Голові разової спеціалізованої вченої ради
Національного університету
«Київський авіаційний інститут»
д.т.н., проф. Гнатюку Сергію Олександровичу
пр. Любомира Гузара 1, Київ, 03058, Україна

Відгук

офіційного опонента Залужного Олексія Вікторовича

на дисертацію Самборського Євгена Івановича на тему «Моделі і методи управління подіями безпеки комп'ютерних систем критичних інформаційних інфраструктур», поданої на здобуття ступеня доктора філософії зі спеціальності 122 Комп'ютерні науки

Актуальність теми дисертаційного дослідження зумовлена стрімким розвитком цифрових технологій, масштабним впровадженням інформаційно-комунікаційних мереж та зростанням залежності державних структур від стабільного функціонування об'єктів критичної інформаційної інфраструктури.

В умовах постійного зростання кількості та складності сучасних інформаційних загроз особливого значення набувають питання забезпечення стійкого функціонування комп'ютерних систем критичної інфраструктури, що вимагає нових підходів до управління подіями інформаційної безпеки.

Практичний досвід останніх років свідчить про високий рівень уразливості об'єктів критичної інформаційної інфраструктури до сучасних кібератак. Інциденти, пов'язані з порушенням функціонування інформаційно-комунікаційних мереж, державних інформаційних ресурсів та цифрових сервісів, продемонстрували суттєву обмеженість традиційних підходів до моніторингу, аналізу та реагування на події безпеки комп'ютерних систем критичних інформаційних інфраструктур. Як правило, це призводило до значних технічних, економічних і соціальних наслідків.

Сучасні системи управління подіями безпеки переважно базуються на технологіях SIEM-систем, які забезпечують централізований збір та кореляцію даних. Водночас більшість існуючих рішень використовують статичні механізми аналізу та не повною мірою враховують динаміку розвитку інцидентів інформаційної безпеки, взаємозалежність компонентів критичних систем і можливість виникнення каскадних ефектів. Це обумовлює необхідність розроблення нових підходів до оцінювання критичності подій безпеки та оперативної підтримки прийняття управлінських рішень для компенсації їх деструктивних впливів на комп'ютерні системи критичних інформаційних інфраструктур.

З позицій спеціальності 122 «Комп'ютерні науки» дана науково-прикладна проблематика належить до напрямів моделювання складних інформаційних систем, інтелектуального аналізу даних та підтримки прийняття рішень. Перспективним напрямом її розв'язання є використання логіко-динамічних моделей і технології цифрових двійників, які дозволяють враховувати часову динаміку подій, прогнозувати розвиток можливих інцидентів кібербезпеки та реалізувати проактивне управління процесами безпеки комп'ютерних систем критичних інформаційних інфраструктур.

Таким чином, розроблення моделей і методів управління подіями безпеки комп'ютерних систем критичних інформаційних інфраструктур на основі логіко-динамічного підходу та застосування цифрових двійників є актуальним науково-прикладним завданням у галузі комп'ютерних наук, спрямованим на підвищення ефективності виявлення, оцінювання критичності та прогнозування розвитку подій безпеки, а також забезпечення безпекової стійкості об'єктів критичної інформаційної інфраструктури.

Зв'язок роботи з науковими програмами, планами та темами

Дисертаційна робота пов'язана з реалізацією пріоритетних напрямів розвитку науки і техніки в Україні, визначених Законом України «Про пріоритетні напрями розвитку науки і техніки», зокрема у сфері

інформаційних та комунікаційних технологій, кібербезпеки та забезпечення стійкості функціонування об'єктів критичної інформаційної інфраструктури.

Тематика дисертаційного дослідження відповідає пріоритетним напрямам наукових досліджень Міністерства освіти і науки України та завданням щодо підвищення захищеності інформаційно-комунікаційних систем в умовах сучасних загроз безпеці їх ефективного функціонування та постійних інтенсивних гібридних впливів.

Дисертаційна робота виконувалася в Національному університеті «Київський авіаційний інститут» у межах науково-дослідної роботи №54-2023/09.01.04 «Технології створення високопродуктивних захищених комп'ютерних систем». У рамках цієї НДР автором досліджувалися питання моделювання, оцінювання критичності та управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури.

Таким чином, дисертаційне дослідження безпосередньо пов'язане з виконанням державних і галузевих науково-технічних програм у сфері інформаційних технологій, а його результати спрямовані на розв'язання актуальних завдань забезпечення функціональної стійкості важливих об'єктів критичної інформаційної інфраструктури держави.

Наукова новизна представлених у роботі результатів

До найбільш вагомих наукових результатів, отриманих у процесі дисертаційних досліджень автором особисто, і які характеризуються науковою новизною, слід віднести такі.

Вперше:

1. Розроблено логіко-динамічну модель управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури, яка забезпечує формалізоване подання критичних подій як послідовності логічних переходів між станами системи та дозволяє враховувати часову динаміку їх розвитку, взаємозалежність компонентів інформаційно-комунікаційних мереж і каскадний характер поширення негативних впливів.

2. Запропоновано метод адаптивного управління подіями безпеки на основі логіко-динамічної моделі цифрового двійника, який забезпечує комплексну обробку потокових даних, підтримує процедури їх аналізу, оцінювання та інтерпретації і створює передумови для переходу від реактивного до проактивного управління безпекою комп'ютерних систем критичної інфраструктури.

3. Розроблено інформаційну технологію цифрового двійника системи управління подіями безпеки інформаційно-комунікаційних мереж, яка інтегрує засоби потокової обробки даних, графового подання структури мережі та інтелектуального аналізу подій, що забезпечує її сумісність із сучасними SIEM/SOC-контурами без порушення штатного режиму їх функціонування.

Удосконалено:

метод ризик-орієнтованого виявлення та оцінювання критичності подій безпеки комп'ютерних систем інформаційно-комунікаційних мереж, який, на відміну від існуючих підходів, враховує топологічні взаємозв'язки між активами мережі, каскадне поширення впливу загроз та динамічне коригування вагових коефіцієнтів під час оцінювання ризиків.

Набули подальшого розвитку теоретичні засади формалізації інформаційних процесів управління подіями безпеки в комп'ютерних системах критичної інформаційної інфраструктури шляхом інтеграції логіко-динамічних моделей і цифрових двійників у єдине інформаційно-аналітичне середовище, що забезпечує можливість моделювання сценаріїв розвитку критичних подій, прогнозування їх наслідків та підтримки прийняття управлінських рішень.

Наведені результати є науково обґрунтованими, мають ознаки наукової новизни та в сукупності розв'язують важливе науково-прикладне завдання підвищення ефективності управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури.

Практичне значення отриманих результатів дисертаційної роботи

Практичне значення результатів, отриманих автором особисто у дисертаційній роботі, полягає у доведенні розроблених моделей, методів та

інформаційної технології до рівня практичного використання в системах управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури, а саме – інформаційно-комунікаційних мережах.

Запропоновані рішення забезпечують підвищення ефективності виявлення та оцінювання критичності подій безпеки, скорочення часу реагування на інциденти інформаційної безпеки, а також покращення якості підтримки прийняття управлінських рішень у SIEM/SOC-контурах комп'ютерних систем критичних інформаційних інфраструктур.

Практичну цінність становлять розроблені алгоритмічне та програмне забезпечення цифрового двійника системи управління подіями безпеки, що можуть бути інтегровані до існуючих інформаційно-комунікаційних мереж без зміни їх штатної архітектури та використовуватися для моніторингу, прогнозування і аналізу сценаріїв розвитку загроз.

Важливим є те, що результати дисертаційної роботи впроваджені та використовуються у діяльності профільних установ і організацій, а також у навчальному процесі закладу вищої освіти, що підтверджує їх практичну значущість, достовірність та можливість подальшого застосування для підвищення рівня захищеності об'єктів критичної інформаційної інфраструктури.

Повнота викладу основних результатів дисертаційних досліджень у наукових публікаціях

Основні наукові результати дисертаційної роботи достатньою мірою висвітлені в наукових публікаціях автора. За темою дисертації опубліковано 16 наукових праць, серед яких 8 статей у фахових наукових виданнях, з них одна стаття – у виданні категорії А, що індексується міжнародною наукометричною базою Web of Science, а також 8 тез доповідей на міжнародних та всеукраїнських науково-практичних конференціях.

Опубліковані праці охоплюють основні положення дисертаційного дослідження, зокрема питання логіко-динамічного моделювання подій безпеки, оцінювання їх критичності, розроблення методів адаптивного

управління та використання технології цифрових двійників у системах управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури.

Зміст публікацій відповідає тематиці дисертації, відображає основні наукові положення, результати та висновки роботи, а обсяг і рівень апробації результатів дослідження слід вважати достатніми для здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки».

Апробація результатів дисертаційних досліджень

Основні положення, результати та висновки дисертаційної роботи пройшли належну апробацію на восьми міжнародних наукових форумах, серед яких міжнародні науково-технічні конференції «ABIA-2023» та «ABIA-2025», XI Всесвітній конгрес «Авіація в XXI столітті», міжнародні науково-практичні конференції «Інновації та перспективні шляхи розвитку інформаційних технологій» (ІПШРІТ-2024, ІПШРІТ-2025), конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії», міжнародна конференція «Physical and Technological Problems of Transmission, Processing and Storage of Information in Infocommunication Systems», а також XXV міжнародна науково-практична конференція здобувачів вищої освіти і молодих учених «Політ».

Представлення та обговорення результатів дисертаційних досліджень на зазначених наукових заходах дозволило отримати їх позитивну фахову оцінку, підтвердити наукову обґрунтованість запропонованих рішень та їх практичну значущість для розвитку методів управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури.

Наведені відомості свідчать про достатній рівень апробації результатів дисертаційної роботи та їх відповідність сучасним напрямам розвитку інформаційних технологій.

Ступінь наукової обґрунтованості та достовірності отриманих результатів дисертаційних досліджень

Наукова обґрунтованість і достовірність результатів дисертаційного дослідження забезпечуються коректною постановкою науково-прикладного завдання, використанням сучасних методів системного аналізу, логіко-динамічного моделювання, математичного та імітаційного моделювання, методів аналізу даних, ризик-орієнтованого оцінювання та технологій цифрових двійників.

Обґрунтованість отриманих результатів підтверджується узгодженістю теоретичних положень із відомими науковими результатами у галузі комп'ютерних наук, кібербезпеки та управління інформаційними процесами, а також логічною послідовністю проведених досліджень і розв'язання поставлених завдань.

Достовірність запропонованих моделей, методів та інформаційної технології підтверджена результатами експериментальних досліджень, апробацією на міжнародних наукових конференціях, впровадженням результатів роботи у практичну діяльність установ та організацій, а також їх використанням у навчальному процесі закладу вищої освіти.

Наведене дає підстави вважати, що сформульовані в дисертації наукові положення, висновки та рекомендації є достатньо обґрунтованими, достовірними та мають практичну цінність.

Оцінка рівня виконання поставленого наукового завдання, володіння здобувачем методологією наукової діяльності

Аналіз змісту дисертаційної роботи свідчить про те, що автором у повному обсязі виконано поставлене науково-прикладне завдання щодо розроблення моделей і методів управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури на основі логіко-динамічного моделювання та технології цифрових двійників.

У роботі проведено аналіз сучасного стану проблеми, розроблено логіко-динамічні моделі, методи оцінювання критичності та адаптивного

управління подіями безпеки, запропоновано інформаційну технологію цифрового двійника системи управління подіями безпеки, а також виконано експериментальну перевірку ефективності запропонованих рішень у SIEM/SOC-середовищі.

Дисертаційна робота характеризується логічною послідовністю викладення матеріалу, взаємопов'язаністю наукових результатів та практичною спрямованістю проведених досліджень. Структура роботи є цілісною та завершеною, а сформульовані висновки адекватно відображають зміст проведених досліджень і отримані результати. Рівень виконання дисертаційної роботи, коректність застосованого методичного апарату та якість викладення матеріалу свідчать про належне оволодіння здобувачем методологією наукової діяльності. Дисертація відповідає встановленим вимогам щодо структури та оформлення, а ознак порушення принципів академічної доброчесності в роботі не виявлено.

Таким чином, дисертаційна робота є завершеним науковим дослідженням, у якому успішно вирішено актуальне науково-прикладне завдання у галузі комп'ютерних наук, що має важливе значення для підвищення ефективності управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури.

Зауваження та недоліки:

1. У роботі значну увагу приділено побудові логіко-динамічних моделей процесів управління подіями безпеки, проте окремі питання їх масштабування для територіально розподілених об'єктів критичної інформаційної інфраструктури могли б бути висвітлені більш детально.

2. Під час дослідження технології цифрового двійника основний акцент зроблено на функціях моніторингу, оцінювання та прогнозування подій безпеки. Водночас доцільним було б розширити аналіз можливостей використання запропонованих рішень для автоматизованого формування та реалізації керуючих впливів у контурах SOAR-систем.

3. У дисертаційній роботі наведено результати експериментальних досліджень запропонованих моделей і методів, однак для більш повного підтвердження їх ефективності доцільно було б виконати порівняльний аналіз із ширшим спектром сучасних платформ управління подіями безпеки.

4. Окремі положення, пов'язані з оцінюванням критичності подій безпеки та впливом топологічних особливостей інформаційно-комунікаційних мереж на рівень ризику, мають дискусійний характер і можуть стати предметом подальших наукових досліджень.

Однак, вказані зауваження, недоліки та побажання не мають принципового характеру, не впливають на загальну позитивну оцінку дисертаційної роботи та суттєво не знижують наукової та практичної цінності отриманих результатів дисертаційних досліджень.

Висновок

Дисертаційна робота Самборського Євгена Івановича на тему «Моделі і методи управління подіями безпеки комп'ютерних систем критичних інформаційних інфраструктур» є завершеним самостійним науковим дослідженням, у якому вирішено актуальне науково-прикладне завдання у галузі комп'ютерних наук щодо розроблення моделей, методів та інформаційної технології управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури на основі логіко-динамічного моделювання та технології цифрових двійників.

Отримані результати характеризуються науковою новизною, є обґрунтованими та достовірними, мають теоретичне і практичне значення, пройшли належну апробацію та впроваджені у практичну діяльність і навчальний процес.

Дисертаційна робота відповідає вимогам наказу Міністерства освіти і науки України від 12.01.2017 № 40 «Про затвердження вимог до оформлення дисертації» (зі змінами), а за актуальністю, ступенем наукової новизни, обґрунтованістю та практичною значущістю отриманих результатів відповідає вимогам пунктів 6, 7, 8 «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 (зі змінами, внесеними згідно з Постановами Кабінету Міністрів України № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024).

Автор дисертаційної роботи Самборський Євген Іванович заслуговує на присудження ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Офіційний опонент
доцент кафедри кібербезпеки
факультету кіберборотьби
Військового інституту телекомунікацій
та інформатизації імені Героїв Крут
кандидат технічних наук Олексій ЗАЛУЖНИЙ

ПІДПИС ЗАСВІДЧУЮ
Заступник начальника Військового інституту
телекомунікацій та інформатизації
імені Героїв Крут з наукової роботи
кандидат технічних наук, професор Григорій РАДЗІВІЛОВ