Голові спеціалізованої вченої ради
ДФ 26.204.001
в Інституті проблем математичних машин і систем НАН України
доктору технічних наук, професору
Литвинову Валерію Андрониковичу

ВІДГУК

офіційного опонента **ГНАТЮКА Сергія Олександровича**,
доктора технічних наук, професора, проректора з наукових досліджень та трансферу технологій Державного університету «Київський авіаційний інститут» на дисертацію **ГУЛАКА Євгена Геннадійовича**
«Моделі та методи забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору»
подану на здобуття ступеня доктора філософії за спеціальністю
122 Комп'ютерні науки

1. Актуальність теми дослідження

Енергетичний сектор є критичною інфраструктурою, яка часто стає мішенню для кібератак. Атаки на системи управління енергетичними мережами можуть призвести до серйозних наслідків, включаючи зупинку роботи енергосистем, перебої в електропостачанні, економічні втрати та загрозу національній безпеці Сучасний енергетичний сектор активно впроваджує інтелектуальні мережі (smart grids), Інтернет речей (IoT), автоматизовані системи управління та аналітику великих даних. Це підвищує залежність від інформаційно-комунікаційних систем (ІКС), які потребують високого рівня гарантоздатності та захисту від зовнішніх і внутрішніх загроз. Уряди багатьох країн та міжнародні організації впроваджують жорсткі стандарти безпеки для критичної інфраструктури. Наприклад, NERC CIP

(Critical Infrastructure Protection) у Північній Америці чи ISO/IEC 27001 задають обов'язкові рамки для забезпечення кібербезпеки в енергетичній галузі.

Безперервність роботи енергосистем є пріоритетом. Впровадження моделей та методів, які забезпечують високу надійність, стійкість до збоїв і швидке відновлення після інцидентів, є ключовим завданням для захисту життєво важливих функцій суспільства. Розробка та впровадження ефективних методів кібербезпеки ускладнюється через різноманітність використовуваних технологій, архітектурну складність систем та інтеграцію з іншими секторам. Кібератаки на енергетичні системи можуть завдати багатомільярдних збитків. Інвестиції в кібербезпеку є не лише необхідністю, а й економічно виправданим заходом, що дозволяє уникнути катастрофічних втрат.

Отже, вивчення моделей та методів забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору є доцільним компонентом сучасних наукових і прикладних досліджень в інформаційній безпеці.

2. Зв'язок теми дисертаційної роботи з науковими планами, програмами, фундаментальними та прикладними дослідженнями

Дисертація виконана в Інституті проблем математичних машин і систем Національної академії наук України відповідно до теми науково-дослідної роботи. Дослідження здійснене відповідно до наукових тем «Ситуаційне управління» (№0122U201115, ІПММС, м. Київ) та шифр «ІПММС-2021» (№0121U000107, ІПММС, м. Київ).

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій та їхня достовірність

Автор розробив і представив у своїй дисертації наукові положення, висновки та рекомендації, які мають достатню обґрунтованість. Дисертант

провів обширний аналіз літературних джерел зарубіжних та вітчизняних учених та приділив увагу дослідженню та можливої адаптації зарубіжного досвіду. У процесі вирішення завдань, поставлених у дисертації, автор критично оцінював досягнення вітчизняних та зарубіжних учених, висловлюючи свою думку та демонструючи високий рівень наукової культури. Висновки та рекомендації, представлені в дисертації, логічні та є результатом всебічного та об'єктивного аналізу досліджуваних явищ з використанням сучасного наукового інструментарію. У ході дослідження було використано загальнонаукові та спеціальні методи пізнання, що дозволило дисертантові обґрунтувати теоретичні, методичні та практичні аспекти моделей та методів забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору.

4. Новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації

В рамках дисертаційного дослідження сформульовано та обґрунтовано низку наукових положень, висновків та рекомендацій, що відрізняються наявністю наукової новизни. Ключовим науково новим результатом цього дослідження є концептуальне вирішення нової наукової проблеми щодо забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору шляхом захисту інформаційних ресурсів та технологічної інформації від загроз конфіденційності, цілісності та доступності за рахунок реалізації концепції корпоративного кіберзахисту, розробки молей і методів криптографічного захисту інформації, що збирається, передається та обробляється в ІКС-ЕС.

Найбільш значущі наукові досягнення, які розкривають особистий внесок автора у вирішення проблеми, що вивчається, і відображають новизну дослідження, полягають, у наступному:

- запропонований метод декомпозиції складної інформаційної системи критичної інфраструктури, оцінки характеристик підсистеми

криптографічного захисту та їх раціонального визначення;

- запропонована модель підсистеми криптографічного захисту інформації в ІКС-ЕС, що враховує можливість взаємодії інформаційних підсистем із різними рівнями щодо забезпечення безпеки інформації, та запропоновано метод оцінки безпеки шифрування коротких повідомлень у мобільних компонентах ІКС-ЕС;
- запропонована модель розмежування доступу в мережі центру кібербезпеки на основі часткової децентралізації підсистеми управління доступом.

5. Теоретична цінність і практична значущість наукових результатів

Результати аналізу дисертації та опублікованих праць свідчать про важливість отриманих результатів проведеного дослідження. Основним досягненням є можливість забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору шляхом захисту інформаційних ресурсів та технологічної інформації від загроз конфіденційності, цілісності та доступності за рахунок реалізації концепції корпоративного кіберзахисту, розробки молей і методів криптографічного захисту інформації, що збирається, передається та обробляється в ІКС-ЕС.

Зазначені теоретичні положення становлять основу для створення системного та єдиноутвореного підходу до управління кібербезпекою підприємств енергетичного сектору, що підтверджує вагомість проведеної роботи.

Висновки та пропозиції дисертаційного дослідження мають практичне значення і прийняті до впровадження в діяльність Інституту проблем безпеки атомних електростанцій НАН України, Київського столичного університету імені Бориса Грінченка та Інституту проблем математичних машин і систем НАН України.

6. Повнота викладення наукових результатів дисертації в опублікованих працях

За темою дослідження опубліковано 9 наукових праць, із них: у фахових виданнях, затверджених МОН України – 4; у Scopus – 3, з яких 3 мають підтверджений ISSN-номер. За матеріалами виступів на науково-технічних конференціях опубліковано 2 тези доповідей.

У публікаціях розкрито ключові результати проведеного дослідження та його наукову новизну, що дозволяє стверджувати, що висновки та пропозиції, викладені у дисертаційній роботі, є апробованими.

7. Відсутність (наявність) порушення академічної доброчесності.

За результатами перевірки дисертації Гулака Є.Г. на наявність ознак академічного плагіату встановлено коректність посилань на першоджерела для текстових та ілюстративних запозичень; навмисних спотворень не виявлено. Звідси можна зробити висновок про відсутність порушень академічної доброчесності.

8. Дискусійні положення та зауваження до дисертації.

1. У розділі 1 згадується модель профілів безпеки галузі електроенергетики MOSES. Щодо вказаної моделі наголошується її корисність у плані формування функціональних профілів захисту інформаційних систем електроенергетики. Враховуючи комплексний характер моделі було б доречним розглянути її застосування у більш ширшому розумінні, а саме у розрізі забезпечення стійкості функціонування інформаційних систем енергетики в умовах швидко змінюваного ландшафту кіберзагроз.

2. Гарантоздатність (рис. 1.3, с. 38), як комплексна характеристика інформаційної системи, у якості важливої складової включає функціональну безпеку, що спрямована на мінімізацію ризиків реалізації загроз здоров'ю та життю людини. Це становить інтерес для побудови сучасних технологій,

натомість, ця характеристика у рамках дослідження не зазнала відповідного аналізу.

3. Не зовсім коректно, на мою думку, сформульовано наукову новизну отриманих результатів. Зокрема, не вказано ефект від отриманого результату, а також в п. 1 (с. 24) як наукову новизну визначено «методику декомпозиції складної інформаційної системи критичної інфраструктури», проте більш коректно було визначити як новизну саме «метод декомпозиції складної інформаційної системи критичної інфраструктури» (так як методика – це більш практичний результат роботи).

4. У роботі як перспективний напрям майбутньої трансформації енергетики згадується архітектура інтелектуальних енергетичних систем (Cyber-Physical Power System), але проблеми і завдання забезпечення кібербезпеки і гарантоздатності у цьому випадку викладені дуже конспективно.

5. У висновках відсутні кількісні показники, що ускладнює розуміння переваг розроблених методів над аналогами.

6. Текст дисертації містить низку помилок технічного характеру:

- перше та друге речення останнього абзацу на сторінці 31 не узгоджені у сенсі логіки викладення (можливо, це наслідок пропуску слова або не видалення зайвої частини речення);
- модель логічних ланцюгів впливу загроз на погіршення спроможності стійкого функціонування електроенергетики зображена на рис. 1.9 (с. 65);
- в ітераційному рівнянні що описане формулою (2.1) на с. 85 та визначає процес функціонування системи управління безпекою енергосистеми підчас формування команди опрацювання кіберінциденту опущені індекси, які вказані у формулі (2.2);
- на рисунках, що супроводжують викладення положень дисертації, використовуються нестандартизовані піктограми.

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

9. Загальна оцінка дисертаційної роботи, її відповідність встановленим вимогам.

Дисертаційне дослідження Гулака Євгена Геннадійовича на тему «Моделі та методи забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору» є завершеним науковим дослідженням, яке за актуальністю, достовірністю отриманих результатів, їхньою науковою новизною і практичною цінністю відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 року №44, а її автор, Гулак Євген Геннадійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 122 Комп'ютерні науки.

Офіційний опонент:

проректор з наукових досліджень та трансферу технологій
Державного університету «Київський авіаційний інститут»,
доктор технічних наук, професор Сергій ГНАТЮК