РЕЦЕНЗІЯ

кандидата технічних наук, старшого дослідника Охріменко Тетяни Олександрівни, заступника декана факультету комп'ютерних наук та технологій Національного університету «Київський авіаційний інститут» на дисертацію Самборського Євгена Івановича на тему «Моделі і методи управління подіями безпеки комп'ютерних систем критичних інформаційних інфраструктур», подану на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології»

Актуальність теми дисертаційного дослідження. Стрімка цифровізація сфери державного управління, енергетики, транспорту, телекомунікацій та інших сфер, що належать до критичної інформаційної інфраструктури, супроводжується суттєвим зростанням кількості та складності гібридних інформаційних загроз. За цих умов особливого значення набуває створення ефективних моделей і методів управління подіями безпеки, втілення яких забезпечить своєчасне виявлення, оцінювання критичності та підтримку прийняття рішень щодо реагування на інциденти інформаційної безпеки.

Дисертаційне дослідження Самборського Є.І. присвячене вирішенню актуального науково-прикладного завдання щодо розроблення моделей і методів управління подіями безпеки комп'ютерних систем критичних інформаційних інфраструктур із використанням логіко-динамічного моделювання, інформаційної технології цифрових двійників та інтелектуального аналізу даних.

Запропонований підхід спрямований на підвищення оперативності, достовірності та адаптивності процесів управління подіями безпеки комп'ютерних систем критичних інформаційних інфраструктур в умовах динамічної зміни інформаційних загроз для цих об'єктів.

Актуальність роботи зумовлена тим, що традиційні засоби моніторингу та ідентифікації подій безпеки наразі не забезпечують необхідного рівня ефективності захисту сучасних розподілених інформаційно-комунікаційних систем. Запропоновані автором моделі та методи орієнтовані на комплексне вирішення проблемних задач прогнозування розвитку подій безпеки, оцінювання їхньої критичності та автоматизації підтримки прийняття й реалізації управлінських рішень.

Таким чином, тема дисертації є актуальною, повністю відповідає сучасним тенденціям розвитку комп'ютерних наук та має важливе теоретичне і практичне значення для підвищення стійкості функціонування об'єктів критичних інформаційних інфраструктур.

Ступінь обґрунтованості та достовірності наукових положень, висновків і рекомендацій, сформульованих у дисертації. Наукові положення, висновки та рекомендації, наведені у дисертації, є достатньо обґрунтованими і достовірними. Їх обґрунтованість забезпечується коректною постановкою наукового завдання, використанням сучасних методів системного аналізу, логіко-динамічного підходу, математичного моделювання, методів аналізу даних та технологій цифрових двійників, адекватних меті й завданням дослідження.

Достовірність отриманих результатів підтверджується їх експериментальною перевіркою, узгодженістю теоретичних положень із результатами моделювання, а також апробацією основних результатів на наукових конференціях і публікацією у фахових наукових виданнях. Зроблені та викладені в дисертації висновки є логічними, взаємопов'язаними, повністю відповідають поставленій меті дослідження та випливають із отриманих автором результатів.

Наукова новизна одержаних результатів дисертаційних досліджень. Наукова новизна результатів дисертаційної роботи здобувача Самборського Є.І. полягає в комплексному розв'язанні актуального науково-прикладного завдання управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури на основі поєднання логіко-динамічного моделювання, технології цифрового двійника та сучасних методів інтелектуальної обробки даних. У роботі запропоновано цілісну науково-методичну концепцію, у межах якої моделі, методи, інформаційна технологія та алгоритмічні рішення утворюють взаємопов'язану систему підтримки прийняття рішень у процесах управління подіями безпеки комп'ютерної системи.

До найбільш вагомих результатів, що визначають наукову новизну дисертації, слід віднести розроблення логіко-динамічної моделі управління подіями безпеки, яка забезпечує формалізований опис станів комп'ютерної системи, їх часової еволюції та причинно-наслідкових зв'язків між подіями безпеки.

Значний науковий інтерес також становить запропонований метод адаптивного управління подіями безпеки. Він реалізує перехід від реактивного до проактивного управління подіями безпеки за рахунок використання цифрового двійника як інструмента для аналізу, прогнозування та підтримки прийняття управлінських рішень.

Важливою складовою наукової новизни є розроблена інформаційна технологія побудови цифрового двійника системи управління інформацією і подіями безпеки. Вказана технологія гнучко інтегрує логіко-динамічне моделювання, засоби збору й аналізу телеметричних даних, механізми кореляції подій та сценарний аналіз розвитку безпекових інцидентів. Запропонований автором дисертації підхід створив наукові передумови для підвищення ефективності функціонування сучасних SIEM/SOC-систем інформаційно-комунікаційних мереж та забезпечує більш обґрунтоване оцінювання критичності подій безпеки.

Позитивною рисою дисертації є те, що отримані наукові результати не носять фрагментарного характеру. Вони логічно взаємопов'язані та формують завершену систему моделей, методів і практичних рішень, орієнтованих на підвищення ефективності управління подіями безпеки критичних інформаційних інфраструктур.

Отримані автором результати відповідають критеріям наукової новизни, розширюють існуючі наукові підходи до управління подіями безпеки комп'ютерних систем критичних інформаційних інфраструктур. Ці результати є вагомим особистим внеском здобувача у розвиток теоретичних засад і практичних методів управління подіями безпеки.

Повнота викладу матеріалів дисертації в опублікованих наукових працях, особистий внесок здобувача. Розроблені наукові положення, математичні моделі, методи, інформаційна технологія, алгоритмічні рішення та результати експериментальних досліджень отримані автором самостійно. У публікаціях, виконаних у співавторстві, використано виключно результати, що належать здобувачу особисто, про що чітко зазначено в дисертації. Характер дослідження, внутрішня логіка побудови роботи, взаємозв'язок між теоретичними положеннями, математичним апаратом, програмною реалізацією та експериментальною перевіркою свідчать про самостійність виконання дисертаційних досліджень і належний рівень наукової кваліфікації дисертанта.

Основні наукові результати дисертаційного дослідження всебічно та у повному обсязі висвітлені у наукових публікаціях автора. Основні результати дослідження пройшли належну апробацію на наукових форумах, що підтверджується їх фаховим обговоренням науковою спільнотою.

Наведені матеріали дають підстави стверджувати, що дисертація відповідає вимогам Постанови Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами) щодо повноти апробації та оприлюднення результатів дисертаційного дослідження, а також підтверджують належний особистий внесок здобувача у отримання наведених наукових результатів.

Вказане свідчить, що повнота оприлюднення результатів дослідження, їх апробація у фаховому науковому середовищі, відповідність опублікованих праць змісту дисертації та підтверджений особистий внесок здобувача дають підстави вважати, що результати дисертаційної роботи відповідають вимогам чинного законодавства, а рівень їх наукового представлення є достатнім для дисертації на здобуття ступеня доктора філософії.

Апробація результатів дослідження, повнота їх висвітлення у наукових публікаціях та особистий внесок здобувача. Основні результати дисертаційного дослідження пройшли належну апробацію та були представлені на восьми міжнародних і всеукраїнських науково-технічних та науково-практичних конференціях, що свідчить про їх широке фахове обговорення у науковому середовищі. За результатами дослідження опубліковано достатню кількість наукових праць, у яких повною мірою відображено основні положення, висновки та практичні результати дисертаційної роботи.

Загалом вважаю, що апробація результатів дослідження, повнота їх висвітлення у наукових публікаціях та особистий внесок здобувача відповідають вимогам Постанови Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами) та є достатніми для дисертаційної роботи на здобуття ступеня доктора філософії.

Практичне значення одержаних результатів. Практичне значення дисертаційної роботи полягає у доведенні можливості використання запропонованих моделей, методів та інформаційної технології цифрового двійника для підвищення ефективності управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури. Розроблені автором наукові рішення орієнтовані на практичне застосування під час проєктування, впровадження та експлуатації сучасних систем моніторингу й управління інформаційною безпекою та забезпечують скорочення часу

виявлення й аналізу інцидентів, підвищення обґрунтованості їх пріоритизації та підтримку прийняття управлінських рішень.

Важливою перевагою дисертаційної роботи є підтвердження практичної цінності отриманих результатів їх впровадженням у діяльність трьох організацій різного профілю та видів діяльності.

Результати дослідження впроваджено у Волинському національному університеті імені Лесі Українки. У цьому навчальному закладі вони використовуються в освітньому процесі під час підготовки фахівців з комп'ютерних наук і інформаційних технологій, що сприяє суттєвому підвищенню якості професійної підготовки здобувачів вищої освіти.

Практична ефективність запропонованих рішень підтверджена також їх реалізацією у діяльності ТОВ «CI2», де використання розроблених моделей і методів дозволило підвищити ефективність оброблення подій інформаційної безпеки та оптимізувати процеси виявлення інцидентів у корпоративних комп'ютерних мережах.

Також результати впроваджено у Державній службі спеціального зв'язку та захисту інформації України. Використання запропонованих автором моделей і методів спрямоване на підвищення рівня захищеності об'єктів критичної інформаційної інфраструктури, скорочення часу реагування на інциденти інформаційної безпеки та підвищення ефективності функціонування відомчих інформаційно-комунікаційних мереж. Такий рівень впровадження свідчить про практичну затребуваність результатів дисертації у сфері забезпечення інформаційної безпеки держави.

Таким чином, практичне значення дисертації підтверджується не лише наявністю актів впровадження, а й різноплановістю сфер застосування отриманих результатів - у закладі вищої освіти, на підприємстві та в державному органі, відповідальному за захист критичної інформаційної інфраструктури. Це свідчить про універсальність запропонованих рішень, їх прикладну цінність та готовність до практичного використання.

Структура та зміст дисертації. Структура дисертаційної роботи є логічною, послідовною та складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел і додатків. Основний зміст викладено на 200 сторінках, робота містить 50 рисунків, 53 таблиці та 130 найменувань використаних джерел, що свідчить про достатній рівень інформаційного забезпечення проведеного дослідження.

У першому розділі виконано аналіз сучасного стану проблеми та обґрунтовано напрями дослідження; у другому – розроблено теоретичні засади, математичні моделі та методи оцінювання подій безпеки; у третьому – запропоновано метод адаптивного управління та інформаційну технологію цифрового двійника; у четвертому – наведено результати експериментальних досліджень, оцінено ефективність запропонованих рішень і підтверджено можливість їх практичного застосування. Представлена автором структура роботи забезпечує логічний взаємозв'язок між усіма етапами дослідження та послідовне досягнення поставленої мети.

Особливістю дисертаційної роботи є її комплексний характер. Автор послідовно поєднав теоретичні дослідження з розробленням математичних

моделей, методів, інформаційної технології, алгоритмічного та програмного забезпечення, завершивши роботу їх експериментальною перевіркою та практичним впровадженням. Такий підхід свідчить про завершеність наукового дослідження та його прикладну спрямованість.

Структура, зміст та оформлення дисертації відповідають вимогам Постанови Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами), а також вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії. Зміст роботи повною мірою розкриває тему дослідження, забезпечує досягнення поставленої мети та вирішення визначених наукових завдань.

Оцінка мови та стилю дисертації. Відомості про відсутність текстових запозичень та порушень академічної доброчесності. Дисертаційна робота викладена державною мовою, характеризується чітким, логічним і послідовним стилем викладу матеріалу. Використана наукова термінологія є коректною, сучасною та відповідає предметній області комп'ютерних наук. Матеріал структурований, результати дослідження викладені послідовно, а сформульовані положення, висновки та рекомендації є зрозумілими, аргументованими й достатньо обґрунтованими.

Під час рецензування дисертаційної роботи не виявлено ознак академічного плагіату, фабрикації, фальсифікації або інших порушень академічної доброчесності. Використання наукових праць інших авторів здійснено з належними посиланнями на джерела, а запозичення мають коректний характер і не порушують вимог академічної етики. Подані у дисертації результати мають ознаки самостійно виконаного наукового дослідження, що узгоджується із заявленим особистим внеском здобувача.

Відповідність дисертації спеціальності та рекомендації щодо подальшого розвитку досліджень. Зміст дисертаційної роботи, сформульовані мета, завдання, об'єкт і предмет дослідження, використаний математичний апарат, розроблені моделі, методи, інформаційна технологія та отримані наукові результати повністю відповідають спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Дисертація присвячена розробленню моделей, методів і інформаційних технологій аналізу та управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури, що повністю узгоджується з предметною областю зазначеної спеціальності.

Дисертаційна робота є завершеним науковим дослідженням, а висловлені нижче рекомендації не знижують її наукової та практичної цінності й можуть бути враховані автором у подальших дослідженнях.

1. Доцільно в подальшому розширити дослідження у напрямі інтеграції запропонованої технології цифрового двійника з хмарними та розподіленими платформами управління подіями безпеки, що сприятиме значному підвищенню масштабованості розроблених рішень.

2. Перспективним є подальший розвиток методів прогнозування подій безпеки із застосуванням сучасних моделей штучного інтелекту та генеративних технологій для підвищення точності виявлення складних багатостадійних загроз.

3. Практичний інтерес становить експериментальна перевірка запропонованих моделей на ширшому спектрі об'єктів критичної інформаційної

інфраструктури, зокрема в енергетичній, транспортній та промисловій галузях, що дозволить оцінити універсальність запропонованих підходів.

Таким чином, дисертаційна робота за своїм змістом, предметною областю дослідження, використаними методами та отриманими результатами повністю відповідає спеціальності 122 «Комп'ютерні науки». Наведені рекомендації мають перспективний характер, не впливають на загальну позитивну оцінку дисертації та визначають можливі напрями подальшого розвитку отриманих наукових результатів.

Загальна оцінка дисертаційної роботи. Дисертаційна робота справляє позитивне враження як цілісне завершене наукове дослідження, виконане на актуальну тему та спрямоване на вирішення важливого науково-прикладного завдання у сфері комп'ютерних наук.

Автором послідовно реалізовано повний цикл наукового дослідження: від аналізу сучасного стану проблеми й обґрунтування теоретичних засад до розроблення моделей, методів, інформаційної технології, програмної реалізації, експериментальної перевірки та практичного впровадження отриманих результатів.

Особливістю дисертації є її системний характер. У роботі сформовано цілісну науково-методичну систему, що поєднує логіко-динамічне моделювання, технологію цифрового двійника, методи аналізу даних та механізми підтримки прийняття рішень у єдиному контурі управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури. Саме ця комплексність, на мою думку, є найбільш вагомою науковою перевагою дисертаційної роботи Самборського Є. І.

Результати дослідження характеризуються належним рівнем наукової новизни, теоретичної обґрунтованості, практичної значущості та підтверджуються експериментальними дослідженнями, апробацією, науковими публікаціями й актами впровадження. Отримані результати мають не лише наукову, а й практичну цінність, що підтверджується їх використанням закладами вищої освіти, діяльності ІТ-підприємства та державного органу, який забезпечує захист критичної інформаційної інфраструктури України.

У цілому дисертаційна робота є самостійним, логічно завершеним і якісно виконаним науковим дослідженням, результати якого становлять вагомий внесок у розвиток моделей і методів управління подіями безпеки комп'ютерних систем критичної інформаційної інфраструктури та мають перспективи подальшого наукового і практичного розвитку.

На підставі всебічного аналізу дисертаційної роботи, її змісту, наукових положень, одержаних результатів, їх теоретичної обґрунтованості, практичної значущості, рівня апробації та повноти висвітлення у наукових публікаціях зроблено висновок, що дисертаційна робота на тему «Моделі і методи управління подіями безпеки комп'ютерних систем критичних інформаційних інфраструктур» є завершеним, самостійно виконаним науковим дослідженням, у якому розв'язано актуальне науково-прикладне завдання, що має істотне значення для розвитку комп'ютерних наук, зокрема у сфері забезпечення сталого функціонування критичних інформаційних інфраструктур.

Висловлені у рецензії зауваження мають рекомендаційний характер, стосуються переважно перспектив подальшого розвитку дослідження та не впливають на загальну позитивну оцінку дисертаційної роботи, її наукової новизни, достовірності, теоретичної та практичної цінності.

Таким чином, дисертаційна робота повністю відповідає вимогам, установленим Законом України «Про вищу освіту», Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженим постановою Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами), а також вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії.

З огляду на вищезазначене, вважаю, що САМБОРСЬКИЙ Євген Іванович заслуговує на присудження йому ступеня доктора філософії у галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Рецензент
заступник декана факультету комп'ютерних наук
та технологій Національного університету
«Київський авіаційний інститут»
кандидат технічних наук, старший дослідник Тетяна ОХРІМЕНКО