ВІДГУК

офіційного опонента доктора технічних наук, доцента Гнатюка Сергія Олександровича про дисертацію Комарова Максима Юрійовича на тему «Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури», що представлена на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти»

Актуальність теми дисертаційного дослідження

Низка кібератак на критичну інфраструктуру зокрема й нашої держави, показали нагальну потребу у забезпеченні інформаційної безпеки (кібербезпеки) та захисту від кібервпливів комп'ютерних систем та мереж (КСМ) об'єктів критичної інформаційної інфраструктури України. Зокрема, це стосується енергетичного сектору, який зазнав чи не найбільшої шкоди від дій зловмисників. На сьогодні багато досліджень пов'язано із захистом інформації від кібервпливів в КСМ об'єктів критичної інфраструктури, проте залишається не вирішеним багато завдань, які не втратять своєї актуальності ще протягом тривалого періоду часу, а саме розробка методів і засобів підвищенням рівня захисту інформації від кібервпливів в КСМ об'єктів критичної інформаційної інфраструктури. Саме розв'язанню цієї актуальної науково-технічної задачі і присвячена дисертаційна робота Комарова Максима Юрійовича, яка, на мою думку, має важливе теоретичне і прикладне значення.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Викладені наукові положення, методики, висновки і рекомендації є повністю обґрунтованими, а достовірність запропонованих дисертантом гіпотез і математичних моделей підтверджується відповідними експериментальними даними та результатами верифікації розробленого алгоритмічного забезпечення та програмного застосунку захисту інформації, яка циркулює в КСМ об'єктів критичної інфраструктури,

Отримані, під час експериментів, дані відповідають теоретичним висновкам роботи і повністю підтверджують їх, що доведено проведенням робіт щодо створення КСЗІ захищеного вузла Інтернет доступу «Фарлеп-Інвест» та здійсненні державної експертизи КСЗІ в автоматизованій інформаційній системі «Централізована база даних перенесених номерів» державного підприємства «Український державний центр радіочастот».

До того ж, на мою думку, дисертантом було коректно застосовано методи

- теорії захисту інформації та системному аналізі;
- теорії ймовірності і випадкових процесів;
- методи і засоби об'єктно-орієнтовного програмування тощо.

Ідентичність змісту автореферату й основних положень дисертації

Проаналізувавши автореферат і дисертацію здобувача, можна зробити висновки, що в авторефераті з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертаційної роботи. Для основних положень дисертації та змісту автореферату характерна повна ідентичність. Крім того, варто зауважити, що усі компоненти дисертаційної роботи оформлено відповідно до чинних вимог 2017 року.

У **вступі** автором представлена загальна характеристика роботи, обґрунтован актуальність наукової теми, сформульовані мета і задачі дослідження, відображено науков новизну та практичну цінність отриманих результатів і висновків, наведено дані щодо ї апробації та впровадження.

У **першому розділі** дисертації проведено аналіз сучасних методів та засобів захист інформації від кібервпливів за темою дисертаційної роботи. Досліджено національн нормативно-правове забезпечення кібербезпеки та захисту інформації в КСМ об'єкті критичної інфраструктури. Проведено аналіз існуючих робіт та можливі підходи щод таксономії загроз інформаційній безпеці КСМ об'єктів критичної інфраструктури.

Другий розділ присвячений розробці таксономії кіберзагроз інформаційній безпец КСМ об'єктів критичної інформаційної інфраструктури, складено матрицю залежност інформаційних об'єктів захисту від типу потенційних загроз, що можуть на них впливати, т схильності до конкретних загроз, а також розроблено модель бази даних кіберзагро інформаційним об'єктам захисту КСМ об'єктів критичної інформаційної інфраструктури.

У третьому розділі дисертантом наведено розроблення методу розпізнаванн кіберзагроз інформаційній безпеці КСМ об'єктів критичної інфраструктури, розроблен структурна модель багаторівневої системи виявлення підозрілих впливів на КСМ об'єкті критичної інфраструктури, а також було розроблено методику оцінювання кіберстійкост КСМ об'єктів критичної інфраструктури.

Четвертий розділ дисертації присвячено практичним реалізаціям т експериментальним дослідженням розроблених рішень. Зокрема, розроблено алгорит функціонування багаторівневої системи виявлення підозрілих впливів та програмний з стосунок, який реалізує даний алгоритм, проведено експериментальні дослідження систе захисту інформації КСМ об'єктів критичної інфраструктури. З використанням методу т засобів, розроблених у даній дисертаційній роботі, проводилися роботи по створенню КСЗ захищеного вузла Інтернет доступу «Фарлеп-Інвест» та здійсненні державної експертиз КСЗІ в автоматизованій інформаційній системі «Централізована база даних перенесени номерів» державного підприємства «Український державний центр радіочастот».

У **додатках** вміщено акти впровадження результатів дисертаційної роботи, а також лістинги розроблених дисертантом програмних застосунків.

Наукова цінність результатів роботи

Наукова новизна отриманих результатів роботи полягає у наступному:

– вперше розроблено таксономію кіберзагроз інформаційній безпеці КСМ об'єкті критичної інформаційної інфраструктури, яка дозволяє описувати багатоетапні атаки (які н сьогоднішній день отримали дуже широку розповсюдженість);

– вперше розроблено модель бази даних кіберзагроз інформаційним об'єкта захисту КСМ об'єктів критичної інформаційної інфраструктури, яка дозволяє розробити баз даних кіберзагроз безпеці КСМ об'єктів критичної інформаційної інфраструктури;

– вперше розроблено комбінований метод розпізнавання кіберзагроз безпеці КСМ об'єктів критичної інформаційної інфраструктури, який дозволяє розширити спект виявлених кіберзагроз.

Основні положення дисертаційного дослідження опубліковано у 22 науковій праці, тому числі: 9 наукових статей у фахових наукових журналах та збірниках наукових праць,

яких 5 – у наукових журналах, що індексуються міжнародними наукометричними базами даних, 1 патент України на корисну модель, 1 свідоцтво про реєстрацію авторського права на твір, а також 11 матеріалів та тез доповідей конференцій.

Крім того, зазначені положення дисертаційної роботи пройшли обов'язкову і достатню апробацію на наукових конференціях та семінарах, зокрема: XVII Міжнародна науково-практична конференція «Безпека інформації у інформаційно-телекомунікаційних системах» (Київ, 2015 р., 2018 р.); VI Міжнародна наукова конференція «Моделювання-2018» (Київ, 2018 р.); Всеукраїнська науково-практична конференція «Безпека соціально-економічних процесів в кіберпросторі» (Київ, 2019 р.); науково-практична конференція «Кібербезпека енергетики» (Одеса, 2018 р., 2019 р.); науково-технічна конференція «Інформаційна безпека України» (Київ, 2018 р.); XII Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології» (Київ, 2019 р.); всеукраїнська науково-практична конференція «Безпека соціально-економічних процесів в кіберпросторі» (Київ, 2019); науково-практична конференція «Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн» (Житомир, 2019 р.), науково-практична конференція «Безпека енергетики в епоху цифрової трансформації» (Київ, 2020 р.).

Значення результатів для практики

Отримані в дисертаційній роботі результати можуть бути використані для підвищення оцінювання стану та підвищення рівня кіберстійкості КСМ критичної інфраструктури. Зокрема, практична цінність роботи полягає у такому:

– розроблено методику оцінювання кіберстійкості КСМ об'єктів критичної інформаційної інфраструктури, яка дозволяє оцінювати стан критичної інформаційної інфраструктури, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз;

– розроблено алгоритмічне забезпечення на основі запропонованого комбінованого методу розпізнавання кіберзагроз для реалізації відповідного ПЗ, що дозволяє здійснювати автоматизоване розпізнавання кіберзагроз та здійснювати захист від них;

– розроблено алгоритмічне забезпечення на основі запропонованої методики оцінювання кіберстійкості для реалізації відповідного ПЗ, що дозволяє здійснювати автоматизований розрахунок кіберстійкості з урахуванням таких показників як кібернадійність, кіберзахищеність та кіберстійкість;

– на основі запропонованих алгоритмів розроблений програмний застосунок, що використовує запропоновану методику для захисту інформації в КСМ об'єктів критичної інфраструктури.

Результати теоретичних та практичних досліджень знайшли застосування у таких науково-дослідних роботах:

– «Розробка методів оцінювання чутливості Об'єднаної енергосистеми України до кібернетичних впливів» (шифр «ВПЛИВ», державний реєстраційний номер 0118U005320);

– «Розроблення методів забезпечення кібербезпеки функціонування Об'єднаної енергетичної системи України в рамках впровадження концепції інтелектуальних мереж» (шифр «ІНТЕЛЕНЕРГО», державний реєстраційний номер 0119U101856).

Результати дисертаційної роботи впроваджено у діяльність Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, Державного підприємства

«Український державний центр радіочастот», Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, ПрАТ «Фарлеп-Інвест», ТОВ «ІНТЕСИС».

Зауваження та недоліки

1. У першому розділі дисертації (стр. 46) та в авторефераті (стр. 6) дисертант наводить порівняльну таблицю підходів до розробки таксономій кіберзагроз за визначеними критеріями. Проте, на мою думку, автору слід було б проводити аналіз чітко за предметом дослідження, який у вступі визначено як «методи та засоби захисту інформації від кібервпливів в КСМ об'єктів критичної інфраструктури». Це дозволило б порівняти отримані в дисертаційному дослідженні результати зокрема й з аналогічними розробками науковців, яких автор згадує у вступі до дисертації.

2. Четвертий науковий результат автор сформулював наступним чином: «вперше розроблено методику оцінювання кіберстійкості КСМ об'єктів критичної інформаційної інфраструктури». Проте, я вважаю, що зазначену методику слід було б віднести до практичних результатів, а не наукових (якими є моделі, методи, методології тощо). До того ж, у дисертації на рис. 3.4 (стор. 94) методика відображена у вигляді алгоритму, що також повинен відноситись до практичних результатів роботи.

3. Усі чотири пункти наукової новизни визначено на думку автора отримано уперше – це найвищий рівень новизни, що свідчить про повну відсутність аналогів. Проте, на мою думку, деякі результати є удосконаленням існуючих – наприклад, модель бази даних кіберзагроз чи метод розпізнавання кіберзагроз. Тому, дисертанту слід було б для деяких результатів вживати ступінь новизни «удосконалено» або «отримав подальший розвиток».

4. У дисертації та авторефераті здобувач вживає деякі поняття не у відповідності до стандартів у галузі кібербезпеки, зокрема:

– «кіберзагрози інформаційній безпеці» – необхідно було б сформулювати як «загрози кібербезпеці», або «кіберзагрози безпеці» (з тих міркувань, що кібербезпека є складовою інформаційної безпеки);

– «комп'ютерні системи та мережі об'єктів критичної інформаційної інфраструктури» – комп'ютерні системи та мережі власне і є об'єктами критичної інформаційної інфраструктури. Коректніше було б вживати поняття «комп'ютерні системи та мережі об'єктів критичної інфраструктури». Проте, слід відмітити, що у назві дисертації здобувач вживає коректну термінілогію.

5. Метою дисертаційного дослідження є підвищення рівня захисту інформації від кібервпливів в КСМ об'єктів критичної інформаційної інфраструктури… Проте, з висновків і експериментальної частини роботи не зрозуміло на скільки відсотків (чи у скільки разів) розроблені автором рішення дозволяють підвищити рівень захисту інформації у порівнянні з уже відомими методами і засобами. Це не дає можливість у повній мірі оцінити досягнення мети дисертаційної роботи. Крім того, варто відзначити, що жодного кількісного параметру в загальних висновках до дисертації не було виявлено.

6. Деякі таблиці не містять назви – це дещо ускладнює їх загальне розуміння (наприклад, табл. 4.1, 4.2 у дисертаційній роботі, табл. 3, 4 у авторефераті).

7. Тексти дисертаційної роботи та автореферату містять велику кількість скорочень, абревіатур, спеціальних позначень та формул, що значно ускладнює загальний процес оцінки роботи при її читанні. До того ж, не всі абревіатури та скорочення пояснені у відповідному переліку, що наведений на стор. 10-11 дисертації.

Висновки

Проте, не зважаючи на зазначені недоліки, дисертаційна робота Комарова Максима Юрійовича є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для розвитку комп'ютерних систем та мереж (зокрема, у контексті їх захисту від кібервпливів). Усі одержані наукові результати можуть застосовуватися у різних галузях критичної інфраструктури держави для визначення стану та підвищення ефективності захисту комп'ютерних систем та мереж від кібервпливів. Отже, вважаю, що дисертаційна робота «Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури» повністю відповідає чинним вимогам МОН України до кандидатських дисертацій, зокрема «Порядку присудження наукових ступенів», затвердженого Постановою КМУ від 24.07.2013 р. № 567 (із змінами, внесеними згідно з Постановами КМУ № 656 від 19.08.2015 р., № 1159 від 30.12.2015 р. № 567 від 27.07.2016 р., № 943 від 20.11.2019 р., № 607 від 15.07.2020 р.), а її автор Комаров Максим Юрійович заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – «Комп'ютерні системи та компоненти».

Офіційний опонент
заступник декана з наукової роботи
Факультету кібербезпеки, комп'ютерної та програмної інженерії
Національного авіаційного університету,
доктор технічних наук, доцент С.О. Гнатюк

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ 01132330 МІСТО КИЇВ

Підпис гр. Гнатюка С.О.
засвідчую
Вчений секретар
Національного авіаційного університету
М. Лелецький