

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 **СМІРНОВА Олексія Анатолійовича**, доктора технічних наук, професора, завідувача кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету 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

Енергетика в сучасному суспільстві, виразно кажучи, виконує функцію тягового локомотива економіки, потужність і стабільність функціонування якого визначає прогрес у інших галузях виробництва, науки і техніки.

Безпека функціонування енергетичного сектору, що суттєво залежить від кіберстійкості та гарантоздатності його інформаційних та управляючих систем, за суттю є одним з визначальних факторів для забезпечення обороноздатності держави. Саме таке переплетіння проблем інформаційних систем і технологічних процесів в енергетичному секторі визначено у всеосяжному документі – Стратегії безпеки Європейського союзу.

Зазначене актуалізує розв'язок проблеми підвищення спроможностей до стійкого функціонування об'єктів енергетики шляхом підвищення кіберстійкості та гарантоздатності їхньої інформаційної інфраструктури в умовах змін у ландшафті кіберзагроз та безжалісних руйнуючих ударів агресора.

Досягнення визначеної мети потребує вирішення низки завдань що полягають в удосконаленні існуючих та розробці нових методів захисту складних інформаційних та управляючих систем електроенергетики в специфічних умовах її функціонування. Серед факторів, що негативно впливають на пошук адекватних рішень у вітчизняних умовах є велика кількість систем, вимоги щодо їх побудови визначені різними власниками, поєднання застарілих технологій і новітніх рішень, обмеженість ресурсів для проведення масштабної трансформації галузі, недосконалість нормативного забезпечення та багато інших чинників.

Отже наведене підкреслює актуальність та своєчасність вибраної теми науково-прикладного дослідження, що полягає у розробці моделей та методів забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору

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

Дисертація виконана відповідно до планів наукової і науково-технічної діяльності Інституту проблем математичних машин і систем Національної академії наук України в рамках виконання за державним замовленням науково-дослідних робіт: шифр «Ситуаційне управління» (№ д.р. 0122U201115, ІПММС, м. Київ) та шифр «ІПММС-2021» (№ д.р. 0121U000107, ІПММС, м. Київ)

Обрана тема октрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертаційна робота виконана у відповідності до доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України.

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

Отримані наукові результати та висновки дисертаційної роботи характеризуються належним рівнем обґрунтованості, що підтверджується аналізом значної кількості наукової та технічної літератури та використанням загальнонаукових та спеціальних методів дослідження, зокрема методів теорії ризиків в системах безпеки, теорії ймовірностей та математичної статистики, методів моделювання систем управління інформаційною безпекою.

Достовірність, отриманих в дисертації результатів, ґрунтується на комплексному, експериментальному і теоретичному вивченні моделей і методів забезпечення гарантоздатності та кібербезпеки інформаційно-комунікаційних систем енергетичного сектору. Перелік наукових праць дисертанта та довідки щодо впровадження результатів дослідження засвідчують фаховий підхід здобувача до обрання дослідницької проблематики та високий рівень його наукової компетентності.

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

Представлені в дисертації положення, концептуальні засади, структура, постановка завдань та їх вирішення, узагальнені висновки є результатом реалізації авторських ідей і самостійно виконаної наукової праці. У дисертаційній роботі Гулака Є.Г. обґрунтовано низку концептуальних положень, узагальнень та висновків, які відповідають критеріям наукової новизни, зокрема:

1. Вперше запропоновано методику декомпозиції складної інформаційної системи критичної інфраструктури, оцінки характеристик підсистеми криптографічного захисту та їх раціонального визначення.

2. Вдосконалено 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.

3. Подальшого розвитку набула модель розмежування доступу в мережі центру кібербезпеки на основі часткової децентралізації підсистеми управління доступом.

Всі отримані автором результати можуть слугувати складовою частиною впровадження методології кібербезпеки для забезпечення конфіденційності, доступності та цілісності інформації.

5. Теоретична цінність і практична значущість наукових результатів.

Наукові положення, висновки та рекомендації дисертаційної роботи Гулака Є.Г. мають теоретичну цінність і практичну значущість. Отримані результати є певним внеском у розвиток інформаційної та кібернетичної безпеки.

Теоретичне значення дослідження полягає в обґрунтуванні необхідності та дослідженні можливості впровадження методів захисту інформації підприємств критичної інфраструктури.

Практичне значення отриманих результатів полягає у їхній застосовності для підвищення кібербезпеки інформаційно-комунікаційних систем енергетичного сектору, що є критично важливими для функціонування держави. Розроблена методика декомпозиції складних систем на основі класів еквівалентності дозволяє ефективно сегментувати системи та оптимізувати їхній захист, враховуючи специфічні вимоги до безпеки окремих підсистем.

Вдосконалена модель корпоративного центру кібербезпеки енергетичного сектору забезпечує динамічну обробку кіберінцидентів у реальному часі, відповідаючи сучасним викликам безпеки та специфіці енергосистем. Це сприяє зниженню ризиків каскадних ефектів та підвищенню стійкості енергетичних об'єктів як критичної інфраструктури. Розроблені моделі криптографічного захисту, включаючи двоконтурне шифрування та методику розподілу секрету, дозволяють значно знизити ризики несанкціонованого доступу до інформаційних ресурсів. Їх масштабованість та адаптивність забезпечують ефективний захист у складних децентралізованих системах. Запропоновані рішення були впроваджені у межах виконання державних науково-дослідних програм в Інституті проблем математичних машин і систем НАН України, де вони використовувались для вдосконалення архітектури та функціональності ситуаційних центрів об'єктів критичної інфраструктури. Також результати знайшли застосування в Інституті проблем безпеки атомних електростанцій НАН України для посилення кібербезпеки інформаційної інфраструктури енергосистем. Крім того, розробки інтегровані в освітній процес Київського університету імені Бориса Грінченка, що сприяє підготовці висококваліфікованих фахівців для потреб енергетичного сектору.

6. Повнота викладення наукових результатів дисертації в опублікованих працях.

Результати дисертації відображені у 9 публікаціях: чотирьох статтях у журналі, що входить до наукових фахових видань (Категорія "Б"), трьох, які

представлені на Workshop on Cybersecurity Providing in Information and Telecommunication Systems (Scopus) та двох тез доповідей на всеукраїнських конференціях.

Аналіз публікацій автора дозволяє зробити висновок про повноту викладення основних наукових положень дисертаційного дослідження у науковій літературі. Також зазначено особистий внесок здобувача у тих наробках, які виконано колективно.

7. Відсутність (наявність) порушення академічної доброчесності.

У дисертації та наукових публікаціях Гулака Є.Г. відсутні порушення академічної доброчесності. Запозичень матеріалу без посилання на відповідне джерело не виявлено. Перевірка проводилася сертифікованою програмою Turnitin.

8. Дискусійні положення та недоліки дисертаційної роботи.

Відзначаючи позитивні сторони роботи Гулака Є.Г., слід звернути увагу на певні зауваження та дискусійні положення, які потребують додаткової аргументації.

1. У запропонованій моделі динамічного реагування на кіберінциденти було б доречним врахувати той факт, що ефективність заходів з протидії майбутнім загрозам та покращення культури кібербезпеки залежить від якості та глибини розслідування інциденту що відбувся, оскільки воно дає умовно кажучи цільовказівку щодо існуючих вразливостей.

2. Підчас розгляду ітераційному рівнянні що описане в другому розділі формулою (2.1) та визначає процес функціонування системи управління безпекою енергосистеми підчас опрацювання кіберінциденту було б корисно, з точки зору побудови практичних систем, проаналізувати процес накопичення знань про інциденти та застосування для цього системи штучного інтелекту.

3. Відомо, що оцінка якостей критосистем крім проведення їх математичного аналізу, включає їх інженерно-криптографічний аналіз, але у дисертаційному дослідженні це питання не розглядається, що може бути перешкодою у плані запропонованої моделі критосистеми.

4. У тексті дисертаційної роботи присутні деякі помилки та неточності технічного характеру:

– для запропонованого застосунку двоконтурного шифрування не надані умови його застосування;

– концепція компанії CISCO побудови архітектури центру оперативного реагування (рис. 2.5 с. 83) наведена англійською мовою;

– в тексті присутні деякі граматичні та пунктуаційні помилки;

– схеми виконані не в одному стилі.

Вказані недоліки не носять принципового характеру та не впливають на загальну позитивну оцінку представленої до захисту дисертаційної роботи, оскільки в основному носять дискусійний характер та спрямовують дисертанта на дослідження зазначеної проблематики. Також слід зауважити, що наявність

дискусійних питань, насамперед, характеризує складність, актуальність і багатоаспектність досліджуваної теми та власний підхід до її розгляду дисертантом.

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

Дисертаційна робота 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:

доктор технічних наук, професор
завідувач кафедри кібербезпеки
та програмного забезпечення
Центральноукраїнського національного
технічного університету



Олексій СМІРНОВ

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету,
кандидат технічних наук, доцент
“ ____ ” _____ 2025 року

Андрій ТИХИЙ