НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ
ІМ. Г.Є. ПУХОВА

КОРОБЕЙНІКОВ ФЕДІР ОЛЕКСАНДРОВИЧ

УДК 004.056

МЕТОДИ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ СИСТЕМ

Спеціальність 05.13.21 – «Системи захисту інформації»

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2024

Дисертацією є рукопис.
Робота виконана в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ.

Науковий керівник чл.-кор. НАН України
доктор технічних наук, професор,
Мохор Володимир Володимирович,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України,
директор інституту

Офіційні опоненти: доктор технічних наук, професор
Лахно Валерій Анатолійович,
Національний університет біоресурсів та природокористування України,
кафедра комп'ютерних систем, мереж та кібербезпеки, професор кафедри

доктор технічних наук, професор,
Корченко Анна Олександрівна,
Національний технічний університет «Дніпровська політехніка»,
кафедра безпеки інформації та телекомунікацій,
професор кафедри.

Захист відбудеться "27" листопада 2024 року о 14 годині на засіданні спеціалізованої вченої ради Д 26.185.01 Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, г. Київ, вул. Генерала Наумова, 15.

З дисертацією можна ознайомитися в бібліотеці Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, г. Київ, вул. Генерала Наумова, 15.

Автореферат розісланий "____" жовтня 2024 р.

Вчений секретар
спеціалізованої вченої ради Душеба В.В.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Глобалізація дестабілізуючих факторів, таких як соціально-економічні кризи, пандемії, екологічні катастрофи і зростання впливу авторитарних режимів на світову адженду, актуалізує завдання переосмислення та адаптації стратегій, спрямованих на забезпечення гарантоспроможності систем обробки і захисту інформації, критичних для функціонування організацій. Пов’язаний з цим поступовий перехід від парадигми захисту до парадигми резильєнтності, знаходить відображення у відповідних постановах ООН та нормативних документах Ради ЄС, які визначають нові пріоритети в забезпеченні безпеки широкого класу організацій та спільнот. Наприклад, відповідно до директив та рекомендацій Ради ЄС, зокрема, Директиви 2022/2557 від 14 грудня 2022 року щодо резильєнтності критично важливих об’єктів, та Директиви 2022/2555 від 14 грудня 2022 року - про заходи для забезпечення високого спільного рівня кібербезпеки в ЄС, а також згідно Рекомендацій 2023/С 20/01 щодо загальноєвропейського скоординованого підходу до посилення резильєнтності критичної інфраструктури від 8 грудня 2022 року, напрямок підвищення резильєнтності національної та загальноєвропейської критичної інфраструктури визначено одним із пріоритетів безпекової політики ЄС. Тенденція переходу від концепції захисту до резильєнтності в ЄС також переконливо підтверджується ще й тим, що директива 2022/2557 скасовує попередню Директиву 008/114/ЄС від 8 грудня 2008 року про ідентифікацію та визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту, у зв'язку з тим, що через дедалі більш взаємопов'язаний та транскордонний характер операцій з використанням критично важливої інфраструктури, захисних заходів, що стосуються лише окремих активів, виявляється недостатньо.

Сутнісна трансформація парадигмального базису побудови систем обробки та захисту інформації зумовлює потребу в розробці методологічного підґрунтя, що забезпечуватиме ефективну імплементацію нововведених концептів резильєнтності на всіх рівнях їхньої застосовності. В той час, як методики забезпечення резильєнтності на рівні окремих інформаційних систем детально описані в існуючих фреймворках, зокрема у NIST Special Publication (SP) 800-160 Volume 2 або MITRE Cyber Resiliency Engineering Framework (CREF), наразі відсутні методики або настанови з підвищення резильєнтності на організаційно-технічному рівні, тобто, на рівні організацій, місій, на національному та наднаціональному рівнях, які були б загальновизнаними науковою і апробовані професійною спільнотою. Наявний стандарт ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes (і відповідний ДСТУ ISO 22316:2022 «Безпека та адаптивність. Адаптивність організації. Принципи та ознаки») надає лише загальні рекомендації щодо зміцнення організаційної резильєнтності, не заглиблюючись у конкретні методики або практичні аспекти реалізації систем обробки і захисту інформації. Окрім того, існуючі фреймворки з резильєнтності, навіть на рівні інформаційно-технічних систем, не містять чітко визначених способів взаємодії з наявними системами управління інформаційною

безпекою (СУІБ), створеними у відповідності до міжнародних стандартів ISO/NIST та механізмів інтеграції з комплексними системами захисту інформації (КСЗІ), що відповідають Закону України «Про захист інформації в інформаційно-телекомунікаційних системах». Таким чином, на сучасному етапі розвитку науки і техніки існує *об'єктивне протиріччя*, яке полягає з одного боку у наявності факторів, які обумовлюють необхідність впровадження заходів з забезпечення резильєнтності організаційно-технічних систем, та з іншого боку - відсутністю методів і методик впровадження, що враховують специфіку цілей, задач і способів забезпечення резильєнтності таких систем, та інтегрують концепції резильєнтності в наявні СУІБ/КСЗІ.

З огляду на викладене вище, тема дослідження, присвячена вирішенню важливого *науково-прикладного завдання* розробки методів забезпечення резильєнтності організаційно-технічних систем усіх рівнів ієрархії, та інтеграції цих методів в СУІБ (КСЗІ) задля їхнього вдосконалення, *є актуальною*.

Дослідженню проблем, пов'язаних із процесом забезпечення резильєнтності організаційно-технічних систем, що являють собою об'єкт дисертаційного дослідження, присвячується значна частина публікацій вітчизняних і зарубіжних вчених, таких як: Holling, C. S., Walker, B., Hollnagel E., Woods D.D., Linkov I., Prigogine I., Bodeau D., Бурячок В., Богданов О., Горбенко І., Гнатюк С., Гончар С., Грищук Р., Додонов О., Зубок В., Кобозєва А., Корченко О., Лахно В., Лужецький В., Новіков О., Потій О., Харченко В., Хорошко В., Яремчук Ю. та інші. Однак, незважаючи на значну кількість підходів до вирішення даного завдання, воно залишається актуальним не тільки для України, але і для всієї світової спільноти.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження проведено протягом 2015−2024 рр. Тематика дисертаційної роботи та отримані результати безпосередньо пов'язані з Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р., Законом України «Про електронні комунікації» від 16.12.2020 р., Законом України «Про критичну інфраструктуру» від 16.11.2021 р., Законом України «Про захист персональних даних» від 01.06.2010 р., Постановою Кабінету Міністрів України від 19.06.2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», Постановою Кабінету Міністрів України від 09.10.2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури», Постановою Кабінету Міністрів України від 16.05.2023 р. № 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», НДР Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за темою: «Розроблення науково-обґрунтованих критеріїв та принципів побудови системи кіберзахисту об'єктів атомної енергетики» (шифр "АТОМ", державний реєстраційний номер 0123U100909).

Мета та задачі дослідження. Метою дисертаційного дослідження є вдосконалення КСЗІ (СУІБ) шляхом розробки та інтеграції в них методів забезпечення резильєнтності організаційно-технічних систем.

Для досягнення цієї мети в даній роботі необхідно було розв'язати такі основні задачі:

- провести аналіз існуючих підходів та методів забезпечення резильєнтності організаційно-технічних систем, визначити їх обмеження, дослідивши цілі, задачі і передумови виникнення парадигми резильєнтності та фактори, які зумовили її розвиток у безпековому домені;
- розробити метод формування множин критичних ризиків та упорядкування елементів цих множин в контексті забезпечення резильєнтності;
- розробити онтологію, яка б об'єднувала високорівневі конструкти резильєнтності з елементами організаційної інфраструктури;
- запропонувати модель оцінювання ризиків, здатну агрегувати різні типи ризиків організаційно-технічних систем, поєднавши ризики безпеки і резильєнтності в одній стратегії управління ризиками СУІБ/КСЗІ;
- розвинути метод хаос-інжинірингу в якості ітеративного інструменту забезпечення резильєнтності організаційно-технічних систем;
- розробити метод високорівневого оцінювання стану резильєнтності організаційно-технічних систем;
- розробити програмний застосунок, за допомогою якого здійснюється аналіз і оцінювання критичних ризиків в процесі забезпечення резильєнтності організаційно-технічних систем;
- підтвердити коректність отриманих результатів дослідження на прикладі реорганізації критичного сегменту інфраструктури та СУІБ/КСЗІ реально діючої організаційно-технічної системи.

Об’єктом дослідження є системи захисту інформації (системи управління інформаційною безпекою) організаційно-технічних систем.

Предметом дослідження є методи забезпечення резильєнтності організаційно-технічних систем.

Методи дослідження. Проведені дослідження базуються на методологічній основі парадигми резильєнтності та теорії ризиків, системному аналізі сучасних фреймворків побудови резильєнтних систем, методі експертних оцінок. В роботі також були використані елементи теорії хаосу, теорії катастроф і теорії самоорганізації систем. Як засоби розв’язування поставлених задач використовувалось математичне та комп’ютерне моделювання.

Наукова новизна отриманих результатів полягає в тому, що:

- вперше описані обмеження існуючих методів і підходів, покладених в основу наявних фреймворків резильєнтності, які унеможливлюють їхню інтеграцію в СУІБ/КСЗІ та застосовність до організаційно-технічних систем;
- розроблено метод виокремлення критичних ризиків в контексті резильєнтності та їхньої пріоритизації шляхом ранжування у порядку зменшення очікуваної корисності, який надає можливість планувати витрати на оброблення ризиків в межах фіксованого бюджетарного обмеження;
- вперше розроблено онтологію забезпечення резильєнтності організаційно-технічних систем, яка містить високорівневі конструкти резильєнтності та їхню взаємодію з сутностями організаційно-технічної системи, що дозволяє

формалізувати їхнє застосування при проектуванні СУІБ/КСЗІ організаційно-технічних систем;

- вперше запропоновано модель оцінювання ризиків, яка дозволяє агрегувати усі типи ризиків організаційно-технічної системи в рамках єдиної стратегії управління ризиками СУІБ/КСЗІ та конкретизує ризик-апетит організації;

- отримав подальший розвиток метод хаос-інжинірингу стосовно його застосування для забезпечення резильєнтності організаційно-технічних систем шляхом збільшення їхнього адаптаційного потенціалу;

- вперше розроблено метод високорівневого оцінювання стану резильєнтності організаційно-технічних систем, що ґрунтується на лонгітюдному підході і дає можливість вимірювати не тільки власне стан резильєнтності, але й оцінювати ефективність фінансових інвестицій в безпеку і резильєнтність та операційні результати цих інвестицій.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати є корисними для забезпечення резильєнтності, як ключового елементу загальної трастоспроможності організаційно-технічних систем, шляхом опрацювання критичних ризиків та інтеграції відновлювальних і адаптаційних механізмів у критичні процеси при проектуванні, побудові, або вдосконаленні систем обробки інформації, систем управління інформаційною безпекою та систем захисту інформації.

Практична цінність роботи полягає у наступному:

- запропоновано візуальний інструмент оцінювання ризиків – тривимірну матрицю (де кожен ризик організаційно-технічної системи представлений як точка в тривимірному просторі, координати якої задаються ймовірністю реалізації ризику, потенційним збитком, обсягом необхідних ресурсів для його опрацювання), здатну відображати упорядковану множину усіх ризиків організації, включно з резильєнтними, що надає можливість краще розуміти та оцінити різноманітні ризики, а також пріоритезувати їх для подальшого аналізу та реагування;

- запропоновано метрику – індекс резильєнтності (*Resilience index*) організаційно-технічних систем, яка надає можливість оцінити ступінь їхньої резильєнтності враховуючи ефективність фінансових інвестицій в безпеку і резильєнтність, а також і операційні результати таких інвестицій;

- запропоновано програмний застосунок, який надає можливість аналізувати і оцінювати критичні ризики організаційно-технічних систем в контексті резильєнтності, а також відстежувати ключові показники ризику, оновлювати оцінки ризиків та здійснювати моніторинг ефективності планів реагування на ризики;

- на основі одержаних результатів реорганізовано критичний сегмент інфраструктури та вдосконалено СУІБ/КСЗІ реально існуючої організаційно-технічної системи, що забезпечило її резильєнтність на досліджуваному часовому періоді.

Результати дисертаційної роботи впроваджено у діяльність Адміністрації Державної служби спеціального зв’язку та захисту інформації України, Центру

протидії кіберзагрозам, АТ «System Capital Management» та Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України при виконанні НДР «Розроблення науково-обґрунтованих критеріїв та принципів побудови системи кіберзахисту об'єктів атомної енергетики» (шифр "АТОМ", державний реєстраційний номер 0123U100909).

Особистий внесок здобувача. Усі представлені та винесені на захист наукові та науково-технічні результати отримано автором самостійно. У працях, опублікованих у співавторстві, здобувачеві належать: [2] – аналіз резильєнтної поведінки відкритих нелінійних дисипативних систем; [7] – аналіз та дослідження високорівневих конструктів резильєнтності та лонгітюдних метрик вимірювання ефективності підвищення резильєнтних характеристик критичних процесів; [8] – дослідження компонентів трастоспроможності, способів їхньої імплементації у комплексні системи захисту інформації. [10] – дослідження цілей резильєнтності і методів її оцінювання на організаційному рівні. З робіт, опублікованих у співавторстві, для вирішення проблеми та задач, поставлених у дисертаційному досліджені, використовуються результати, отримані особисто здобувачем наукового ступеня.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідались і обговорювались на наукових конференціях, серед яких: науково-практичний семінар-практикум «Менеджмент інформаційної безпеки» (2015-2018 р.); науково-практична конференція «Кібербезпека енергетики» (2018-2023 р.); всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2023, Київ, 2023р.); міжнародна науково-практична конференція «Survivability & Resilience» (Київ, 2023 р.); науково-практична конференція «Резильєнтність критичної інфраструктури – 2023» (Київ, 2023 р.); науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (Київ, 2015-2024); 13th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2023 (2023, Athens, Greece); IX International Scientific and Practical Conference «Theoretical and practical aspects of the development of science» (Prague, Czech Republic. 2024), X International Scientific and Practical Conference «Problems and prospects of modern science (Stockholm, Sweden, 2024).

Публікації. Основні положення дисертаційного дослідження опубліковано у 21-й науковій праці, у тому числі: 1 стаття у періодичному науковому виданні держави, яка входять до країн ЄС [1], 8 наукових статей у вітчизняних фахових наукових журналах категорії «Б», що рекомендовані МОН України [2-9], 10 матеріалів та тез доповідей конференцій [10-19], з яких 1 наукова публікація індексується реферативною базою даних Scopus [10], 2 свідоцтва про реєстрацію авторського права на науковий твір і комп'ютерну програму [20-21].

Структура та обсяг роботи. Дисертаційна робота складається з анотації, вступу, змісту, чотирьох розділів, висновків, 3 додатків, списку використаних джерел, та містить 166 сторінок основного тексту, 19 рисунків. Список використаних джерел налічує 142 найменувань на 14 сторінках. Загальний обсяг дисертаційної роботи складає 218 сторінок.

ОСНОВНА ЧАСТИНА

У анотації та вступі представлена загальна характеристика дисертації, обґрунтовано актуальність обраної теми дослідження, сформульовано мету і задачі дослідження, визначено наукову новизну отриманих результатів та їхнє практичне значення, наведено інформацію про впровадження результатів, їхню апробацію та публікації, структуру, об'єм та ключові слова.

У першому розділі проведено аналіз наукової літератури за темою дисертаційної роботи. Досліджено передумови, що ініціювали зародження парадигми резильєнтності, її подальший розвиток у домені безпеки та зумовили інтеграцію в СУІБ та КСЗІ організаційно-технічних систем. Проведено вивчення чинників нестабільності відкритих нелінійних дисипативних систем, їхня здатність до адаптації та самоорганізації розглянута як підґрунтя виникнення парадигми резильєнтності. Акцентовано, що факторами, які зумовили розвиток парадигми в домені безпеки, виступають необхідність гарантування ефективного функціонування критичних процесів систем, місій та організацій в умовах невизначеності. Висвітлено розуміння зв'язку резильєнтності з непередбачуваними ризиками, які виникають внаслідок перманентного зростання складності інформаційних систем взагалі та організаційно-технічних систем зокрема.

В дисертації досліджено спроби поєднання резильєнтності і безпеки в рамках єдиної концепції трастоспроможності, де пріоритетність їхньої значущості виділена з-поміж інших компонентів, які визначають довіру до інформаційних систем і організацій. Проведений аналіз показав, що хоча у науковій літературі досить детально аналізуються методи підвищення резильєнтності на рівні технічних систем, вони не дають можливості ефективно вирішувати задачі, пов'язані із забезпеченням резильєнтності на рівні організаційно-технічних систем та більш високих рівнях ієрархії з подальшою інтеграцією в СУІБ (КСЗІ) таких систем.

ХАРАКТЕРИСТИКИ	ФРЕЙМВОРКИ ТА СТАНДАРТИ						
	NIST	ISO	MITRE	UK Gov.	ICOR's	DHS	Розроблюваний
ЗАСТОСОВАНІСТЬ НА РІВНІ ТЕХНІЧНИХ СИСТЕМ	+	+	+	-	-	+	+
ЗАСТОСОВНІСТЬ НА ВСІХ РІВНЯХ ОРГАНІЗАЦІЙНОЇ ІЄРАРХІЇ	-	-	-	-	-	-	+
УПРАВЛІННЯ СТОХАСТИЧНИМИ І СПОРАДИЧНИМИ РИЗИКАМИ	-	-	-	-	-	-	+
НАЯВНІСТЬ ІТЕРАТИВНИХ СПОСОБІВ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ	-	-	+	-	-	-	+
НАЯВНІСТЬ МЕТРИК ОЦІНЮВАННЯ РЕЗИЛЬЄНТНОСТІ	+	+	+	-	-	+	+
ВРАХУВАННЯ БЮДЖЕТАРНИХ ОБМЕЖЕНЬ НА ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ	-	-	-	-	-	-	+
ІНТЕГРАЦІЯ З НАЯВНИМИ СУІБ/КСЗІ	+	+	-	-	-	-	+

Рисунок 1 – Порівняння характеристик фреймворків резильєнтності

Для проаналізованих методів, що зумовили характеристики наявних фреймворків резильєнтності, встановлено характерні обмеження (рис. 1), які

унеможливлюють їхнє застосування на рівні організаційно-технічних систем з інтеграцією в СУІБ та КСЗІ таких систем, на підставі чого визначено відповідні характеристики розроблюваних рішень.

Таким чином, у першому розділі, на основі проведеного аналізу сформульовано та обґрунтовано основні задачі дослідження, розв'язання яких необхідне для досягнення мети, що поставлена в дисертаційній роботі.

У другому розділі визначено, що ключовим чинником, який визначає резильєнтність системи, виступає її здатність до безперервної адаптації, концептуалізована як адаптаційний потенціал (адаптаційний ресурс[1]), що дає змогу системі не тільки уникати деструкції у разі критичних інцидентів, а й еволюціонувати завдяки їм. Критичний інцидент – подія, яка своїм впливом здатна викликати деструкцію системи, порушивши функціонування одного або декількох критичних процесів, безпосередньо пов'язаних з її інваріантами.

Відомою є узагальнена періодизація реакції систем на події впливу критичних інцидентів[2]. Якщо вважати, що будь-який критичний інцидент спричиняє свій вплив протягом певного інтервалу часу, тоді незалежно від конкретного типу систем та виду критичних інцидентів узагальнена реакція систем досить суворо поділяється на п'ять характерних періодів (стадій), однакових для будь-якої системи. Це такі стадії: 1) готовність системи, 2) перебування системи під дією критичного інциденту, 3) абсорбція факторів впливу критичного інциденту, 4) відновлення системи, 5) адаптації системи. Таку відому періодизацію можемо розглядати окремо для кожного типу систем і кожного типу критичних інцидентів. Тоді в таку періодизацію для кожної, окремо визначеної системи, можемо додатково ввести конкретні моменти часу початку та завершення кожної зі стадій реакції системи на подію впливу критичного інциденту окремо визначеного типу. А саме, T_S^0 – момент часу входу системи в стадію перебування системи в стані початкової готовності, T_F^0 – момент часу завершення стадії перебування системи в стані початкової готовності, T_S^δ – момент часу початку стадії впливу події критичного інциденту визначеного типу; T_F^δ – момент часу завершення стадії впливу події критичного інциденту визначеного типу; T_S^w – момент часу початку стадії абсорбції системою факторів впливу критичного інциденту; T_F^w - момент часу завершення стадії абсорбції системою факторів впливу критичного інциденту; T_S^B – момент часу початку стадії відновлення системою свого функціоналу; T_F^B – момент часу завершення стадії відновлення системою свого функціоналу; T_S^A – момент часу початку стадії адаптації системи до повторення події впливу критичного інциденту певного типу, T_F^A – момент часу завершення стадії адаптації системи до повторення події впливу критичного інциденту певного типу, T_s^∞ – момент часу входу системи в стадію перебування системи в стані кінцевої готовності.

Можемо визначити, що еволюція окремої системи під дією послідовності подій впливу критичних інцидентів певного типу, приймає характер циклічного

[1] https://doi.org/10.1016/j.plrev.2021.03.001

[2] https://www.osce.org/files/f/documents/a/d/242651.pdf

процесу. Кожна *j*-та ітерація цього циклічного процесу повторює п’ять стадій, зазначених вище. Без втрати загальності подальших міркувань, будемо припускати, що тривалість кожної зі стадій зазначеного циклічного процесу не залежить від номеру ітерації в циклічному процесі еволюції системи, а значення елементів в кортежі значущих моментів часу (1) є незмінними протягом всього процесу еволюції системи.

$$T_S^0,\ T_F^0,\ T_S^\delta\ \ T_F^\delta,\ \ T_S^w,\ \ T_F^w,\ T_S^B,\ T_F^B,\ T_S^A,\ \ T_F^A,\ T_s^\infty. \qquad (1)$$

Час t на кожній j-тій ітерації процесу еволюції системи змінюється в інтервалі ($t \in [0, T_s^\infty]$). Рівень адаптаційного потенціалу системи на кожній *j*-ій ітерації циклу еволюції системи будемо позначати $P_j(t)$. Будемо вважати, що в середині кожної з ітерації кожен момент часу завершення попередньої стадії цієї ітерації співпадає з моментом часу початку наступної стадії цієї ітерації, тобто умовні переключення між стадіями процесу еволюції в межах однієї ітерації відбуваються миттєво. Тоді можемо записати, що

$$T_F^0 = T_S^\delta;\ \ T_F^\delta = T_S^w;\ \ T_F^w = T_S^B;\ \ T_F^B = T_S^A,\ \ T_F^A = T_s^\infty.$$

Підставляючи ці значення в кортеж (1) приведемо його до наступного вигляду

$$T_S^0,\ \ T_S^\delta,\ \ T_S^\delta, T_S^w,\ \ T_S^w,\ \ T_S^B, T_S^B, T_S^A, T_S^A,\ \ T_S^\infty, T_s^\infty. \qquad (2)$$

Однакові елементи цього кортежу, що розташовані в парі один поряд з одним, змістовно означають один і той же момент часу. Тож кортеж (2) можемо спростити, шляхом видалення в кожній з таких пар по одному елементу, і привести цей кортеж до такого вигляду:

$$T_S^0,\ \ T_S^\delta,\ T_S^w,\ T_S^B, T_S^A, T_s^\infty. \qquad (3)$$

Оскільки всі елементи цього кортежу розрізняються лише верхніми індексами, остільки для спрощення подальших міркувань і викладок позбавимося однакових нижніх індексів і на звільнені нижні місця перенесемо (для зручності) верхні індекси, тобто

$$T_s^0 = T_0,\ T_S^\delta = T_\delta,\ T_S^w = T_W,\ T_S^B = T_B,\ T_S^A = T_A,\ T_s^\infty = T_\infty.$$

Тоді кортеж моментів часу (3) прийме наступний вигляд:

$$T_0,\ T_\delta,\ T_W,\ T_B,\ T_A,\ T_\infty. \qquad (4)$$

Змістовна складова елементів цього кортежу така: T_0 – це момент часу початку стадії перебування системи в стан початкової готовності, T_δ – це момент завершення стадії перебування системи в стані початкової готовності і, водночас, це момент початку стадії впливу події критичного інциденту визначеного типу, T_W – це момент часу завершення стадії впливу події критичного інциденту визначеного типу і, водночас, це момент початку стадії абсорбції системою факторів впливу критичного інциденту, T_B – це момент часу завершення стадії абсорбції системою факторів впливу критичного інциденту і, водночас, це момент

часу початку стадії відновлення системою свого функціоналу, $T_A -$ це момент часу завершення стадії відновлення системою свого функціоналу, і водночас, це момент часу початку стадії адаптації системи до можливого повторення події впливу критичного інциденту певного типу, $T_\infty -$ це момент часу завершення стадії адаптації системи до повторення події впливу критичного інциденту певного типу і, водночас, це момент часу входу системи в стадію перебування в стані кінцевої готовності. Особливістю циклічного процесу еволюції однієї, окремо визначеної системи, що перебуває під дією послідовності однакових подій впливу критичних інцидентів певного типу, полягає в тім, що рівень адаптаційного потенціалу системи, досягнутий на кінець *j*-ої ітерації циклу еволюції, є тотожно рівним рівню адаптаційного потенціалу системи, з якого вона починає (*j+1*)-й цикл своєї еволюції

$$P_{j+1}(T_0) = P_j(T_\infty).$$

Без втрати загальності можемо прийняти, що $T_0 = 0$. Тоді на підставі вищенаведених міркувань динаміку зміни рівню адаптаційного потенціалу $P_j(t)$ однієї, окремо визначеної системи протягом *j*-ої ітерації циклу її еволюції, можемо описати наступним співвідношенням:

$$P_j(t) = \theta(t)P_j(0) - \theta(t - T_\delta)I_j(t - T_\delta) + \theta(t - T_W)W_j(t - T_W) + \\ +\theta(t - T_B)B_j(t - T_B) + \theta(t - T_A)A_j(t - T_A). \quad (5)$$

Тут $\theta(t) -$ ступінчата функція Хевісайда. $I_j(t) -$ функція, яка характеризує зміну в часі здатності інциденту до впливу на рівень адаптивного потенціалу системи протягом *j*-ої ітерації циклу еволюції системи. $W_j(t)$ – функція абсорбції, яка характеризує зміну в часі здатності системи поглинути певний вплив інциденту на рівень її адаптивного потенціалу. $B_j(t)$ - функція відновлення, що описує здатність системи реанімуватися до свого початкового рівня адаптаційного потенціалу після завершення події впливу інциденту. $A(t)$ – це функція адаптації, яка характеризує зміну в часі здатності резильєнтної системи підвищувати рівень свого адаптаційного потенціалу під впливом критичних інцидентів певного типу.

Таким чином, ітеративне управління рівнем адаптаційного потенціалу задля запобігання деструкції системи в наслідок критичних інцидентів, реалізоване за рахунок управління пов'язаними з ними ризиками, можна визначити як підґрунтя для розробки методів забезпечення резильєнтності організаційно-технічних систем. Зокрема, це обумовлює доцільність опрацювання усіх таких ризиків, у разі, якщо існує ненульова ймовірність їхньої реалізації, зважаючи на те, що реалізація будь-якого з них може призвести до стагнації СУІБ/КСЗІ та катастрофічних наслідків для організації загалом. В подальшому такі ризики будемо називати критичними (резильєнтними).

Нехай *R* позначає ризик, *Σ* – вартість усіх активів організації, *L* – збиток, а *C* - множину усіх критичних процесів організації. Тоді ризик *R* може бути класифікований як резильєнтний, якщо виконуються такі умови:

- Критичність процесу: $\exists c \in C$, такий, для якого існує ризик *R>0.* Ця умова вказує, що має існувати принаймні один критичний процес *c* у множині всіх критичних процесів *C*, з яким безпосередньо пов'язаний ризик *R*.

- Масштаб фатальності впливу ризику: Реалізація $R \Rightarrow (c=0) \vee (L \geq \Sigma)$. Ця умова описує, що реалізація ризику R повинна призвести або до повної дисфункції критичного процесу c, або до збитків, які дорівнюють (або навіть перевищують) загальну вартість усіх активів організації.

Для управління критичними ризиками організаційно-технічної системи запропоновано методику, в основу якої покладено розрахунок очікуваної корисності опрацювання кожного ризику. Алгоритмізована форма подання методики представлена на рис. 2. Ключовий елемент методики – це бюджет на опрацювання ризиків, який є об'єктивною квантифікованою величиною, що відображає обмежену кількість ресурсів, доступних для опрацювання та мітигації ризиків і корелює з ризик-апетитом організації.

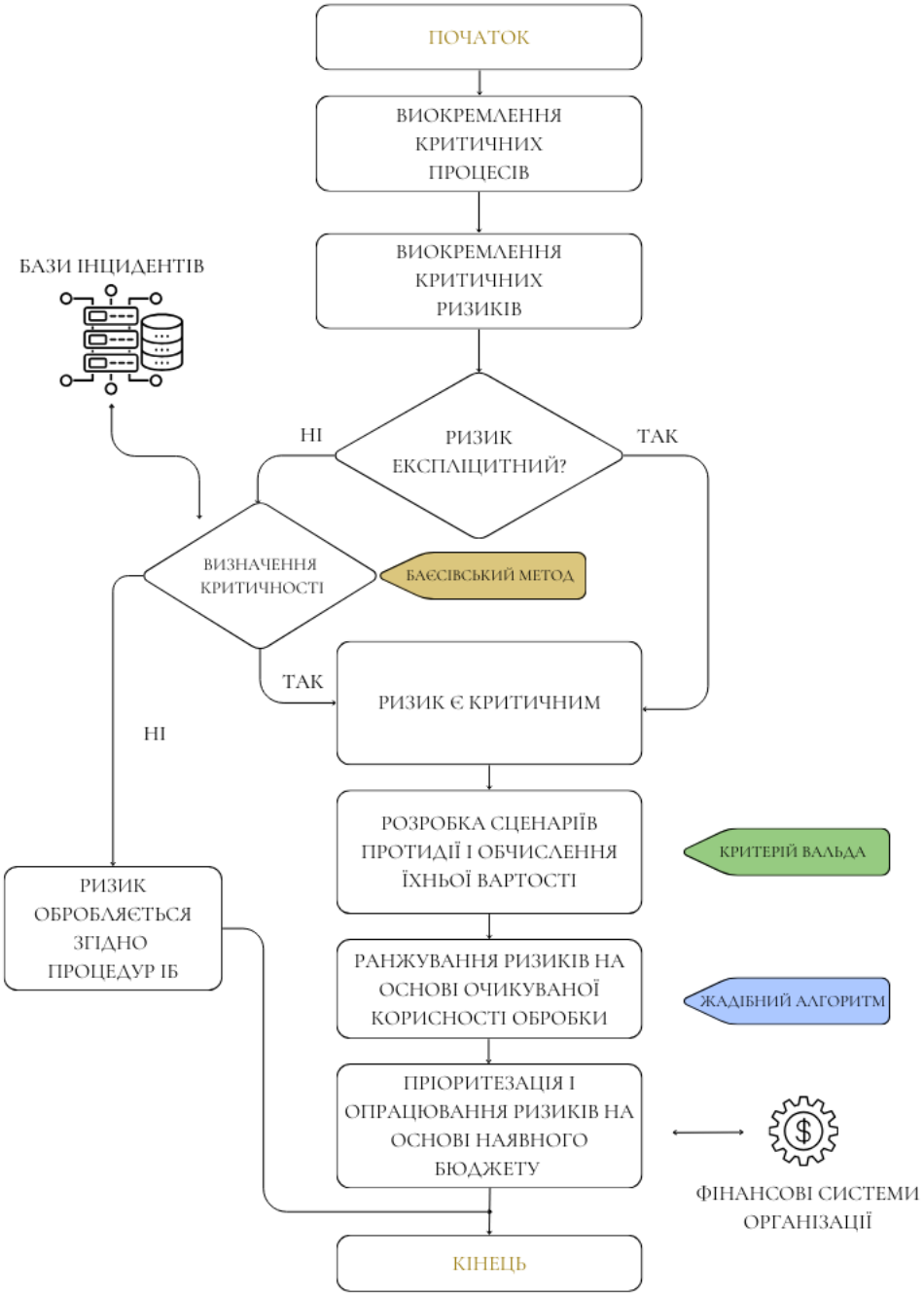

Рисунок 2 – Алгоритмізована форма подання методики управління критичними ризиками

Ризики, що становлять загрозу для критичних процесів, поділені на дві категорії: експліцитні (явні) і імпліцитні (неявні). Для доведення деструктивності імпліцитних ризиків і мінімізації витрат на їхню мітигацію запропоновано використання інтерпретації баєсівського підходу, застосувавши який до аналізу гіпотез реалізації загроз (ризиків), ми можемо виділити ті з них, які призведуть до дисфункції критичних процесів з найбільшою імовірністю. Для цього визначається множина гіпотез H_i та дані D, що відносяться до гіпотез, які аналізуються. У контексті резильєнтності, гіпотези можуть являти собою різні типи безпекових загроз, а дані – це індикатори компрометації або ж статистичні данні, threat intelligence data, тощо. Теорема Баєса допомагає оновити впевненість у гіпотезах H_i на основі спостережуваних даних D. Тоді інтерпретація складових з формули теореми Баєса

$$P(H_i|D) = \frac{P(D|H_i)\cdot P(H_i)}{P(D)} \quad (6)$$

набуває такого змісту: $P(H_i|D)$ - апостеріорна ймовірність гіпотези після врахування даних D; $P(D|H_i)$ - ймовірність спостерігати дані D, якщо гіпотеза H_i вірна; $P(H_i)$ - апріорна ймовірність гіпотези H_i ; $P(D)$ - загальна ймовірність спостерігати дані, яка може бути обчислена як сума ймовірностей D, для всіх гіпотез, що розглядаються. Щоб знайти найімовірнішу гіпотезу, необхідно обчислити $P(H_i|D)$ для кожної гіпотези H_i і вибирати ту з них, у якої апостеріорна ймовірність найвища.

Практична реалізація баєсівського підходу в нашому випадку передбачає квантифікацію порога критичності. У разі отримання значень $P(H_i|D)$, вищих за цей поріг, імпліцитні ризики вважаються критичними. Значення ймовірностей можуть використовуватися надалі під час аналізу ризиків та їхньої пріоритизації.

Після ідентифікації та верифікації критичних ризиків, наступним етапом методики є розроблення та кількісна оцінка сценаріїв реагування на ці ризики. На цьому етапі пропонується використовувати критерій Вальда як інструмент раціонального вибору в умовах невизначеності. Він передбачає вибір таких сценаріїв реагування, які забезпечують найкращий результат в найгірших умовах, що є винятково релевантним для царини резильєнтності, бо розроблювані сценарії реагування мають оцінюватися відповідно до їхньої здатності впоратися з найгіршими можливими наслідками, і перевага надається тим стратегіям, які забезпечують найкращий результат за найнесприятливішого збігу обставин. Запропоновано використання дивергентного підходу до прийняття рішень – розглядається відразу декілька можливих сценаріїв реагування на ризик з урахуванням найгірших обставин перебігу подій, кожен з яких оцінюєтеся із погляду потенційних збитків (які для критичних ризиків максимальні) і витрат ресурсів і часу, пов'язаних із його реалізацією. Обирається той з сценаріїв, що запобігає деструкції системи за найгіршого перебігу подій, який має найменшу вартість реалізації. Таким чином, використання критерію Вальда відповідає принципам раціонального вибору в умовах невизначеності, де рішення приймаються на основі мінімізації максимальних можливих збитків, що особливо важливо при управлінні ризиками з потенційно катастрофічними наслідками.

Після отримання множини усіх критичних ризиків і оцінки вартості сценаріїв протидії кожному з них (із урахуванням найнесприятлівішого сценарію перебігу подій), наступним етапом є ранжування ризиків на основі очікуваної корисності їхньої обробки, яка зазвичай вираховується по формулі: $u_i = l_i - q_i$, де l_i – збиток у разі реалізації ризику, а q_i – вартість сценарія протидії. Але, в разі реалізації будь-якого ризику з означеної множини критичних ризиків, збитки будуть максимальними, і це дає змогу дійти висновку, що l є константою ($l = const$) для всіх ризиків у даній підмножині, і при цьому значення l прямує до нескінченності ($l \to \infty$). У зв'язку з цим, при ранжуванні критичних ризиків слід брати до уваги виключно вартість сценарію протидії.

Ранжувати ризики пропонується на підставі очікуваної корисності їхньої обробки, з використанням жадібного алгоритму. Ризики з найменшою вартістю сценарію протидії, згідно з запропонованою методикою, мають найвищий пріоритет в обробці. Використання жадібного алгоритму для оптимізації вибору ризиків у межах обмеженого бюджету ґрунтується на припущенні, що в даному випадку послідовність локально оптимальних рішень потенційно може привести до глобально оптимального результату. Процес починається з ранжування ризиків за зростанням вартості їхньої мітигації. Ризик із найменшими витратами на опрацювання обирають першим, за умови, що його вартість не перевищує виділений бюджет. Бюджет коригується шляхом віднімання вартості мітигації обраного ризику, і процес повторюється для наступного ризику у відсортованому списку. Ітерації тривають до вичерпання бюджету або повного опрацювання всіх ризиків.

У третьому розділі на підставі онтології резильєнтності організаційно-технічних систем, побудованої за допомогою стенфордської платформи Protégé, обґрунтовано, що резильєнтність складної організаційної структури не може бути просто агрегована з резильєнтності її складових частин.

Стратегію управління ризиками в онтології виокремлено як центральний документ, з якого починається процес забезпечення резильєнтності на організаційному рівні. Для ефективного агрегування усіх типів ризиків організації (включно зі стохастичними і спорадичними) в рамках єдиної стратегії запропоновано використовувати тривимірну матрицю ризиків, яка також є одним зі способів поєднання концепцій резильєнтності та безпеки при побудові СУІБ/КСЗІ організаційно-технічних систем. Обсяг ресурсів, необхідних для опрацювання кожного ризику в рамках повного спектру визначених ризиків організації, включно з тими, що належать до царин як інформаційної безпеки, так і до резильєнтності, власне і є тим самим додатковим виміром, що перетворює стандартну двовимірну матрицю, яка ґрунтується на зіставленні ймовірності та величині потенційного збитку, на більш комплексну тривимірну модель (рис. 3).

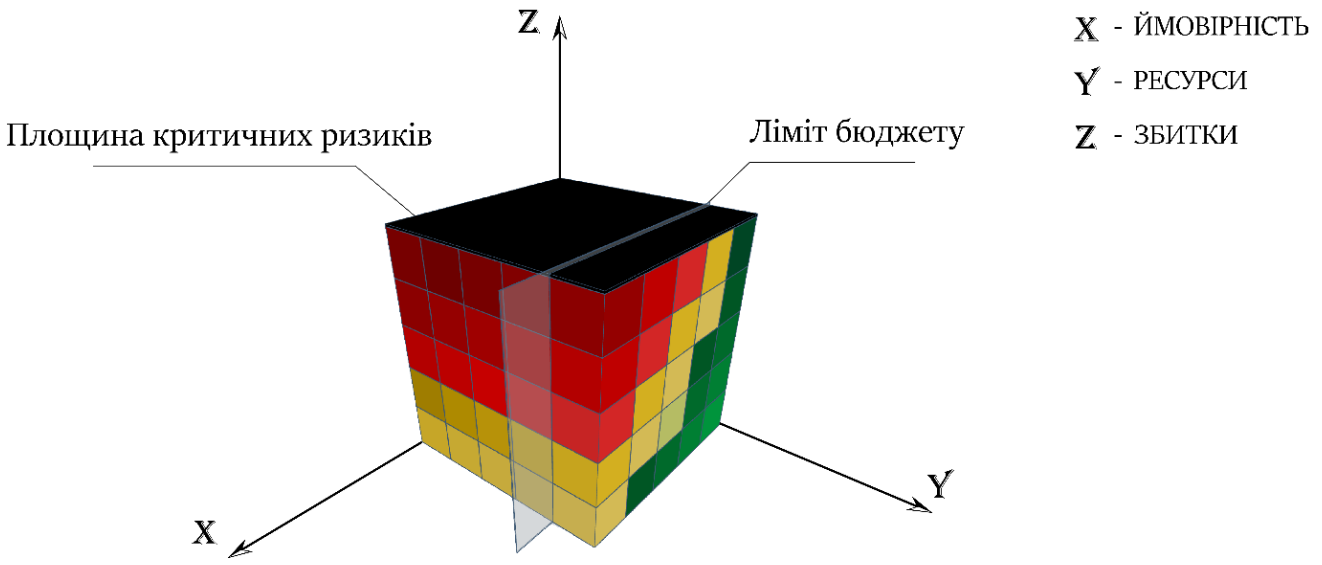

Рисунок 3 – Тривимірна матриця «куб» ризиків

Кожна координата (вісь) цієї матриці представляє відповідний ключовий аспект аналізу ризику:

- Вісь X (Імовірність реалізації ризику): Відображає ймовірність настання ризикової події, де 0 відповідає нульовій ймовірності, а 1 - 100% ймовірності.
- Вісь Z (Потенційний збиток): Зображає максимально можливий збиток від реалізації ризику для організації, починаючи від відсутності збитку - 0, до критичного збитку, здатного призвести до краху організації - 1.
- Вісь Y (Обсяг ресурсів): Демонструє шкалу ресурсів необхідних для опрацювання ризиків, де 0 – відсутність ресурсів, 1 – загальна кількість ресурсів, необхідна для опрацювання усіх виокремлених ризиків організації.

У рамках цієї тривимірної моделі, кожен ризик організації концептуалізується у вигляді точки в тривимірному просторі. Наприклад, точка (1, 0, 0) у цій матриці означає ризик, що реалізується з ймовірністю 100%, але без збитку, і вимагає мінімальних витрат на управління, тоді як точка (1, 1, 0) відображає ризик із максимальним потенційним збитком, ймовірністю настання і найменшими витратами на його мітигацію. Наявний бюджет організації відображено у вигляді площини "ліміт бюджету", що проходить через точку на осі Y, місце якої чітко визначається у залежності від кількісті доступних фінансових ресурсів, виділених організацією для опрацювання ризиків. Ця площина, проведена паралельно осям X (ймовірність реалізації ризику) і Z (потенційний збиток), ділить тривимірний простір куба ризиків на дві області, кожна з яких представляє різні категорії ризиків:

- Область куба від 0 до точки перетину площини «ліміт бюджету» з віссю Y включає в себе ризики, які організація може дозволити собі обробити в рамках встановленого бюджету. Ці ризики перебувають у межах фінансових можливостей організації для їхньої мітигації, зниження або усунення.
- Область куба від точки перетину площини «ліміт бюджету» з віссю Y до 1 на осі Y: Містить ризики, опрацювання яких потребує вищих витрат, ніж це

дозволяє наявний бюджет. Для управління такими ризиками організації потрібно або збільшити бюджет, або вжити заходів для їхнього зниження до прийнятного рівня без значних додаткових витрат.

Класифікація ризиків у рамках моделі з тривимірною матрицею, яка розділяє їх на критичні, що мають бути опрацьовані з погляду резильєнтності, та інші, що підлягають опрацюванню в контексті інформаційної безпеки, допомагає агрегувати різні типи ризиків організаційно-технічних систем.

Верхня грань куба – критичні резильєнтні ризики. Ці ризики являють собою найбільш серйозні загрози, які можуть завдати фатальної шкоди організації та її операціям. Опрацювання цих ризиків орієнтоване на забезпечення резильєнтності, що охоплює готовність і здатність організації швидко відновлюватися після збоїв або атак і адаптуватися до них. Грань має чорне кольорове кодування.

Увесь об'ємний простір куба, за винятком його верхньої грані, являє собою сегмент, який займають ризики, релевантні для інформаційної безпеки. Цей сегмент характеризується комбінаціями значень імовірності (X), витрат на обробку (Y) і збитків (Z), які не досягають критичного порогу, визначеного верхньою гранню.

На рис. 3. простір ризиків інформаційної безпеки має вигляд розширення стандартної двовимірної матриці ризиків 5x5 до тривимірної матриці розмірністю 5x5x5, що означає, що він умовно поділений на 125 малих кубів. Кожен малий куб $K_{i,j,k}$ являє собою підмножину простору $\mathbb{R}^3$ і визначається як:

$$K_{i,j,k} = \{ (x, y, z) \mid i \leq x < i + 1, j \leq y < j + 1, k \leq z < k + 1 \}, \qquad (7)$$

де i, j, k приймають значення від 0 до 4 відповідні дискретним інтервалам оцінки кожного параметра. Ризики, що належать одному й тому самому малому кубу, формують групу зі схожими характеристиками за всіма трьома параметрами. Умовно кажучи, кожен малий куб – це окремий клас еквівалентності, в якому всі ризики не розрізняються один від одного. Це дає змогу аналізувати й управляти групами ризиків залежно від їхніх загальних характеристик.

Кольорове кодування малих кубів у тривимірній матриці ризиків, включно з відтінками червоного, жовтого і зеленого кольорів, слугує для візуального представлення і категоризації рівнів ризику.

Тривимірна матриця ризиків може застосовуватися для управління всім спектром ризиків організації, включно як з резильєнтними ризиками, так і ризиками інформаційної безпеки, з огляду на їхній взаємозв'язок і взаємозалежність. Ризики, які стосуються і резильєнтності, і інформаційної безпеки, за умови $z(r) = 1$ виключаються з множини ризиків інформаційної безпеки та підлягають опрацюванню згідно із запропонованою методикою управління критичними ризиками в контексті забезпечення резильєнтності.

В якості інструмента, який надає можливість не тільки оцінювати наявну систему управління ризиками та інцидентами, а й такого, що сприяє безперервному збільшенню адаптаційного потенціалу і є фундаментальним для забезпечення резильєнтності на всіх рівнях системної та організаційної ієрархій, пропонується використовувати метод хаос-інжинірингу. Ідея розвинення методу хаос-інжинірингу полягає як в штучному контрольованому ітеративному стимулюванні аутопоезису і адаптаційних механізмів організаційно-технічних систем, так і в

перевірці диверсності способів реалізації їхніх критичних функцій. З певною долею впевненості можемо припустити, що в процесі експериментів, які проводять у рамках хаос-інжинірингу, збільшення адаптаційного потенціалу системи відбувається за рахунок навмисно створюваних точок біфуркації - моментів в параметричному просторі системи, де відбуваються якісні зміни в її динаміці, які слугують каталізаторами для переходу системи до нових станів рівноваги. Атрактор, у контексті резильєнтності, не обмежується граничним циклом. Фазова траєкторія резильєнтної системи має динамічно змінюватися, враховуючи еволюційні перетворення і відображаючи наслідки адаптації, отримані як результат протистояння реалізованим загрозам, імітованим у рамках хаос-інжинірингу, включно з кібератаками, технічними збоями та іншими критичними ситуаціями.

Для опису динамічної зміни фазової траєкторії системи можна використовувати таку формалізацію:

$$S_{\text{нов}} = S_{\text{початк}} + \Delta S_{\text{адапт}}\ (V, \tau), \quad (8)$$

де: $S_{\text{нов}}$ - стан системи після адаптації; $S_{\text{початк}}$ - вихідний стан системи до введення збурень; $\Delta S_{\text{адапт}}$ - зміна в стані системи, зумовлена адаптацією до збурень, V - вектор збурень, що являє собою сукупність усіх штучно створених змін (наприклад, атаки, збої); τ - час, упродовж якого система зазнавала впливу збурень і проходила процес адаптації. Функція $\Delta S_{\text{адапт}}\ (V, \tau)$ символізує процес адаптації системи, який залежить від характеру і тривалості впливу збурень. Ця функція являє собою сукупність механізмів зворотного зв'язку, самоорганізації та поліпшень, які система розвиває у відповідь на випробувальні стреси.

Показано доцільність застосування лонгітюдного аналізу в контексті високорівневого оцінювання резильєнтності. Запропоновано використання метрик Uptime, MTTR (*Mean Time To Repair*), MTTA (*Mean Time To Acknowledge*), и MTBF (*Mean Time Between Failures*)[3], які надають змогу агрегувати й аналізувати дані щодо продуктивності та стійкості систем до інцидентів в уніфікованій і стандартизованій формі.

Запропоновано ввести метрику *Resilience index*, яка об'єднує як операційні, так і економічні аспекти, дає змогу отримати більш повне уявлення про резильєнтність організації, оцінюючи не тільки здатність швидко відновлюватися після збоїв і адаптуватися до них, а й ефективність використання ресурсів для запобігання та управління інцидентами в рамках загальної стратегії сталого розвитку:

$$Resilience\ index = \left(\frac{G - K_{rs}}{G}\right) \times \left(1 - \frac{N}{T}\right), \quad (9)$$

де: K_{rs} - річні витрати на безпеку і резильєнтність; G – річний прибуток організації; N - загальний час простою критичних функцій за рік; T - загальний доступний час роботи критичних функцій за той самий період.

Перший компонент - $\left(\frac{G - K_{rs}}{G}\right)$ відображає частку чистого прибутку (прибуток за вирахуванням витрат на резильєнтність) відносно загального прибутку. Компонент

[3] Naik, K., & Tripathy, P. (2011). Software testing and quality assurance: theory and practice. John Wiley & Sons.

$\left(1 - \frac{N}{T}\right)$ оцінює вплив інвестицій на операційну діяльність, враховуючи час простою критичних функцій щодо загального часу їхньої доступності.

Високе значення показника *Resilience index* вказує на ефективність інвестицій в резильєнтність і дієвість заходів з забезпечення резильєнтності організаційно-технічних систем. Застосування цієї метрики забезпечує можливість не просто вимірювати витрати на безпеку, а й аналізувати реальний вплив цих витрат на операційну діяльність.

У четвертому розділі адекватність розроблених методів забезпечення резильєнтності перевірено шляхом реорганізації критичного сегменту інфраструктури та СУІБ/КСЗІ реально діючої організаційно-технічної системи.

Для автоматизації процесу управління критичними ризиками в контексті резильєнтності, на основі розроблених методів створено програмний застосунок, за допомогою якого здійснюється аналіз і оцінювання критичних ризиків організаційно-технічної системи, відстеження ключових показників ризику, оновлення оцінок ризиків та моніторинг ефективності планів реагування на ризики.

Дані, отримані в результаті реорганізації, дали змогу виявити ключові вразливості та потенційні загрози, що зумовило необхідність впровадження запропонованих змін шляхом використання конструктів фреймворку резильєнтності, які було виокремлено в процесі побудови онтології. Архітектура СУІБ/КСЗІ діючої системи, яка була модифікована в рамках реалізації запропонованого підходу, початково базувалася на принципах ISO 27001 і моделі Zero Trust. Відповідно до розробленої методики управління критичними ризиками в контексті забезпечення резильєнтності, було реалізовано етап оцінювання критичності ризику втрати інтернет-з'єднання, який полягає у визначенні ймовірності банкрутства організації у разі перевищення встановленого 24-годинного ліміту вимкнення. Для кількісної оцінки цього ризику було застосовано теорему Баєса. Для визначення апріорної ймовірності деструкції системи було застосовано статистичні моделі машинного навчання: логістичну регресію і метод штучних нейронних мереж (ANN) – вона склала 2%. Апостеріорна ймовірність порушення функціонування критичних процесів системи, безпосередньо пов'язаних з її інваріантами, за умови, що інтернет буде відключено більш ніж на добу, склала 67%, що перевищило затверджений поріг у 49%, що надало змогу визначити цей ризик як такий, що належить до категорії критичних. Під час вибору заходів з мітигації визначено, що вжиті раніше, в рамках СУІБ, контрзаходи (у вигляді використання резервного оптичного каналу іншого провайдера) не могли ні нейтралізувати, ні навіть пом'якшити жоден зі стохастичних сценаріїв реалізації ризику. Для реалізації стратегії забезпечення резильєнтності шляхом адаптації сегмента інформаційної системи, що відповідає за критично важливі процеси до потенційно найгірших сценаріїв ризиків, було обрано методи з фреймворку SP 800-160 Vol. 2 Rev. 1 (NIST): *реорганізація; скоординований захист; різноманітність; резервування; сегментація; обман*. Практична реалізація стратегії реорганізації критичного сегмента інфраструктури організації включала такі заходи:

- Заміна резервного оптичного каналу на мобільний користувацький термінал глобальної супутникової системи Starlink.
- Інсталяція автономної енергосистеми.
- Перенесення другорядних сайтів і веб-додатків організації на зовнішній хостинг.
- Інтеграція в IT-інфраструктуру організації десепшн-системи з відкритим вихідним кодом.
- Використання методу хаос-інжинірингу для ітеративного стимулювання аутопоезису і адаптивних механізмів організаційно-технічної системи.

Вартість обраного сценарію опрацювання ризика шляхом реорганізації інфраструктури не перевищила сукупної вартості обслуговування зазначеного сегменту до реорганізації, що, згідно із запропонованою методикою, підвищило пріоритет опрацювання цього ризику до максимального і дало змогу оперативно впровадити контрзаходи, передбачивши реалізацію описаних стохастичних сценаріїв. У результаті вжитих заходів апостеріорна ймовірність порушення функціонування критичних процесів системи знизилася до прийнятних 6%.

Таким чином, опрацювання навіть одного критичного ризику дало змогу не тільки напрацювати контрзаходи для найгірших сценаріїв його реалізації, але й забезпечило резильєнтність усієї організації, що підтверджує ефективність запропонованих методів, інтегрованих до СУІБ/КСЗІ організаційно-технічної системи.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальне науково-прикладне завдання з розробки методів забезпечення резильєнтності організаційно-технічних систем та інтеграції цих методів в СУІБ (КСЗІ) задля їхнього вдосконалення.

При цьому отримано такі наукові та практичні результати:

1. Виконано аналіз передумов виникнення парадигми резильєнтності та факторів, які зумовили її розвиток у безпековому домені, що дозволило визначити недоліки існуючих методів і підходів, покладених в основу наявних фреймворків з резильєнтності, які унеможливлюють інтеграцію проаналізованих методів в СУІБ/КСЗІ організаційно-технічних систем.

2. Розроблено метод виокремлення і ранжування критичних ризиків (включно зі стохастичними і спорадичними ризиками) шляхом застосування Баєсівського підходу, критерію Вальда та жадібного алгоритму, який надає можливість планувати витрати на обробку в межах фіксованого бюджетарного обмеження.

3. Розроблено онтологію резильєнтності організаційно-технічних систем, що містить високорівневі конструкти парадигми резильєнтності, елементи організаційної структури, безпекові концепти та відображає їхні зв'язки та взаємодію, що дозволяє формалізувати їхнє застосування при проектуванні СУІБ/КСЗІ організаційно-технічних систем.

4. Запропоновано модель оцінювання ризиків, яка відображає квантифікований ризик-апетит організації і вміщує відранжовану послідовність

усіх виокремлених ризиків організації, що дозволяє обробляти різні їх типи в рамках єдиної стратегії управління ризиками СУІБ/КСЗІ.

5. Розвинуто метод хаос-інжинірингу для забезпечення резильєнтності організаційно-технічних систем, шляхом штучного контрольованого ітеративного стимулювання їхніх адаптаційних механізмів і перевірки диверсності способів реалізації їхніх критичних функцій.

6. Розроблено метод високорівневого оцінювання стану резильєнтності організаційно-технічних систем, що ґрунтується на лонгітюдному підході та об'єднує метрики вимірювання часу безвідмовної роботи, середнього часу відновлення, середнього часу до вжиття заходів та середнього часу між відмовами, з економічними показниками витрат на забезпечення безпеки та резильєнтності у відношенні до доходу організації.

7. Запропоновано програмний застосунок для аналізу і оцінювання критичних ризиків організаційно-технічних систем в контексті забезпечення їхньої резильєнтності.

8. Коректність результатів дисертаційного дослідження підтверджено на прикладі успішної реорганізації критичного сегменту інфраструктури реально діючої організаційно-технічної системи та її СУІБ/КСЗІ, побудованої за принципами ISO 27k та Zero Trust.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Korobeynikov F. Building resilience through risk management: methodology and strategy. *International Science Journal of Engineering & Agriculture*. 2024, Vol. 3, no. 4, P. 78–85, ISSN: 2720-6319 URL: https://doi.org/10.46299/j.isjea.20240304.08 ***(EU)***
2. Mokhor V., Korobeynikov F. Resilience and stability in security domain. *Data Recording, Storage & Processing*, 2024. Vol. 26, No. 1, P. 113–120, ISSN 1560-9189 URL: https://doi.org/10.35681/1560-9189.2024.26.1.308655
3. Korobeynikov F. Developing a conceptual framework for resilience in information systems. *Prombles in programming*, 2024. No. 1, P. 96–102, ISSN 1727-4907. URL: https://pp.isofts.kiev.ua/index.php/ojs1/article/download/611/661
4. Korobeynikov F. O. Resilience in Focus: Rethinking the Risk Matrix. *Electronic modeling*, 2024. Vol. 46, no. 2, P. 35–42, ISSN 0204–3572. URL: https://doi.org/10.15407/emodel.46.02.035 .
5. Korobeynikov F. Ontology of Goals and Objectives for Organizational Resilience. *Electronic Modeling,* 2023, Vol. 45, no. 5, P. 67–80, ISSN 0204–3572. URL: https://doi.org/10.15407/emodel.45.05.067
6. Korobeynikov F. Using the Wald Maximin Criterion for Risk Analysis of Hard-To-Predict Threats in the Context of Resilience. *Electronic Modeling*, 2023. Vol.

45, no. 6, P. 31–40, ISSN 0204–3572. URL: https://doi.org/10.15407/emodel.45.06.031.

7. Korobeynikov F., Bakalynskyi O. Defining of Goals in the Development of Cyber Resilient Systems According to NIST. *Theoretical and Applied Cybersecurity*, 2023. Vol. 5, no. 1, ISSN 2664-2913. URL: https://doi.org/10.20535/tacs.2664-29132023.1.287751
8. Korobeynikov F., Bakalynskyi O. Defining the Sequence of Integrating Trustworthiness Components Into Information Security Systems. *Ukrainian Information Security Research Journal*, 2023. Vol. 4, no. 25, P. 268–274, ISSN 2410-7840. URL: https://jrnl.nau.edu.ua/index.php/ZI/article/view/18233.
9. Korobeynikov F. Resilience Paradigm Development In The Security Domain. *Electronic Modeling*, 2023. Vol. 45, no. 4, P. 88–111, ISSN 0204–3572. URL: https://doi.org/10.15407/emodel.45.04.088.

Праці апробаційного характеру:

10. Korobeynikov F., Bakalynskyi O. Establishing Goals in the Creation of Cyber-Resilient Systems. *DESSERT, IEEE Xplore*, 2023. ISBN 979-8-3503-9611-9. URL: https://www.scopus.com/record/display.uri?origin=myalerts&eid=2-s2.0-85185837395 ***(*Scopus, IEEE*)***
11. Коробейніков Ф. Цілі кібербезпеки та кіберрезильєнтності: порівняння спрямувань. *Матеріали науково-практичної конференції «Кібербезпека енергетики»*, м. Київ, 31 трав. 2023 р. С. 78–81. URL: https://ipme.kiev.ua/wp-content/uploads/2023/06/1-Матеріали-КБЕ-2023.pdf.
12. Коробейніков Ф. Визначення цілей при розробці кіберрезильєнтних систем. *Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity»* (TACS-2023) присвячена 100-річному ювілею академіка В.М. Глушкова, м. Київ, 26 трав. 2023 р. С. 79–89. URL: https://is.ipt.kpi.ua/pdf/TACS-23.pdf.
13. Korobeynikov F. Key Sybersecurity Risks 2023. *Proceedings of the VI International Scientific and Practical Conference «SCM IA»*, Amsterdam, Netherlands, 2023. URL: http://dx.doi.org/10.13140/RG.2.2.33022.80963
14. Коробейніков Ф. Резильєнтний підхід до побудови розподіленої системи забезпечення інформаційної безпеки. Матеріали міжнародної *науково-практичної конференції «Survivability & Resilience – 2023»*), м. Київ, 19 жовт. 2023 р. С. 71–74. URL: https://ipme.kiev.ua/wp-content/uploads/2023/11/Матеріали_ конференції_Survivability_and_Resilience-2023-4.pdf.
15. Коробейніков Ф. та ін. Втілення парадигми резильєнтності в забезпечення функціонування критичної інфраструктури ЄС. Матеріали *науково-практичної конференції «Резильєнтність критичної інфраструктури – 2023»*, м. Київ, 21 черв. 2023 р. С. 48–51. URL: https://ipme.kiev.ua/wp-content/uploads/2023/06/Матеріали-конференції-Critical-Infrastructure-Resilience-–-2023.pdf.
16. Коробейніков Ф. Аналіз визначень терміна "резильєнтність" та його інтерпретацій у міжнародних стандартах. Збірник матеріалів *XLI науково-*

технічної конференції молодих вчених Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 17 трав. 2023 р. С. 145–149. URL: https://ipme.kiev.ua/wp-content/uploads/2023/05/Матеріали-конференції-2023.pdf.

17. Korobeynikov F. Chaos engineering as a strategy for strengthening resilience. Proceedings of the *IX International Scientific and Practical Conference «Theoretical and practical aspects of the development of science and education»*, Prague, Czech Republic, 5 March 2024. P. 312–315. URL: https://doi.org/10.46299/ISG.2024.1.9.
18. Korobeynikov F. Artificial intelligence in cyber warfare. Proceedings of the *X International Scientific and Practical Conference «Problems and prospects of modern science»*, Stockholm, Sweden, 15 March 2024. P. 313–316. URL: https://doi.org/10.46299/ISG.2024.1.10.
19. Коробейніков Ф. Резильєнтність в контексті концепції тріади часу. Збірник матеріалів *XLII науково-технічної конференції молодих вчених Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, м. Київ, 15 трав. 2024 р. С. 7–10. URL: https://ipme.kiev.ua/wp-content/uploads/2024/05/Матеріали-конференції-2024-v-2.pdf

Праці, які додатково відображають наукові результати дисертації:

20. *Свідоцтво про реєстрацію авторського права на комп'ютерну програму* «Алгоритм обробки резильєнтних ризиків для критичних систем в рамках побудови систем захисту інформації» : а. с. No 123657 Україна. Опубл. 09.02.2024, Бюл. № CR1959090224. URL: https://sis.nipo.gov.ua
21. *Свідоцтво про реєстрацію авторського права на науковий твір* «Алгоритм обробки резильєнтних ризиків для критичних систем в рамках побудови систем захисту інформації» : а. с. No 123658 Україна : CR1972090224. Опубл. 09.02.2024. URL: https://sis.nipo.gov.ua.

АНОТАЦІЯ

Коробейніков Ф.О. Методи забезпечення резильєнтності організаційно-технічних систем. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2024.

Дисертаційну роботу присвячено вирішенню актуального науково-прикладного завдання з розробки методів забезпечення резильєнтності організаційно-технічних систем та інтеграції цих методів в СУІБ (КСЗІ) задля їхнього вдосконалення Актуальність дослідження зумовлена парадигмальною еволюцією в безпековому демені, що призвела до заміни домінуючої концепції - з захисту на резильєнтність..

Для розробки методів забезпечення резильєнтності організаційно-технічних систем виконано аналіз передумов виникнення парадигми резильєнтності та факторів, які зумовили її розвиток у безпековому домені. Розроблено метод виокремлення і ранжування критичних ризиків (включно зі стохастичними і спорадичними) шляхом застосування Баєсівського підходу, критерію Вальда та жадібного алгоритму, який надає можливість планувати витрати на обробку в межах фіксованого бюджетарного обмеження. Створено онтологію резильєнтності організаційно-технічних систем. Запропоновано модель оцінки ризиків, яка відображає квантифікований ризик-апетит організації і вміщує відранжовану послідовність усіх виокремлених ризиків організації. Розвинуто метод хаос-інжинірингу, який полягає як в штучному контрольованому ітеративному стимулюванні адаптаційних механізмів інформаційних систем до змін операційного середовища, зовнішніх загроз і внутрішніх збоїв, що забезпечує їхнє спрямування на виявлення прихованих вразливостей та оцінку механізмів відновлення функціональності систем після потенційних інцидентів, так і в перевірці диверсності способів реалізації їхніх критичних функцій. Розроблено метод високорівневого оцінювання стану резильєнтності організаційно-технічних систем. Запропоновано метрику *Індекс резильєнтності*, яка надає можливість оцінювати як ефективність фінансових інвестицій в безпеку і резильєнтність, так і операційні результати цих інвестицій. Запропоновано візуальний інструмент пріоритизації ризиків в контексті резильєнтності у вигляді тривимірної матриці, здатної агрегувати усі типи ризиків. Реорганізовано критичний сегмент інфраструктури організаційно-технічної системи, її СУІБ/КСЗІ, побудованої за принципами ISO 27k та Zero Trust.

Вирішення цих задач створило належні умови для забезпечення резильєнтності і трастоспроможності організаційно-технічних систем всіх типів і рівнів ієрархії, шляхом вдосконалення СУІБ (КСЗІ).

Ключові слова: резильєнтність, адаптаційний потенціал, управління ризиками, трастоспроможність, системи захисту інформації.

ABSTRACT

F. Korobeynikov. Methods for Ensuring the Resilience of Organisational and Technical Systems. – As the manuscript.

Thesis for technical sciences candidate degree in specialty 05.13.21 – Information security systems. – Pukhov Institute for Modelling in Energy Engineering of the National Academy of Sciences of Ukraine, Kyiv, 2024.

The paradigmatic shifts in the security domain, which have resulted in the replacement of the concept of protecting organisations' information assets with the resilience of their critical functions, necessitate not only a re-evaluation of the principles underlying the construction of information security management systems (ISMS) and comprehensive information protection systems (CIPS), but also the development of a methodological framework for ensuring resilience that would guarantee the successful integration of the latest concepts at all levels of their applicability.

The objective of this research is to develop methods for ensuring the resilience of organisational and technical systems, as well as their integration into information security management systems and complex information protection systems. In order to achieve this objective, the conditions for the emergence of the resilience paradigm and the factors that contributed to its development in the field of security were analysed. A method for identifying and ranking critical risks (including stochastic and sporadic risks) was developed by applying the Bayesian approach, the Wald criterion, and a greedy algorithm that allows planning processing costs within a fixed budget constraint. A risk assessment model has been proposed that reflects the quantified risk appetite of an organisation and contains a ranked sequence of all the identified risks of an organisation. This allows for the handling of different types of risks within a single strategy. A method of chaos engineering has been developed, comprising two principal elements. The initial element entails the intentional and repeated stimulation of information systems' adaptation mechanisms. The second element comprises the identification of hitherto unidentified vulnerabilities and the assessment of potential restoration mechanisms for system functionality following a potential incident. A method is proposed for a comprehensive, longitudinal evaluation of the resilience of organisational and technical systems. A resilience index metric is proposed for the assessment of both the effectiveness of financial investments in security and resilience and the operational outcomes of these investments. A visual tool for prioritising risks in the context of resilience, in the form of a three-dimensional matrix capable of aggregating all types of risks, including stochastic and sporadic ones, has been proposed. Reorganisation of a critical segment of the infrastructure of the existing organisational and technical system based on the principles of ISO 27000 and Zero Trust. The solution of these tasks created the appropriate conditions for ensuring the resilience and trustworthiness of organisational and technical systems of all types and hierarchical levels by improving the ISMS and CIPS.

Keywords: resilience, information security systems, risk management, trustworthiness, adaptation