ВІДГУК

офіційного опонента на дисертацію 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

Зростаюча залежність суспільства від сталості функціонування складних інформаційних систем виявила нагальну потребу в розвитку технологій, які не лише забезпечують механізми захисту таких систем в умовах дії різноманітних деструктивних впливів, але й надають таким системам властивість адаптуватися до непередбачуваних інцидентів та відновлюватися після їхніх проявів. Таку властивість систем визначають терміном «резильєнтність». Слід зазначити, що на поточний час в сфері захисту інформації та інформаційної безпеки немає методологій, фреймворків та стандартів, спрямованих безпосередньо на підвищення резильєнтності як власне самих систем захисті інформації, так і резильєнтності відповідних інформаційних систем. Що стосується забезпечення резильєнтності організаційно-технічних систем, складовою яких є відповідні інформаційні системи з їхніми відповідними ж системами управління інформаційною безпекою (СУІБ) та комплексними системами захисту інформації (КСЗІ), в останні роки світова наука та передова практика вже приділяє їм стрімко зростаючу увагу. Але поза увагою дослідників залишались аспекти впливу характеристик резильєнтності організаційно-технічних систем на досконалість систем управління інформаційною безпекою взагалі та комплексних систем захисту інформації зокрема. Саме тому, дослідження, спрямовані на вдосконалення СУІБ/КСЗІ шляхом забезпечення певного рівня резильєнтності для відповідних організаційно-технічних систем, до складу яких входять згадані СУІБ/КСЗІ, є актуальними і мають зрозумілу практичну цінність.

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

Актуальність тематики дисертаційної роботи підтверджується її гармонізованістю із завданнями, визначеними планами наукових досліджень Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, зокрема за темами «Математичні моделі резильєнтної поведінки динамічних систем» (0124U004637) та «Розроблення науково-обґрунтованих критеріїв та принципів побудови системи кіберзахисту об'єктів атомної енергетики» (0123U100909).

3. Загальна оцінка змісту дисертаційної роботи

Дисертація складається з анотації, вступу, 4 розділів, загальних висновків, списку використаних джерел, додатків. Загальний обсяг дисертації становить 218 сторінок, в тому числі 166 сторінок основного тексту, який включає 19 рисунків. Список використаних джерел нараховує 142 найменування.

Вступ. У вступі визначені об'єкт і предмет дослідження, обґрунтована актуальність, наведені формулювання основної мети та часткових завдань, скорочено подано переказ наукової новизни та практичної цінності, викладені загальні відомості про апробацію та впровадження результатів роботи, а також про структуру дисертації.

Перший розділ. Проаналізовано масив існуючих джерел наукової літератури за темою дослідження. На підставі аналізу визначено, що необхідність гарантування працездатності критичних функцій організаційно-технічних систем в умовах невизначеності безпекового середовища відповідних інформаційних систем зумовлює зростання уваги до резильєнтності, як властивості, яка здатна нівелювати ризики невизначеності, пов'язані зі зростанням складності і взаємопов'язаності інформаційних систем та асоційованих з ними систем управління інформаційною безпекою і комплексних систем захисту інформації. Автором запропоновано розглядати механізми забезпечення резильєнтності та безпеки організаційно-

технічних систем в контексті парадигми трастоспроможності, як методологічної платформи для вдосконалення СУІБ/КСЗІ.

Другий розділ присвячено дослідженню часових особливостей запропонованої автором циклічної моделі резильєнтної поведінки систем. Показано, що особливістю циклічного процесу еволюції однієї, окремо визначеної системи, що перебуває під дією послідовності подій впливу критичних інцидентів певного типу, є те, що рівень адаптаційного потенціалу системи, досягнутий на кінець кожної попередньої стадії циклу її еволюції, є тотожно рівним рівню адаптаційного потенціалу системи, з якого вона починає кожну наступну стадію циклу своєї еволюції. Це дало можливість автору визначити алгоритмізовану методику управління критичними ризиками, в основу якої покладено ідею ітеративного управління рівнем адаптаційного потенціалу. Для аналізу та пріоритизації критичних ризиків запропоновано використовувати оцінку очікуваної корисності опрацювання кожного ризику. Для виокремлення та ранжування критичних ризиків автор використовує оцінки, отримані ним на основі застосування теореми Байєса, жадібного алгоритму і критерію Вальда.

Третій розділ. В цьому розділі на основі побудованої онтології основних сутностей резильєнтності для складної системи показано, що задача формування визначеного рівня резильєнтність не може бути вирішена за рахунок довільного компонування складових частин системи. Тому на підставі методики управління критичними ризиками, розробленої в другому розділі дисертації, автором запропоновано визначати і здійснювати пріоритизація обробки певних виокремлених ризиків шляхом розрахунку очікуваної корисності опрацювання кожного з них. В якості візуального інструменту для управління всім спектром можливих ризиків організаційно-технічної системи, запропоновано використовувати тримірну матрицю ризиків, в якій присутні крім ймовірності та втрат ще й обсяги відповідних ресурсів. Особливістю є те, що ризики, які стосуються водночас інформаційної безпеки і резильєнтності, власне і утворюють множину критичних ризиків (тобто тих ризиків, які спричиняють критичні руйнування системи), а тому такі ризики мають розглядатися не лише в сфері уваги системи управління інформаційною безпеки, а в першу чергу, в сфері уваги системи забезпечення резильєнтності. З цією метою визначено і запропоновано використовувати спеціальний показник - Індекс_резильєнтності, який враховує не тільки фінансові інвестиції в резильєнтність, а й операційні результати цих інвестицій, а також якість управління інцидентами. В цьому ж розділі автор пропонує використовувати методи стрес-тестування (названі автором як хаос-інжиніринг) в якості інструменту забезпечення вихідних даних для ітеративного зростання рівня резильєнтності організаційно-технічних систем.

Четвертий розділ. В цьому розділі наведено інформацію про програмний застосунок, створений автором для автоматизації процесу управління критичними ризиками в контексті резильєнтності. Викладено результати перевірки теоретичних висновків та практичних напрацювань, отриманих в дисертаційній роботі, шляхом проведення натурного експерименту з реорганізації в контексті забезпечення резильєнтності критичного сегменту інфраструктури та відповідної СУІБ реально діючої організаційно-технічної системи. Надано детальний опис застосування методів забезпечення резильєнтності організаційно-технічних систем на національному і наднаціональному рівнях.

4. Новизна наукових результатів

1. Вперше показано неможливість інтеграції наявних нині фреймворків забезпечення резильєнтності в СУІБ/КСЗІ існуючих організаційно-технічних систем.

2. Вперше запропоновано визначати критичність ризиків резильєнтності на підставі упорядкування множини таких ризиків за показником питомої очікуваної корисності їх обробки (на одиницю витрат), що забезпечує можливість співставляти такі ризики з ризик-апетитом організації при визначенні вимог до подальшого формування відповідних СУІБ/КСЗІ.

3. Вперше онтологія сутності «резильєнтність» побудована з урахуванням високорівневих сутностей організаційно-технічних систем (наприклад, таких як «стратегія»), що дозволило формалізувати ролі цих сутностей в процесі забезпечення резильєнтності СУІБ/КСЗІ організаційно-технічних систем;

4. З метою забезпечення резильєнтності організаційно-технічної системи щодо різних типів ризиків вперше запропоновано застосовувати тривимірну матрицю ризиків, яка передбачає можливість обліку не лише розміру потенційного збитку та ймовірності реалізації такого потенційного збитку, а ще й ресурсів, необхідних для опрацювання відповідного ризику, що дозволяє конкретизувати вимогу врахування ризик-апетиту організації при формуванні відповідних СУІБ/КСЗІ.

5. Для формування ітеративного процесу забезпечення резильєнтності організаційно-технічних систем запропоновано застосовувати механізми стрес-тестування (які в роботі названі «метод хаос-інжинірингу») в якості засобу визначення певних «градієнтів» для адаптації СУІБ/КСЗІ організаційно-технічних систем в кожному циклі їхньої еволюції;

6. Вперше визначено показник резильєнтності (названий Resilience index) який дає можливість оцінювали операційні результати інвестицій в резильєнтність СУІБ/КСЗІ організаційно-технічних систем, а не лише вимірювати ефективність цих фінансових інвестицій.

5. Обґрунтованість висновків і одержаних результатів

Обґрунтованість наукових результатів, отриманих автором, не викликає сумнівів, оскільки вона обумовлена коректним інтерпретуванням положень сучасної теорія ризиків інформаційної безпеки в контексті резильєнтності, змістовним застосуванням елементів теорії множин і теорії ймовірності при розгляді граничних станів, в яких може перебувати система управління інформаційною безпекою, коли обсяг втрат організаційно-технічної системи стає критичним для виконання нею своїх основних функцій. Розробка онтології резильєнтності виконана на базі сучасної відкритої платформи моделювання онтологій Стенфордського університету Protégé, зареєстрована на цій платформі під окремим акаунтом і вже має схвальні відгуки серед користувачів.

6. Практична цінність одержаних результатів

Практична цінність одержаних результаті підтверджується офіційними документами про їх впровадження у діяльність Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Центру протидії кіберзагрозам, АТ «System Capital Management» та власне Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, а також додатково підтверджується наявністю свідоцтва про реєстрацію права інтелектуальної власності на відповідну комп'ютерну програму. Впровадження результатів дисертаційної роботи підтверджується відповідними документами.

7. Рекомендації щодо використання наукових результатів

Результати, отримані у дисертаційні роботі, можуть використовуватися для забезпечення резильєнтності організаційно-технічних систем всіх типів і рівнів ієрархії – від об'єктів критичної інфраструктури, до спільнот і міжнаціональних об'єднань.

8. Повнота викладення основних результатів дисертації

Результати дисертації опубліковані в 21 наукових працях, серед яких 16 публікацій – без співавторів. Основні наукові результати дисертації висвітлено у 8 статтях, які опубліковані у наукових виданнях, включених до переліку наукових фахових видань України, а також одна стаття - у періодичному науковому виданні інших держав, які входять до Організації економічного співробітництва та розвитку та/або Європейського Союзу, з наукового напряму, за яким підготовлено дисертацію. Крім того, ще одна праця здобувача опублікована у закордонному виданні з індексацією у базі Scopus (Q1). Загалом, перелік праць апробаційного характеру за темою дисертації нараховує 10 найменувань, в тому числі 8 – без співавторів.

9. Автореферат дисертації

Зміст автореферату повністю відображає основні положення дисертації.

10. Зауваження до дисертаційної роботи

1. Автор застосовує в своїй роботі хаос-інжиніринг на концептуальному рівні, хоча методи хаос-інжинірингу в цій дисертації не розкриті.

2. В розділі 3.2 дисертаційної роботи декларується, що "Хаос-інжиніринг - це суто експериментальна практика, на відміну від традиційного тестування або ж використання метрик", але немає пояснення, чому "в контексті хаос-інжинірингу традиційне тестування має негативну конотацію".

3. На сторінці 174 дисертації автор пропонує використовувати метрики Uptime, MTTR (Mean Time To Repair), MTTA (Mean Time To Acknowledge), и MTBF (Mean Time Between Failures) для високорівневого оцінювання стану резильєнтності, але з практичних міркувань використання метрик MTTR і MTTA виглядає надлишковим.

4. Назва розділу 4.2 дисертації «Моделювання застосування методики підвищення резильєнтності організаційно-технічних систем на національному та наднаціональному рівні» виглядає занадто глобалізованою.

5. Критерій "підвищення обізнаності персоналу", який згідно контролів ІБ, визначений як одним із найбільш вагомих (ISO 27k, A 8.2.2) не вказано як значущий критерій, що впливає на резильєнтність організаційно-технічної системи.

6. В дисертаційній роботі недостатньо чітко диференційовано вирази: «стохастичні ризики», «спорадичні ризики» і «HILP-ризики». Доцільно надати більш ясне визначення та опис кожного з вищенаведених виразів для підвищення академічної строгості та розуміння матеріалу.

Висновок

Незважаючи на вказані зауваження загальна оцінка роботи є позитивною. Роботу характеризує актуальність обраної теми, обґрунтованість наукових положень, висновків і рекомендацій, їх новизна і загальнонаціональне значення, повнота викладу в наукових публікаціях, зарахованих за темою дисертації, відсутність академічного плагіату. Дисертаційна робота Коробейнікова Ф.О. «Методи забезпечення резильєнтності організаційно-технічних систем» є завершеною науковою працею, що виконана на достатньо високому науковому рівні, і відповідає паспорту наукової спеціальності 05.13.21 – системи захисту інформації, затвердженому МОН. За своїм рівнем, обсягом і якістю досліджень дисертаційна робота задовольняє 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
професор кафедри комп'ютерних
систем, мереж та кібербезпеки
Національного університету
біоресурсів та природокористування
України, доктор технічних наук

Валерій ЛАХНО