0 – ризик відсутній, 5– ризик максимальний);

– за формулами, які складаються відповідно до сценаріїв реалізації загроз і враховують, наприклад, що для порушення цілісності інформації в активі зловмисник спочатку повинен порушити конфіденційність, тобто отримати несанкціонований доступ до цього активу.

Наявне на ринку спеціалізоване ПЗ для управління РІБ базується певних нормативних документах і реалізує певний метод або методику аналізу і оцінювання ризиків, які часто створюються самими розробниками ПЗ. В результаті окремі відомі методи (рис.2.2) мають тільки власні методики (наприклад, *OCTAVE*), а окреми - методики і спеціалізоване ПЗ (наприклад, *CRAMM*).

Оцінка ризиків здійснюється згідно національних і ратифікованих країною міжнародних стандартів, галузевих нормативних документів, розпоряджень і наказів по конкретній організації.

Нормативні акти можуть містити рекомендації або загальнообов'язкові чи обов'язкові для виконання в конкретній сфері МІБ вимоги, наприклад, вимоги для організацій, в яких циркулює інформація, що є державною таємницею чи іншою таємницею, збереження якої гарантується державою, для об'єктів критичної інфраструктури тощо.

Інструменти і процедури оцінки ризиків є унікальними для кожної організації, але вони містять п'ять типових етапів:

етап 1 – визначення активів, на якому не тільки складається список усіх активів організації із визначеними вимогами щодо їх захисту і зв'язками із бізнес-процесами та технологіями обробки інформації, а й перелік засобів контролю;

етап 2 – виявлення вразливостей, на якому, зазвичай із застосуванням спеціальних програмно-апаратних засобів, пентестингу тощо виявляють вразливості апаратного забезпечення, ПЗ, активів системи захисту інформації;

етап 3 – визначення загроз, на якому складають максимально повний перелік загроз ІБ для ОІД, визначають ймовірності їх виникнення і можливості реалізації через визначені на етапі 2 вразливості, а також ймовірності успішної реалізації загроз з врахуванням ефективності пов'язаних із загрозами і активами засобів контролю та ймовірні негативні наслідки;

етап 4– оцінка ризиків, на якому обчислюють ризики за обраною формулою, наприклад – за якоюсь із формул (2.1)-(2.5), і визначається їх рейтинг;

етап 5 - оцінка критичності загроз (оцінювання ризиків рис.2.2), на якому за окремими правилами загрози і асоційовані з ними ризики відносяться до певних груп критичності, тобто отримують якісну оцінку, наприклад, «прийнятний ризик», «середній ризик», «високий ризик», «піковий ризик» тощо.

Наступним кроком алгоритму менеджменту РІБ є прийняття рішень щодо обробки ризиків за правилами, сформулюваними на етапі визначення контексту.

На рис.2.3 наведені процеси управління ризиками за *NIST SP* 800-39.

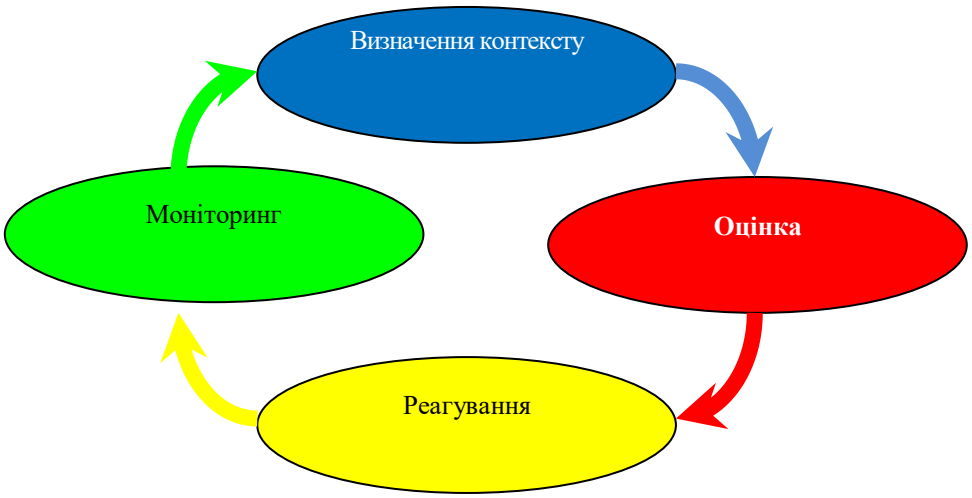

Рисунок 2.3 – Модель управління ризиками за *NIST* 800-39

На рис.2.4 наведені результати зіставлення етапів впровадження систем захисту інформації за НД ТЗІ 2.3-025-24 [36] і моделлю *PDCA* за *ISO/IEC* 27001.

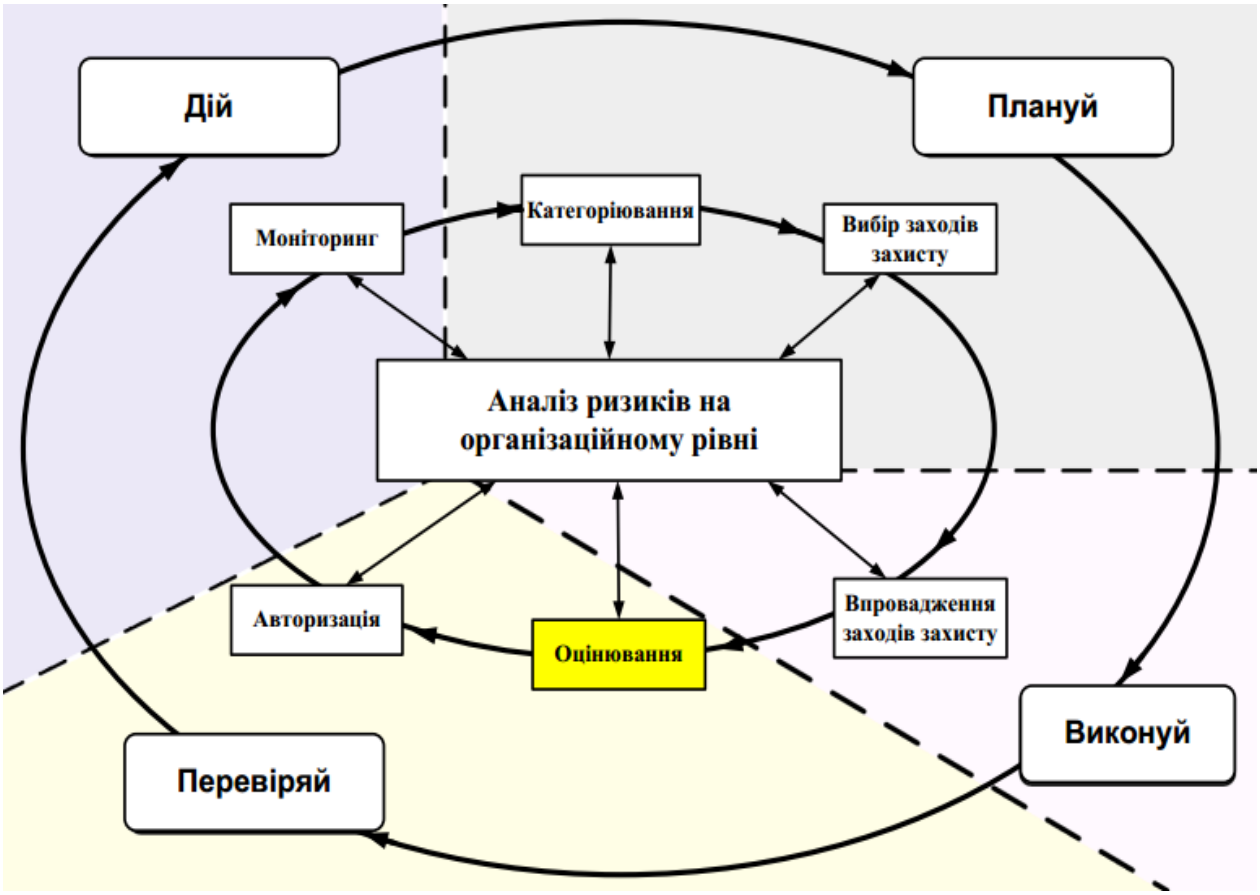

Рисунок 2.4 - Зіставлення етапів впровадження систем захисту інформації за НД ТЗІ 2.3-025-24 [36] і моделлю *PDCA* за *ISO/IEC* 27001

2.3 Методи оцінювання загроз

2.3.1 Загальна характеристика методів аналізу і оцінювання загроз

Методи аналізу і оцінювання загроз і ризиків можна поділити на:

1) методи апріорного оцінювання, згідно з якими при оцінюванні загроз використовуються:

–визначені провідними організаціями в галузі кібербезпеки як актуальні на поточний момент і як прогнози на майбутній період (див. п.2.5 даної кваліфікаційної роботи) тренди і топ-загрози в світі, в країні, в галузі;

–тренди і актуальні загрози, визначені з врахуванням власного досвіду організації і зібраних організацією статистичних даних;

–тренди і оцінки актуальних загрози, існування яких доведено в наукових публікаціях;

2) практичні методи, адекватність яких доведена багаторічною практикою їх застосування в світі, або в галузі діяльності, або в самій організації;

3) методи, що рекомендуються нормативними документами актуальних версій, зокрема *ISO/IEC* 31010 і відповідним ДСТУ *EN IEC* 31010:2022 «Керування ризиками - методи оцінки ризиків» (*EN IEC* 31010:2019, *IDT; IEC* 31010:2019, *IDT*) [14]. В *ISO/IEC* 31010 наведено короткі описи більше тридцяти методів оцінки ризиків і надані рекомендації із їх застосування;

4) новітні методи, ефективність яких практично не доведена, але теоретично обґрунтована на момент вибору методу в наукових публікаціях. Такі методи можуть застосовуватися для досліджень загроз і ризиків в рамках певної сфери МІБ, однак на момент прийняття рішень щодо обробки ризиків висновки, отримані із застосуванням цих методів, повинні мати практичне підгрунття.

Методи і методики оцінки і оцінювання ризиків та загроз представляються певними алгоритмами дій, що ґрунтується на нормативно-правовій базі, прийнятих моделях загроз і порушників і можуть мати спеціалізоване ПЗ (див.рис.2.2).

При аналізі і оцінюванні загроз можуть застосовуватися віртуальні експерименти на математичних моделях для отримання віртуальної статистики інцидентів ІБ в процесі функціонування об’єкта дослідження і його системи захисту. Для побудови моделей при цьому широко використовуються методи системного аналізу, нечіткої логіки, теорії ігор, систем масового обслуговування, методи

дослідження систем на мережах Петрі та інші математичні апарати. У віртуальних експериментах в моделі загроз, уразливостей і засобів контролю вбудовуються засоби опису пов’язаних із ними невизначеностей, зокрема, генератори псевдовипадкових чисел, що дозволяє методом Монте-Карло провести серію експериментів, накопичити віртуальні статистичні дані щодо інцидентів ІБ і визначити ризики, асоційовані з різними сценаріями інцидентів та ефективність системи захисту.

Визначення зв’язків, напряму і ступеня взаємного впливу активів, засобів контролю, загроз, вразливостей, бізнес процесів тощо може бути здійснене методами на базі онтологій і когнітивних карт.

При оцінюванні загроз дані про джерела загроз, сценарії і наслідки їх реалізації найчастіше є неповними або недостатньо достовірними. Це обумовлює проблему отримання адекватних оцінок загроз при невизначеності вхідних даних, тому в моделі різного типу часто вбудовують засобт опису нечітких даних і засоби отримання висновку на нечітких або неповних даних.

2.3.2 Оцінювання і ранжування загроз при невизначеності вхідних даних

При побудові моделі загроз і моделі порушника використовуються:

– детерміновані дані;

– дані, які мають враховуватися лише при виконанні певної умови;

– дані, щодо яких експерти не мають повної впевненості;

– дані, значення яких відомі експертам лише в деякому діапазоні (з повною чи неповною мірою впевненості);

– дані, значення яких невідомі взагалі.

Таким чином, при оцінюванні загроз існує проблема отримання висновку при невизначеності вхідних даних. Наприклад, всі системи виявлення вторгнень і запобігання вторгненням є нечіткими системами.

Невизначеність вхідних даних може мати різну природу (див. рис.2.2):

– об’єктивна невизначеність, зумовлена випадковим характером процесів в досліджуваній системі. Дані з об’єктивною невизначеністю в моделях можуть бути представлені ймовірнісними характеристиками (математичне очікування, середньоквадратичне відхилення, закон розподілу із визначеними параметрами тощо), які визначаються шляхом статистичного аналізу результатів реальних або віртуальних експериментів;

– суб’єктивна невизначеність, зумовлена тим, що наявні відомості та особистий досвід експерта не дозволяють йому з абсолютгою впевненістю зробити висновок про істинність якогось твердження, наприклад, про те, що певний антивірусник зможе нейтралізувати нові невідомі віруси. Суб’єктивна невизначеність даних описується нечіткими моделями (лінгвістичними змінними, нечіткими множинами з визначеними функціями належності) і передбачають отримання висновків спеціальними методами (Мамдані, Сугено-Такагі тощо).

При оцінюванні загроз за моделями з невизначеністю, якщо аналізуються певні сценарії розвитку загроз, то аналізу підлягають лише ті сценарії, невизначеність яких не перевищує задану граничну величину, а недостовірні сценарії та сценарії з непередбачуваними наслідками не розглядаються. Крім того, поширюється [24] застосування інтегрованих моделей загроз і порушників, які не обмежуться галуззю ІБ та адаптуються до поточних умов. Адаптовні моделі є основою систем виявлення і запобігання вторгнень.

Ранжування елементів багатофункціональної системи може [51-54] виконуватися із застосуванням нечітких відношень впливу та подібності на основі нечіткого транзитивного замикання. Ранг ρ_i складової системи $x_i \in X$, де $X=\{x_i\}$, $i=\overline{1,n}$ – множина елементів системи, визначається її інтегральним впливом на виконання системою множини функцій $Y=\{y_j\}$, $j=\overline{1,m}$

$$\rho_i = \sum_{j=1}^{m} \mu_{ij} \, . \qquad (2.6)$$

де μ_{ij} – ступінь впливу складової x_i на ефективність виконання функції $y_j \in Y$ системи. Значення $\mu_{ij} \in [0…1]$ може бути визначене експертним оцінюванням з врахуванням частоти виконання системою функції y_j або як оцінка найменшого впливу з впливів x_i на ефективність виконання кожної функції $y_j \in Y$, отримана попарним порівнянням (методом найменшого впливу запропонованим у [51]).

Метод [51] рекомендується автором для аналізу багатофункціональних систем з погано вираженою структурою, таких як організаційні і військові системи. Цей метод придатний і для аналізу систем захисту інформації, наприклад в [53, 54] він застосовується для ранжування загроз з метою визначення допустимої інтенсивності зниження рівня захищеності об’єкта КІ.

В монографіях [28, 29] розглянуті питання автоматизації процедур оцінювання РІБ з використанням чітких числових вхідних даних і нечітких даних, представлених у вигляді лінгвістичних змінних. При цьому враховуються період часу, на який оцінки залишаються дійсними, галузеві особливості застосування і специфіка МІБ досліджуваної організації. Лінгвістичні змінні в [28, 29], які застосовуються для формування кортежа, що описує ризик ІБ при оцінюванні загроз і РІБ, перевизначаються в реальному часі. При цьому використовуються метрики з відкритих баз даних уразливостей, наприклад, з бази даних записів уразливостей *US-CERT*, з банку даних загроз безпеки інформації, з баз даних уразливостей *SecurityFocus*, *IBM X-Force*, *Open Sourced Vulnerability Database*, *National Vulnerability Database*.

Частина компонентів кортежу ризику в [28, 29] є ідентифікуючими компонентами, а частина – оціночними. Для оціночних компонент можуть бути визначені аналітичні або кореляційні залежності. Кореляційні залежності можуть бути одержані в системі отримання висновку за системою правил продукційної бази знань, наприклад «ЯКЩО (ймовірність= «Низька» і частота= «Середня») ТО небезпека= «Низька».

В тезах [62] моделі ризиків вторгнень в ІКС в умовах невизначеності будуються з використанням математичного апарату нечіткої логіки і аналізуються за допомогою програмної методики *Coras*. Сценарій розвитку загрози в [62] описується послідовністю станів ІКС, кожний з яких описується деякою нечіткою величиною або функцією з нечітко заданими параметрами. Для опису залежностей властивостей об'єктів і відносин у діаграмі загроз від параметрів процесів в реальній ІКС використовується апарат мереж Петрі–Маркова. За методологію *Coras*, яка доповнена апаратом нечіткої дескриптивної логіки, в [62] визначаються оцінки ризиків ІБ, які потім ранжуються і оцінюються за допомогою системи правил отримання нечітких висновків про стан ІБ. Автори [62] стверджують, що висновки отримуються для реального моменту часу більш точно і прозоро, ніж при застосуванні ймовірнісних оцінок.

В дисертації [52] пропонується методика оцінювання загроз і стану кібербезпеки із застосуванням нечітких когнітивних карт (рис.2.5-2.7), яка дозволяє спростити розрахунки і зменшити тривалість опрацювання даних.

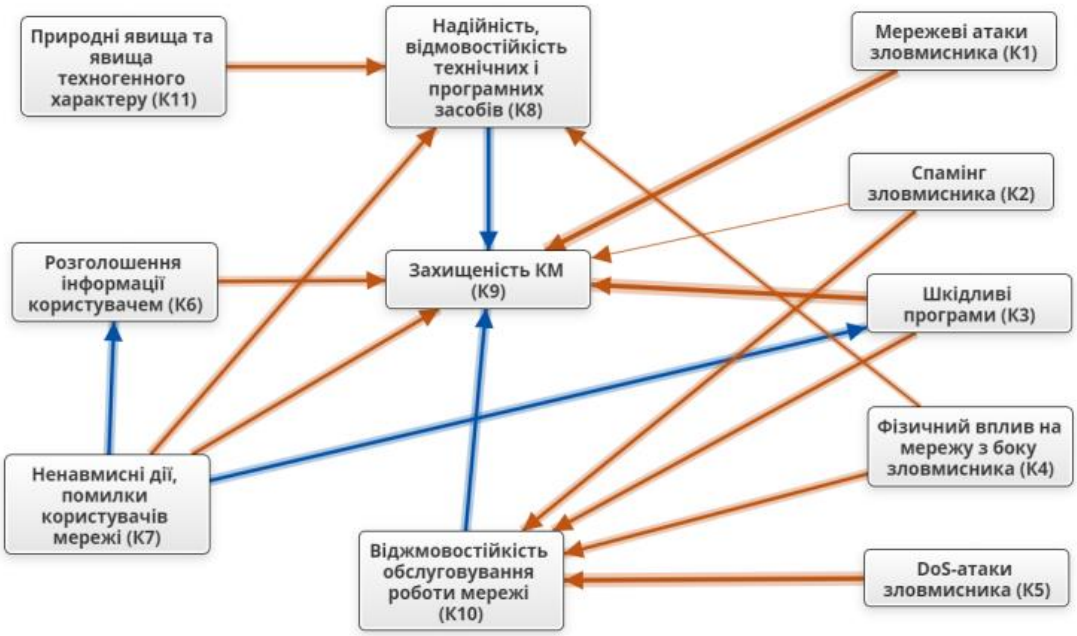

Рисунок 2.5 – Нечітка когнітивна карта стану кібербезпеки [52]

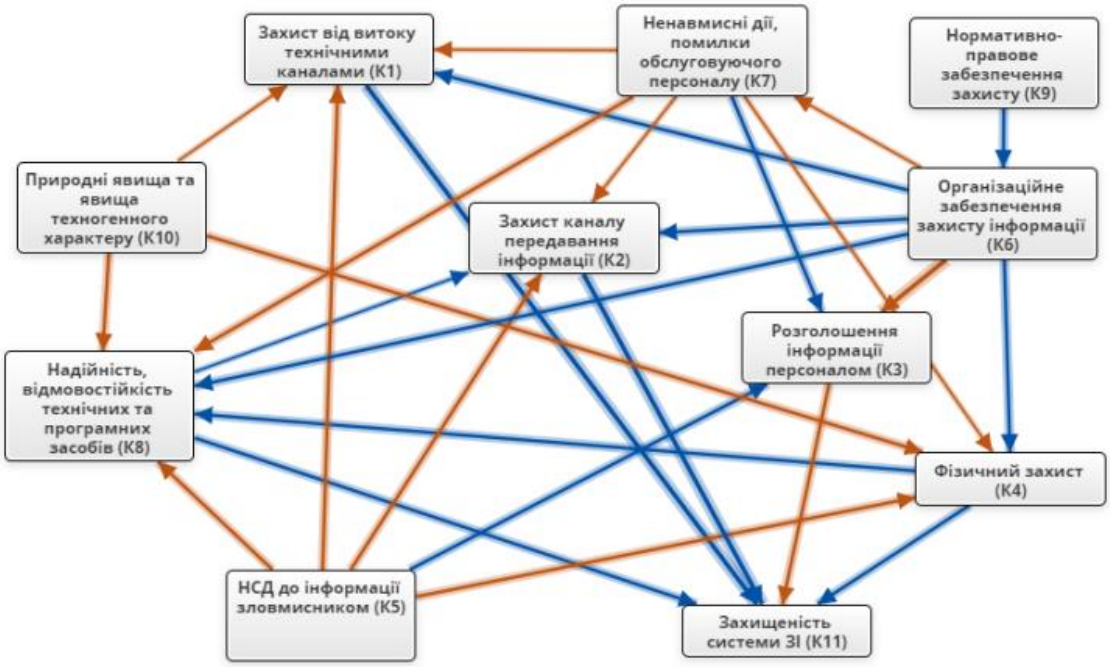

Рисунок 2.6 – Нечітка когнітивна карта стану захищеності системи захисту інформації [52]

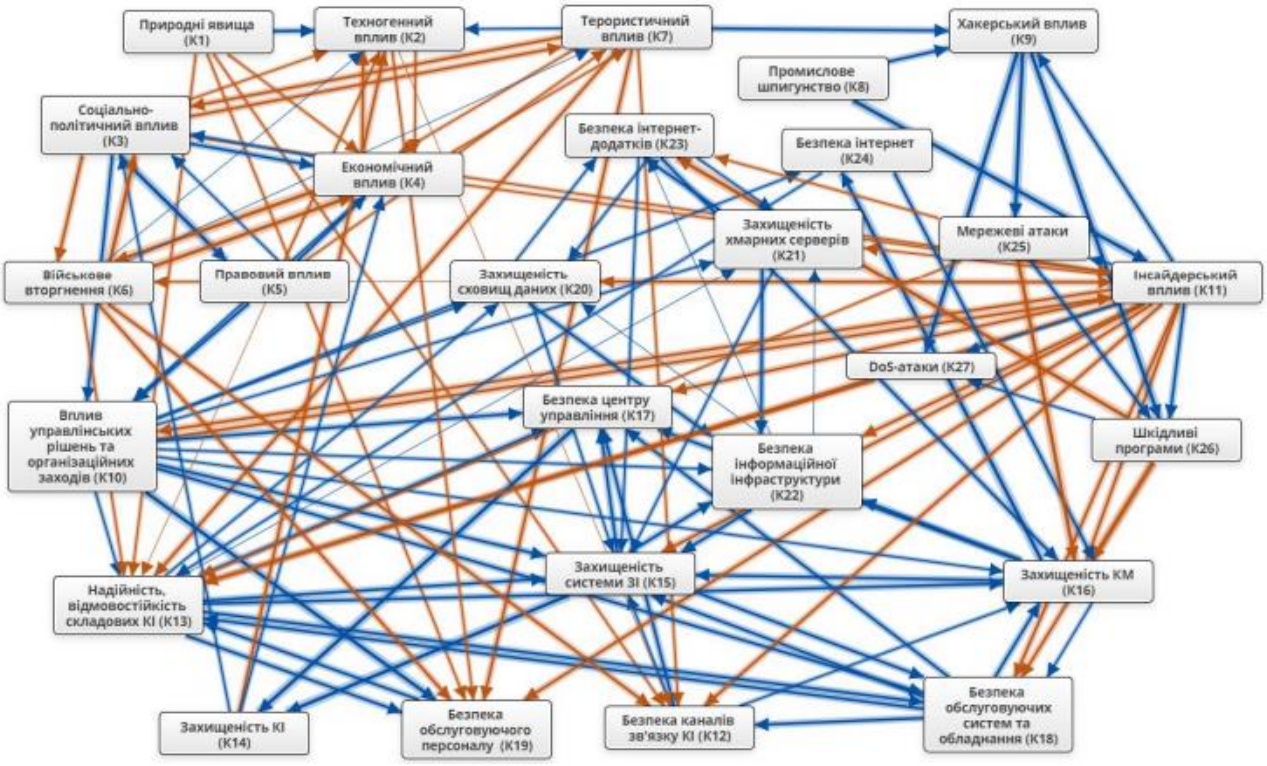

Рисунок 2.7 – Нечітка когнітивна карта рівня захищеності об’єкта КІ [52]

Ранжування загроз в [52] здійснюється із застосуванням теорії нечітких відношень, а визначені ранги загроз використовуються для оцінки доцільності інвестицій в ІБ, виходячи із балансу між рівнем РІБ і витратами на ІБ.

2.3.3 Оцінювання і ранжування загроз з використанням онтології

У статті [26] моделі загроз і порушників будуються з використанням онтології проведення випробувань КСЗІ, яка за класифікацією є онтологією предметної області, тобто враховує її специфіку.

Модель випробувань КСЗІ представляється ондографом, фрагмент якого з [26] наведено на рис.2.8. Цей ондограф складається із взаємно пов'язаних функціонально спеціалізованих модулів, до складу яких входить «Модель загроз», фрагмент ондографа якої наведено на рис.2.9.

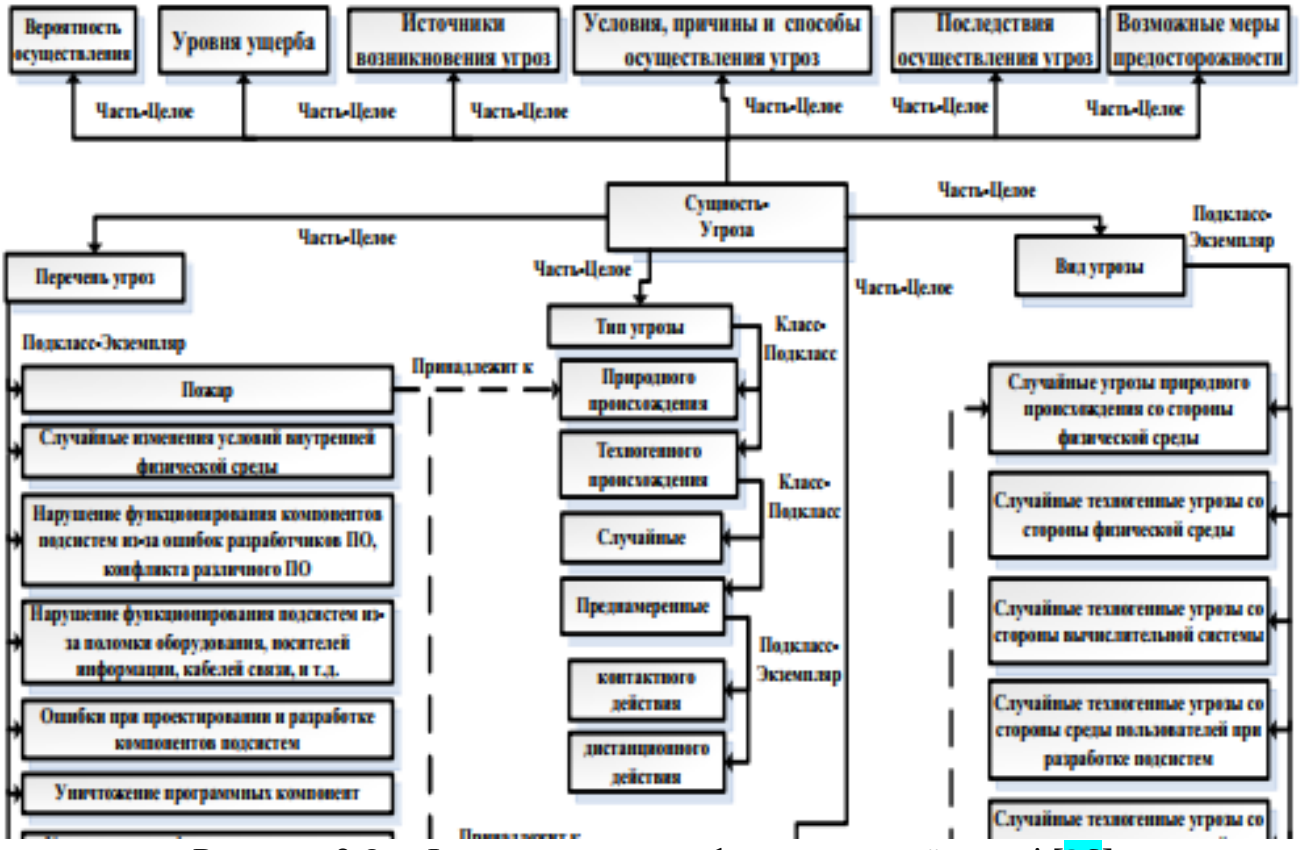

Рисунок 2.8 – Фрагмент онтографа предметної галузі [26]

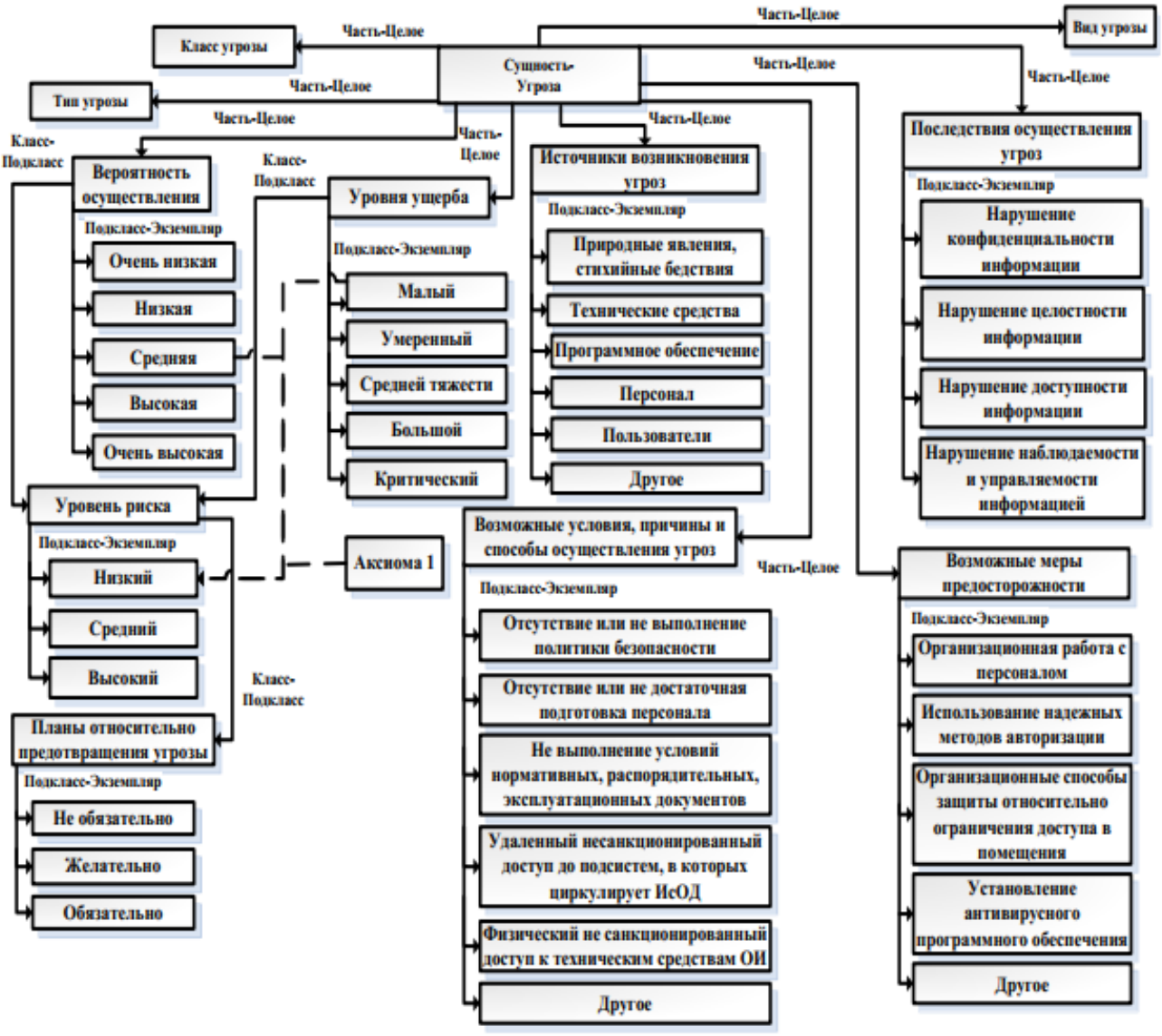

Рисунок 2.9 – Фрагмент онтографа модуля «Модель загроз» [26]

Онтографи, фрагменти яких наведені на рис.2.8 і рис.2.9, призначені для інформування користувача при побудові ним моделі загроз для об'єкта випробувань КСЗІ за допомогою бази знань, заснованої на онтології [26]. В модулі «Об'єкт випробувань» для кожного його класу, підкласу чи екземпляру визначаються характерні загрози і встановлюються відношеня з екземплярами класу «Перелік загроз» модуля «Модель загроз».

Перевагою онтологій як способу представлення знань є їх формальна структура, що спрощує їх автоматизовану обробку.

2.3.4 Оцінювання і ранжування загроз на графах

Крім когнітивних карт, принципри застосування яких розглянуті в п.2.3.2 даної кваліфікаційної роботи, оцінювання ступеня впливу загроз на захищеність інформації може бути здійснене на інших моделях із застосуванням графів, наприклад, на мережах Петрі і на графах атак.

Мережі Петрі дозволяють проводити віртуальні дослідження процесів функціонування будь-якої системи. В тезах [62] для аналізк загроз використовуються мережі Петрі–Маркова і програма *Coras*. В побудованих у [62] мережахі Петрі-Маркова кожний стан мережі S_i відповідає етапам атаки, а переходи t_j спрацьовують, якщо наявні умови для старту наступного етапу атаки. Кожна атака асоціюється із якоюсь загрозою, спрямованою щонайменше на один актив. В моделі [62] враховані також взаємозв'язки атак, за рахунок чого вони можуть мати негативний вплив на інщі активи. Наприклад, модель на рис.2.10 відповідає атаці «підміна довіреного об'єкта», яка вимагає перевантаження легального хоста мережі.

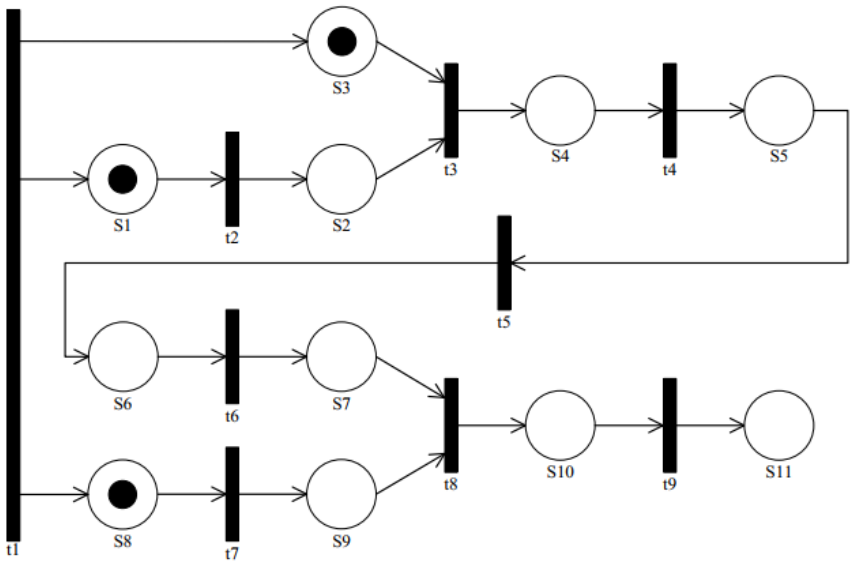

Рисунок 2.10 - Модель атаки «підміна довіреного об'єкта» з попередньою *DDoS*-атакою [62]

Стани *S*1-*S*5 на рис.2.10 відповідають *DDoS*-атаці, а інші стани – процесу підміни довіреного об'єкта. Перехід *t*1 відповідає початковій затримці спрацьовування мережі внаслідок *DDoS*-атаки. В [62] пропонується проводити дослідження на моделях за різними сценаріями, наприклад, замінити *DDoS*-атаку на нечітку випадкову величину, що характеризує випадкове перевантаження хоста, а «підміну довіреного об'єкта» на «сканування мережі».

Графи атак також ґрунтуються на описах змін стану системи і є одним із засобів [22, 60] виявлення атак на ІКС шляхом аналізу станів системи і можливих послідовностей дій зловмисника, які називають шляхами атак. Розрізняють наступні типи графів атак [22]:

– граф переліку станів, вершини якого відповідають атакам і описуються тріадами (джерело, мета, тип - елементарна атака або використання певної вразливості), а дуги - переходам між станами;

– граф умово-орієнтованих залежностей, вершини якого відповідають наслідкам атак, а дуги – елементарним атакам, що спричиняють ці наслідки;

– граф реалізації залежностей, вершини якого відповідають наслідкам атак або елементарним атакам, а дуги - умовам, які необхідні для реалізації атаки і досягення зловмисником бажаних наслідків атак.

Аналогічно графу атак будується граф системи захисту. Аналіз цих графів дозволє визначити: найбільш критичні вразливості, ефективність засобів і заходів безпеки, шляхи удосконалення системи захисту, перелік атак, які можуть мати успіх, але не виявляються системою виявлення вторгнень.

В моделі ІКС [60], яка також є орієнтованим графом, з вузлами, що відповідають станам ІКС, деякі стани ІКС визначаються як небезпечні для ІКС, а шляхи, що ведуть до таких кінцевих станів, позначаються як неприпустимі. Виявлення атаки за таким графом полягає у визначенні досяжності небезпечних станів з поточного стану системи.

2.3.5 Оцінювання і ранжування загроз на моделях систем масового обслуговування

Системи масового обслуговування (СМО) використовуються для моделювання і аналізу систем, які містять пункти обслуговування, що можуть мати різне функціональне призначення, і до яких надходить потік вимог (заявок) на обслуговування, які генеруються користувачами, приладами або подіями. Заявки надходять у випадкові моменти часу, обслуговуються випадковий час і, в залежності від прийнятої дисципліни черги, можуть не утворювати черги (СМО з відмовами), утворювати черги обмеженої чи необмеженої довжини.

При аналізі процесів захисту інформації загрози розглядаються як заявки на обслуговування, а засоби контролю - як пункти обслуговування. За допомогою моделей СМО можуть бути досліджені також процеси роботи взаємопов’язаних електронних схем, телефонного зв’язку, комп’ютерних мереж тощо.

При побудові моделей СМО зазвичай приймають, що вхідний і вихідний потоки вимог підпорядковуються закону Пуассона. Час надходження вимог і час їх обслуговування описуються експоненційним законом розподілу, з параметрами, які визначаються за статистичними даними, зібраними для досліджуваної системи або для її систем-прототипів.

Процес зміни станів СМО є марківським процесом (випадковий процес без післядії) і описується графом переходів між станами системи, за яким складають систему диференційних рівнянь. Рішення цієї системи рівнянь дозволяє визначити усереднені показники роботи системи: середній час очікування в черзі, середню кількість зайнятих каналів, очікувану довжину черги, ймовірності простою системи і відмови в обслуговуванні.

Процес взаємодії загроз і засобів захисту може розглядатися як функціонування багатоканальної СМО з очікуванням, на моделі якої може бути оцінені ймовірності успіху загроз загроз, ефективність засобів контролю тощо.

2.3.6 Оцінювання і ранжування загроз на формалізованих моделях

Формалізовані моделі оцінювання загроз ІБ будуються на основі прийнятої класифікації і моделі загроз, з врахуванням сценаріїв розвитку загроз. В роботі [54], наприклад, прийнята класифікація загроз *CIA*, а в сценаріях враховують:

–здатність зловмисника порушити цілісність інформації тільки після отримання ним несанкціонованого доступу до носія інформації;

– здатність зловмисника отримати несанкціонований доступ до носія інформації тільки після подолання ним засобів захисту, зокрема засобів контролю фізичного доступу (до ОІД, до приміщень, до апаратних засобів і ПЗ обробки і захисту ІзОД), охоронної сигналізації, засобів канального захисту ресурсів локальної мережі; засобів адміністрування доступу, засобів антивірусного захисту, організаційних заходів обмеження доступу;

–здатність зловмисника порушити конфіденційність інформації тільки після отримання доступу до інформації при умові, що він має достатні навички і засоби для зламу системи криптографічного захисту інформації;

–здатність зловмисника порушити доступність інформації тільки при виконанні однієї з двох умов: або він отримав можливість організувати потужний потік запитів певних типів активу, що є об’єктом атаки, він подолав засоби контролю прав доступу на рівні адміністратора безпеки і отримав можливість втрутитися в роботу системи управління доступом.

Таким чином, ймовірність успішної реалізації загрози залежить від сценарію атаки. Наприклад, для певного активу ймовірність порушення доступності $P_Д$ [9, 10] визначається за умови, що існує ймовірність отримання зловмисником необхідного доступу P_{MD} і ймовірність того, що під час звертання до певного активу лігітимного суб’єкта будуть виконуватися інші запити на використання цього активу P_U. Ймовірність P_U залежить від щільності потоку запитів на використання атакованого активу λ_Q -і середнього часу використання

атакованого активу різними суб'єктами t_{UR}. Тоді формалізована модель порушення доступності і порушення ІБ ($P_{ІБ}$) в цілом матиме вигляд:

$$P_{Д} = 1-(1-P_{U})(1-P_{UBAA}); \quad (2.7)$$

$$P_{U} = 1-e^{-t_{UR}\lambda_{Q}}; \quad (2.8)$$

$$P_{UBAA} = 1 - P_{MD}, \quad (2.9)$$

$$P_{ІБ} = 1-(1- P_{К})(1- P_{Ц})(1-P_{Д}). \quad (2.10)$$

де P_{UBAA} - ймовірність неподолання зловмисником системи управління доступом (стійкість системи управління доступом);

$P_{К}$ - ймовірність порушення конфіденційності;

$P_{Ц}$ – ймовірність порушення цілісності.

2.3.7 Оцінювання і ранжування загроз шляхом тестування

Одним із методів отримання оцінок критичності загроз є тестування, яке може проводитися різними методами, найбільш розповсюдженими з яких є пен-тестування з урахуванням оцінки ризиків, тестування «червоною командою» і пен-тестування (пентестинг, пен-тест), характеристики яких наведені в табл.2.1.

При тестуванні з урахуванням ризиків пріоритети дій визначаються з урахуванням вже виявлених загроз і ризиків. Група внутрішньої безпеки та зовнішній експерт приймають рішення щодо потенційних ризиків і оцінюють їх за рівнем критичності. Даний вид тестування доцільний, якщо час на тестування дуже обмежений або оцінку ризиків треба провести терміново.

Тестування «червоною командою» та пентестинг імітують атаку на захищене середовище. «Червона команда» визначає типи даних, які вона хоче отримати в результаті тестування, складає список відомих та потенційних вразливостей і визначає дії, що є необхідними для імітації «складної постійної

загрози» (*apt*-атаки), при якій використовуються ручні засоби тестування і методи соціальної інженерії. Тестування «червоною командою» порівняно з пентестингом є більш продуманою і контрольованою атакою, спрямованою на конкретні цілі, однак воно триває довше.

Таблиця 2.1 – Порівняння методів тестування

Параметри	Тестування на основі ризиків	Тестування «червоною командою»	Пент-тестинг
Ціль	Визначення найбільш незахищених напрямків	Оцінка ризиків за конкретним напрямом	Комплексна оцінка ризиків та загроз
Результат	Тестування у прискореному режимі, швидке виявлення основних ризиків та посилення безпеки	Звіт з глибокою оцінкою певної компоненти безпеки або тестування впливу ризиків та величини можливих втрат	Повний звіт про виявлені недоліки системи захисту
Умови проведення	Обмежений час для оцінки ІБ; термінове тестування	Глибоке дослідження конкретних уразливостей та загроз	Періодично; після зміни конфігурації системи
Учасники	Група внутрішньої безпеки, зовнішній експерт	Зовнішній експерт	Група внутрішньої безпеки, зовнішній експерт
Тривалість	Коротка	Тривала	Середня
Вартість	Низька	Висока	Середня
Інструменти	Автоматизовані засоби тестування ІБ	Ручні засоби тестування; методи соціальної інженерії; імітація реальних атак	Автоматизовані та ручні засоби тестування ІБ

Пентестинг імітує атаку з використанням набору ручних інструментів та автоматизованих засобів, зокрема, засобів сканування вразливостей. Використання різноманітних автоматизованих засобів дозволяє скоротити час тестування порівняно з тестуванням «червоною командою», визначити та оцінити всі загрози та ризики. Регулярне проведення пентестингу є вимогою багатьох нормативних документів з ІБ. Як випливає з табл.2.1, за критеріями часу, охоплення та повноти результатів пентестинг є найбільш збалансованим методом і забезпечує ефективну оцінку ризиків і загроз.

2.4 Особливості оцінювання і ранжування загроз за стандартом *ISO/IEC* 27005:2022

Перша версія міжнародного стандарту *ISO/IEC* 27005 «*Information technology – Security techniques – Information security risk management*» була прийнята у 2008 році. *ISO/IEC* 27005:2008 замінив дві частини (*Part 3: «Techniques for the management of IT Security», Part 4: «Selection of safeguards»*) застарілого технічного стандарту *ISO/IEC TR* 13335 «*Information technology — Guidelines for the management of IT Security*» (*TR – technical report* – технічний звіт), який діяв з 1998 року. Після 2008 року виходили нові версії стандарту *ISO/IEC* 27005 – у 2011 [3], 2018 і 2022 [4] роках. На даний час є чинною версія стандарту *ISO/IEC* 27005:2022 [4].

В Україні міжнародний стандарт *ISO/IEC* 27005 вперше було імплементовано у формі держстандарту України ДСТУ *ISO/IEC* 27005:2015 (*ISO/IEC* 27005:2011, *IDT*) «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки» у 2015 році за Наказом №193 Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18.12.2015 «Про прийняття нормативних документів України, гармонізованих з міжнародними та європейськими нормативними документами і скасування національних стандартів України». ДСТУ *ISO/IEC* 27005:2015 на чотири роки відставав від актуальної на той час версії міжнародного стандарту *ISO/IEC* 27005:2011. Друга і третя версії ДСТУ *ISO/IEC* 27005 (ДСТУ *ISO/IEC* 27005:2019 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки» (*ISO/IEC* 27005:2018, *IDT*) [13] та ДСТУ *ISO/IEC* 27005:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (*ISO/IEC* 27005:2022, *IDT*)» відставали від версій

міжнародного стандарту *ISO/IEC* 27005:18 і *ISO/IEC* 27005:2022 [4] вже тільки на один рік. Назва ДСТУ *ISO/IEC* 27005:2023 відрізняється від назв попередніх держстанартів, прийнятих у відповідності до *ISO/IEC* 27005.

За поточною версією міжнародного стандарту *ISO/IEC* 27005:2022 [4] і відповідного ДСТУ ДСТУ *ISO/IEC* 27005:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки» процес менеджменту РІБ реалізується у шість етапів.

Етап 1 «Створення контексту» передбачає:

–проведення загального аналізу всієї інформації про організацію, яка є необхідною для визначення контексту;

–визначення сфери дії менеджменту РІБ;

–прийняття основних критеріїв і правил, необхідних для управління РІБ.

Контекст вперше визначається, коли проводиться узагальнена оцінка високорівневого ризику. Якщо узагальнена оцінка дозволяє прийняти однозначне рішення щодо прийняття або обробки ризику, то задача вважається виконаною і на наступній ітерації управління РІБ в контекст вносяться зміни тільки в опис застосованих засобів і заходів контролю, наприклад, опис нового ПЗ або процедури перекладання ризику. Якщо узагальнена оцінка не дозволяє прийняти однозначне рішення щодо прийняття або обробки ризику, то вважається, що контекст містить недостатньо інформації для прийняття рішень і має бути уточнений або змінений. Зміни (точка прийняття рішення №1 на рис.2.1) можуть стосуватися критеріїв оцінки ризиків, критеріїв прийняття ризиків, критеріїв впливу, звуження сфери застосування МІБ тощо. Корекція контексту починає новиу ітерацію управління РІБ.

Етап 2 «Оцінка ризиків» передбачає:

–ідентифікацію активів, загроз, вимог нормативних документів стейкхолдерів, уразливостей і наслідків;

–визначення оцінок ризиків. При визначенні якісних оцінок вартостей активів, ймовірностей та потенційних наслідків реалізації загроз використовується шкала кваліфікації атрибутів, наприклад: «низький», «середній» «високий». Кількісна оцінка вартостей активів, ймовірностей та потенційних наслідків реалізації загроз є числовим значенням в грошових (для активів і наслідків) або бальних одиницях вимірювання. Оцінка ймовірностей може проводитися на підставі власного досвіду експерта (який усереднюється для групи експертів з врахуванням їх вагових коефіцієнтів) або на підставі наявної статистики інцидентів (у світі, в країні, в галузі чи в самій організації). Результатами цього етапу будуть оцінки ризиків, ймовірностей виникнення загроз, ймовірностей реалізації загроз через певні вразливості, ймовірностей і рівнів негативних наслідків, ймовірностей і ризиків для сценаріїв розвитку загроз, які підлягали аналізу;

–складання опису загроз і ризиків із визначеними якісними, кількісними або комбінованими оцінками;

–визначення рангів ризиків і загроз за пріоритетами, по визначених групах (для всієї сфери менеджменту РІБ, для підрозділів організації, для певних активів, для певних бізнес-процесів, для певних технологій, для загроз певного типу, для вразливостей тощо;

–визначення ризиків, що підлягають обробці, за критеріями, які були прийняті на етапі 1.

Етап 3 «Обробка ризиків» передбачає застосування правил і критеріїв, прийнятих на етапі 1, для визначення методів (зниження, збереження, запобігання чи перенесення ризику) і засобів обробки ризиків. На цьому етапі можуть бути прийняті рішення навіть щодо припинення окремих бізнес-процеів, які асоціюються з високоймовірними тяжкими наслідками реалізації загроз. Ефективність обробки ризику визначається за результатами оцінци ризиків на наступній ітерації управління РІБ. Якщо на наступній ітерації ризик залишається

неприйнятним, то застосовуються додаткові засоби контролю, і повторюється процес оцінки загроз і ризиків. Якщо застосування додаткових засобів контролю вже неможливе, тоді розглядається доцільність зміни контексту (точка прийняття рішення №2 на рис.2.1) – деталізації ризику або прийняття нових критеріїв і правил оцінювання, прийняття та обробки ризиків.

Етап 4 «Прийняття ризику» передбачає прийняття ризиків низького рівня, що не є критичними для організації, і прийняття високих ризиків (найчастіше малоймовірних ризиків, що асоціюються із тяжкими наслідками), якщо організація не має ресурсів для їх обробки. До прийняття рішення щодо залишкових ризиків необхідно впевнитися в тому, що керівництво організації розуміє і однозначно приймає їх. Це особливо важливо тоді, коли засоби контролю для зниження ризиків, заходи із запобігання чи перенесення ризиків не можуть бути застосовані через високу вартість або їх впровадження відкладається.

Етап 5 «Комунікації ризику» передбачає повідомлення зацікавлених сторін про результати проведеного аналізу і оцінювання ризиків. Під час управління РІБ на будь-якому етапі важливим є обмін інформацією щодо ризиків між керівництвом та персоналом, оскільки навіть попередня інформація про про ідентифіковані ризики є важливою для прийняття рішень щодо напрямів розвитку бізнесу, управління інцидентами та зниження потенційних збитків. Інформація стейкхолдерами надається стейкхолдерами вже після прийняття рішень щодо обробки ризиків.

Етап 6 «Моніторинг та перегляд РІБ» є необхідним для своєчасного виявлення змін у стані кібербезпеки і вживання заходів щодо його коригування.

Таким чином, процес управління РІБ є циклічним і ітераційним. Ранжування ризиків і загроз проводиться на кожній ітерації. Ітеративний підхід до оцінювання ризиків і загроз, який передбачає можливість поглибленої оцінки на кожній ітерації, дозволяє зменшити витрати часу та інших ресурсів на визначення засобів контролю, гарантуючи водночас, що високорівневі небезпечні ризики будуть оцінені і оброблені.

ISO/IEC 27005:2022 містить опис процесу менеджменту РІБ та пов'язаних з ним видів діяльності. Складові управління РІБ по кожному етапу структуровані у розділах *ISO/IEC* 27005:2022 і представлені сукупністю вхідних даних, які необхідні для виконання дій на даному етапі; дій, які підлягають виконанню на даному етапі; рекомендацій із виконання цих дій та вихідних даних етапу.

Оцінка критичності і ранжування загроз є основою управління РІБ на протязі всього життєвого циклу СУІБ.

2.5 Топ-загрози у галузі кібербезпеки

2.5.1 Тренди 2024 року у галузі кібербезпеки України за даними компанії *ESET*

Визначення найбільш ймовірних загроз можна здійснити апріорно на основі досліджень, проведених за світовою статистикою провідними фірмами і організаціями в галузі інформаційної безпеки і IT-технологій.

Словацька компанія *ESET*, яка є автором легендарного продукту *ESET NOD32 Antivirus* і працює в Україні з 2003 року, представила [2] звіт з аналізу кіберпростору України, в якому визначений рейтинг найбільш поширених кіберзагроз з червня по листопад 2024 року.

У структурованому вигляді виявлені компанією *ESET* у кіберпросторі України тренди і загрози наведені на рис.2.11.

Період з червня по листопад 2024 року характеризується тим, що:

– у соцмережах на 335% зросла кількість нових схем шахрайства з використанням діпфейків та шахрайства під виглядом брендів компаній, спрямованих на заманювання жертв у шахрайські інвестиційні схеми;

– було виявлене нове шахрайство, спрямоване на користувачів популярних платформ бронювання житла *Booking.com* та *Airbnb*. Шахраї використовують

набір інструментів *Telekopye* і скомпрометовані облікові записи готелів та орендарів житла на онлайн-ринках, обирають людей, які нещодавно забронювали житло, і надсилають їм шахрайські сторінки для оплати;

Рисунок 2.11 - Тренди і загрози у кіберпросторі України у другому півріччі 2024 року за даними компанії *ESET*

– кіберзлочинці активно шукали недоліки у безпеці та інноваційні способи інфікування мобільних пристроїв для збільшення кількості жертв. *ESET* виявила нові вектори атак та нові загрози, зафіксувала поширення використання методів соціальної інженерії;

– поширилися загрози, спрямовані на викрадення даних;

– найчастіше для викрадення даних зловмисники застосовували *Formbook*, який є інфостилером - трояном, призначеним для збирання інформації з системи жертви. *Formbook* може збирати облікові дані з різних браузерів, робити знімки

екрану, відслідковувати і реєструвати натискання клавіш, завантажувати і виконувати файли за командами свого керуючого серверу. *Formbook* вперше був виявлений у 2016 році і розповсюджувався за допомогою тематичних компаній *Covid*-19. У липні 2021 року було виявлено новий штам цього шкідливого ПЗ – *XLoader*, націлений на користувачів *macOS*. *Formbook* був визнаний найбільш небезпечною кіберзагрозою у серпні 2021 року;

– за даними телеметрії *ESET* майже на 400% за останні пів року зросло виявлення загрози *Lumma Stealer*. *Lumma Stealer* - це шкідливе ПЗ для крадіжки інформації, яке доступне за допомогою програми *Malware-as-a-Service* (*MaaS*), що спеціалізується на крадіжці конфіденційних даних, таких як паролі, інформація про браузер і деталі гаманця криптовалюти. Зловмисники удосконалили свою тактику, перейшовши від традиційного фішингу до підробленої перевірки *CAPTCHA*, і використовуючи законне ПЗ для доставки *Lumma Stealer* [8];

– однією з головних цілей для зловмисників у другій половині 2024 року були дані криптовалютних гаманців, що зумовлено рекордним зростанням вартості крипто валют;

– збільшилась кількість виявлених загроз викрадення криптовалюти на багатьох платформах;

– більш ніж удвічі порівняно з попереднім періодом зросла зареєстрована кількість загроз викрадення паролів і облікових даних киптовалютних гаманців на пристроях *macOS*;

– було виявлено шкідливе ПЗ для викрадення паролів і облікових даних киптовалютних гаманців на пристроях *macOS*;

– на 20% зросли фінансові загрози для *Android*, спрямовані на банківські програми та також криптовалютні гаманці; Україна опинилася серед 6 країн з найбільшою кількістю виявлених фінансовихі загроз для Android, націлених на

викрадення грошей з банківських додатків, разом із Туреччиною, Бразилією, Мексикою, Індією та Німеччиною;

– виявлені нові технології атак на пристрої *Android* та *iOS*, які не вимагають надання дозволу користувачів на встановлення програм із невідомих джерел. Зловмисники використовували технології обходу традиційних заходів безпеки на смартфонах, які базуються на використанні *WebAPK* та *PWA*, що є гібридом звичайної вебсторінки та мобільного додатку.

2.5.2 Топ-10 кіберзагроз на 2030 рік за даними *ENISA*

Агентство Європейського Союзу з мережевої та інформаційної безпеки (англ. *European Union Agency for Cybersecurity, ENISA*) провело аналіз і опублікувало топ-10 кіберзагроз на 2030 рік [7] (рис.2.12).

Рисунок 2.12 – Топ-10 кіберзагроз на 2030 рік за даними *ENISA* [7]

ENISA рекомендує урядам, організаціям і окремим особам звернути особливу увагу на наступні загрози, які можуть спричинити значні збої і втрати:

1) порушення ланцюга поставок ПЗ, яке може спричинити в умовах посилення інтеграції компонентів і послуг від зовнішніх постачальників появу нових та непередбачених вразливостей і порушення ІБ як постачальників, так і клієнтів;

2) розширені дезінформаційні кампанії, спрямовані на маніпулювання спільнотами через грунтовніі фейкові атаки як з геополітичних, так і з фінансових міркувань;

3) поширення цифрового стеження та втрата приватності. Зловмисники можуть використовувати системи розпізнавання облич і транспорту, цифрове спостереження на інтернет-платформах та сховища даних цифрової ідентифікації для збирання конфіденційної інформації про особу;

4) використання помилок користувачів і персоналу та застарілих систем кіберзахисту. Швидке впровадження *IoT,* необхідні часті зміни в системах захисту з метою їх адаптації до мінливих умов функціонування можуть спричинити проблеми з ІБ внаслідок невідповідності систем захисту поточним вимогам і відсутності у персоналу та користувачів розуміння, навичок і досвіду роботи в поточному кіберфізичному середовищі;

5) поширення цілеспрямованих, персоналізованих і вдосконалених атак із використанням інформації, отриманої від підключених до Інтернету смарт-пристроїв;

6) неадекватний актуальним викликам моніторинг та аналіз кібербезпеки інфраструктури та елементів. Неадекватне розуміння, оцінювання та регулювання ІБ інфраструктури, зокрема, без врахуввання перетину кіберпросторів приватних і державних інфраструктур, можуть спричинити збої в роботі інфраструктурних об’єктів та інфраструктур в цілому, порушити їх кіберстійкість та кіберготовність;

7) зростання кількості новітніх гібридних загроз, зумовлене зростанням кількості і розширенням функціональності смарт-пристроїв, використанням хмарних сервісів і сховищ данихи, поширенням сайтів соціальних мереж,

збільшенням кількості засобів визначення і приховування онлайн-ідентичності. Фізичні або офлайн-атаки все частіше поєднуються з кібератаками;

8) активізація атак зловмисників на організації з обмеженими можливостями забезпечення кібербезпеки, найнижчими рівнями зрілості систем захисту і недостатньо компетентним в галузі кіберзахисту персоналом;

9) покладання зловмисниками на транскордонних постачальників послуг ІКТ ролі спільної (єдиної) точки відмови у разі будь-якого майбутнього конфлікту. Сектор ІКТ, що об'єднує критично важливі служби (транспорт, мережі електроживлення, промисловість, прикордонні служби тощо) тоді, за прогнозом *ENISA*, стане об'єктом зловмисних дій із застосуванням бекдорів, фізичних маніпуляцій, *DDoS* і зброї;

10) поширення застосування зловмисниками засобів штучного інтелекту для створення дезінформації та хибного вмісту, формування упередженості, проектування атак із складними стратегіями, автоматизації процесів генерації і управління реалізацією загроз, розробки військових роботів, пошкодження даних, збирання біометричних даних та іншої конфіденційної інформації тощо.

Висновки фахівців *ENISA*, отримані в результаті аналізу і прогнозування процесів у сучасному кіберпросторі, багато в чому співпадають з висновками *ESET* щодо топ-загроз у кіберпросторі України в 2024 році [2] і з прогнозами *ISACA* щодо топ-загроз 2023 року [6]. *ISACA* (англ. *Information Systems Audit and Control Association*) об'єднує більше 115,000 членів в 180-ти країнах і спеціалізується на розробці стандартів управління, аудиту і безпеки інформаційних технологій. Головним висновком фахівців *ENISA* є: «Зменшення майбутніх ризиків неможливо відкласти або уникнути№ тому «краще попередити, ніж лікувати... Ми зобов'язані заздалегідь вжити всіх можливих заходів … для покращення ландшафту кібербезпеки у 2030 році та надалі» [7].

2.5.3 Російські кібероперації проти України за перше півріччя 2024 року

Також визначити найбільш ймовірні загрози можна з аналітичних звітів державних органів, наприклад ДССЗЗІ.

Фахівці ДССЗЗІ підготували і оприлюднили аналітичний звіт «Російські кібероперації» H1 '2024 [23], який розкриває нові тенденції в поведінці ворожих хакерів за результатами всеебічного аналізу кіберзагроз, що спостерігалися у кіберпросторі України протягом першого півріччя 2024 року.

Головним трендом першої половини 2024 року визнано значне зростання кількості кібератак на органи влади (як на урядові організації, так і на місцеві). На сектори енергетики, безпеки та оборони було спрямовано більша ніж вдвічі .кількість кіберінцидентів порівняно з попереднім періодом спостережень.

Основними інструментами кібершпигунства у першому півріччі 2024 року був фішинг та інфікування шкідливим ПЗ, головним засобом кіберзахисту від яких є підвищення обізнаності користувачів і персоналу з основними правилами кібергігієни та з актуальними на поточний момент кіберзагрозами.

Діяльність ворога спрямована на дестабілізацію ситуації в Україні, для чого активно застосовуються кібератаки. Деструктивні кібератаки є ефективним засобом знищення цивільної критичної інфраструктури, оскільки вони дешевші за балістичні ракети, але можуть призвести до таких самих руйнівних наслідків.

3 РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО РАНЖУВАННЯ ЗАГРОЗ

3.1 Вхідні і вихідні дані системи підтримки прийняття рішень

Вхідні дані для ранжування загроз отримуються на етапі визначення контексту та етапі ідентифікації ризиків процесу менеджменту РІБ (див. рис.2.1).

На етапі визначення контексту визначаються:

– наближена сфера застосування СППР ранжування загроз, яка відповідає сфері дії визначених правил менеджменту ризиків;

– місце розроблюваної СППР у складі процедур менеджменту ризиків ІБ.

Сфера дії менеджменту ризиків ІБ і, відповідно, сфера застосування СППР ранжування загроз) має бути окреслена таким чином, щоб забезпечити можливість визначення комплексного впливу загроз на ІКС, організацію та середовище її функціонування. Тому сфера застосування СППР повинна включати значимі активи, пов’язані з ними технології, бізнес-процеси та об’єкти як в межах визначеної сфери менеджменту ризиків, так і поза нею, враховуючи:

– структуру організації;

– стратегічні цілі бізнесу;

– бізнес-процеси різного ступеню важливості, зокрема ті, що пов’язані із виконанням задач, спрямованих на досягнення стратегічних цілей бізнесу, і спрямованих на оперативне вирішення найбільш важливих поточних задач;

– функції організації;

– розподіл функцій між структурними підрозділами організації;

– чинні для конкретної організації вимоги нормативно-правових актів і зобов’язання за договорами, які можуть бути порушені під впливом загроз;

– очікування стейкхолдерів від діяльності організації, зокрема очікувані економічні результати і ставлення до репутаційних збитків;

– інформаційні активи організації та поза організацією, що використовуються за різними технологіями у різних бізнес-процесах і потрапляють під негативний вплив загроз,

– особливості процесів інформаційного обміну між організацією і середовищем її йункціонування;

– особливості інтерфейсів обміну інформацією між організацією і середовищем її функціонування;

– параметри середовища функціонування організації та обмеження, що діють на організацію, такі як характеристики політичного та соціокультурного середовища, наявність засобів комунікації, енергетичних та інших ресурсів, географічне розташування організації, її віддаленість від ринків товарів та послуг, необхідних для функціонування організації, та від ринків збуту продукції організації.

На етапі ідентифікації ризиків для СППР ранжування загроз мають бути послідовно проведені п’ять процесів ідентифікації складових, що у сукупності дозволяють ідентифікувати ризики:

1) процес ідентифікації активів;

2) процес ідентифікації загроз;

3) процес ідентифікації засобів контролю;

4) процес ідентифікації вразливостей;

5) процес ідентифікації наслідків реалізації загроз.

Кожен з цих процесів ідентифікації характеризується притаманними йому процедурами, вхідними та вихідними даними.

Типовими процедурами в процесі ідентифікації ризиків є:

– для процесу ідентифікації активів: визначення цінності активів, значимості бізнес-процесів, зв’язків активів з бізнес-процесами;

– для процесу ідентифікації загроз: визначення ймовірностей загроз, рейтингів загроз за ймовірностями їх виникнення, найбільш і найменш ймовірних загроз;

– для процесу ідентифікації засобів контролю: визначення засобів контролю, які виконують певні функції, розташовані в певному місці в структурі організації і/або ІКС; визначення статистичних або експертних оцінок частоти використання і ефективності засобів контролю;

– для процесу ідентифікації вразливостей: виявлення вразливостей активів, а серед них - вразливостей, що можуть бути використані для реалізації кожною загрозою, і ймовірностей успішної реалізації кожної загрози в разі експлуатації нею кожної вразливості;

– для процесу ідентифікації наслідків реалізації загроз: формування переліку наслідків реалізації загроз і сценаріїв інцидентів.

Вхідними даними в процесі ідентифікації ризиків є:

– для процесу ідентифікації активів: сфера дії менеджменту ризиків із визначеними границями, структурним складом і параметрами (розташування, власник, середовище функціонування (стейкхолдери, їх фінансові і репутаційні інтереси), функції, бізнес-процеси); експертні оцінки цінності активів, значимості бізнес-процесів, щільності зв’язків активів з бізнес-процесами;

– для процесу ідентифікації загроз: інформація про загрози, отримана з різних джерел (від власників активів і користувачів, з реєстрів загроз, результати аналізів інцидентів тощо) стосовно типів загроз, сценаріїв інцидентів, використовуваних вразливостях, ймовірнісних характеристик загроз і наслідків;

– для процесу ідентифікації засобів контролю: список засобів контролю із визначеними функціями і очікуваною ефективністю, документація на них, план реалізації обробки ризиків;

– для процесу ідентифікації вразливостей: переліки активів із визначеною цінністю, засобів контролю із визначеною ефективністю, загроз із визначеними типами та джерелами;

– для процесу ідентифікації наслідків реалізації загроз: переліки активів із визначеною цінністю, бізнес-процесів з оцінкою їх значимості, загроз із визначеними властивостями, вразливостей із визначеними зв’язками з елементами інших переліків та показниками значимості.

Вихідними даними в процесі ідентифікації ризиків є:

– для процесу ідентифікації активів: переліки активів із визначеною цінністю та пов’язаних з ними бізнес-процесів із оцінкою їх значимості;

– для процесу ідентифікації загроз: перелік загроз із визначеними властивостями (джерело загрози, тип загрози, ймовірність виникнення загрози);

– для процесу ідентифікації засобів контролю: список наявних і запланованих для використання засобів контролю із визначеними параметрами (розташування, виконувані функції, частоти використання, ефективність);

– для процесу ідентифікації вразливостей: перелік вразливостей із визначеними зв’язками із загрозами, активами та засобами контролю та переліки вразливостей для кожної ідентифікованої загрози, активу та засобу контролю що пов’язані/не пов’язані з ними;

– для процесу ідентифікації наслідків реалізації загроз: перелік сценаріїв інцидентів ІБ із визначеними ймовірнісними показниками і наслідками для активів і бізнес-процесів.

Для організації процесу ранжування загроз користувачем мають бути задані кількість рангів ризиків NR та кількість рангів загроз NZ. Вихідними даними СППР є рейтинговий список загроз і/або списки загроз певного рангу.

3.2 Алгоритми ранжування загроз за стандартом *ISO/IEC* 27005:2022

Ранжування загроз в СППР здійснюється за розробленим у даній роботі узагальненим алгоритмом, наведеним на рис.3.1.

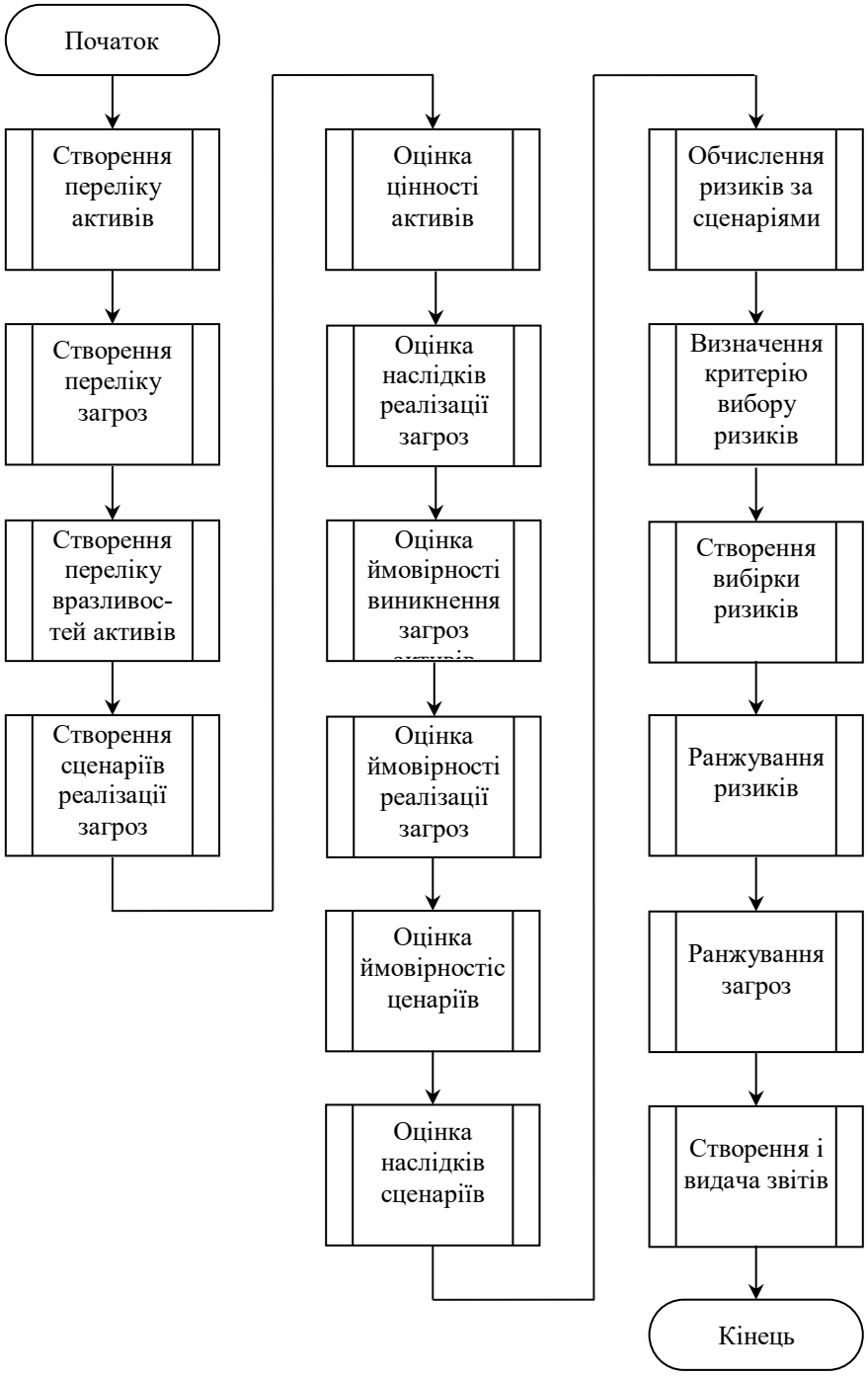

Рисунок 3.1 - Узагальнений алгоритм ранжування загроз

В СППР передбачено, що кількості рангів ризиків і загроз можуть бути однаковими (*NR*=*NZ*). Тоді ранги ризиків і загроз також приймаються однаковими і достатнім є алгоритм рис.3.2, а в іншому випадку при ранжуванні загроз здійснюється поділ діапазону рангів ризиків [1…*NR*] на інтервали, кількість яких

відповідає кількості рангів загроз *NZ*, що вимагає послідовного виконання алгоритмів рис.3.2 і рис.3.3 для кожного активу.

Ризики R_{ijk} визначаються для кожного сценарію. Сценарій *ijk* відповідає події успішної реаліації *j*-ої загрози за рахунок експлуатації *k*-ої вразливості для *i*-ого активу. Для кожного *i*-го активу за алгоритмом рис.3.3 послідовно переглядаються всі загрози, і для кожної з них перевіряються ризики, які асоційовані із успішною реалізацією *j*-ої загрози загрози через кожну можливу *k*-ту вразливість, тобто ризики за всіма можливими сценаріями, на належність *n*-ому діапазону ризиків, який обмежений границями $[a_n \ldots b_n]$, починаючи з діапазону найбільших ризиків.

Значення a_n та b_n в алгоритмі рис.3.2 визначаються, виходячи з визначеної користувачем кількості рангів ризиків *NR*, мінімальних $R_{\min}$ (верхня границя діапазону найменших ризиків $R_{\min}=b_1$) та максимальних $R_{\max}$ (нижня границя діапазону найбільших ризиків $R_{\max}=a_n$) значень ризиків за правилами:

$$a_1=0,\ b_1=R_{\min}; \tag{3.1}$$

$$a_2=R_{\min},\ b_2 = a_2 + \frac{R_{\max} - R_{\min}}{NR-2}; \tag{3.2}$$

$$a_n=b_{n-1},\ b_n = a_n + \frac{R_{\max} - R_{\min}}{NR-2}; \tag{3.3}$$

$$a_{NR}= b_{NR-1},\ b_2 = \infty. \tag{3.4}$$

Належність ризику до певного *n*-го діапазону $\left(n=\overline{1, NR}\right)$, тобто присвоєння ризикам певних рангів, визначається за правилами:

R_{ijk} має ранг $r_{ijk}=1$, якщо $R_{ijk} < b_1=R_{\min}$; (3.5)

R_{ijk} має ранг $r_{ijk}=n$, якщо $a_n \le R_{ijk} < b_n$ і $n<NR$; (3.6)

R_{ijk} має ранг $r_{ijk}=NR$, якщо $R_{\max} \le R_{ijk}$. (3.7)

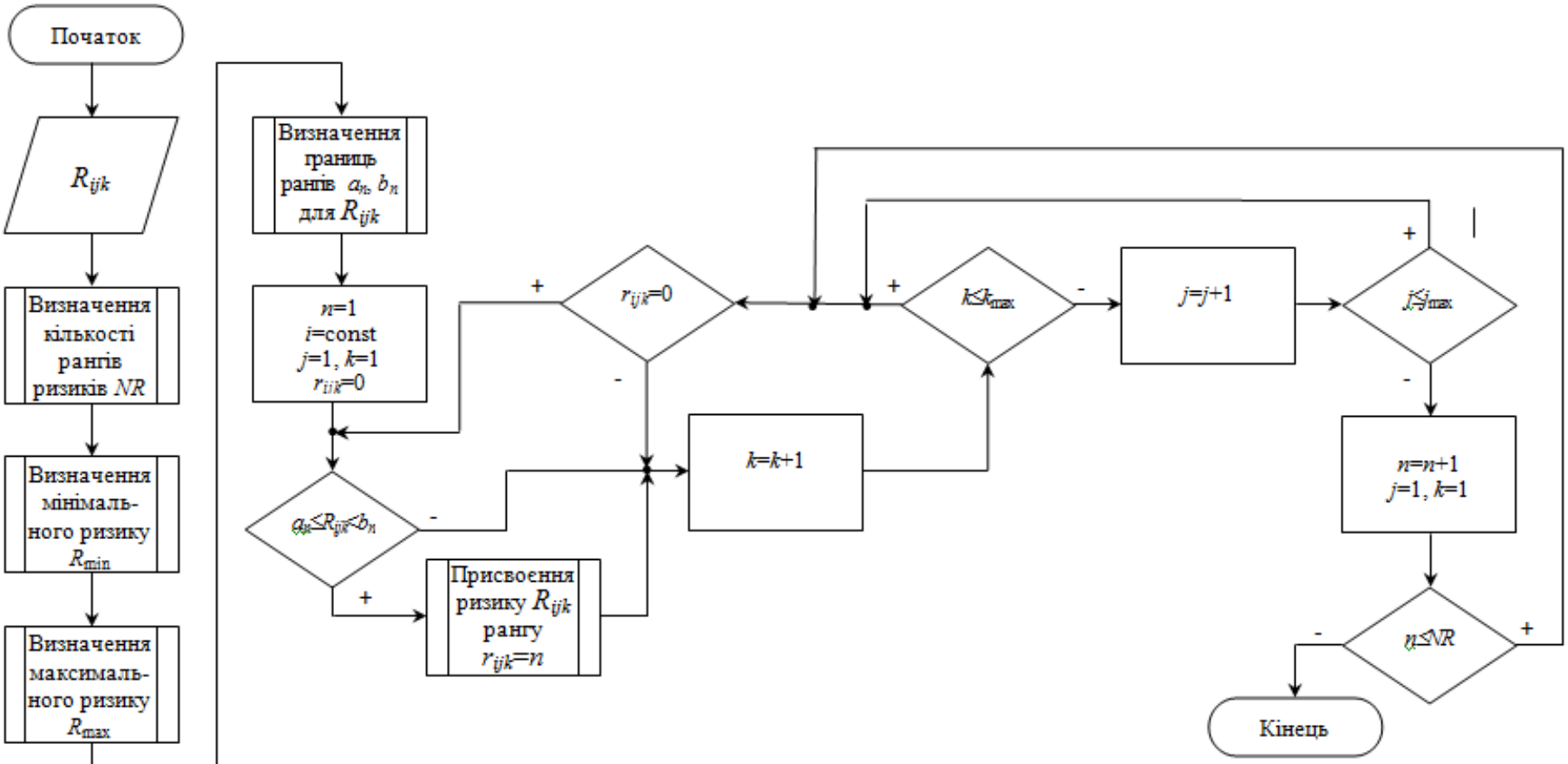

Рисунок 3.2 – Алгоритм ранжування ризиків за стандартом *ISO/IEC* 27005:2022

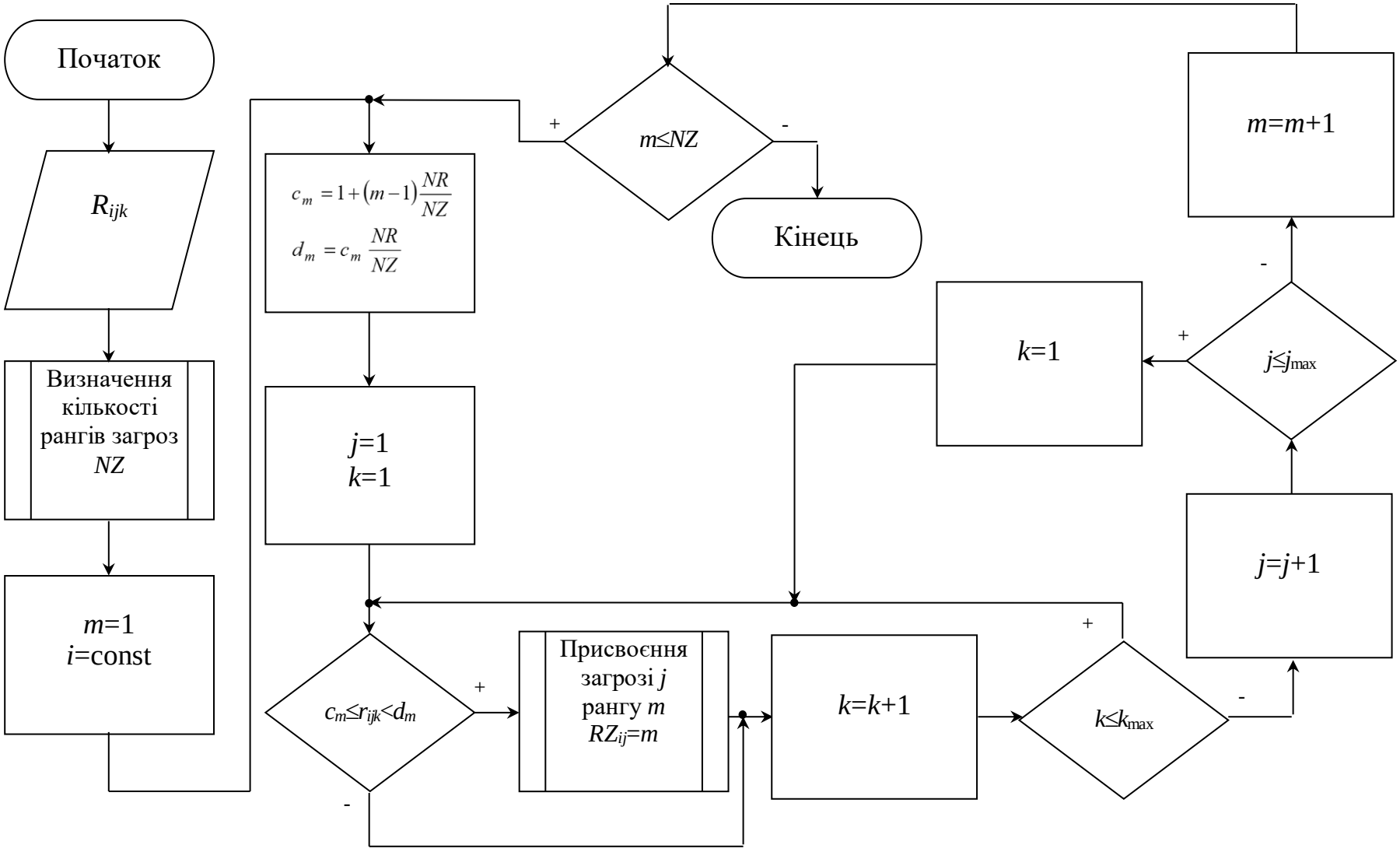

Рисунок 3.3 – Алгоритм ранжування загроз за стандартом *ISO/IEC* 27005:2022 для *i*-го активу

При ранжуванні загроз, якщо *NR=NZ*, то ранг *j*-ої загрози дорівнює max(r_{ijk}).

Якщо *NR≠NZ*, то ранг *j*-ої загрози визначається за належністю рангів r_{ijk} асоційованих із *j*-ою загрозою ризиків R_{ijk} до *m*-го діапазону, що відповідає *m*-ому рангу $\left(m=\overline{1, NZ}\right)$ загроз. Границі *m*-го діапазону рангів загроз обмежуються значеннями c_m і d_m, що визначаються визначеними за формулами (3.8) і (3.9):

$$c_m = 1 + (m-1)\frac{NR}{NZ}; \tag{3.8}$$

$$d_m = c_m \frac{NR}{NZ}. \tag{3.9}$$

Ранги загроз переглядаються у порядку зростання ризиків (від 1 до *NZ*), тому, якщо *j*-та загроза має можливості реалізації шляхом експлуатації різних вразливостей різних активів і асоціюється внаслідок цього з ризиками різних рангів, то ранг загрози, згідно алгоритму рис.3.3 буде перевизначатися від мінімального до максимального значення, і остаточне значення рангу *j*-ої загрози для *i*-го активу буде визначатися за рангом максимального асоційованого із загрозою ризику $\max\limits_{k}\left(r_{ijk}\right)$. Умовою присвоєння *j*-ій загрозі для *i*-го активу рангу $RZ_{ij}=m$ є (3.10), а присвоєння *j*-ій загрозі рангу *m* за всією сферою менеджменту ризиків здійснюється за правилом (3.11)

$$c_m \le r_{ijk} < d_m. \tag{3.10}$$

$$R_j=m, \text{ якщо } c_m \le \max_{k,\,i}\left(r_{ijk}\right) < d_m. \tag{3.11}$$

3.3 Структура системи підтримки прийняття рішень

Структура розробленої моделі представлена на рис.3.4, а інформаційні потоки в ній – на рис.3.5.

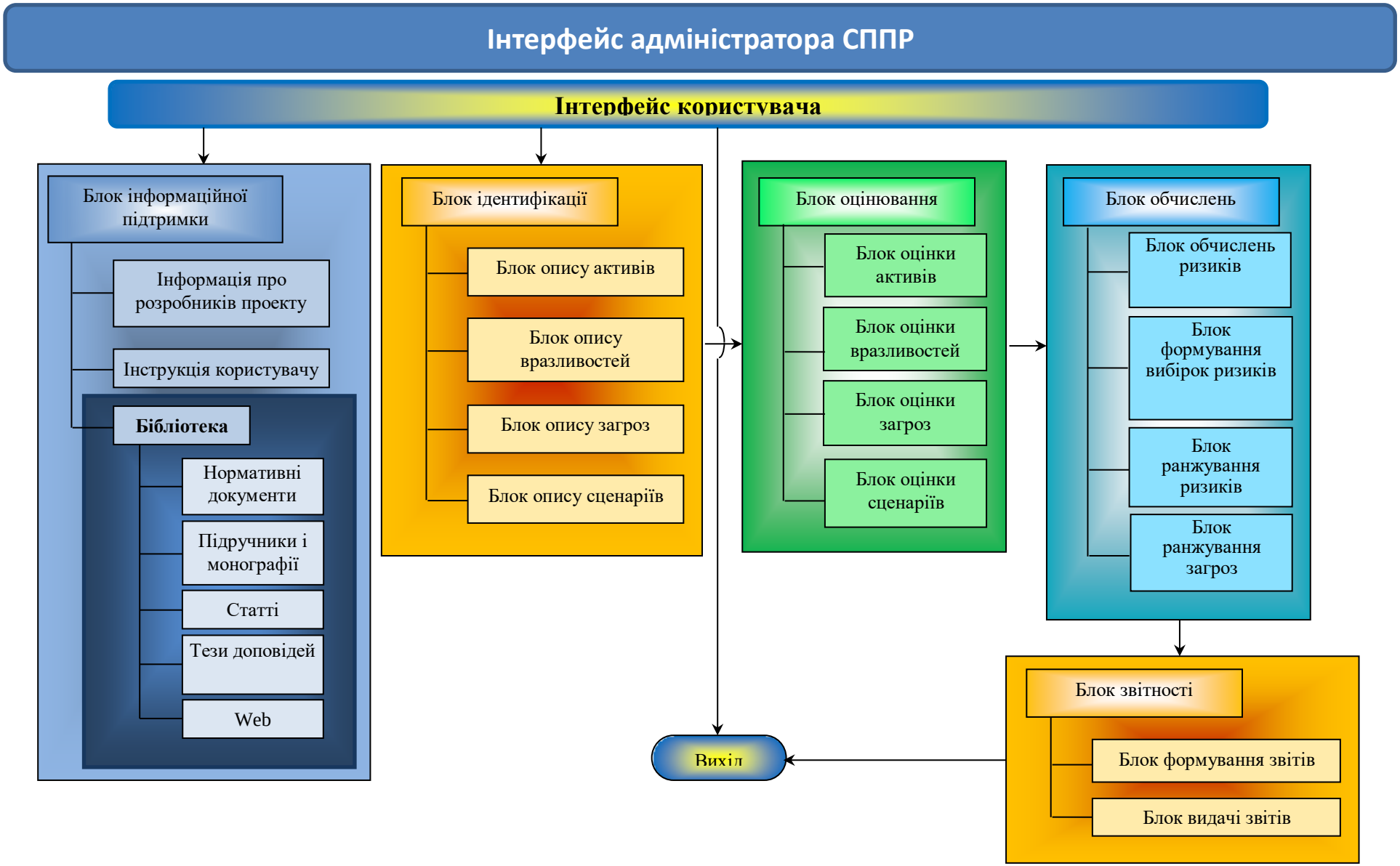

Рисунок 3.4 – Структура СППР ранжування загроз

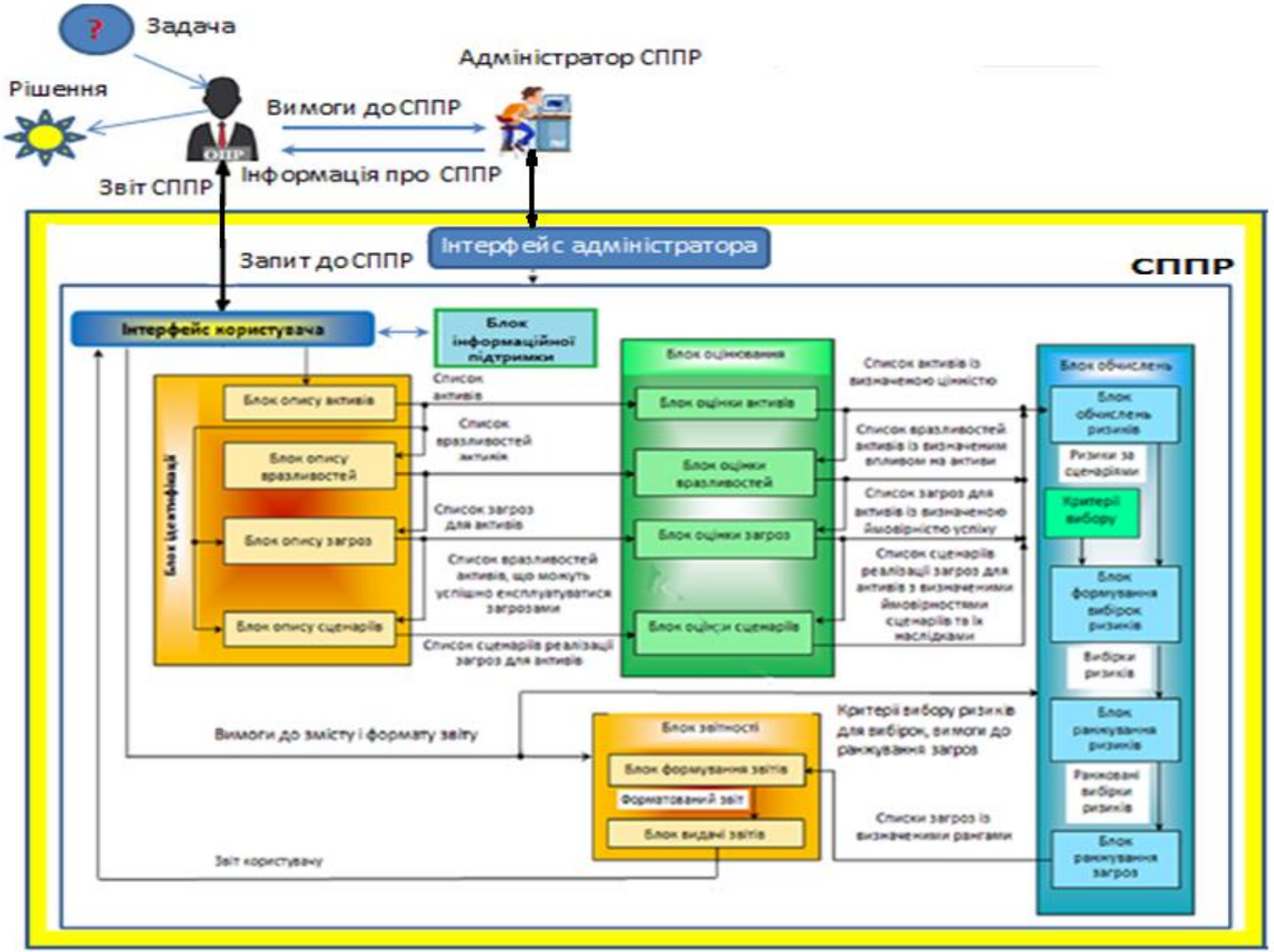

Рисунок 3.5 – Інформаційні потоки в СППР

4 АПРОБАЦІЯ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО РАНЖУВАННЯ ЗАГРОЗ ЗА СТАНДАРТОМ *ISO/IEC* 27005:2022

4.1 Інтерфейс користувача і структура системи підтримки прийняття рішень щодо ранжування загроз за стандартом *ISO/IEC* 27005:2022

Апробація розробленої СППР була здійснена шляхом реалізації основних алгоритмів в MS Access. Розроблений інтерфейс користувача наведено на рис.4.1.

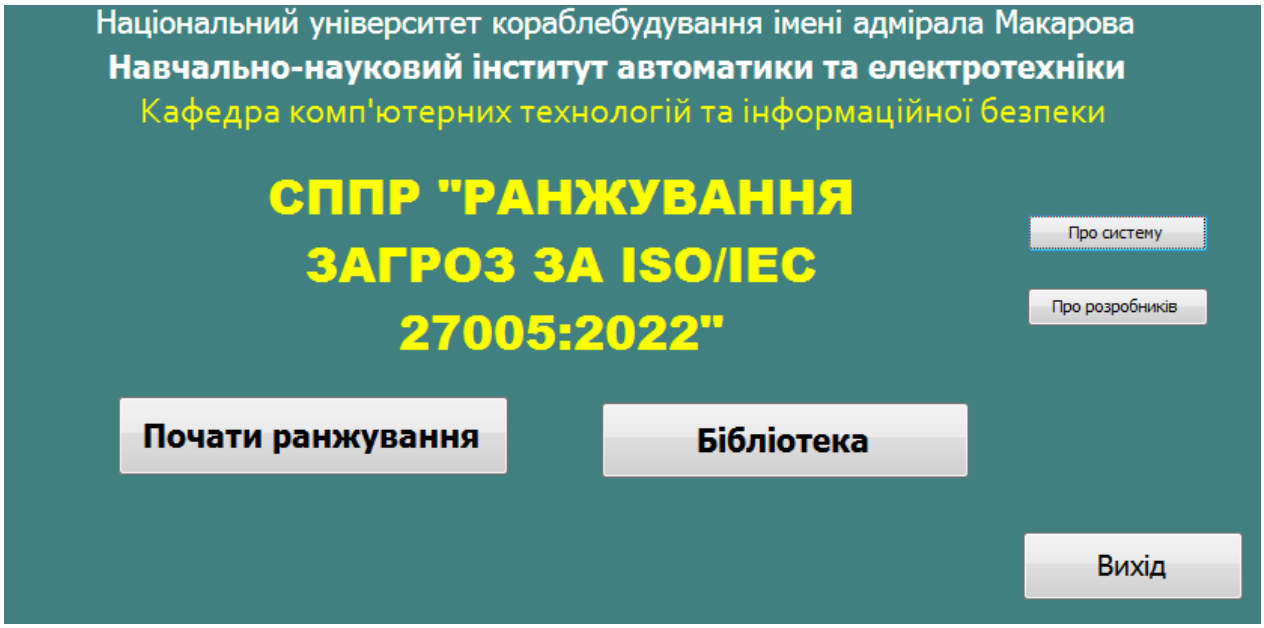

Рисунок 4.1 – Інтерфейс СППР

Для вирішення задач ранжування загроз було створено низку таблиць з урахуванням вимог нормалізації баз даних. Склад таблиць наведено на рис.4.2.

Схема зв’язків, встановлених між таблицями бази даних наведена на рис.4.3. Встановлена системи зв’язків дозволила розробити низку форм, запитів і звітів для введення вхідних даних зручним для користувача способом і виведення результатів ранжування загроз в наочній формі.

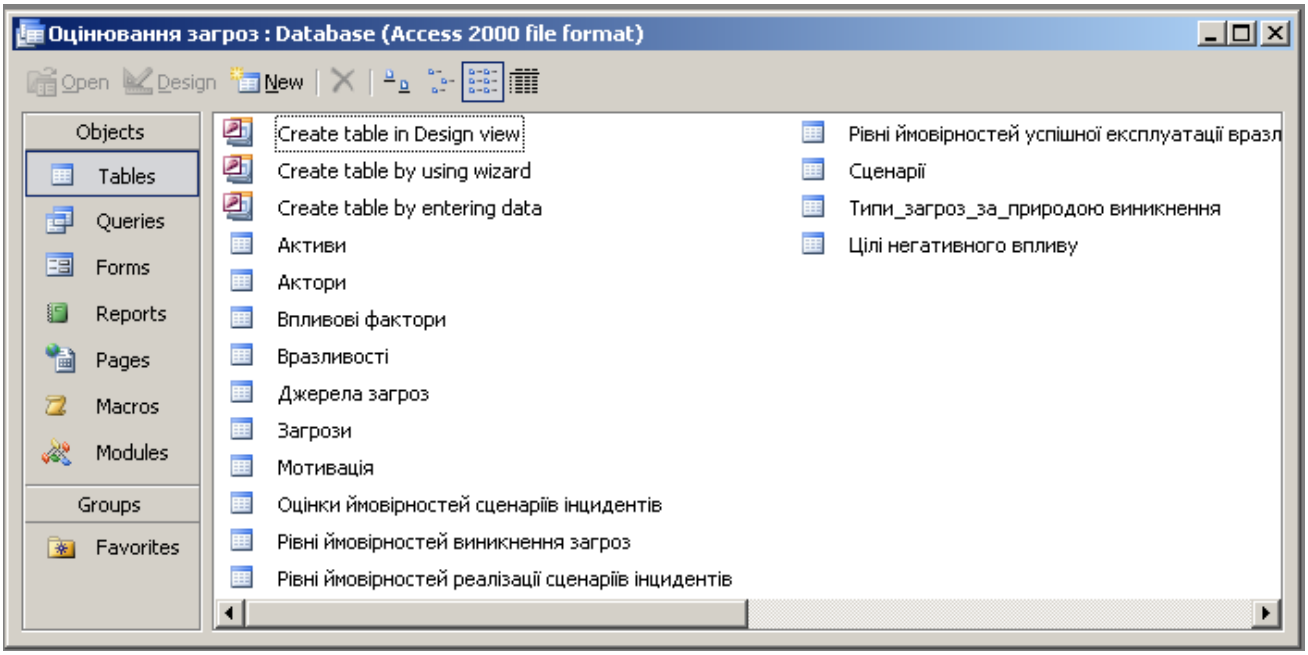

Рисунок 4.2 – Таблиці бази даних СППР

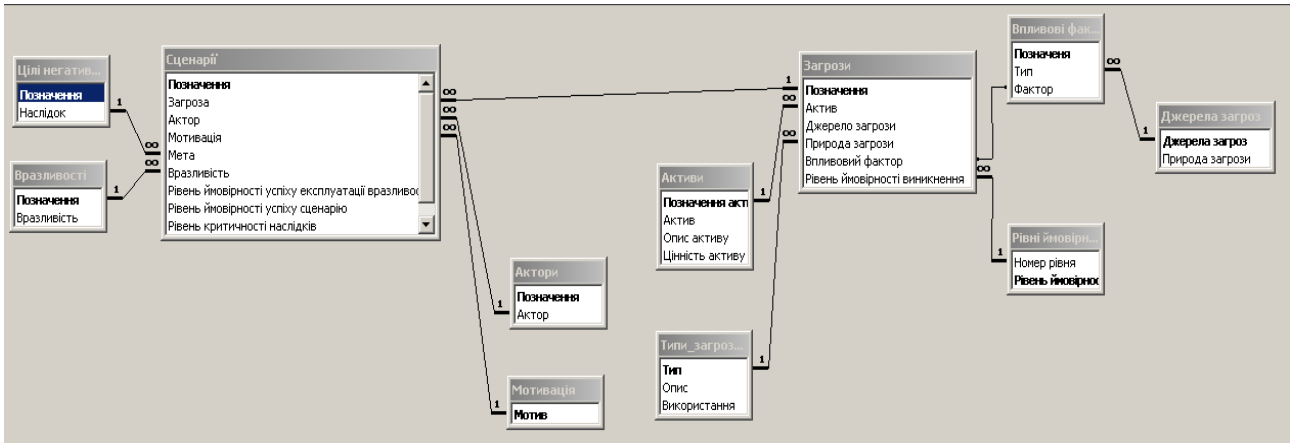

Рисунок 4.3 – Схема зв’язків таблиць бази даних

4.2 Апробація процедур введення в систему підтримки прийняття рішень вхідних даних

Першим етапом ранжування загроз в даній СППР є введення користувачем у відповідних таблицях (або у формах) натупних даних:

– інформація про активи (рис.4.4);
– інформація про акторів (рис.4.5);
– інформація про джерела загроз (рис.4.6);
– інформація про впливові фактори (рис.4.7);
– інформація про мотивацію дій акторів (рис.4.8);
– інформацію про можливі цілі негативного впливу (рис.4.9);
– інформацію про вразливості (рис.4.10).

Рисунок 4.4– Таблиця «Активи» в процесі заповнення

Позначення	Актор
АК1	Хакер
АК10	Інсайдер_зловмисний співробітник
АК11	Випадкові зовнішні впливи
АК12	Випадкові процеси в системі обробки інформації
АК13	Випадкові процеси в системі захисту інформації
АК2	Терорист
АК3	Комп'ютерний злочинець
АК4	Промисловий шпигун_на користь конкуруючої кампанії
АК5	Промисловий шпигун_на користь іноземного уряду
АК6	Промисловий шпигун_на користь інших урядових інтересів
АК7	Інсайдер_звільнений співробітник
АК8	Інсайдер_некваліфікований чи недбалий співробітник
АК9	Інсайдер_невдоволений співробітник
АК14	Природа

Рисунок 4.5 – Таблиця «Актори»

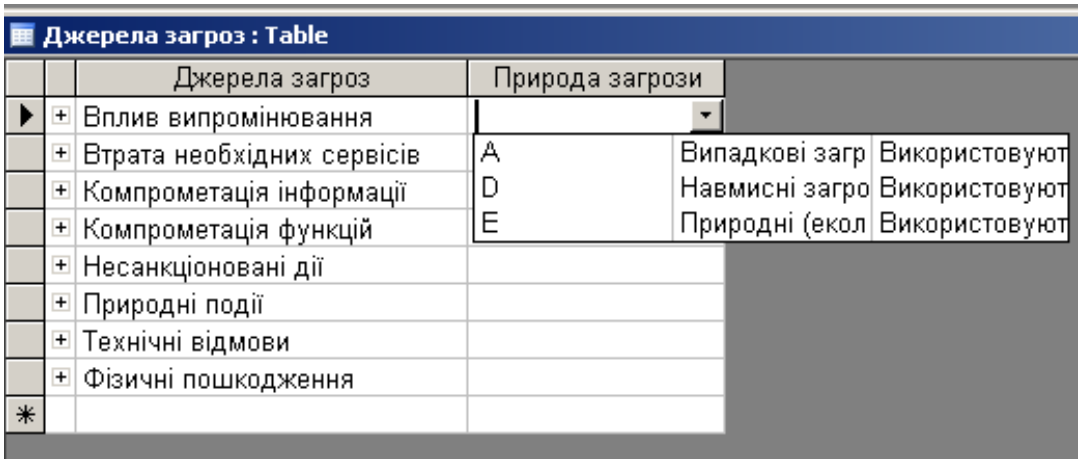

Рисунок 4.6 – Таблиця «Джерела загроз» в процесі заповнення

Позначеня	Тип	Фактор
F1	Фізичні пошкодження	Пошкодження вогнем
F10	Природні події	Сейсмічні явища
F11	Природні події	Вулканічні явища
F12	Природні події	Кліматичні явища
F13	Природні події	Метеорологічні явища
F14	Природні події	Повінь
F15	Втрата необхідних сервісів	Відмова телекомунікаційного обладнання
F16	Втрата необхідних сервісів	Відмова системи кондиціонування
F17	Втрата необхідних сервісів	Відмова системи водопостачання
F18	Втрата необхідних сервісів	Втрата електроживлення
F19	Вплив випромінювання	Негативний вплив теплового випромінювання

Рисунок 4.7 – Фрагмент таблиці «Впливові фактори»

Мотив
Виклик
Грошова вигода
Его
Конкурентні переваги
Ненавмисні помилки
Політичні преференції
Помста
Розвідка
Статус
Цікавість
Відсутня

Рисунок 4.8 – Таблиця «Мотивація»

Позначення	Наслідок
H1	Несанкціонований доступ в систему
H10	Інформаційна війна
H11	Системна атака
H12	Втручання в роботу системи
H13	Крадіжка інформації
H14	Крадіжка персональних даних
H16	Економічна розвідка
H17	Несанкціонований доступ до активів із службовою ІзОД
H18	Несанкціонований доступ до активів із технологічною ІзОД
H19	Соціальна розробка (замах на недоторканність особистого життя)

Рисунок 4.9 – Фрагмент таблиці «Цілі негативного впливу»

Позначення	Вразливість
B1	Недостатня міцність парольного захисту
B2	Недостатня міцність криптографічного захисту
B3	Недостатня міцність антивірусного захисту

Рисунок 4.10 – Таблиця «Вразливості»

Таблиця «Типи загроз за природою виникнення» (рис.4.11) є вбудованою в СППР, відповідає *ISO/IEC* 27005 і може змінюватися тільки адміністратором СППР. Дані, які використовуються для підстановки при формуванні користувачем описів джерела загроз (рис.4.6), впливових факторів, мотивації дій акторів і цілей негативного впливу також відповідають *ISO/IEC* 27005.

Тип	Опис	Використання
A	Випадкові загрози	Використовуються для всіх дій людини, що можуть пошкодити інформаційні активи
D	Навмисні загрози	Використовуються для всіх навмисних акцій, спрямованих на інформаційні активи
E	Природні (екологічні) загрози	Використовуються для всіх впливів зовнішнього середовища, що не пов'язані з діями людини

Рисунок 4.11 – Таблиця «Типи загроз за природою виникнення»

СППР надає користувачу можливість самостійно визначити шкали для оцінювання складових ризику, таких як рівні ймовірностей виникнення загроз (рис.4.12), успіху експлуатації загрозою вразливостей (рис.4.13), розвитку атаки за певним сценарієм (рис.4.14). Для визначення цінності активів (рис.4.4) використовується вбудована шкала).

Номер рівня	Рівень ймовірності загроз
3	Високий
1	Низький
2	Середній

Рисунок 4.12 – Таблиця «Рівні ймовірностей виникнення загроз»

Номер рівня	Рівень ймовірності використання
3	Високий
1	Низький
2	Середній

Рисунок 4.13 – Таблиця «Рівні ймовірностей успіху експлуатації вразливостей»

Номер рівня	Рівень ймовірності реалізації сценарію	Оцінка рівня ймовірності реалізації сценарію
5	Високоймовірний	4
1	Дуже малоймовірний	0
3	Ймовірний	2
2	Малоймовірний	1

Рисунок 4.14 – Таблиця «Рівні ймовірностей сценаріїв інцидентів»

Оцінювання ймовірностей сценаріїв інцидентів здійснюється за таблицею рис.4.15, яка є базою знань і передбачає наявність девяти рівнів ймовірностей сценаріїв інцидентів, які різняться сполученнями рівнів ймовірності виникнення і ймовірності успішної реалізації загрози шляхом експлуатації вразливості.

Оцінки ймовірностей сценаріїв інцидентів : Table

Сценарій інциденту	Ймовірність виникнення загрози	Ймовірність успішної реалізації загрози	Рівень ймовірності сценарію
Сценарій 1	Низький	Низький	Дуже малоймовірний
Сценарій 2	Низький	Середній	Малоймовірний
Сценарій 3	Низький	Високий	Ймовірний
Сценарій 4	Середній	Низький	Малоймовірний
Сценарій 5	Середній	Середній	Ймовірний
Сценарій 6	Середній	Високий	Розповсюджений
Сценарій 7	Високий	Низький	Ймовірний
Сценарій 8	Високий	Середній	Розповсюджений
Сценарій 9	Високий	Високий	Високоймовірний
		Високий	
		Низький	
		Середній	

Рисунок 4.15 – Заповнення таблиці«Оцінки ймовірностей сценаріїв інцидентів»

На наступному етапі користувач формує опис загроз (рис.4.16).

	Позначення	Актив	Природа загрози	Впливовий фактор	Рівень ймовірності виникнення
▶	Z1	База клієнтів	D	Знищення носіїв інформації	Середній
	Z2	База клієнтів	E	Пошкодження вогнем	Низький
	Z3	Планові проєкт	A	Фальсифікація прав	Середній
	Z4	Архів проєктів	D	Зловживання правами	Високий

Рисунок 4.16 – Таблиця «Загрози» в процесі заповнення

Останнім кроком користувача із введення вхідних даних є опис сценаріїв (рис.4.17).

Цілі впливу	Природа загрози	Впливовий фактор	Ймовірність
Крадіжка персональних даних	Навмисні загрози	Зловживання правами	Середній
Крадіжка персональних даних	Навмисні загрози	Несанкціоноване використання	Середній
Руйнування даних	Випадкові загрози	Помилка у використанні	Високий
Несанкціонований доступ до ак	Навмисні загрози	Фальсифікація прав	Високий
Несанкціонований доступ в сис	Навмисні загрози	Несанкціоноване використання	Низький
Руйнування даних	Природні (екологічні	Пошкодження вогнем	Низький

Код сценарію	Актив	Актор	Мотивація	Цілі впливу	Природа загрози	Впливовий фактор	Ймовірність
▶ C1	База клієнтів	Інсайдер_зловмисний співробітник	Помста	Крадіжка персональних даних	Навмисні загрози	Зловживання правами	Середній
C2	База клієнтів	Хакер	Конкурентні переваги	Крадіжка персональних даних	Навмисні загрози	Несанкціоноване використання	Середній
C3	База клієнтів	Інсайдер_некваліфікований чи нед	Ненавмисні помилки	Руйнування даних	Випадкові загрози	Помилка у використанні	Високий
C4	База проєктів	Промисловий шпигун_на користь і	Грошова вигода	Несанкціонований доступ до ак	Навмисні загрози	Фальсифікація прав	Високий
C5	Планові проєк	Інсайдер_звільнений співробітник	Его	Несанкціонований доступ в сис	Навмисні загрози	Несанкціоноване використання	Низький
C6	Архів проєктів	Природа	Відсутня	Руйнування даних	Природні (екологічні	Пошкодження вогнем	Низький
*							

	Код сценарію	Актив	Актор	Мотивація
▶	C1	База клієнтів	Інсайдер_зловмисний співробітник	Помста
	C2	База клієнтів	Хакер	Конкурентні переваги
	C3	База клієнтів	Інсайдер_некваліфікований чи нед	Ненавмисні помилки
	C4	База проєктів	Промисловий шпигун_на користь і	Грошова вигода
	C5	Планові проєк	Інсайдер_звільнений співробітник	Его
	C6	Архів проєктів	Природа	Відсутня
*				

Рисунок 4.17 – Фрагмент таблиці «Сценарії»

На цьому введення даних користувачем завершується, і СППР автоматично приступає до ранжування загроз, перелік яких і параметри яких були задані користувачем.

4.4 Апробація процедур отримання висновків щодо рангів загроз

Шляхом застосування запиту на вибірку із взаємопов'язаних таблиць отримуються параметри, які використовуються для розрахунку ризиків (рис.4.18).

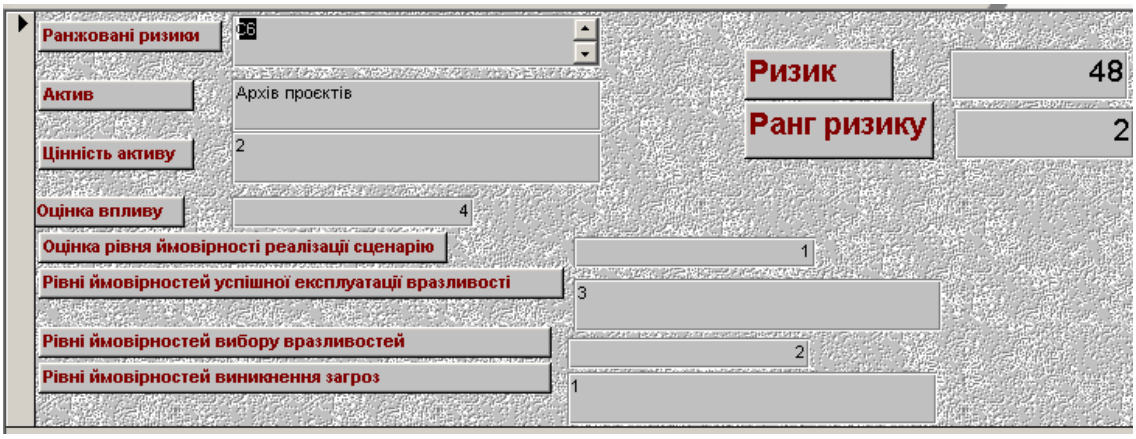

Рисунок 4.18 – Форма із визначеними рангами ризиків

Розраховані ризики потім впорядковуються і розподіляються по категоріям ризиків (рис.4.19), і за категоріями ризиків за формулами (3.1)-(3.3) визначаються категорії загроз.

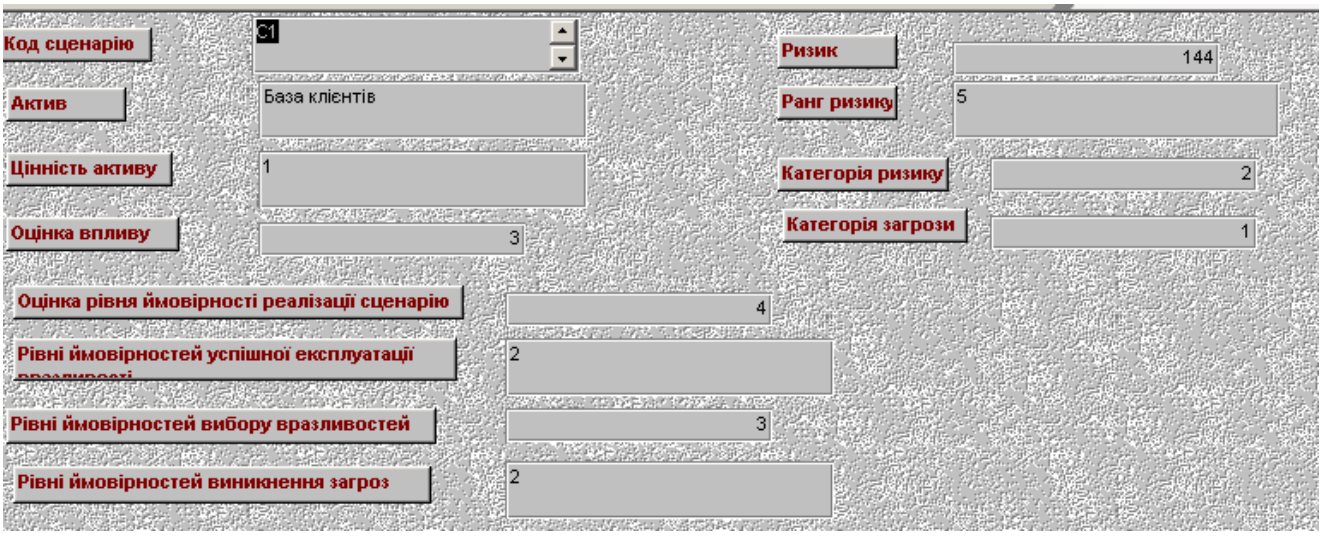

Рисунок 4.19 – Форма із визначеними категоріями ризиків і загроз

Якщо кожна загроза використовує лише одну вразливість, то її ранг співпадає із рангом ризику асоційованого з нею ризику.

Якщо кількість градацій шкали для оцінювання ризиків і загроз однакова, то категорії ризиків і загроз співпадають. В наведеному прикладі було прийнято $NR=4$, $NZ=3$, тому категорії ризиків і загроз різняться (рис.4.19).

ВИСНОВКИ

В ході виконання даної кваліфікаці ної роботи:

- проведено аналіз відкритої нормативно-правової бази;
- визначені принципи та процедури ранжування загроз;
- визначені критерії і правила прийняття рішень щодо рангів загроз;
- розроблені і апробовані основні алгоритми та структура системи підтримки прийняття рішень щодо ранжування загроз за міжнародним стандартом ISO/IEC 27005:2022;
- результати апробації підтвердили працездатність розробки.

Робота має практичну значимість, її результати можуть бути використані при проектуванні та оцінюванні ефективності комплексних систем захисту інформації та в навчальному процесі за освітньою програмою «Системи технічного захисту інформації, автоматизація її обробки» зі спеціальностей 125 «Кібербезпека» та 141 «Електроенергетика, електротехніка та електромеханіка».

Результати даної кваліфікаційної роботи були апробовані на XII Всеукраїнській науково-технічній конференції з міжнародною участю “Сучасні проблеми інформаційної безпеки на транспорті” 2024 р.

ПЕРЕЛІК ПОСИЛАНЬ

1. *Carfora M., Martinelli F. Cyber Risk Management: An Actuarial Point of View* //*Journal of Operational Risk*. - 2021. – *Vol.*4. – №4. – *URL*: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3778061*

2. *ESET Threat Report H2* 2024. *URL*: *https://www.welivesecurity.com /en/eset-research/eset-threat-report-h2-2024/*

3. *ISO/IEC* 27005:2011 *Information technology – Security techniques – Information security risk management. URL*: *https://www.iso.org/standard/ 56742.html*

4. *ISO/IEC* 27005:2022(*en*) *Information security, cybersecurity and privacy protection – Guidance on managing information security risks. URL*: *https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-4:v1:en*

5. Threat Modeling Methodology: OCTAVE. URL: https://www.iriusrisk.com /resources-blog/octave-threat-modeling-methodologies

6. *Top 10 Cybersecurity trends for 2023*. *URL: https://networkinterview.com /cybersecurity-trends/*

7. *Top 10 emerging cyber-security threats for* 2030. *URL*: *https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward*-2030

8. *Vishwajeet Kumar, Unmasking Lumma Stealer: Analyzing Deceptive Tactics with Fake CAPTCHA. URL: https://blog.qualys.com/vulnerabilities-threat-research/2024 /10/20/unmasking-lumma-stealer-analyzing-deceptive-tactics-with-fake-captcha*

9. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. – К.: ДУТ, 2015. — 288 с. *URL*: *http://www.dut.edu.ua/uploads/p_303_79299367.pdf*

10. Бурячок В. Л., Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки. Навчальний посібник.– К.: ДУТ, 2018. – 320 с.. *URL*: *https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok _Posibnik_ 2019_FITU.pdf*

11. Василенко В.С., Бордюк О.С., Полонський С.М. Оцінювання ризиків безпеці інформації в локальних обчислювальних мережах. *URL*: *http://www. rusnauka.com/11_EISN_2010/Informatica/ 64068.doc.htm*

12. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник. – Дніпро: Дніпропетровський держ. ун-т внутріш. справ, 2020. – 144 с. *URL*: *https://er.dduvs.edu.ua/bitstream/123456789/5717/1/%d0%9f%d0%9e%d0%a1I%d0%91%d0%9d%d0%98%d0%9a%20%d0%9e%d0%a3I%d0%91%20.pdf*

13. ДСТУ *ISO/IEC* 27005:2019 (*ISO/IEC* 27005:2018, *IDT*). Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. *URL*: *http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797*

14. ДСТУ *ISO/IEC* 31010:2013. Керування ризиком. Методи загального оцінювання ризику (*ISO/IEC* 31010:2009, *IDT*). *URL*: *https://khoda.gov.ua/ image/catalog/files/dstu%2031010.pdf*

15. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. *URL*: *http://www.dut.edu.ua/ru/lib/60/category/925/ view/*

16. ДСТУ 7731:2015. Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (*ISO/IEC* 29100:2011, *MOD*). *URL*: *https://online.budstandart.com/ ua/catalog /doc-page?id_doc=66872*

17. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. – К. : НІСД, 2014. – 328 с. *URL*: *https://niss.gov.ua/sites/default/ files/ 2015-02/Dubov_mon-89e8e.pdf*

18. Закон України «Про внесення змін до деяких законів України щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі». *URL*: *https://zakon.rada.gov.ua/laws/show/2470-20#n21*

19. Закон України «Про захист персональних даних». *URL*: *https://zakon.rada.gov.ua/laws/show/2163-19#Text*

20. Закон України «Про національну безпеку України». *URL*: *https://zakon.rada.gov.ua/laws/show/2469-19*

21. Закон України «Про основні засади забезпечення кібербезпеки України». *URL*: *https://zakon.rada.gov.ua/laws/show/2163-19*

22. Карпович І., Гладка О., Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки //Технічні науки та технології. – 2021. – №1(23). – С.62–68. *URL*: *http://tst.stu.cn.ua/article/view/233549/232282*

23. Кібероперації РФ: нові цілі, інструменти та групи. Аналітика хакерських атак проти України за 1 півріччя 2024 року. *URL: https://cybersec.net.ua/statti/715-kiberoperatsii-rf-novi-tsili-instrumenty-ta-hrupy-analityka-khakerskykh-atak-proty-ukrainy-za-1-pivrichchia-2024-roku.html*

24. Кіреєнко О. В. Модель порушника з неповною інформацією. *URL*: *https://ela.kpi.ua/bitstream*/123456789/20787/1/2.Кіреєнко.с.125-128.*pdf*

25. Класифікація загроз інформаційній безпеці. Інформаційна безпека особистості. *URL*: *https:// sites.google.com/ site/ infobezosob/ klasifikacia - zagroz-informacijnij-bezpeci*

26. Колтик М.А. Построение модели угроз и нарушителей информации для объекта испытаний с использованием онтологии проведения испытаний КСЗИ // Проблеми програмування. – 2014. – № 4. – С.48-58. *URL*: *http://irbis-nbuv.gov.ua /cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN &IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Progr_2014_4_7.pdf*

27. Конвенція про кіберзлочинність. *URL*: *https://zakon.rada.gov.ua/laws/show/994_575#Text*

28. Корченко А.Г., Архипов А.Е., Казимирчук С.В. Анализ и оценивание рисков информационной безопасности. – К.: ООО «Полиграф-Лазурит», 2013. – 275 с. *URL*: *https://er.nau.edu.ua/bitstream/NAU/40480/1/%d0%9c_22.04.3013_less_ %21.pdf*

29. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія. – Київ: ЦП «Компринт», 2017 – 435 с. *URL*: *https://er.nau.edu.ua/bitstream /NAU/ 40482/1/Monografiya _ukr.pdf*

30. Манжай О.В. Використання кіберпростору в оперативно-розшуковій діяльності // Право і безпека. – 2009. – №4(31). – С.215-219. *URL*: *https://dspace.univd.edu.uaxmlui/bitstream/handle/123456789/7080/Vykorystannia%20kiberprostoru% 20 v% 20 operatyvno-rozshukovii % 20 diialnosti _ Manzhai _ 2009.pdf?sequence=1&isAllowed=y*

31. Мануілов Я.С. Щодо концепції організаційно-технічної моделі кіберзахисту // Інформація і право. – 2021. – №2(37). – С.115-122. *URL*: *http://il.ippi.org.ua/article/view/*238345

32. Моделі загроз безпеці інформації. *URL*: *https://studfile.net/preview/*9649913/

33. Морська економіка і морська безпека мають розвиватися паралельно – інтерв'ю з Юлією Клименко. *URL*: *https://cfts.org.ua/articles/morska_ekonomika _i_morska _bezpeka_mayut_rozvivatisya_paralelno__intervyu_z_yulieyu_klimenko_1990/137899*

34. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. *URL*: *https://tzi.ua/ assets /files/1.1_003_99.pdf*

35. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі *URL*: *http://dstszi.kmu.gov.ua/dstszi/control /uk/publish/ article ?show Hidden=1 &art_id=102122&cat_id=46556& ctime*=13445 02595077

36. НД ТЗІ 2.3-025-24. Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. *URL*: *https://cip.gov.ua/ services/cm/api/ attachment/download?id=66113*

37. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. *URL*: *http://www.dsszzi. gov.ua/dsszzi/doccatalog/document?id*=106342

38. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціоно-ваного доступу.- *URL*: *http://dstszi.kmu.gov.ua/dstszi/control/uk/ publish/article; jsessionid=afd6198c23cb1f96abafd7189bbdce03?showhidden=1&art_id=101870&cat_id =89734&ctime=1344501089407*

39. НД ТЗІ 2.6-004-21. Порядок авторизації безпеки інформаційних систем. *URL*: *https://cip.gov.ua/services/cm/api/attachment/download?id=65411*

40. НД ТЗІ 3.6-004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. *URL*: *https://cip.gov.ua/services/cm/api/attachment/download?id=53375*

41. НД ТЗІ 3.6-005-21. Порядок категоріювання безпеки інформаційної системи та інформації. *URL*: *https://cip.gov.ua/services/cm /api/attachment/ download?id=53376*

42. НД ТЗІ 3.6-006-21. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. *URL*: *https://cip.gov.ua/services/cm/api /attachment /download?id=64620*

43. НД ТЗІ 3.6-007-21. Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. *URL*: *https://cip.gov.ua/services/cm /api/ attachment/download?id=53387*

44. НД ТЗІ 3.6-008-21. Порядок моніторингу безпеки інформаційних систем. *URL*: *https://cip.gov.ua/services/cm/api/attachment /download?id=53390*

45. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. *URL*: *http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?showHidden =1&art_id= 102232 &cat_id=46556&ctime=1344503967308*

46. План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України, затверджений Розпорядженням Кабінету міністрів України № 1163-р.від 19 грудня 2023 року. *URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text*

47. План реалізації Стратегії кібербезпеки України. *URL*: *https://zakon.rada.gov.ua/laws/show/n0087525-21#Text*

48. Положення про організаційно-технічну модель кіберзахисту. *URL*: *https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text*

49. Поради (рекомендації) щодо створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет. *URL*: *https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet*

50. Работа №1. Анализ модели угроз ИБ и уязвимостей. *URL: https://studfile.net/preview/3245995/*

51. Ротштейн А. Ранжирование элементов системы на основе нечеткого отношения влияния и транзитивного замыкания // Кибернетика и системный аналіз. – 2017. – Том 53. – №1. – С. 68-78, *URL*: *http://dspace.nbuv. gov.ua/bitstream /handle/123456789/144685/06-Rotshtein.pdf?sequence=1*

52. Салієва О.В. Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (12 «Інформаційні технології»). – Вінницький національний технічний університет, Вінниця, МОН України. – Національний університет «Львівська політехніка», МОН України, Львів, 2021. – 208 с. *URL*: *https://lpnu.ua/sites/default/files/2021/radaphd/12288/dissaliievao.pdf*

53. Салієва О.В., Яремчук Ю.Є. Ранжування загроз для визначення витрат на забезпечення захищеності системи захисту інформації на основі теорії нечітких відношень // Захист інформації. – 2020. – Том 22. – №1. – С.51-59. *URL*: *https://jrnl.nau.edu.ua/index.php/ZI/article/view/14664*

54. Салієва О.В., Яремчук Ю.Є. Визначення допустимої інтенсивності зниження рівня захищеності об’єкта критичної інфраструктури ранжуванням загроз //Реєстрація, зберігання і обробка даних. – 2020. – Т. 22. – № 2. – С.63-76. *URL*: *http://drsp.ipri.kiev.ua/article/view/211279*

55. Собакарь А. О. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки України. // Матеріали VI Міжнародної науково-практичної конференції «Російсько-українська війна: право, безпека, світ». Тези наукових доповідей. – Тернопіль: Західноукраїнський національний університет, 2022. – С.264-267. *URL*: *http://confuf.wunu.edu.ua/index.php /confuf/article/view/951*

56. 4Стратегія забезпечення державної безпеки. *URL*: *https://zakon.rada.gov.ua/laws/show/56/2022?find=1&text=%D0%BA%D1%96%D0%B1%D0%B5%D1%80#w1_9*

57. Стратегія кібербезпеки України. Безпечний кіберпростір- запорука безпечного розвитку країни. *URL*: *https://zakon.rada.gov.ua/laws/show /447/2021#n7*

58. Стратегія національної безпеки України. *URL*: *https://zakon.rada.gov.ua/laws/show/392/2020#n12*

59. Турти М.В., Доценко В.В. Інформаційна модель ранжування загроз за BS ISO/IEC 27005:2011 //Матеріали X Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».–Миколаїв: НУК, 2022. – С.134-140.

60. Чунарьова А.В., Чунарьов А.В. Принципи організації захисту інформації в сучасних інформаційно-комунікаційних системах і мережах. *URL*: *http://www.rusnauka.com/16_ADEN_2010/Informatica/68642.doc.htm*

61. Шандрівська О. Є., Шинкаренко Н. В. Прикладна оцінка ризиків у системі забезпечення безпеки соціально-економічних процесів у кіберпросторі //Вісник Національного університету “Львівська політехніка”. Серія “Проблеми економіки та управління”. – 2020. – №2(8). – С.94-104.

62. Шапорин В. О., Копытчук Н. Б., Тишин П. М., Шапорин Р. О. Разработка нечетких лингвистических моделей сетевых атак для анализа рисков в распределенных информационных системах // Труди XV Міжнародної науково-практичної конференції (CIET-2014) «Сучасні інформаційні та електронні технології». Одеса, Україна 29—31 травня 2014 р. – Одеса: *ART-V,* 2014. – С.131-132. *URL: http://www.tkea.com.ua/siet/archive/2014-t1/131.pdf*

63. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія. – К.: НАУ, 2015. – 214 с. *URL*: *https://er.nau.edu.ua/bitstream/NAU/31911/1/Monogr_klas_zagroz_Yudin_Buchyk.pdf*