Голові спеціалізованої вченої ради Д 26.255.01
Інститут телекомунікацій і глобального
інформаційного простору НАН України

03186, м. Київ, бул. Чоколівський, 13

ВІДГУК

офіційного опонента – завідувача спеціальної кафедри № 5 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" доктора технічних наук, доцента Субача Ігоря Юрійовича на дисертаційну роботу Кузьменко Лідії Володимирівни на тему: "Інформаційна технологія для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури", подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 - інформаційні технології

Актуальність теми дисертації

У теперішній час, до автоматизованих систем (АС), включених у контури управління інформаційними або технологічними процесами (ІТП) об'єктів критичної інфраструктури (ОКІ), а також інформаційними ресурсами (ІР), які в умовах кібернетичних втручань і загроз забезпечують необхідні послуги та сервіси ОКІ, висуваються нові вимоги щодо їхнього гарантоздатного функціонування.

Проте, незважаючи на нормативно-правову урегульованість питань створення інформаційно-телекомунікаційних систем для потреб ОКІ та оцінювання стану їх захищеності від впливу шкідливого програмного забезпечення, на сьогодні спостерігається недостатність наукових досліджень щодо створення для потреб ОКІ новітніх гарантоздатних АСУ, а також недосконаліть методів, моделей і методик їх побудови.

Тому дослідження, що спрямовані на розроблення теоретичних і прикладних засад побудови інформаційних технологій для створення

перспективних гарантоздатних (ПГ) автоматизованих систем управління (АСУ) об'єктами критичної інфраструктури, а також визначення впливу на процеси функціонування таких систем антропогенними і техногенними втручаннями є **актуальними**.

Значення дисертації для науки й практики

Наукова новизна одержаних результатів визначається наступним:

1. Уперше розроблено метод визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКІ, впровадження якого шляхом реалізації семантичної моделі протиборства системи захисту ПГ АСУ ОКІ з атакуючою стороною, процедури детектування та відновлення даних і моделі оцінки стану захищеності такої системи від загроз порушення цілісності, конфіденційності та доступності (ЦКД) дозволяє відслідкувати вплив шкідливих програм, фальшивого програмного забезпечення (ПЗ) і злоякісних шифруючих кодів на ІТП в АСУ ОКІ, відшукати вразливості та/або істинні значення ключів, застосованих для шифрування даних в ПГ АСУ ОКІ, оцінити стан захищеності сформованого прототипу варіанту побудови ПГ АСУ ОКІ від впливу кібератак та убезпечити АСУ ОКІ від НСД до її ресурсів та інформації, що в ній циркулює.

2. Удосконалено метод формування типового варіанту побудови перспективної гарантоздатної АСУ, впровадження якого за рахунок розробки процедури вибору прототипу топології мережевої інфраструктури, процедури вибору типового автоматизованого робочого місця (АРМ) раціональної конфігурації, процедури раціонального вибору ПЗ прикладного рівня (ПР) та процедури вибору типового варіанту побудови ПГ АСУ ОКІ дозволяє, на відміну від існуючих, організувати доступ до мережі та надання обчислювальних ресурсів і послуг абонентам для спільного використання ними власних і зовнішніх ІР, забезпечити доступ користувачам до таких ІР, керування їх обміном, передачею та машинною переробкою, автоматизувати процеси пошуку і збору інформації у зовнішніх і внутрішніх джерелах, її реєстрації, трансформації та функціональної обробки, а також процеси захисту ІР в АСУ від кібернетичних загроз.

Практичне значення отриманих результатів полягає в тому, що вони дозволили розробити прикладні засади побудови інформаційної технології для створення ПГ АСУ ОКІ, впровадження якої забезпечує гарантоване надання абонентам необхідних послуг та сервісів, яким у заданих режимах і умовах застосування з урахуванням стану захищеності таких систем від загроз порушення ЦКД можливо виправдано довіряти.

Практична цінність дисертаційної роботи полягає у тому, що отримані результати дозволяють:

1. Підвищити ефективність дій осіб, відповідальних за забезпечення безпеки ПГ АСУ ОКІ (за рахунок оперативного визначення найбільш значимих загроз та своєчасного реагування на стан захищеності АСУ від загроз порушення ЦКД) на 12%.

2. Скоротити час на прийняття виважених управлінських рішень щодо побудови ПГ АСУ ОКІ з відповідним програмно-апаратним засобом (ПАЗ) та їх впровадження не менше ніж на 20%.

Практична цінність роботи, також, підтверджується актами впровадження основних результатів дослідження, що додаються до дисертаційної роботи.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, їхня достовірність і новизна

Обґрунтованість наукових результатів, висновків та рекомендацій забезпечена коректним використанням апробованого математичного апарату, повнотою врахування початкових даних та визначенням і дотриманням доцільних обмежень та припущень.

Достовірність наукових положень підтверджена результатами апробації процедур, які було розроблено у процесі побудови інформаційної технології для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури.

Висновки та рекомендації щодо наукового та практичного використання здобутих результатів

Результати дисертаційної роботи доцільно використовувати в науково-дослідних інститутах і конструкторських бюро для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури.

Повнота викладу в опублікованих працях

Основні положення та результати дисертаційної роботи достатньо повно опубліковані у 21 науковій праці, з яких: 2 публікації – розділ колективної монографії; 12 – у вітчизняних фахових наукових виданнях, які входять до міжнародних наукометричних баз даних (*Index Copernicus*, *CORE*, *BASE*, *ResearchBib*, *PKP*, тощо); 3 – у міжнародних рецензованих виданнях, що входять до баз даних *Scopus* та *Web of Science* та 4 тези доповідей у публікаціях матеріалів міжнародних та вітчизняних наукових конференцій.

Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення

За своїм змістом дисертація Кузьменко Л.В. відповідає діючим вимогам щодо дисертацій на здобуття наукового ступеня кандидата наук і являє собою наукову працю, яка містить сукупність наукових положень та результатів, виставлених автором для публічного захисту, має внутрішню єдність і свідчить про особистий внесок автора у науку.

Оформлення дисертації та автореферату відповідає вимогам Державних стандартів України. Текст дисертації та автореферату написані грамотною технічною мовою, ясно та зрозуміло.

У *вступі* обґрунтовано актуальність теми дисертації, сформульовано мету, об'єкт, предмет, завдання дослідження, наукову новизну одержаних результатів, практичне значення результатів, зв'язок роботи з науковими програмами, планами та темами досліджень. Визначено особистий внесок здобувача, відомості про апробацію результатів роботи, публікації.

У *першому розділі* дисертації: сформовано перелік об'єктів, які потенційно можуть бути віднесенеми до критичної інфраструктури; обґрунтовано, що під гарантоздатністю АСУ ОКІ слід розуміти їх комплексну властивість надавати необхідні послуги та/або сервіси, яким в заданих режимах і умовах застосування можна виправдано довіряти; досліджено множину загроз для АСУ ОКІ, а також уразливості програмно-апаратних засобів АСУ ОКІ, що впливають на її функціонування; проведено оцінку низки математичних моделей побудованих на розподілі Вейбулла, використання яких дозволяє ефективно проводити налаштування і випробування ПАЗ, оцінювати та прогнозувати надійність таких систем при їх проектуванні та експлуатації, а також стисло розглянуто критерії, застосування яких дозволяє об'єктивно оцінити якість функціонування АСУ ОКІ у цілому; сформовано основні принципи забезпечення технологічної безпеки ПАЗ АСУ ОКІ на різних етапах їх життєвого циклу.

У *другому розділі* дисертації запропоновано метод формування типового варіанту побудови перспективної гарантоздатної АСУ ОКІ.

Розглянуто процедури, які входять до запропонованого методу та складають його чотири етапи: вибір прототипу топології мережевої інфраструктури перспективної гарантоздатної АСУ ОКІ; вибір типового АРМ раціональної конфігурації перспективної гарантоздатної АСУ ОКІ; раціональний вибір програмних засобів прикладного рівня перспективної гарантоздатної АСУ ОКІ; вибір типового варіанту побудови перспективної гарантоздатної АСУ ОКІ.

У *третьому розділі* дисертації описано метод визначення впливу загроз на процеси функціонування ПГ АСУ ОКІ, який поєднує в собі семантичну модель протиборства системи захисту ПГ АСУ ОКІ з атакуючою стороною, процедуру детектування та відновлення даних в системі та модель оцінки стану захищеності системи від загроз порушення ЦКД, які, у свою чергу, ґрунтуються на частковій моделі загроз безпеці ПГ АСУ ОКІ.

Четвертий розділ дисертації присвячений дослідженню процедур, розроблених у процесі побудови інформаційної технології для створення ПГ АСУ ОКІ: вибору прототипу мережевої інфраструктури ПГ АСУ ОКІ; вибору типового АРМ раціональної конфігурації ПГ АСУ ОКІ; раціонального вибору ПЗ прикладного рівня ПГ АСУ ОКІ; вибору типового варіанту побудови ПГ АСУ ОКІ; детектування та відновлення даних в ПГ АСУ ОКІ.

У висновках наводяться основні наукові та практичні результати.

Отже поставлені наукові завдання в повному обсязі вирішені та наведені в дисертаційній роботі. Вищенаведене дозволяє зробити висновок про відповідність назви дисертації її змісту.

Відповідність змісту автореферату основним положенням дисертації

Зміст автореферату повністю відображає основні результати досліджень, які подані в дисертації. В авторефераті в повній мірі викладені усі наукові положення та результати з достатньою детальністю.

Недоліки та зауваження

1. У першому розділі роботи під час аналізу чинного нормативно-правового забезпечення здобувач, на мій погляд, досить однобоко розглядає його сучасний стан. Як випливає з результатів аналізу основний акцент поставлено на розгляді національного законодавства у сфері захисту інформації. Проте питання, що стосуються створення об'єктів критичної інфраструктури, а також віднесення певних об'єктів до об'єктів критичної інфраструктури, залишились поза увагою.

2. У розділі 2 дисертаційної роботи недостатньо обґрунтованим є застосування саме експертних методів для реалізації процедур вибору прототипу топології мережевої інфраструктури та типового варіанту побудови перспективної гарантоздатної АСУ ОКІ, а також процедури раціонального вибору програмних засобів прикладного рівня для забезпечення функціонування системи.

3. Моделі протиборства системи захисту перспективної гарантоздатної АСУ ОКІ з атакуючою стороною та оцінки стану захищеності такої системи

від загроз порушення цілісності, конфіденційності та доступності, які визначені у розділі 3 дисертації, описані не зовсім повно і потребують подальшого дослідження та обґрунтування. Зокрема, потребує додаткового розкриття метод розрахунку функції прийняття рішення про атаку в умовах часових обмежень, які задані виразом (3.4).

4. Для оцінки стану захищеності обраного варіанту побудови перспективної гарантоздатної АСУ ОКІ від стороннього кібернетичного впливу та загроз (розділ 3 дисертації), автором запропоновано комплексний показник (вираз 3.23). Цілком доцільно було б оцінити ефективність застосування розробленої інформаційної технології за цим показником.

5. На мій погляд, вільне оперування та ототожнення здобувачем таких споріднених за суттю категорій, як "інформаційна безпека" та "безпека інформації" не дозволили, як наслідок, строго формалізувати подану у розділі 3 та додатку А до дисертації модель загроз АСУ ОКІ. Очевидно, що в контексті чинної нормативно-правової бази категорія "інформаційна безпека" стосується захищеності людини, суспільства, держави та використовуваних ними АСУ ОКІ від деструктивних інформаційних впливів, а "безпека інформації" розглядається в контексті захищеності АСУ ОКІ від порушення її базових властивостей – цілісності, конфіденційності та доступності.

6. Експериментальні дослідження, результати яких розкрито у розділі 4 дисертаційної роботи, повинні бути оформлені більш строго, як того вимагає теорія планування та оформлення експерименту. Додержання таких вимог зробило б більш зрозумілим зв'язок між метою експерименту, його завданнями, одержаними результатами та способами їх оброблення. При цьому слід відмітити, що ознаки планування експерименту та його результат представлені в роботі, але не структуровані.

7. Тексти дисертації та автореферату містять велику кількість скорочень та абревіатур, що певною мірою ускладнює загальний процес розуміння та оцінки результатів роботи.

Проте, зазначені недоліки не знижують ступінь наукової новизни та практичного значення одержаних в дисертації наукових результатів і, відповідно, позитивну оцінку роботи у цілому.

Висновки

Дисертаційна робота Кузьменко Лідії Володимирівни є завершеною актуальною науковою працею, що має значну наукову та практичну цінність у розробленні теоретичних і прикладних засад побудови інформаційної

технології для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури, а також визначення впливу на процеси функціонування таких систем антропогенних і техногенних втручань та загроз.

За глибиною теоретичного обґрунтування та практичної значущості дисертація відповідає вимогам п.п 9, 11, 12, 13 "Порядку присудження наукових ступенів", затвердженого постановою КМУ №567 від 24.07.2013 р. (зі змінами, внесеними згідно з Постановами КМУ №656 від 19.08.2015., №1159 від 30.12.2015 р., та №567 від 27.07.2016 р.), а її автор, Кузьменко Лідія Володимирівна, заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 - інформаційні технології.

Офіційний опонент
Завідувач спеціальної кафедри № 5
Інституту спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
доктор технічних наук, доцент І.Ю. Субач
«15» лютого 2021 року

Підпис Субача І.Ю. засвідчую.
Заступник начальника
Інституту спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
(з наукової роботи)

кандидат технічних наук, доцент С.М. Конюшок