Голові спеціалізованої вченої ради
Д 26.861.06 Державного університету
телекомунікацій
03110, м. Київ, вул. Солом'янська, 7

ВІДГУК

офіційного опонента, доктора технічних наук, професора Міщенка Андрія Віталійовича на дисертаційну роботу Галахова Євгена Миколайовича «Моделі кібератак в системі інформаційної безпеки підприємства на основі використання фріланс-ресурсу», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 «Інформаційна безпека держави»

Актуальність теми. З появою нових ІТ-технологій зростає інтенсивність нових кібератак на ІТ-системи підприємства. Традиційні заходи кібербезпеки не можуть в повному обсязі запобігти частим кібератакам. Комплексна система інформаційної безпеки підприємства включає в себе як тактичні аспекти інформаційного захисту (експрес-аудит інформаційних загроз підприємства), так і стратегічні пріоритети, що відображаються в інформаційній політиці та інформаційній стратегії підприємства. Для забезпечення заданого рівня кібербезпеки необхідно визначити суб'єкти загрози, наміри нападів на ІТ-інфраструктуру та слабкі місця інформаційної безпеки підприємства. Для досягнення зазначених цілей, підприємства потребують нових заходів інформаційної безпеки, які мають значний потенціал розвитку та враховують сучасні тенденції розвитку галузі інформаційної безпеки в цілому. Дослідженню інтенсивності кібератак, їх передбаченню та прогнозуванню в науковій літературі приділено не так багато уваги, що пов'язано зі складністю передбачення кібератак, а також відсутністю сучасних релевантних методів їх прогнозування.

Внаслідок поширення фріланс-відносин (як сучасного типу бізнес-відносин підприємства) постає необхідність в обробці та аналізі статистичних даних кібератак у площині ІТ-діяльності підприємства, що залучає фріланс-ресурс. Ці дослідження мають проводитись з використанням часових кореляцій між кількістю кібератак за період часу з метою передбачення майбутньої інтенсивності кіберінцидентів. Це дозволить створити ефективну систему прогнозування. Отже, передбачення кількості кібератак за встановлений раціональний період часу є необхідним для визначення ефективної частоти аудиту.

Таким чином, на сьогоднішньому етапі розвитку ІТ-інфраструктур підприємств на практиці виявлено існування протиріччя між вимогою до

підвищення ефективності системи інформаційної безпеки підприємства, що залучає фріланс-ресурс, та зниженням рівня кібербезпеки підприємства внаслідок залучення сторонніх осіб до виробничого процесу. Разом із тим, це обумовлює протиріччя в теорії між необхідністю розробки точної моделі динамічної поведінки часових рядів кібератак, дослідженнями уразливостей ІТ-інфраструктури підприємства для попередження кібератак та можливостями існуючих математичних методів розрахунку ефективної частоти аудиту.

Отже, поставлене в дисертації наукове завдання щодо розробки науково-методичного апарату визначення зв'язку між рівнем кіберризику та частотою аудиту, що дає можливість забезпечити ефективну автоматизацію процесів кібербезпеки підприємства, що залучає фріланс-ресурс, є актуальним.

Наукова новизна одержаних результатів. Найбільш суттєвими новими науковими результатами, які одержані автором, є такі:

1. Вперше розроблено математичну модель процесу управління кіберризиками на підприємстві на основі розкладів кусково-неперервних аналітичних апроксимуючих функцій кібератак в ряди Фур'є. Вона дає можливість перейти системі аудиту кіберзагроз підприємства від дискретного до неперервного автоматизованого процесу аудиту. Запропонована модель відрізняється від існуючих моделей тим, що дозволяє визначити рекомендовану частоту для процесу управління кіберризиками на підприємстві, а також визначає основні принципи, ключові питання, підходи щодо ефективної реалізації даної моделі в сучасних умовах діяльності підприємства.

2. Удосконалено методику дослідження уразливостей ІТ-інфраструктури підприємства в моделях кібератак з виокремленням чинників, які впливають на тривалість часу між аудитами. На відміну від існуючих методик, що впроваджують встановлення аудиту кібербезпеки підприємства через однакові проміжки часу, запропонована методика ґрунтується на дослідженні часових рядів кібератак, їх згладжуванні та апроксимації аналітичними функціями, що дає можливість звузити область пошуку оптимального рішення проведення аудиту кібербезпеки підприємства.

3. Набула подальшого розвитку методика визначення оптимального часу проведення спеціального аудиту за умови еластичності та чутливості функції інтенсивності кібератак. Вона відрізняється від існуючих тим, що функціональна залежність інтенсивності кібератак описується нелінійним диференціальним рівнянням Бернуллі та підлягає логістичному закону. Аналіз функції інтенсивності кібератак проводиться аналітично за допомоги степеневого p-перетворення, що дозволяє встановити оптимальний час проведення спеціального аудиту для покращення рівня кіберзахисту і надання пріоритетних та перевірених заходів для зменшення ризику виникнення кіберінциденту.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій. Достовірність висновків і рекомендацій, сформульованих у дисертації, забезпечена теоретичною обґрунтованістю вихідних положень,

кількісним та якісним дослідженням фактичного матеріалу, який отримав дисертант у процесі дослідження.

Зазначимо, що дисертація Галахова Є.М. відзначається як за своїм змістом, так і характером викладу основних теоретичних положень. Текст дисертації характеризується науковим математичним стилем, смисловою завершеністю, цілісністю, що є свідченням високої загальної культури автора, вмінням дисертанта правильно добирати слова, точно і ясно висловлювати наукову думку.

Достовірність результатів досліджень. У роботі дисертант використовував основні положення теорії нелінійних диференціальних рівнянь, математичної теорії наближення (для аналізу часових рядів функції інтенсивності кіберзагроз), теорії ймовірностей і математичної статистики (для оцінювання довірчих інтервалів математичного сподівання нормального розподілу випадкової величини інтенсивності кібератак).

Усі основні результати дисертаційного дослідження підтверджуються комп'ютерним моделюванням та адекватністю математичних викладок, відповідним експериментам, що підтверджує їх достовірність.

Практичне значення одержаних автором наукових результатів полягає в тому, що в роботі на основі аналізу часових рядів інтенсивності кібератак підприємства з проведенням їх аналітичного вирівнювання за допомогою логістичної кривої знайдено інтервал еластичності аналітичної функції інтенсивності кібератак на IT-інфраструктуру підприємства. Обчислено чутливість безрозмірної функції інтенсивності кібератак від параметра p за встановлений часовий період за умови проведення попередньої фільтрації часового ряду за трьома точками. Визначено оптимальний час проведення спеціального аудиту після проведення планового аудиту для підприємств, що залучають фріланс-ресурс.

Запропонований науково-методичний апарат досліджує уразливості, проблеми безпеки, моделі атак мережевої інфраструктури, рівні виправлень, конфігурації сервера, стандартне програмне забезпечення і пропрієтарні додатки. Він дозволяє виокремити найбільш важливі із кібератак, знизити обчислювальну складність, підвищити оперативність обчислень з контролем точності на 15 – 20 % у порівнянні з традиційними обчисленнями, які враховують загальну не агреговану кількість кібератак та підвищити рівень захищеності інформаційної системи на 5 – 7 %. Дослідження також дають можливість агрегування моделей атак для збору статистичної інформації для подальшої її обробки ймовірнісно-статистичними методами.

Результати досліджень прийняті до впровадження в ПрАт «Бліц-Інформ» та ТОВ «А.А.Г.», а також використовуються в навчальному процесі в Державному університеті телекомунікацій для студентів спеціальності 125 «Кібербезпека». Всі впровадження підтверджені відповідними актами, що містяться в додатку дисертації..

Відповідність змісту дисертації встановленим вимогам щодо оформлення. Дисертаційна робота й автореферат написані логічно з дотриманням правил викладу і написанням технічних робіт. Кожен розділ

роботи закінчується логічними висновками. Висновки й рекомендації в достатній мірі відображають основні результати роботи, їх логічну послідовність та необхідні вказівки для розробки методики оцінювання ризиків втрат під час забезпечення інформаційної безпеки фондового ринку.

Стиль викладення матеріалу як в дисертації, так і в авторефераті, дозволяє сприймати поданий матеріал без зайвих зусиль та чітко відстежувати структуру роботи. Автор вірно та однозначно використовує загальновідомі технічні терміни та поняття. Як дисертація, так і автореферат, відповідають вимогам МОН України щодо їх оформлення.

Зміст дисертації і автореферату відповідають паспорту спеціальності 21.05.01 «Інформаційна безпека держави» щодо дисертацій на здобуття наукового ступеня кандидата технічних наук. Слід також відмітити ідентичність змісту автореферату й основних положень дисертації.

Аналіз основного змісту дисертації.

У першому розділі проведено огляд відомої літератури щодо існуючих наукових методів запобігання ненавмисній втраті, пошкодженню чи наданню несанкціонованого доступу до конфіденційної інформації. Це дало можливість окреслити стратегічні пріоритети системи інформаційної безпеки підприємства, що залучає фріланс-ресурс.

Крім того, здійснюється огляд сучасних наукових публікацій для виявлення основних етапів наукових досліджень та подальшого вирішення сформульованого в дисертації наукового завдання. Виявлено протиріччя в теорії та практиці, на основі якого сформульовано наукові завдання дисертаційної роботи, та шляхи їх вирішення. Визначено основні етапи дисертаційних досліджень.

Результати власних наукових досліджень, які направлені на вирішення поставлених наукових завдань, викладаються в другому та третьому розділах.

У другому розділі представлено дослідження уразливостей, моделей кібератак та часових рядів інтенсивності кібератак у площині видів їх загроз на підприємство, що залучає фріланс-ресурс; дослідження підходів до впровадження автоматизованого аудиту на підприємстві у розрізі кіберзагроз; удосконалення методики уразливостей ІТ-інфраструктури підприємства в моделях кібератак; розробка математичної моделі процесу управління кіберризиками на підприємстві на основі рядів Фур'є. Також, проаналізовано уразливості, проблеми безпеки та моделі атак мережевої інфраструктури, рівня виправлень, конфігурації сервера, стандартного програмного забезпечення і пропрієтарних додатків з виявленням найнебезпечніших вірусів кібератак за допомогою знайденої частки у загальній кількості кібератак. Це дає можливість агрегування моделей атак для збору статистичної інформації для подальшої її обробки ймовірнісно-статистичними методами та короткострокового прогнозування для майбутнього упередження.

Третій розділ містить дослідження щодо розробки математичних моделей кібератак у системі інформаційної безпеки підприємства, що залучає

фріланс-ресурс. Представлено аналіз функції інтенсивності кібератак за допомогою степеневого р-перетворення; розроблено алгоритм аналітичного вирівнювання часового ряду логістичною регресією з визначенням інтервалу еластичності функції інтенсивності кібератак; удосконалено методику визначення оптимального часу проведення спеціального аудиту за умови еластичності та чутливості функції інтенсивності кібератак та представлено практичні рекомендації щодо визначення оптимального часу проведення спеціального аудиту на підприємстві, що залучає фріланс-ресурс.

Розглянутий плановий автоматизований аудит на підприємстві у розрізі кіберзагроз типу Спаму. Знайдено розв'язок нелінійного диференціального рівнянням Бернуллі, яке описує процес часового ряду інтенсивності кібератак. Доведено, що інтегральна функція інтенсивності кібератак підлягає логістичному закону, який знайдено в аналітичному вигляді. Одержано інтервал еластичності функції інтенсивності кібератак за часом, що дає можливість визначити часовий інтервал проведення спеціального аудиту кібербезпеки підприємства. Подальшого розвитку набула методика визначення оптимального часу проведення спеціального аудиту за умови еластичності та чутливості функції інтенсивності кібератак, яка відрізняється від існуючих тим, що функціональна залежність інтенсивності кібератак описується нелінійним диференціальним рівнянням Бернуллі та підлягає логістичному закону.

Показано, що запропонований науково-методичний апарат визначення зв'язку між рівнем кіберризику та частотою аудиту надає можливість впровадження автоматизованого аудиту рівня кібербезпеки на підприємстві, що залучає фріланс-ресурс.

Повнота викладення результатів дисертації в публікаціях. Основні наукові положення викладено у 7 наукових статтях, серед яких 5 опубліковані у спеціалізованих фахових виданнях України, 2 опубліковані у закордонних наукових виданнях, з них одна стаття у науковому журналі, що входить до науко-метричної бази SCOPUS. За матеріалами виступів на науково-технічних конференціях опубліковано 11 тез доповідей. Додатково результати досліджень відображені у двох статтях.

Недоліки та зауваження щодо змісту дисертаційної роботи та автореферату.

1. У дисертації не враховано використання групи стандартів ISO 27000 (Overview and vocabulary): підходи, принципи, термінологія. Тому при викладенні результатів досліджень та використання термінології виникають деякі протиріччя даному стандарту. Все це обумовлює доцільність урахування зазначеної групи стандартів.

2. Здобувач в роботі використовує поняття «уразливість», «кіберризик» та «кіберзагроза», але не наведено визначення цих понять.

3. Під час викладення наукових положень в дисертації чітко не прописано, що таке фріланс-ресурс, які особливості враховуються. Разом із тим, у більшості випадків, краще використовувати термін «віддалений доступ».

4. Під час проведення досліджень доцільно було б розглянути дискретне перетворення, бо перехід до неперервних функцій з розкладом в ряд Фур'є відображається на точності прогнозу. Доцільно було б це врахувати та запропонувати більш точну дискретну модель.

5. У дисертації не прописані особливості забезпечення певного рівня кібербезпеки підприємства саме із залученням фріланс-ресурсу. Проте, в роботі немає відомостей, яким чином всі результати досліджень можна застосувати до підприємств без фріланс-ресурсу.

6. У дисертації вирішується лише завдання визначення оптимального терміну аудиту за статистикою спостереження кібератак на підприємстві. На мою думку, разом із цим необхідно представити розробку заходів їх протидії, із організацією захищених каналів доступу для фрілансерів, заходами аудиту, тощо.

7. Під час проведення дисертаційних досліджень автор вводить поняття плановий та спеціальний аудит. На мою думку доцільно було б більш розгорнуто надати пояснень в чому різниця між аудитами.

8. У дисертації спостерігаються поодинокі стилістичні помилки, граматичні та логічні неточності (стор. 24,33,50,52,70,88,104,120, задвоєння слів стор.23, 67, не наведено значення скорочень стор.51)

9. Зустрічаються наведені в розділі 1. рисунки мовою джерела.

Разом із тим, зазначені недоліки не є визначальними та не впливають на загальну високу оцінку проведеної роботи, а також на наукову та практичну цінність дисертації.

Загальна оцінка роботи та висновки.

Дисертаційна робота Галахова Євгена Миколайовича є завершеним науковим дослідженням, що спрямоване на вирішення актуального наукового завдання щодо розробки науково-методичного апарату визначення зв'язку між рівнем кіберризику та частотою аудиту, що дає можливість забезпечити ефективну автоматизацію процесів кібербезпеки підприємства, що залучає фріланс-ресурс.

Дисертаційна робота за актуальністю вибраної теми, обсягом і рівнем теоретичних та експериментальних досліджень, достовірністю та обґрунтованістю висновків, науковою новизною, значенням отриманих результатів для науки і практики задовольняє вимогам до кандидатських дисертацій, зокрема пунктам 9, 11 «Порядку присудження наукових ступенів», а її автор, Галахов Євгеній Миколайович, заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 «Інформаційна безпека держави».

Офіційний опонент
Технічний директор Комунального підприємства
Міжнародний аеропорт «Київ» (Жуляни)

доктор технічних наук, професор А.В. Міщенко

«9» червня 2020 року

Київ * Україна * Комунальне підприємство Міжнародний аеропорт «КИЇВ» (ЖУЛЯНИ) Ідентифікаційний код 31[illegible]1514