**ВІДГУК**

офіційного опонента

на дисертаційну роботу *Кузьменко Лідії Володимирівни*

«Інформаційна технологія для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури», представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології».

**Актуальність теми дослідження.** Основним трендом сучасного суспільства є активне впровадження цифрових інформаційних технологій у всі сфери життя. Експерти фінансового ринку прогнозують динамічне зростання цифрової економіки, сфери цифрових послуг і, як наслідок, зростання залежності виробничих, технологічних, управлінських, безпекових та інших процесів від інформаційних технологій. Стає очевидним, що такий стан справ вимагатиме суттєвої трансформації інформаційно-телекомунікаційної індустрії. Перш за все, це стосуватиметься систем управління інформаційними та технологічними процесами об'єктів критичної інфраструктури (ОКІ), а також інформаційними ресурсами, які в умовах кібернетичних втручань і загроз забезпечують необхідні послуги та сервіси. Негативними наслідками такої трансформації може бути виникнення нових ризиків для безпеки інформаційно-технологічних процесів та інформаційних ресурсів, що й формує потребу в побудові і впровадженні сучасних інформаційних технологій для створення перспективних гарантоздатних (ПГ) автоматизованих систем управління (АСУ), захищених від впливу антропогенних і техногенних загроз.

Незважаючи на розроблену нормативно-правову базу з питань створення інформаційно-телекомунікаційних систем для потреб ОКІ та оцінювання стану їх захищеності від впливу шкідливих програм, неліцензійного ПЗ і шифруючих кодів, на сьогодні є низка проблем, які потребують досконаліших розв'язків: дублювання інформаційних потоків та накопичення навантаження на засоби зберігання інформації; технологічна нерівність ОКІ у сфері інформаційних, телекомунікаційних та інших технологій; недостатність наукових досліджень щодо створення новітніх захищених АСУ, а також інколи повна відсутність рішень щодо специфіки їх функціонування; недосконалість методів, моделей і методик розв'язання відповідних завдань.

Такий стан справ визначає актуальність дисертаційної роботи Л. В. Кузьменко, пов'язаної з проблемою побудови перспективних гарантоздатних

АСУ та визначення впливу на процеси функціонування таких систем антропогенних і техногенних втручань та загроз.

**Ступінь обґрунтованості наукових положень, висновків та рекомендацій.** Основні теоретичні положення дисертації отримані шляхом коректного застосування методів прийняття рішень в умовах невизначеності, експертних методів оцінювання, методів лінійного програмування, функціонально-вартісного та кластерного аналізу тощо. Відповідність та обґрунтованість результатів досліджень підтверджуються граничними переходами до відомих окремих випадків, отриманих в рамках інших теоретичних підходів; впровадженням результатів досліджень; достатньою кількістю публікацій у виданнях, що входять до переліку фахових видань з технічних наук в Україні і за кордоном; виступами на наукових конференціях національного та міжнародного рівня.

Все це свідчить про високий ступінь достовірності та обґрунтованості результатів дисертації.

**Структура, обсяг роботи.** Дисертація загальним обсягом 181 стор. складається із вступу, чотирьох розділів, загальних висновків, списку використаних джерел до кожного розділу (загалом 150 найменувань) і додатків, у які винесені, зокрема, документи, що підтверджують впровадження результатів роботи.

**Характеристика роботи, новизна розроблених наукових положень.**

У вступі автором подано загальну характеристику дисертації, визначено актуальність теми, сформульовано об'єкт, предмет і мету дослідження, окреслено коло наукових та прикладних задач, розв'язання яких забезпечує реалізацію мети роботи, показана наукова новизна та практична цінність роботи. Наведено публікації автора за темою дисертації.

В першому розділі дисертації авторкою на основі огляду літературних джерел сформовано перелік об'єктів, які потенційно можуть бути віднесеними до критичної інфраструктури, обґрунтовано поняття гарантоздатності АСУ, досліджено множину загроз для АСУ ОКІ, а також вразливості програмно-апаратних засобів (ПАЗ) та сформульовано основні принципи забезпечення технологічної безпеки ПАЗ АСУ ОКІ на різних етапах їх життєвого циклу. Це дозволило сформувати завдання і вибудувати структурно-логічну схему дослідження.

Другий розділ роботи присвячений розробленню методу формування типового варіанту побудови ПГ АСУ ОКІ. Метод поєднує такі

взаємодоповнюючі процедури, як вибір прототипу топології мережевої інфраструктури (МІ), вибір типового АРМ раціональної конфігурації, раціональний вибір ПЗ прикладного рівня та вибір типового варіанту побудови ПГ АСУ ОКІ.

Комплексним рішенням в межах розробленого методу є процедура вибору раціонального варіанту побудови ПГ АСУ ОКІ. Її застосування дозволить ПГ АСУ ОКІ, як результат, якісно задовольняти потреби користувачів у поданні повної і достовірної інформації та її ефективної обробки, а також гарантовано надавати необхідні сервіси та виконувати потрібні функції в заданих режимах і умовах застосування.

Третій розділ роботи описує метод визначення впливу загроз на процеси функціонування ПГ АСУ ОКІ. Метод 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, які ґрунтуються на частковій моделі загроз безпеці ПГ АСУ ОКІ.

Четвертий розділ присвячено дослідженню процедур, розроблених в процесі побудови інформаційної технології для створення ПГ АСУ ОКІ. У розділі наведено результати експериментальних досліджень з вивчення процесів функціонування альтернативних топологій мереж та результати обчислення їх глобальних пріоритетів. Показано, що найбільш раціональним варіантом при створенні перспективної гарантоздатної АСУ ОКІ є топологія типу «зірка». Також наведені експериментальні дані вибору раціональної конфігурації автоматизованого робочого місця, якості його ПЗ. Проведено експериментальне дослідження процесу детектування та відновлення даних в ПГ АСУ ОКІ з використанням кластерного аналізу.

У додатки винесено формалізовану модель загроз для об'єктів критичної інфраструктури, лістинги розроблених авторкою програм та документи впровадження результатів дисертаційних досліджень.

**Основні наукові результати досліджень і новизна дисертації.** У дисертаційній роботі вирішена науково-прикладна задача розроблення теоретичних і прикладних засад побудови інформаційної технології та методів 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.

Основними науковими результатами дисертаційних досліджень є:

метод визначення впливу загроз на процеси функціонування перспективних гарантоздатних АСУ ОКІ, впровадження якого дозволяє, на відміну від існуючих, відслідкувати вплив шкідливих програм, фальшивого ПЗ і шифруючих кодів в АСУ ОКІ, шукати вразливості та/або істинні значення ключів, застосованих для шифрування даних, 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;

метод формування типового варіанту побудови перспективної гарантоздатної АСУ, впровадження якого дозволяє організувати доступ до мережі та надання обчислювальних ресурсів і послуг абонентам для спільного використання ними власних і зовнішніх інформаційних ресурсів, забезпечити доступ користувачам до них, керування їх обміном, передачею та обробкою, автоматизувати процеси пошуку та збору інформації у зовнішніх і внутрішніх джерелах, її реєстрації, трансформації та функціональної обробки, а також процеси захисту інформаційних ресурсів в АСУ від кібернетичних загроз.

Тематика виконання наукових досліджень відповідає паспорту спеціальності 05.13.06 – «Інформаційні технології».

**Практичне значення отриманих результатів.** Запропоновані автором методи та інформаційні технології для створення ПГ АСУ ОКІ забезпечують підвищення ефективності дій осіб, відповідальних за забезпечення безпеки гарантоздатних АСУ ОКІ за рахунок оперативного визначення найбільш значимих загроз серед множини можливих та скороченню часу на прийняття виважених управлінських рішень щодо побудови гарантоздатних АСУ ОКІ.

Практичне значення результатів підтверджується також впровадженням результатів досліджень в Інституті проблем математичних машин і систем НАН України при дослідженні проблеми побудови різнорідних інформаційних систем ситуаційних центрів сектору безпеки і оборони та обміну даними між ними, Національному центрі управління та випробувань космічних засобів, НЕК «УкрЕнерго», Азербайджанському Технічному Університеті, що підтверджено відповідними актами впровадження.

**Рекомендації щодо використання результатів дисертації.** Коло практичних застосувань результатів роботи не обмежується розглянутими у ній впровадженням. Основні результати дисертації можуть бути використані для побудови АСУ в органах державної влади та спеціальних службах, таких

як Державна служба України з питань надзвичайних ситуацій, Служба безпеки України тощо.

**Зв'язок роботи з науковими програмами.** Дисертаційна робота та отримані результати пов'язані з вирішенням науково-технічних задач, сформульованих в Стратегії національної безпеки України (Указ Президента України № 287/2015 від 26.05.2015 р.), «Порядку формування переліку ІТС об'єктів критичної інфраструктури держави» (Постанова КМ України № 518 від 19.06.2019 р.), «Основних наукових напрямах та найважливіших проблемах фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014–2018 роки». Дисертаційна робота виконана у рамках таких науково-дослідних робіт: «Розробка інформаційного інструментарію еколого-економічного прогнозування надзвичайних ситуацій техногенного та природного характеру з метою захисту об'єктів критичної інфраструктури» (№ д.р. 0116U000797), «Базис-Наука» (№ д.р. 0119U000042дс) та «Розробка науково-технічних пропозицій з організації віддаленого управління станціями оптико-електронних спостережень типу 1 та типу 2» (№ д.р. 0120U105420), які виконувались в ІТГІП НАН України, ІПММС НАН України і Національному центрі управління та випробувань космічних засобів України.

**Публікація та апробація результатів дисертації.** Кількість і рівень публікацій за темою дисертації відповідають вимогам МОН України для здобувачів наукового ступеня кандидата наук. Основні положення і результати дисертації відображені у 21 науковій публікації, з яких: 3 публікації проіндексовані у міжнародних наукометричних базах Scopus та Web of Science, 2 – у наукових виданнях інших держав, 12 - входять у перелік фахових видань, які рекомендовано МОН України. Окрім цього, авторка має 4 тези доповідей на науково-практичних конференціях. Без співавторів опубліковано 1 наукову статтю і 1 тези доповідей.

Автореферат та опубліковані за темою дисертації наукові публікації з достатньою повнотою розкривають її зміст. Автореферат за структурою, змістом і оформленням цілком відповідає вимогам МОН України до дисертаційних робіт.

**Зауваження до змісту дисертації.**

1. У першому розділі проведено аналіз множини об'єктів критичної інфраструктури, множини загроз для АСУ ОКІ, а також вразливостей програмно-апаратних засобів системи, що впливають на її функціонування. Цей аналіз носить більш оглядовий характер. Крім того, на мою думку, можна було б розширити кількість об'єктів аналізу, щоб отримати більш повну

картину щодо існуючих методів прогнозування надійності таких систем та оцінки якості їх функціонування, а для порівняння програмно-апаратних методів захисту ОКІ застосовувати, наприклад, методи комбінаторно-морфологічного аналізу.

2. У другому розділі автором пропонується чотири обчислювальні процедури, які фактично складають один науковий результат, що отримав подальшого розвитку. Не зовсім зрозуміло в чому саме полягає удосконалення. Дослідження грунтуються в основному на методах експертного оцінювання (попарних порівнянь, методів МАІ та Дельфи), хоча вирішити поставлене завдання – обрати раціональне рішення з множини відомих можна було б й іншими способами, наприклад, шляхом формування та дослідження програмно-апаратних засобів та АСУ в цілому з використанням, наприклад, методу «прогресуючого еталону».
3. З точки зору категорії новизни методу визначення впливу загроз на процеси функціонування перспективної гарантоздатної АСУ ОКІ, описанного у розділі 3 та визначеного, як «вперше розроблений» можна погодитись з автором дисертації. Але за текстом бракує послідовного та еволюційного викладення того, що було розроблено вперше. Наприклад, внесення в процедуру детектування та відновлення даних аспектів кластерного аналізу – звичайна річ. Цей прийом застосовувався раніше та буде застосовуватися в подальшому. Автору слід було обов'язково вказати на це, навести приклади, систематизувати та узагальнити їх, і, на підставі цих відомостей, ввести своє формалізоване тлумачення процесу розпаралелювання операцій криптоаналізу за рахунок їх кластеризації.
4. Технологію проведення експериментального дослідження (розділ 4) автором формалізовано не досить повно й чітко. Це ускладнює розуміння умов, в яких проводились експерименти – на яких комп'ютерах (мережах), з якими обчислювальними потужностями, операційним системами, тощо. Автор, на жаль, не демонструє знання з теорії планування експерименту. Отже, про точність та вірогідність отриманих результатів в дисертації зовсім не йдеться. Більшість наведених результатів експериментів слід сприймати тому як набір точкових оцінок, які хоча й дають загальне уявлення про поведінку зазначених параметрів, але не можуть бути підставою для об'єктивних суджень.
5. У додатку Д дисертації (стор. 173-176), в якому наведено копії документів (актів), що підтверджують впровадження результатів дисертації та на які в авторефераті посилається здобувач, не зовсім чітко виокремлено, яку саме частину дисертаційних досліджень впроваджено.

6. До недоліків також слід додати певні вади змістовної частини автореферату. Зокрема, тотожні відомості щодо практичного значення отриманих наукових результатів міститься в різних розділах автореферату (у загальній характеристиці роботи та у висновках).

Однак, наведені зауваження не знижують високий науковий рівень дисертаційного дослідження і не впливають на його загальну позитивну оцінку.

**Загальні висновки.** Дисертаційна робота Кузьменко Лідії Володимирівни «Інформаційна технологія для створення перспективних гарантоздатних автоматизованих систем управління об'єктами критичної інфраструктури» є завершеним науковим дослідженням і містить нові наукові результати, які в сукупності вирішують актуальну науково-прикладну задачу розроблення теоретичних та прикладних засад побудови інформаційної технології та методів 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 обсягом, якістю дослідження і отриманими теоретичними та практичними результатами дисертаційна робота відповідає вимогам «Порядку присудження наукових ступенів», затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 зі змінами, затвердженими Постановами Кабінету Міністрів України № 656 від 19 серпня 2015 р. та № 1159 від 30.12.2015 р., які висуваються до кандидатських дисертацій, а її авторка Кузьменко Лідія Володимирівна заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології».

Офіційний опонент,
професор ПЗВО «ІТ СТЕП Університет»,
д.т.н., доцент Т.Є.Рак

"ІТ СТЕП УНІВЕРСИТЕТ" 40570842 ПРИВАТНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ УКРАЇНА

Підпис Рака Т.Є. засвідчую
методист Султанова С.Ф.