ВІДГУК

офіційного опонента, доктора технічних наук, професора, Корченко Анни Олександрівни на дисертаційну роботу Коробейнікова Федора Олександровича «Методи забезпечення резильєнтності організаційно-технічних систем», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

1. Актуальність теми дисертаційної роботи

Стабільна діяльність будь-якої організації залежить від збереження її критично важливих функцій, значною мірою підтримуваних інформаційними системами. Це можливо завдяки розробці та впровадженню методів, що підвищують не лише рівень безпеки, а й резильєнтність відповідних систем, інтегруючи їх у комплексні системи захисту інформації організації.

Це створює необхідність у розробці методологічної основи для ефективного впровадження концепцій і принципів резильєнтності на всіх рівнях їх застосування. На даний момент відсутні загальновизнані науковою спільнотою та перевірені практикою методики або рекомендації для підвищення резильєнтності на організаційно-технічному рівні, зокрема на рівні окремих організацій, а також на національному та міжнародному рівнях. Більше того, наявні фреймворки з підвищення резильєнтності навіть на рівні інформаційно-технічних систем не містять чітко визначених способів взаємодії з діючими системами управління інформаційною безпекою, розробленими відповідно до міжнародних стандартів ISO або NIST, а також механізмів інтеграції з комплексними системами захисту інформації (КСЗІ), що відповідають чинному законодавству України. Таким чином, тема дисертації Коробейнікова Ф. О., присвячена вирішенню важливого науково-прикладного завдання – розробці методів забезпечення резильєнтності організаційно-технічних систем на всіх рівнях ієрархії та інтеграції цих методів у СУІБ (КСЗІ) для їхнього вдосконалення, є актуальною.

2. Зв'язок дисертаційної роботи з науковими програмами, планами, темами

Тематика дисертаційної роботи і 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. No 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», Постановою Кабінету Міністрів України від 09.10.2020 р. No 1109 «Деякі питання об'єктів критичної інфраструктури», Постановою Кабінету Міністрів України від 16.05.2023 р. No 497 «Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», Стратегією національної безпеки України від 14.09.2020 р. No 392/2020, Стратегією кібербезпеки України від 26.08.2021 р. No 447/2021, Стратегією інформаційної безпеки від 28.12.2021 р. No 685/2021. Результати

дисертаційної роботи відображені у звіті 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).

3. Загальна оцінка змісту дисертаційної роботи

Структура дисертації відповідає встановленим вимогам для наукових досліджень. Дисертація складається з анотації, вступу, 4 розділів, загальних висновків, списку використаних джерел, 3 додатків.

У вступі надано загальну характеристику дисертаційної роботи, обґрунтовано актуальність та важливість теми дослідження, сформульовано його мету та задачі, окреслено об'єкт і предмет, визначено наукову новизну та практичну цінність. Також наведено відомості про апробацію, впровадження результатів роботи та структуру дисертації.

У першому розділі проведеноаналіз передумов виникнення парадигми резильєнтності, зокрема її появу, що пов'язано з потребою адаптації відкритих нелінійних дисипативних систем до загроз в умовах невизначеності та обмежених ресурсів. Розглянуто припущення, що розвиток парадигми резильєнтності у сфері безпеки зумовлений постійним зростанням складності та взаємозалежності організаційно-технічних систем, а також необхідністю забезпечення надійного функціонування їхніх критичних елементів у контексті глобалізації інформаційного середовища. Показано зв'язок парадигми резильєнтності з критичними ризиками, що виникають через стохастичні та спорадичні загрози. Досліджено взаємозв'язок між концепціями резильєнтності та безпеки в контексті парадигми трастоспроможності.

Проведено аналіз наявних обмежень в існуючих методиках забезпечення резильєнтності, а також зроблено порівняння відомих фреймворків та стандартів за певними характеристиками.

У другому розділі запропоновано моделі резильєнтної і нерезильєнтної поведінки системи у відповідь на миттєві і довготривалі руйнівні події, що мають високий рівень впливу на критичні функції. Описано взаємозв'язок етапів протидії реалізованим загрозам з цілями резильєнтності. Адаптація визначена етапом, який відрізняє резильєнтну поведінку системи від робастної, пластичної і колаптоїдної.

Показано, чому традиційні підходи до управління ризиками недієві в контексті резильєнтності. Актуалізовано необхідність адаптації та доповнення відомих методів аналізу та обробки ризиків новими підходами, орієнтованими на виявлення, ранжування та пріоритизацію ризиків, що впливають на резильєнтність критичних процесів. Для аналізу та пріоритизації критичних ризиків запропоновано використовувати модель, засновану на розрахунку очікуваної корисності опрацювання кожного ризику на одиницю витрат. Розроблені методи виокремлення, ранжування і пріоритизації критичних ризиків в контексті резильєнтності за допомогою теореми Баєса, жадібного алгоритму і критерія Вальда.

У третьому розділі побудовано онтологію високорівневих конструктів резильєнтності організаційно-технічних систем.

Виживання організаційно-технічної системи виокремлено як окремий клас онтології, що визначає цілі і задачі резильєнтності. Зроблено припущення, що в структурах, де одна організація може об'єднувати множину підрозділів або афілійованих організацій, проста агрегація резильєнтності окремих компонентів не дає адекватного розуміння резильєнтності системи в цілому.

Стратегія управління ризиками визначена як центральний елемент методики впровадження резильєнтності на рівні організаційно-технічних систем. Створено фреймворк управління критичними ризиками в контексті резильєнтності, який вміщує: виокремлення критичних процесів, визначення критичних ризиків для таких процесів, розробку і обчислення сценаріїв протидії критичним ризикам, ранжування ризиків, пріоритизацію ризиків та їхню обробку.

Для уточнення критичності експліцитних ризиків запропоновано використання Баєсівського метода, для вибору сценаріїв обробки і пріоритизації – критерію Вальда, для ранжування – жадібного алгоритму.

Для ефективного аналізу та визначення пріоритету (послідовності) обробки критичних ризиків у контексті резильєнтності пропоновано метод, що ґрунтується на розрахунку очікуваної корисності опрацювання кожного критичного ризику на одиницю витрат, створену шляхом інтеграції у стандартну двовимірну матрицю третього виміру – розміру бюджету на опрацювання ризиків.

Запропоновано використання методів хаос-інжинірингу в якості інструментів ітеративного забезпечення резильєнтних характеристик організаційно-технічних систем.

Запропоновано метод лонгітюдного аналізу стану резильєнтності, а також розроблена метрика «Індекс резильєнтності». Відповідний підхід передбачає, що для підвищення резильєнтності важливо не тільки зменшувати час простою, а й оптимізувати витрати на резильєнтність таким чином, щоб вони не мали негативного впливу на загальну фінансову ефективність організації. Високе значення показника Resilience index вказує на ефективність інвестицій в резильєнтність, успішне управління інцидентами і мінімальний вплив цих інцидентів на операційну діяльність.

У четвертому розділі на основі отриманих результатів представлено детальний опис процесу інтеграції розробленого методу управління критичними ризиками в існуючу систему захисту інформації організації, побудовану відповідно до стандарту ISO 27001.

Підтверджено правильність отриманих теоретичних результатів дослідження на прикладі реорганізації критичного сегмента інфраструктури реально діючої організаційно-технічної системи, яка спочатку ґрунтувалася на принципах моделі Zero Trust. Також продемонстровано доцільність застосування методів забезпечення резильєнтності організаційно-технічних систем на національному та міжнародному рівнях.

У висновках стисло сформульовано основні наукові та практичні результати дисертаційної роботи.

У додатках містяться свідотства про реєстрацію авторського права, акти впровадження результатів дисертаційної роботи та лістинг (початковий код) і фронтенд програмного застосунку.

Таким чином, усі положення, винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві. Дисертація написана науковою мовою та оформлена відповідно до існуючих нормативних документів.

4. Наукова новизна результатів дисертаційної роботи

1. 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;
2. 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;
3. 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;
4. 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;
5. Отримав подальший розвиток метод хаос-інжинірингу стосовно його застосування для забезпечення резильєнтності організаційно-технічних систем шляхом збільшення їхнього адаптаційного потенціалу;
6. 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.

5. Обґрунтованість висновків і одержаних результатів

Наукові положення, що захищаються автором роботи, висновки за результатами досліджень базуються на методологічній основі парадигми резильєнтності та теорії ризиків, системному аналізі сучасних фреймворків побудови резильєнтних систем, методі експертних оцінок. Для пояснення підґрунтя виникнення парадигми резильєнтності і її розвитку в безпековому домені були використані елементи теорії хаосу, теорії катастроф і теорії самоорганізації. Для розробки методів визначення критичних ризиків використовувались елементи теорії множин і теорії ймовірності. Для розробки методів пріоритизації обробки критичних ризиків, використовувались алгоритми оптимізації і елементи теорії ігор. Як засоби розв'язування поставлених задач використовувалось математичне та комп'ютерне моделювання.

Отримані результати не суперечать вимогам і настановам міждержавних (серії ДСТУ 24, ДСТУ 34) і міжнародних (NIST, ISO/IEC 27k) нормативних документів; мають широку апробацію на міжнародних і всеукраїнських наукових конференціях, а також експертизу технічних рішень, що підтверджено документами про впровадження та використання результатів дисертаційного дослідження.

6. Практична цінність одержаних результатів

Практична цінність отриманих результатів полягає в забезпеченні резильєнтності, як ключового елемента 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, комплексних систем захисту інформації тощо.

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). Впровадження результатів дисертаційної роботи підтверджується відповідними документами.

7. Рекомендації щодо використання наукових результатів

Отримані у дисертаційні роботі теоретичні та практичні результати можуть бути інтегровані в наявні СУІБ/СЗІ з метою забезпечення резильєнтності організаційно-технічних систем усіх типів і рівнів ієрархії – від об'єктів критичної інфраструктури до спільнот і міжнародних об'єднань.

8. Повнота викладення основних результатів дисертації

Основні результати дисертаційної роботи в повному обсязі відображені в 21-й науковій праці. Серед яких опубліковані статті у наукових виданнях, що входять до переліку фахових видань України з технічних наук та індексуються в міжнародних науково-метричних базах. Результати дисертаційного дослідження пройшли апробацію на багатьох всеукраїнських і міжнародних наукових конференціях.

9. Автореферат дисертації

Зміст автореферату в повному обсязі відображає основні положення дисертаційної роботи.

10.Зауваження до дисертаційної роботи

1. У другому пункті наукової новизни «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» не визначено її рівень, наприклад, «Вперше», «Удосконалено» або «Отримав подальший розвиток».

2. У четвертому пункті наукової новизни «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» не зазначено за рахунок чого досягається визначений ефект.

3. У п'ятому пункті наукової новизни «отримав подальший розвиток метод хаос-інжинірингу стосовно його застосування для забезпечення резильєнтності організаційно-технічних систем шляхом збільшення їхнього адаптаційного потенціалу» чітко не зазначено за рахунок чого досягається заявлений ефект.

4. У першому розділі (рисунок 1.4.1) висвітлені порівняння існуючих фреймворків та стандартів за певними характеристиками, але в тексті відповідного розділу не було розглянуто низку рішенн, таких як UK Gov, ICOR's, DHS, що зазначені на рисунку з відсутністю відповідного обґрунтування наявності тих чи інших характеристик, позначених «+» і «–».

5. У другому розділі дисертаційної роботи складно прослідковується диференціація фаз відновлення та адаптації: ці фази формально розділені в одних частинах роботи, але об'єднані в інших, іноді фаза адаптації підміняє фазу відновлення.

6. В тексті третього розділу дисертації, який описує формування онтології високорівневих конструктів резильєнтності організаційно-технічних систем, не визначено актора, який має затверджувати критичні функції таких систем.

7. В розділі 3.2 дисертаційної роботи немає пояснення, чому бюджет на опрацювання резильєнтних ризиків не враховує вартість відновлення інформаційних систем.

8. На сторінці 143 дисертаційної роботи вказано, що точки біфуркації можуть слугувати каталізаторами для переходу системи до нових станів, або атракторів. Слід зазначити, що перехід системою точки біфуркації не завжди гарантують перехід до нових станів, окрім того, перехід системи до нового атрактора може відбуватися не миттєво, а поступово.

9. З тексту розділу 4.2 дисертаційної роботи не зрозуміло, хто саме має аналізувати вихідні дані з десепшн-систем, сканерів вразливостей та антивірусів - користувачі, чи державні органи.

10. На рис. 4.2.2 дисертаційної роботи відображено, що ПЗ для розподілених обчислень, розподіленого зберігання інформації, екстрених оповіщень і активної протидії кібератакам має мати закритий вихідний код. Не зрозуміло, чому ПЗ із відкритим вихідним кодом не може бути застосовано для зазначених цілей.

Висновок

Розглядаючи роботу в цілому та незважаючи на вказані зауваження, вважаю, що загальна оцінка роботи є позитивною. Дисертаційна робота Коробейнікова Ф.О. «Методи забезпечення резильєнтності організаційно-технічних систем» є завершеною науковою працею, яка виконана здобувачем самостійно і відповідає принципам академічної доброчесності.

Робота містить наукові положення та нові науково обґрунтовані результати, одержані здобувачем особисто, які мають практичну та теоретичну цінність, і відповідає паспорту спеціальності 05.13.21 – системи захисту інформації.

Вважаю, що за актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю

висновків, новизною досліджень, значенням отриманих результатів для науки і практики дисертаційна робота задовольняє кваліфікаційним вимогам, які висуваються до робіт на здобуття наукового ступеня кандидата технічних наук, а її автор, Коробейніков Федір Олександрович, заслуговує на присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент
доктор технічних наук, професор,
професор кафедри
Безпеки інформації та телекомунікацій
Національного технічного університету
«Дніпровська політехніка» Анна КОРЧЕНКО

Підпис д.т.н., проф. Анни КОРЧЕНКО засвідчую.

Учений секретар Таїсія КАЛЮЖНА

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ДНІПРОВСЬКА ПОЛІТЕХНІКА» і.к. 02070743