ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора Ковальчук Л.В.
на дисертаційну роботу Гончара Сергія Феодосійовича
«Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури», поданої на здобуття наукового ступеня доктора технічних наук за спеціальністю
05.13.21 – «Системи захисту інформації»

Актуальність теми досліджень

Події останніх років в Україні і у світі показали нагальну необхідність забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури, особливо енергетичного сектору. Забезпечення кібербезпеки об'єкту критичної інфраструктури, у тому числі енергетичного сектору, досягається створенням системи управління інформаційною безпекою або створенням комплексної системи захисту інформації, одним з основних етапів побудови яких являється оцінювання ризику.

Оцінювання ризику кібербезпеки здійснюється з достатньою точністю, як правило, на підставі статистичних даних кіберінцидентів за певний проміжок часу. Разом з тим, по цілому ряду ризиків, особливо стосовно об'єктів критичної інфраструктури, такі дані відсутні, величина збитків занижена.

Існуючі підходи до визначення поняття ризиків та методи їх оцінювання недостатньо повно описують це поняття, не враховують суб'єктивний ризик, що ускладнює коректне його оцінювання. Невирішеним залишається питання, пов'язане із можливістю розрахунку суми ризиків, що дало би можливість здійснення кількісного оцінювання ризику у цілому, врахування при оцінюванні ризику людського чиннику, що являється надзвичайно актуальним для об'єктів критичної інфраструктури, у тому числі енергетичного сектору.

Відповідно до зазначеного, в дисертаційній роботі Гончара С.Ф. вирішується науково-прикладна проблема, пов'язана з розробкою методології оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури, орієнтованої на розроблення і використання

51.11/02
від 20.03.2020

відповідних методів розрахунку суми ризиків та обчислення комплексного ризику. Отже, в цілому, вищевикладене свідчить про актуальність цієї дисертаційної роботи.

Варто відзначити, що тема дисертаційних досліджень безпосередньо пов'язана з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014–2018 роки», Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017р., Рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», Постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави», Стратегією національної безпеки України від 26 травня 2015 р. №287/2015, Стратегією кібербезпеки України від 15 березня 2016 р. №96/2016, Доктриною інформаційної безпеки України від 25 лютого 2017р. №47/2017.

Наукова новизна результатів дисертації

Основними науковими результатами дисертаційної роботи є:

Удосконалення структурної моделі взаємодії елементів інформаційних систем об'єктів критичної інфраструктури, яка використовується при обчисленні суми ризиків об'єктивної та суб'єктивної складових на другому на третьому етапі реалізації методології оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Зазначена модель дозволяє розробити модель порушника даної інформаційної системи з урахуванням кіберзагроз, об'єктами яких є адміністратор, користувачі, технічний персонал.

Удосконалення методу визначення актуальності загрози кібербезпеки інформаційної системи об'єкту критичної інфраструктури, який використовується при обчисленні суми ризиків об'єктивної та суб'єктивної складових на другому на третьому етапі реалізації методології оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Зазначений метод дозволяє розробити модель загроз даної інформаційної системи з урахуванням кіберзагроз, об'єктами яких є адміністратор, користувачі, технічний персонал.

Розроблення методу для обчислення сумарного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури, які використовуються при обчисленні суми ризиків об'єктивної та суб'єктивної складових на другому на третьому етапі реалізації методології оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Зазначені методи дозволяють розраховувати суму визначеної множини ризиків, загальні наслідки та ймовірність їх реалізації.

Розроблення векторної моделі та моделі комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури, які використовуються в методі обчислення комплексного ризику на четвертому етапі реалізації методології оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Зазначені моделі дозволяють здійснювати векторні операції над векторами ризиків.

Розроблення методу обчислення комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури, який використовується при обчисленні суми ризиків об'єктивної та суб'єктивної складових на четвертому етапі реалізації методології оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Зазначений метод дозволяє здійснювати оцінювання зазначених ризиків з урахуванням величини впливу людського чиннику.

Розроблення методології оцінювання ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури, яка

використовується при побудові апаратно-програмного комплексу оцінки та аналізу ризику. Зазначена методологія дозволяє забезпечити підтримку створення обчислювальних систем для автоматизації процесу оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

Розроблення структурних моделей обчислювальних систем для розрахунку суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури, які використовуються при побудові апаратно-програмних комплексів розрахунку сумарного ризику та комплексного ризику. Зазначені моделі дозволяють автоматизувати процес розрахунку сумарного ризику та обчислення комплексного ризику з урахуванням величин об'єктивної та суб'єктивної складових.

Обґрунтованість та достовірність наукових положень

Основні наукові результати та положення, викладені в роботі, є обґрунтованими та достовірними, що обумовлюється коректністю застосування методів досліджень для досягнення поставленої у дисертаційній роботі мети. Це підтверджується відсутністю принципових помилок, результатами експериментів і впровадженням результатів.

Практична цінність

Основними практичними результатами дисертаційної роботи є:

– розроблено алгоритмічне забезпечення на основі запропонованого структурного рішення обчислювальної системи «Калькулятор ризиків» для реалізації відповідного програмного засобу розрахунку суми ризиків, що дозволяє здійснювати автоматизований розрахунок наслідків від дії сумісних подій, з урахуванням показників, таких як ймовірність подій, що призводять до наслідків, та величина цих наслідків;

– розроблено алгоритмічне забезпечення на основі запропонованого структурного рішення обчислювальної системи «Калькулятор комплексного ризику» для реалізації відповідного програмного

засобу розрахунку суми ризиків, що дозволяє здійснювати автоматизований розрахунок повного ризику, з урахуванням об'єктивної та суб'єктивної його складових, з використанням теорії векторної алгебри та комплексних чисел;

– на основі запропонованого алгоритму розроблено програмний застосунок, що використовує запропоновані методи та здійснює оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

Публікація та апробація автором результатів дисертаційних досліджень

Результати дисертаційних досліджень, які виносяться на захист, опубліковані автором у 1-й монографії, 2-х наукових статтях, що входять до бази даних Scopus, 10-ти наукових статтях у наукових виданнях, що входять до інших міжнародних наукометричних баз даних та 14-и наукових статтях у вітчизняних фахових наукових журналах та збірниках наукових праць. Апробація цих результатів відбулася на 18 конференціях.

Зміст дисертаційної роботи

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

У першому розділі проведено аналіз вітчизняної та зарубіжної наукової літератури за темою дисертаційної роботи. Досліджено національне нормативно-правове забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури та проаналізовано сучасні методи та методології оцінювання ризиків кібербезпеки, у тому числі об'єктів критичної інфраструктури.

У другому розділі удосконалено структурну модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури, а також

удосконалено метод визначення актуальності загрози кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

У третьому розділі розроблено методи розрахунку суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

У четвертому розділі розроблено векторну модель, модель комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури та метод визначення комплексного ризику.

У п'ятому розділі запропонована методологія оцінювання суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури та розроблені структурні рішення обчислювальних систем.

У шостому розділі приведені експериментальні дослідження програмного застосунку систем оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури на основі комп'ютерної реалізації розроблених методів.

Відповідність автореферату дисертаційній роботі

Зміст автореферату повністю відображає зміст дисертаційної роботи та розкриває її суть.

Відповідність паспорту спеціальності

Основні наукові та практичні результати роботи пов'язані із оцінювання ризиків безпеки ресурсів інформаційних систем, як етапу при впровадження комплексної системи захисту інформації, відповідають паспорту спеціальності 05.13.21 - «Системи захисту інформації», а саме напрямкам досліджень «Теоретичні, методологічні, технічні, технологічні й організаційні основи створення комплексних систем захисту інформації (СЗІ), зокрема інформації, що зберігається, оброблюється і передається в комп'ютерних системах і мережах» та «Організація, архітектура, методологія проектування, технологія функціонування СЗІ».

Зауваження до змісту дисертації:

1. В розділі 2 недостатньо зрозумілим є вибір експертного методу для визначення імовірності реалізації загрози кібербезпеки.

2. Удосконалення структурної моделі взаємодії елементів інформаційної системи об'єкту критичної інфраструктури та методу визначення актуальності загрози кібербезпеки порівняно з їх типовими варіантами потребує більш чіткого обґрунтування.

3. Формули, в яких обчислюється імовірності різних подій (наприклад, реалізації загроз), містять деякі некоректності, в деяких випадках навіть суттєві.

4. Моделі, визначені у дисертації (розділ 3), не завжди коректно описані. Крім того, недостатньо обґрунтована адекватність цих моделей.

5. Викладення сутності суб'єктивного ризику при змістовному інтерпретуванні комплексного ризику в розділі 4 (стор. 191-198) є занадто ускладненим для розуміння, зокрема і приклад його змістовної інтерпретації у залежності від значення φ.

6. У оглядових розділах дисертації, у аналізі іноземних робіт, переклад виконано не дуже добре. Особливо це стосується першого параграфу другого розділу, меншою мірою інших розділів.

Дані недоліки не ставлять під сумнів основні наукові та практичні результати дисертаційної роботи і суттєво не впливають на її загальну позитивну оцінку.

Висновок

У дисертаційній роботі «Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури» Гончара Сергія Феодосійовича розв'язано важливу науково-прикладну проблему щодо розробки відповідної методології оцінювання ризиків. Дисертація є завершеною науково-дослідною роботою. За актуальністю вибраної теми,

достовірністю і обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики дисертаційна робота відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 № 567, а її автор - Гончар Сергій Феодосійович заслуговує присудження йому наукового ступеня доктора технічних наук за спеціальністю 05.13.21 - «Системи захисту інформації».

Офіційний опонент
професор СК № 22
Академії зовнішньої розвідки України
доктор технічних наук, професор Людмила КОВАЛЬЧУК
20. 03. 2020р.

Підпис Л.В. Ковальчук засвідчую

Т.в.п. ректора
Академії зовнішньої розвідки України
кандидат технічних наук Дмитро ГРИЩАК