ВІДГУК

офіційного опонента

доктора технічних наук, професора **Хлапоніна Юрія Івановича**

на дисертаційну роботу **Войцеховської Марії Михайлівни**

на тему:

„Інформаційна технологія оцінювання рівня культури інформаційної безпеки організації” на здобуття наукового ступеня доктора філософії, поданої до офіційного захисту в разовій спеціалізованій вченій раді ДФ 79.051.002 Національного університету "Чернігівська політехніка", МОН України за спеціальністю 122 – Комп’ютерні науки

Актуальність теми дисертації визначається тим, що активний еволюційний розвиток технологій, мобільність та доступність послуг в найближчий перспективі стануть одними з рушійних сил успішної бізнес-діяльності організації, установи. Інвестиції в інформаційні активи оцінюються нарівні з матеріальним капіталом, і захист цих інформаційних активів заслужено потребує посиленої уваги. Незважаючи на інтенсивний розвиток технічних засобів захисту інформації, на які власники та особи, відповідальні за інформаційні активи, покладаються в більшості випадків, працівники все ще залишаються не останнім фактором, що впливає на безпеку та цілісність інформаційних активів організації. Захищеність ресурсів, обчислювальної потужності, програмного забезпечення та інтересів користувачів все ще залежить від здатності персоналу протистояти зовнішнім та внутрішнім інформаційним загрозам, здібності своєчасно розпізнавати шкідливі впливи, запобігати виникненню та вчасно реагувати на критичні ситуації.

Однак на даний час інформаційні технології оцінювання рівня інформаційної безпеки спрямовані на оцінку ризиків, які враховують різноманіття ресурсів та їх цінність, загрози та вразливості систем, і майже не враховують важливі фактори безпеки внаслідок людино-машинної взаємодії. Це питання визначається напрямком забезпечення культури інформаційної безпеки організації, яка акцентує увагу на визначенні належних організаційних заходів для формування безпечної поведінки користувачів та адміністраторів інформаційної системи організації.

Культура інформаційної безпеки як наукове явище сьогодні формується на

рівні міжгалузевого комплексного соціоінженерного інституту (наукової дисципліни), який утворився на межі поєднання технічних і гуманітарних наук: правової інформатики, інформаційного права та тектології (теорії організації соціальних систем).

Отже розробка методів, моделей та інформаційної технології оцінювання рівня культури інформаційної безпеки організації є **актуальною науково-прикладною** задачею.

Метою дисертаційної роботи є розробка моделей та методів інформаційної технології комплексного оцінювання рівня культури інформаційної безпеки організації з урахуванням особливостей людино-машинної взаємодії, для підтримки прийняття рішень щодо забезпечення відповідного показника безпеки організації.

Об'єктом дослідження є інформаційні процеси визначення культури інформаційної безпеки організації.

Предметом дослідження є методи, моделі та інформаційна технологія комплексної оцінки рівня культури інформаційної безпеки організації з врахуванням особливостей людино-машинної взаємодії.

Наукова новизна та практична цінність отриманих в дисертаційній роботі результатів.

Наукова новизна результатів, отриманих у дисертаційній роботі:

Вперше:

– розроблена модель інформаційного процесу оцінювання рівня КІБ організації, яка на відміну від існуючих, містить аспекти людино-машинної взаємодії і враховує фактори персональної культури безпеки учасників процесу;

– розроблено метод автоматизованої оцінки рівня КІБ організації, який на відміну від існуючих, базується на використанні нечіткої логіки на основі алгоритму Мамдані, і дозволяє виконувати оцінку поетапно на різних організаційних рівнях.

Набули подальшого розвитку:

– структура системи ІБ організації за рахунок включення факторів персональної КІБ, що дозволяє враховувати вплив людського чинника на загальну систему безпеки організації;

– метод оцінки рівня персональної КІБ на основі компетентнісного

підходу за рахунок використання логіки антонімів, що забезпечує підвищення ефективності проведення таких оцінок.

Практична цінність отриманих результатів.

Наведені вище наукові результати у своїй сукупності утворюють нову інформаційну технологію оцінювання рівня культури інформаційної безпеки організації. Запропонована інформаційна технологія може бути корисною для керівників ІБ-підрозділів та організацій для підтримки впроваджених систем забезпечення інформаційної безпеки. Розроблені бізнес-процеси та архітектура можуть бути використані як основа для розроблення власних систем моніторингу культури інформаційної безпеки; модель оцінки персональної культури інформаційної безпеки – при призначенні певних рівнів доступу до інформаційних систем; моніторингу поточного рівня культури інформаційної безпеки персоналу, структурного підрозділу та саме організації для визначення прогалин в обізнаності та компетенцій в галузі ІБ; формуванні команд реагування на інциденти, тощо.

Дана інформаційна технологія має наступне практичне втілення.

Модель нечіткого логічного виводу дає можливість проводити оцінку рівня культури інформаційної безпеки без спеціальних навичок, що значно розширює можливості її використання в неспеціалізованих організаціях.

Забезпечення швидкого самооцінювання виконується за допомогою розробленої автоматизованої телефонної системи (чатботу).

Результати дисертаційного дослідження впроваджені:

– при виконанні міжнародного наукового проекту «Cyber Rapid Analysis for Defense Awareness of Real-time Situation – CyRADARS» за грантом NATO SPS, (grant agreement number: G5286)», науково-дослідних робіт Національного університету «Чернігівська політехніка» «Моделі та методи оцінювання конвергенції систем компетентностей фахівців з використанням технологій штучного інтелекту» (№0120U101929), «Розробка моделей та методів захисту системи від зовнішніх атак з використанням технологій штучного інтелекту» (№0120U101931), а також науково-дослідної роботи «Розвиток базового моделюючого комплексу мережі ситуаційних центрів державних органів сектору безпеки і оборони України в інтересах захисту критичної інфраструктури держави та кібербезпеки»

(№0119U000058т) Інституту проблем математичних машин і систем Національної академії наук України;

– на ПАТ «ЧЕЗАРА» під час впровадження тестування персоналу на стадії підбору та приймання на роботу на предмет виявлення базового рівня персональної культури інформаційної безпеки;

– в Державному науково-випробувальному інституті випробувань та сертифікації озброєння та військової техніки при розробці документації інформаційних систем «Інформаційна система з доступом до мережі Internet (ІСД-Internet)» та «Система електронного документообігу (СЕДО)»;

– у навчальному процесі Чернігівського національного технологічного університету (Національного університету «Чернігівська політехніка») при проведенні лекцій та лабораторних робіт з дисципліни «Моделі та системи штучного інтелекту» – в процесі навчання бакалаврів спеціальності 121 – «Інженерія програмного забезпечення» на кафедрі інформаційних технологій та програмної інженерії.

Методи досліджень, які використані в дисертаційній роботі. Для вирішення поставлених наукових завдань використовуються аналітичні: *принципи системного аналізу та теорії множин*, які використані при аналізі показників культури інформаційної безпеки (КІБ) організації та її працівників, а також при побудові технології оцінювання рівня КІБ організації; *емпіричні методи отримання інформації*, що були застосовані для організації збору первинної інформації шляхом анкетування та подальшої обробки результатів; *методи експертних оцінок.*

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації. Автор добре розуміє специфіку науково-прикладної задачі, що розглядається у дисертації та точно формулює її постановку.

Репрезентативність результатів дослідження базується на вдалому плануванні наукових досліджень із застосуванням комплексного підходу, адекватній статистично-математичній обробці отриманих результатів, що дозволило ґрунтовно аргументувати положення та висновки дисертаційної роботи. У дисертації Войцеховської М.М. чітко окреслено об’єкт, предмет, мету та методи дослідження,

визначено його завдання та представлено досягнуті результати. В логічній послідовності, відповідно до обраної структури дисертації, висвітлено зміст здійсненого дослідження, розкрито теоретичне підґрунтя та викладено практичні результати. Слід відмітити, що здобутки дослідження достатньо повно викладені у 18 наукових працях, серед яких фахові вітчизняні та закордонні видання, збірники наукових праць та тези доповідей на науково-практичних конференціях, в тому числі і міжнародних. Наукова вагомість вказаних публікацій підтверджується тим фактом, що 4 з них опубліковано у виданнях, що індексуються в міжнародній наукометричній базі Scopus. Апробація результатів дослідження відбулася в процесі обговорення та виступів на 13 міжнародних, всеукраїнських та регіональних наукових конференціях.

Обсяг друкованих робіт та їх кількість відповідають вимогам МОН України щодо публікації основного змісту дисертації на здобуття наукового ступеня доктора філософії. Загалом, слід зазначити, що дисертація є завершеною науковою роботою, в якій отримано нові наукові результати, що мають теоретичне та практичне значення.

Зв’язок дисертаційної роботи з науковими програмами, планами, темами. Представлена дисертаційна робота запланована та виконана в рамках пріоритетного напряму розвитку науки і техніки в Україні «Інформаційні та комунікаційні технології» (Закон України про внесення змін до Закону України про пріоритетні напрями розвитку науки і техніки від 9 вересня 2010 року, № 2519-VI) за пріоритетними тематичними напрямами «Технології та інструментальні засоби електронного урядування. Інформаційно-аналітичні системи, системи підтримки прийняття рішень. Ситуаційні центри» та «Технології та засоби захисту інформації» (відповідно до постанови КМУ «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2020 року» від 07.09.2011 №942).

Обраний у роботі напрямок досліджень тісно пов'язаний з виконанням низки науково-дослідних робіт, у реалізації яких брала участь автор.

Теоретичні і практичні положення дисертаційної роботи були використані та реалізовані в в рамках міжнародного наукового проекту «Cyber Rapid Analysis for

Defense Awareness of Real-time Situation – CyRADARS» за грантом NATO SPS, (grantagreementnumber: G5286)», відповідно до плану науково-дослідних робіт Національного університету «Чернігівська політехніка» «Моделі та методи оцінювання конвергенції систем компетентностей фахівців з використанням технологій штучного інтелекту» (№0120U101929), «Розробка моделей та методів захисту системи від зовнішніх атак з використанням технологій штучного інтелекту» (№0120U101931) та Інституту проблем математичних машин і систем Національної академії наук України «Розвиток базового моделюючого комплексу мережі ситуаційних центрів державних органів сектору безпеки і оборони України в інтересах захисту критичної інфраструктури держави та кібербезпеки» (№0119U000058т).

Результати дисертаційної роботи пропонуються для використання профільним науково-дослідними установам та галузевим підприємствам України при створенні перспективних, а також при удосконаленні існуючих систем забезпечення інформаційної безпеки.

Оцінка змісту дисертації, її завершеність у цілому, відповідність оформлення дисертації вимогам, затвердженим МОН України.

У вступі обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету та завдання дослідження, визначено об’єкт, предмет і методи дослідження, описано наукову новизну й практичне значення одержаних результатів. Наведено відомості про впровадження результатів роботи, апробацію, особистий внесок здобувача та публікації.

У першому розділі проведено аналітичний огляд сучасного стану ІБ на рівні організацій. Результати аналізу звітів за кіберінцидентами показали постійну присутність атак типу «man in the middle». Людина залишається в центрі уваги атакерів. Відкритість та велика кількість інформації надає необмежені можливості для пошуку індивідуального підходу до жертви. Більшість користувачів соціальних мереж забувають про втрату контролю над особистою інформацією після її публікації в мережі. Крім того, користувачі забувають про ймовірність бути використаними для отримання, здавалося б, некритичної інформації, яка потім може бути використана для здійснення атаки, пов’язаної з їх професійною діяльністю.

Показано, що існуючі методи оцінки ІБ організацій пов’язані з певними ускладненнями із самими методологіями оцінки та невизначеністю характеристик, з якими доведеться зіткнутися експертам. Також, у випадку діяльності організації-початківця, чиї можливості обмежені досвідом та кваліфікацією працівників, невеликим бюджетом та рядом інших факторів, що відтісняють на другий план проблеми ІБ, розробка та впровадження СЗІБ покладена на ІТ-фахівців, здебільшого системних адміністраторів, що значно зменшує її ефективність.

Формування КІБ організації на необхідному рівні може бути вирішена за допомогою використання підходів формування та підсилення корпоративної культури організації. Підсилення КІБ має бути засновано на підвищенні технологічної культури персоналу через підвищення обізнаності в галузі ІБ та залученні керівництва до розвитку КІБ організації.

Сформульована науково-прикладна задача дослідження – розробка інформаційної технології оцінювання рівня культури інформаційної безпеки організації. З метою надання допомоги співробітникам ІТ-підрозділу, в якості набору основних рекомендацій щодо створення КІБ належного рівня, доцільною буде розробка інформаційної системи, яка дозволить визначити рівень наявної КІБ та сформувати ряд рекомендацій щодо усунення або зменшення ризиків, підсилення наявної СЗІБ організації.

У другому розділі запропонована модель визначення вимог до рівня КІБ працівників, яка враховує роль співробітника у загальній системі інформаційної безпеки організації та пов’язані з нею ІБ-ризики. Вона містить технічні та персональні аспекти людино-машинної взаємодії тавраховує ризики, пов’язані з професійною діяльністю; визначені вимоги до персональної КІБ співробітників різних організаційних рівнів та їх оцінка, які покладені в основу моделі оцінки рівня КІБ організації. Запропонована модель може бути використана як для оцінки поточної ситуації з наданням рекомендацій щодо заходів посилення КІБ, так і для отримання пропозицій щодо можливих посад під час оцінки кандидатів; розроблена модель системи інтегральної оцінки рівня КІБ організації, яка враховує розмежування вимог до компетентності в галузі ІБ залежно від ролі, яку співробітники відіграють у загальній системі ІБ організації. Перехід від якісних до кількісних показників здійснюється шляхом використання методів нечіткої

логіки.Такі перетворення можуть відбуватися на останніх трьох рівнях оцінювання, в залежності від того, в якій формі (якісній або кількісній) бажано отримати показники. Інтегральний показник рівня КІБ персоналу можна використовувати при проведенні аудиту системи забезпечення ІБ організації, а також при оцінюванні ефективності впровадження заходів для її розвитку та вдосконалення.

В якості набору основних рекомендацій щодо забезпечення відповідного рівня КІБ організації пропонується розробити інформаційну систему, яка визначатиме рівень існуючої КІБ організації, включаючи оцінку рівня персональної КІБ.

У третьому розділі запропонована концепція інформаційної системи, яка дозволяє визначити поточний рівень КІБ організації, виходячи з результатів оцінки обізнаності співробітників в галузі інформаційної безпеки. Рекомендації щодо заходів з підвищення рівня КІБ формуються з врахуванням ризик-аналізу в галузі ІБ та вимог згідно класу критичності організації або підприємства. Для реалізації інформаційної системи запропоновано архітектуру, що представлена 6 модулями, які забезпечують послідовне виконання технологічних етапів оцінювання КІБ.

Система передбачає можливість створення унікальних моделей (таких як модель ІБ-компетенцій користувачів, структурна модель організації, ролі в рамках посадових обов’язків, та ін.) залежно від класу критичності, до якого належить організація. Використання бази правил забезпечує спрощене створення та редагування СНВ, що, знов ж таки, реалізує можливість адаптації інформаційної системи до оцінювання об’єктів будь-якого класу критичності.

Запропонована система враховує відповідність наявних ІБ-компетенцій працівників до вимог, аналіз системи заходівз розвитку КІБ організаціїта її підтримки на належному рівні, ступінь розвитку співпраці з державними та міжнародними спеціалізованими спільнотами, тощо. За результатами оцінювання система формує набір рекомендацій а рівні структурної одиниці та користувача, а також загальну оцінку рівня КІБ організації.

Четвертий розділ присвячено результатам практичного впровадження запропонованих моделей та методів. Елементи запропонованої інформаційної технології отримали перевірку у вигляді проведеного збору первинної інформації шляхом анкетування з використанням хмарних сервісів. Така форма опитування дозволила створитиі загальні, і індивідуальні набори питань, що спрямовані на

висвітлення певних аспектів ІБ у професійній діяльності працівників. Отримані результати були опрацьовані за допомогою запропонованої нечіткої моделі оцінки персонального рівня КІБ, що виявило «вузькі місця» у системі інформаційної безпеки аспектів людино-машинної взаємодії в рамках бізнес-процесів організації. Це дозволило запропонувати рекомендації щодо підвищення рівня персональної культури інформаційної безпеки.

Розроблений чат-бот забезпечує самооцінювання персонального рівня КІБз подальшими результатами та рекомендований до використання у невеликих організаціях, які не мають можливостей проведення повного аудиту системи інформаційної безпеки.

Підтвердження повноти викладу основних результатів дисертації в наукових фахових виданнях. Наукова новизна безсумнівна та достатня для дисертації доктора філософії. Основні наукові і практичні результати, що отримані в ході дисертаційного дослідження, опубліковано з необхідною повнотою в 18 наукових працях, 4 з них опубліковано у виданнях, що індексуються в міжнародній наукометричній базі Scopus. Зроблено 11 доповідей на міжнародних, всеукраїнських та регіональних наукових конференціях.

Відповідність дисертації встановленим вимогам. Дисертація Войцеховської Марії Михайлівни написана сучасною науково-технічною мовою, послідовно, логічно та відповідає вимогам Наказу Міністерства освіти і науки України від 12.01.2017 № 40 «Про затвердження Вимог до оформлення дисертації». Щодо висвітлення основних наукових результатів, дисертація відповідає вимогам Постанови КМУ від 6 березня 2019 р. № 167 «Про проведення експерименту з присудження ступеня доктора філософії».

Відсутність (наявність) порушення академічної доброчесності.

Підтвердженням відсутності порушень принципів академічної доброчесності автором дисертаційного дослідження є результати перевірки роботи сервісом Strike Plagiarism, аналіз публікацій здобувача, аналіз тексту дисертаційного дослідження та використаних автором джерел.

Зауваження щодо змісту дисертації та її оформлення.

Разом з тим уважний аналіз наукового доробку Войцеховської М.М. дозволяє

зробити певні зауваження та пропозиції:

1. При визначенні властивостей інформації (Конфіденційність, Цілісність, Доступність) здобувач робить посилання на російський навчальний посібник [8], в той час, коли дані визначення наведені в нормативних документах, зокрема в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу". Крім того, здобувач констатує, що *інформація, визначається організацією як цінна*, хоча в більшості випадків організація має виконати вимоги нормативних документів (Закони, Постанови КМ України та НД Держспецзв'язку тощо) щодо віднесення інформації до такої, яка потребує захисту.

2. При створенні комплексних систем захисту інформації в ІТС розробляється модель порушника, яка відображає його практичні та потенційні можливості, апріорні знання, час та місце дії, тощо. При визначенні вимог до рівня персональної КІБ різних учасників інформаційних процесів в корпоративних мережах на рис. 2.1. (стор. 65) бажано було би навести специфікації моделі порушника, а саме: моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ІТС, за показником можливостей використання засобів ІТС для реалізації загроз, за часом дії, за містом дії. В даному контексті мова йде про потенційного внутрішнього порушника - учасника інформаційних процесів в ІТС.

3. На стор. 45 дисертації констатується, що зараз майже кожна сучасна компанія має офіційний профіль у Facebook та власний веб-сайт. Основними елементами є опис послуг або продуктів, інформація про менеджерів або продавців (імена, прізвища та посади), а також канали для зв'язку (гаряча лінія, електронна та фізична пошти, месенджери та інші комунікації). Така інформація є конфіденційною або службовою. Але ж матеріали, які можуть відображатися в інтернеті мають бути визначені в політиці безпеки організації. А відповідно до ПКМ України від 12 квітня 2002 р. N 522 "Про затвердження Порядку підключення до глобальних мереж передачі даних" локальні обчислювальні мережі, а також окремі ПК, на яких обробляють або зберігають інформацію з обмеженим доступом, що є об'єктом державної власності і охороняється згідно з законодавством, забороняється підключати до глобальних мереж.

4. Потребує пояснення, яким чином обираються W_1 і W_2 – вагові коефіцієнти,

встановлені для властивостей (ІБ-компетенцій) C_1 і C_2.

5. Потребує пояснення застосування IDEF0 - методології функціонального моделювання, призначеної для формалізації і опису бізнес-процесів. Як витримана вимога IDEF0 щодо її акценту на підпорядкованість об'єктів від формулювання вимог до рівня КІБ організації через оцінку рівня КІБ організації до створення звіту та надання рекомендацій ?

6. Потребує пояснення Рис. 2.18 – Графічна модель забезпечення КІБ в організації, оскільки він не має входу та виходу, а один з блоків на підписаний.

7. Не зовсім зрозуміло, як визначався вид функції належності в різних підсистемах моделі визначення культури інформаційної безпеки організації, а також у тексті не приведено прикладів бази правил нечіткої системи.

8. На мій погляд, варто було б приділити більше уваги технічній складовій системи забезпечення інформаційної безпеки, адже переважна більшість поведінкових відхилень (як з боку користувачів, так і мережі) виявляється спеціалізованими програмними засобами.

Висловлені зауваження не носять принципового характеру та не применшують значимості роботи, а лише пропонують можливі шляхи подальшого розвитку та вдосконалення досліджуваних проблем.

Висновки

Проведений аналіз дає підстави зробити висновок про те, що дисертація Войцеховської Марії Михайлівни на тему «Інформаційна технологія оцінювання рівня культури інформаційної безпеки організації» подана на здобуття наукового ступеня доктора філософії до офіційного захисту в разовій спеціалізованій вченій раді ДФ 79.051.002 Національного університету "Чернігівська політехніка", МОН України за спеціальністю 122 «Комп’ютерні науки» є актуальним дослідженням, що має очевидну наукову та практичну цінність та логічно й аргументовано представляє підхід авторки до розв'язання актуальної науково-прикладної задачі, що пов’язана з розробкою методів, моделей та інформаційної технології оцінювання рівня культури інформаційної безпеки організації, які дозволять автоматизувати

систему визначення поточного рівня культури інформаційної безпеки організації з врахуванням персональних показників співробітників, актуальних ризиків в галузі інформаційної безпеки та нормативних вимог до ведення безпечної діяльності організації в умовах інформатизації.

Таким чином авторка роботи, Войцеховська Марія Михайлівна, заслуговує на присудження їй наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки».

Офіційний опонент

завідувач кафедри кібербезпеки та комп'ютерної інженерії
Київського національного університету будівництва і архітектури
доктор технічних наук, професор Ю.І. ХЛАПОНІН

Підпис Хлапоніна Ю.І. засвідчую:

Секретар вченої Ради

Київського національного університету будівництва і архітектури

О.С. ПЕТРЕНКО