



Затверджую  
Проректор з наукової роботи  
Національного університету  
"Львівська політехніка"  
доц. І.В. Демидов  
" " " 2021 р.

## ВИТЯГ

з протоколу № 3 фахового семінару кафедри захисту інформації  
Національного університету "Львівська політехніка" від 2 березня 2021 р.

**1. ПРИСУТНІ:** 25 із 35 науково-педагогічних працівників кафедри захисту інформації,  
а саме:

1. Микитин Галина Василівна, професор кафедри, д.т.н., професор;
2. Пархуць Любомир Теодорович, професор кафедри, д.т.н., професор;
3. Ромака Володимир Опанасович, професор кафедри, д.т.н., професор;
4. Хома Володимир Васильович, професор кафедри, д.т.н., професор;
5. Опірський Іван Романович, професор кафедри, д.т.н., доцент;
6. Березюк Богдан Михайлович, доцент кафедри, к.т.н., доцент;
7. Гаранюк Петро Ігорович, доцент кафедри, к.т.н., доцент;
8. Гарасимчук Олег Ігорович, доцент кафедри, к.т.н., доцент;
9. Горпенюк Андрій Ярославович, доцент кафедри, к.т.н., доцент;
10. Кеньо Галина Володимирівна, доцент кафедри, к.т.н., доцент;
11. Лах Юрій Володимирович, доцент кафедри, к.ф.-м.н., доцент;
12. Наконечний Юрій Маркіянович, доцент кафедри, к.т.н., доцент;
13. Отенко Віктор Іванович, доцент кафедри, к.т.н., доцент;
14. Піскозуб Андріан Збігнєвич, доцент кафедри, к.т.н., доцент;
15. Ракобовчук Лариса Маратівна, доцент кафедри, к.т.н., доцент;
16. Совин Ярослав Романович, доцент кафедри, к.т.н., доцент;
17. Стахів Марта Юріївна, доцент кафедри, к.т.н., доцент;
18. Тиханський Михайло Васильович, доцент кафедри, к.ф.-м.н., доцент;
19. Тишик Іван Ярославович, доцент кафедри, к.т.н., доцент;
20. Шандра Зиновій Антонович, доцент кафедри, к.т.н., доцент;
21. Бибик Роман Тарасович, асистент кафедри;
22. Вальчук Андрій Юрійович, асистент кафедри;
23. Журавчак Даниїл Юрійович, асистент кафедри;
24. Кутень Роман Богданович, асистент кафедри;
25. Руда Христина Степанівна, асистент кафедри.

На засідання запрошений:

1. Яремчук Юрій Євгенович, д.т.н., професор, професор кафедри менеджменту та безпеки інформаційних систем, директор Центру інформаційних технологій та захисту інформації Вінницького національного технічного університету.



З присутніх – 6 докторів наук та 15 кандидатів наук – фахівці за профілем представленої дисертації.

Головуючий на засіданні – д.т.н., професор, професор кафедри захисту інформації Пархуць Любомир Теодорович.

## **2. СЛУХАЛИ:**

Доповідь випускниці аспірантури 2020 р., асистентки кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету Салієвої Ольги Володимирівни за матеріалами дисертації: «Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання», представленої на здобуття вищої освіти ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»).

Науковий керівник – д.т.н., професор, професор кафедри менеджменту та безпеки інформаційних систем, директор Центру інформаційних технологій та захисту інформації Вінницького національного технічного університету Яремчук Юрій Євгенович.

Тему дисертації затверджено “27” жовтня 2016 р. на засіданні Вченої ради Вінницького національного технічного університету, протокол № 4.

*Робота виконана на кафедрі менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.*

По доповіді було задано 9 запитань, на які доповідачка дала правильні та ґрунтовні відповіді. Питання задавали:

- професор кафедри захисту інформації, д.т.н., професор Хома Володимир Васильович;
- професор кафедри захисту інформації, д.т.н., професор Пархуць Любомир Теодорович;
- професор кафедри захисту інформації, д.т.н., професор Микитин Галина Василівна;
- професор кафедри захисту інформації, д.т.н., доцент Опірський Іван Романович.

## **3. Виступи присутніх**

З оцінкою дисертації Салієвої О.В. виступили рецензенти:

- професор кафедри захисту інформації, д.т.н., професор Хома Володимир Васильович;
- професор кафедри захисту інформації, д.т.н., доцент Опірський Іван Романович,

які відзначили актуальність тематики дисертаційного дослідження для галузі кібербезпеки, складність наукового завдання, вагомість одержаних науково-прикладних результатів, спрямованих на підвищення захищеності систем захисту інформації, що циркулює в інформаційних системах, особистий внесок здобувача у вигляді функціональних когнітивних моделей для оцінювання рівня захищеності систем захисту інформації та програмних засобів реалізації цих моделей.

З оцінкою дисертації також виступили присутні на фаховому семінарі:

- професор кафедри захисту інформації, д.т.н. Пархуць Любомир Теодорович;
- професор кафедри захисту інформації, д.т.н. Микитин Галина Василівна.

Промовці підкреслили актуальність теми дисертації та її зв'язок з науковим напрямком кафедри менеджменту та безпеки інформаційних систем, значимість одержаних науково-прикладних результатів та їх впровадження у навчальний процес, особистий внесок здобувача, наявність 1 публікації у наукометричній базі Scopus і 10 статей у наукових фахових виданнях України.

*Загальна характеристика дисертації – позитивна.*

З характеристикою наукової зрілості здобувачки виступив науковий керівник д.т.н., професор Яремчук Ю.Є., який відзначив її відповідальне ставлення до виконання своїх обов'язків, відмінний рівень теоретичної підготовки і наукової інтуїції, наполегливість у вирішенні складних наукових завдань, значний професійний досвід у розробленні когнітивних



моделей для оцінювання рівня захищеності систем захисту інформації та програмних засобів реалізації цих моделей.

**4. Заслухавши та обговоривши доповідь Салієвої Ольги Володимирівни, а також за результатами попередньої експертизи представленої дисертації на фаховому семінарі кафедри захисту інформації, прийнято наступні висновки щодо дисертації "Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання":**

#### **Висновок**

**фахового семінару кафедри захисту інформації про наукову новизну, теоретичне та практичне значення результатів дисертації «Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання» здобувача вищої освіти ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»)**

**4.1. Актуальність теми дисертації** зумовлена необхідністю забезпечення інформаційної безпеки в різних сферах суспільної діяльності, де будь-які процеси безпосередньо пов'язані з використанням інформаційних ресурсів та технологій. Водночас через зростаючу складність інформаційних систем, збільшується й кількість потенційних загроз цим системам. Тому важливе місце займає оцінювання рівня захищеності систем захисту інформації, що дозволяє спрогнозувати поведінку досліджуваних систем у конкретних ситуаціях і, відповідно, вчасно розробити чіткий план для підвищення рівня їхньої захищеності.

Відомі підходи вирішення даного завдання спираються на методи статистичного аналізу, проте вони потребують складних розрахунків, значного обсягу експериментальних даних, тривалого часу для їх опрацювання і не забезпечують можливості роботи з якісними факторами. У зв'язку з цим цілком обґрунтованим є застосування для розв'язання зазначених задач когнітивного підходу, що базується на побудові нечітких когнітивних карт. Отже, тематика дисертаційного дослідження є актуальною у галузі кібербезпеки, а застосований до розв'язання сформульованого наукового завдання, методологічний підхід є безперечно новим і перспективним.

**4.2. Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри:**

Основний зміст роботи складають дослідження, які проводилися відповідно до наукового напрямку кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету (ВНТУ). Дослідження виконувалися у Центрі інформаційних технологій та захисту інформації Вінницького національного технічного університету і науково-дослідній лабораторії технічного захисту інформації ВНТУ.

Науково-дослідна робота проводилась відповідно до тематики науково-дослідної роботи Вінницького національного технічного університету. Зокрема, робота над дисертацією проводилася у межах науково-дослідних та науково-технічних робіт:

– створення комплексної системи захисту інформації (КСЗІ) в автоматизованій системі (АС) режимно-секретного органу відокремленого підрозділу «Південно-Західна електроенергетична система» Приватного акціонерного товариства «Національна енергетична компанія «Укренерго» № 5261 від 27.05.2019 р.;

– створення КСЗІ в АС Хмельницького зонального відділу Військової служби правопорядку № 5267 від 11.07.2019 р.;



– створення КСЗІ в АС Головного управління Пенсійного фонду України у Вінницькій області № 5284 від 27.02.2020 р.

#### **4.3. Особистий внесок здобувача в отриманні наукових результатів**

Дисертація є самостійною науковою працею, в якій автором особисто розроблено нові наукові ідеї та одержано результати, що дозволили вирішити конкретне наукове завдання - підвищення захищеності систем захисту інформації, що циркулює в інформаційних системах, шляхом створення функціональних когнітивних моделей для оцінювання рівня їхньої захищеності та програмних засобів реалізації цих моделей. Робота містить прикладні положення та висновки, сформульовані дисертанткою особисто. Ідеї, положення чи гіпотези інших авторів, які присутні у дисертації, мають відповідні посилання і використані лише для підкріплення ідей та результатів здобувача.

#### **4.4. Достовірність та обґрунтованість отриманих результатів та запропонованих автором рішень, висновків, рекомендацій.**

Достовірність та обґрунтованість запропонованих моделей систем захисту інформації, що циркулює в інформаційних системах, забезпечується коректним використанням апарату когнітивного моделювання і прийнятих допущень. Адекватність розроблених моделей підтверджується результатами експериментальних досліджень. Проведені дослідження підтверджують достовірність отриманих результатів впливу загроз на рівень захищеності систем захисту інформації, використовуючи методи статистичного аналізу, зокрема, регресійного та на основі симплексного аналізу, підтверджено результати структурного аналізу досліджуваної моделі. Обґрунтованість та вірогідність наукових результатів забезпечується коректністю виконаних аналітичних розрахунків та результатами експериментальних досліджень, науковими публікаціями у наукових фахових виданнях України та у міжнародному науковому виданні, що індексується у наукометричній базі Scopus, доповідями на наукових конференціях та семінарах різного рівня.

#### **4.5. Ступінь новизни основних результатів дисертації порівняно з відомими дослідженнями аналогічного характеру**

Наукова новизна основних результатів дисертації полягає в розробленні моделей оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання:

1. Вперше запропоновано модель оцінювання рівня захищеності об'єкта критичної інфраструктури на основі когнітивного підходу з використанням нечітких когнітивних карт, який надає можливість спростити розрахунки та зменшити час обробки вхідної інформації; покращити наочність представлення вхідних даних; при побудові нечіткої когнітивної карти врахувати як кількісні, так і якісні фактори, що впливають на захищеність об'єкту; за потреби легко розширити кількість даних факторів, за рахунок введення додаткових вершин і дуг графа когнітивної карти; визначити найвагомші фактори, зокрема, визначено такі фактори як захищеність системи безпеки, інсайдерський вплив, захищеність комп'ютерної мережі; проводити сценарне моделювання, у результаті якого визначено, що рівень захищеності об'єкта критичної інфраструктури підвищиться на 2 % при максимально позитивному впливі найвагомших факторів.

2. Вперше запропоновано модель оцінювання рівня захищеності системи захисту інформації на основі когнітивного підходу з використанням нечітких когнітивних карт, який дозволяє збільшити швидкість обробки вхідної інформації та зменшити час на її опрацювання; покращити наочність представлення даних; використовувати неповну, нечітку інформацію та суб'єктивні судження експертів предметної області; врахувати як кількісні, так і якісні фактори, що впливають на захищеність системи захисту; виявити найвагомші фактори, зокрема як такі визначено фізичний захист, організаційне забезпечення захисту інформації, НСД до інформації зловмисником; проводити сценарне моделювання розвитку ситуації, у



результаті якого визначено, що рівень захищеності системи захисту інформації підвищиться на 19 % при максимально позитивному впливі найвагоміших факторів.

3. Вдосконалено модель для оцінювання рівня захищеності комп'ютерної мережі на основі когнітивного підходу з використанням нечітких когнітивних карт, яка більш точно відображає предметну область та надає можливість краще враховувати мінливість характеру процесів, що відбуваються у досліджуваній системі, у часі; визначити найвагоміші загрози комп'ютерній мережі, зокрема, як такі визначено шкідливі програми, фізичний вплив на мережу з боку зловмисника та ненавмисні дії, помилки користувачів мережі; проводити сценарне моделювання розвитку ситуації, у результаті якого визначено, що рівень захищеності комп'ютерної мережі підвищиться на 63% при максимальному послабленні впливу найвагоміших загроз.

4. Отримав подальшого розвитку підхід до визначення допустимих витрат на забезпечення захищеності об'єкта критичної інфраструктури й системи захисту інформації та допустимої інтенсивності зниження рівня їхньої захищеності на основі ранжування загроз із використанням теорії нечітких відношень, який надає можливість зменшити час обробки вхідної інформації та спростити проміжні розрахунки, оперуючи нечіткими вхідними даними і здійснюючи нечітку формалізацію критеріїв оцінювання; проводити не тільки кількісне, а й якісне оцінювання як вхідних даних, так і вихідних результатів.

#### **4.6. Перелік наукових праць, які відображають основні результати дисертації**

Особистий внесок здобувача у колективно опублікованих працях полягає у формуванні та розробці ключових ідей та результатів. Основні положення та результати дисертації значною мірою викладені в наступних наукових працях здобувача:

##### *Статті у наукових фахових виданнях України:*

1. О. В. Салієва, та Ю. Є. Яремчук, «Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі», *Ресстрація, зберігання і обробка даних*, т. 21, № 4, С. 28–39, 2019. Особистий внесок здобувача: розробка та аналіз когнітивної моделі для визначення рівня захищеності комп'ютерної мережі при впливі на неї потенційних загроз.
2. О. В. Салієва, та Ю. Є. Яремчук, «Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання», *Безпека інформації*, т. 26, № 1, С. 42–49, 2020. Особистий внесок здобувача: розробка та аналіз когнітивної моделі на основі нечіткої когнітивної карти, яка дозволяє визначити рівень захищеності системи захисту інформації.
3. О. В. Салієва, та Ю. Є. Яремчук, «Ранжування загроз для визначення витрат на забезпечення захищеності системи захисту інформації на основі теорії нечітких відношень», *Захист інформації*, т. 22, № 1, С. 51–59, 2020. Особистий внесок здобувача: визначення витрат на забезпечення захищеності системи захисту інформації ранжуванням загроз.
4. О. В. Салієва, та Ю. Є. Яремчук, «Когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури», *Безпека інформації*, т. 26, № 2, С. 64–73, 2020. Особистий внесок здобувача: розробка та аналіз когнітивної моделі для дослідження рівня захищеності об'єкта критичної інфраструктури.
5. О. В. Салієва, та Ю. Є. Яремчук, «Визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури ранжуванням загроз», *Ресстрація, зберігання і обробка даних*, т. 22, № 2, С. 63–76, 2020. Особистий внесок здобувача: ранжування загроз об'єкта критичної інфраструктури та визначення допустимої інтенсивності зниження рівня його захищеності.
6. О. В. Салієва, та Ю. Є. Яремчук, «Дослідження достовірності впливу загроз на рівень захищеності комп'ютерної мережі, визначеного за сценарним моделювання на основі когнітивного підходу», *Вісник Вінницького політехнічного інституту*, № 4, С. 98–104,



2020. Особистий внесок здобувача: встановлення достовірності впливу загроз на рівень захищеності комп'ютерної мережі, визначеного на основі когнітивного підходу.
7. О. В. Салієва, та Ю. Є. Яремчук, «Динамічний часовий аналіз впливу факторів загроз на рівень захищеності об'єкта критичної інфраструктури», *Захист інформації*, т. 22, №3, С. 148–157, 2020. Особистий внесок здобувача: проведення динамічного часового аналізу впливу факторів загроз на рівень захищеності об'єкта критичної інфраструктури та розробка програмного засобу.
  8. О. В. Салієва, та Ю. Є. Яремчук, «Симпліціальний аналіз структури когнітивної моделі для дослідження рівня захищеності об'єкта критичної інфраструктури», *Ресурснація, зберігання і обробка даних*, т. 22, №3, С. 68-75, 2020. Особистий внесок здобувача: визначення управляючих та зв'язних концептів когнітивної моделі для дослідження рівня захищеності об'єкта критичної інфраструктури на основі симпліціального аналізу.
  9. О. В. Салієва, та Ю. Є. Яремчук, «Дослідження достовірності впливу загроз на рівень захищеності системи захисту інформації та об'єкта критичної інфраструктури за результатами когнітивного моделювання», *Вісник Черкаського державного технологічного університету*, №3, С. 85–93, 2020. Особистий внесок здобувача: встановлення достовірності впливу загроз на рівень захищеності системи захисту інформації та об'єкта критичної інфраструктури за результатами когнітивного моделювання.
  10. О. В. Салієва, та Ю. Є. Яремчук, «Дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності систем захисту інформації», *Вісник Вінницького політехнічного інституту*, №5, С. 56–62, 2020. Особистий внесок здобувача: визначення зміни рівня захищеності системи захисту інформації на основі імпульсного моделювання та розробка програмного засобу.

**Стаття у науковому періодичному виданні іншої держави, що включено до міжнародної наукометричної бази даних (Scopus):**

11. N. Mumtaz, A. Begum, B. Gul, S. Noor, R. Odarchenko, I. Machalin and O. Saliieva «Semantic, Digitization, Design and Implementation of Ontology in Social Internet-Services», *Conflict Management in Global Information Networks*, vol. 2588, P. 228–249, 2019. Особистий внесок здобувача: створення концепцій та опис взаємозв'язків між їхніми елементами, необхідними для розробки онтології домену, що підлягає семантичному оцифруванню.

**Наукові публікації у збірниках матеріалів та тез конференцій:**

12. О. В. Салієва, «Системологічне дослідження суб'єктів захисту інформації», у Матеріалах XLV науково-технічної конференції підрозділів ВНТУ, м. Вінниця, 2016, С. 2190-2191.
13. О. В. Салієва, Я. Ю. Яремчук, «Порівняння моделей інформаційної безпеки за характеристиками суб'єктів», у Матеріалах конференції «Управління знаннями та конкурентна розвідка», м. Харків, 2019, С. 67-68. Особистий внесок здобувача: здійснення порівняльного аналізу моделей інформаційної безпеки за характеристиками суб'єктів.
14. О. В. Салієва, «Аналіз впливу загроз безпеці комп'ютерної мережі з використанням когнітивного моделювання», у Матеріалах XLVII науково-технічної конференції підрозділів ВНТУ, м. Вінниця, 2020, С. 2725-2726.
15. О. В. Салієва, «Оцінювання рівня захищеності системи безпеки на основі когнітивного моделювання», у Матеріалах всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи», м. Вінниця, 2020, С. 1215-1216.
16. О. В. Салієва, «Визначення витрат на забезпечення захищеності системи захисту інформації ранжуванням загроз», у Матеріалах VI Міжнародної науково-практичної конференції «Перспективні напрями захисту інформації», м. Одеса, 2020, С. 83-84.
17. Ю. Є. Яремчук, О. В. Салієва, «Оцінювання рівня захищеності об'єкта критичної інфраструктури», у Матеріалах науково-практичної конференції «Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання»,



- м. Київ, 2020, С. 280-281. Особистий внесок здобувача: розробка та аналіз когнітивної моделі для дослідження рівня захищеності об'єкта критичної інфраструктури.
18. О. В. Салієва, «Визначення впливу загроз на рівень захищеності комп'ютерної мережі за когнітивною моделлю на основі регресійного аналізу», у Матеріалах науково-технічної конференції студентів, аспірантів, докторантів та молодих учених «Інноваційні технології», м. Київ, 2020, С. 105-106.

#### **4.7. Апробація основних результатів дослідження на конференціях, симпозіумах, семінарах тощо**

Основні положення роботи та її результати доповідались, обговорювались та були схвалені на таких науково-технічних конференціях та семінарах: XLV науково-технічній конференції підрозділів ВНТУ (м. Вінниця, 2016 р.); 23-му Міжнародному молодіжному форумі «Радіoeлектроніка та молодь у XXI столітті», конференція «Управління знаннями та конкурентна розвідка» (м. Харків, 2019 р.); щорічному міжвідомчому міжрегіональному семінарі Наукової Ради НАН України «Технічні засоби захисту інформації» (м. Київ, 2020 р.); XLVII науково-технічній конференції підрозділів ВНТУ (м. Вінниця, 2020 р.); Всеукраїнській науково-практичній інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи», (м. Вінниця, 2020 р.); VI Міжнародній науково-практичній конференції «Перспективні напрями захисту інформації» (м. Одеса, 2020); науково-практичній конференції «Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання» (м. Київ, 2020); науково-технічній конференції студентів, аспірантів, докторантів та молодих учених «Інноваційні технології» (м. Київ, 2020).

#### **4.8. Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати**

Наукові результати, отримані автором, можуть бути використані при оцінюванні рівня захищеності систем захисту інформації, що циркулює в інформаційних системах.

Також їх можна впровадити у навчальний процес, зокрема, у курсах "Захист комп'ютерних мереж" та "Комплексні системи захисту інформації" для студентів спеціальності 125 Кібербезпека.

#### **4.9. Практична цінність результатів дослідження із зазначенням конкретного підприємства або галузі народного господарства, де вони можуть бути застосовані**

1. Розроблено структуру програми для реалізації оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах, у вигляді п'яти взаємозалежних програмних модулів: модуля створення концептів, модуля побудови матриці взаємовпливів концептів, модуля присвоєння сили зв'язку, модуля обчислення системних показників для дослідження поведінки і стійкості побудованої карти та модуля моделювання сценарію розвитку ситуації. Здійснено програмну реалізацію запропонованих модулів.

2. Розроблено програмні засоби для реалізації оцінювання рівня захищеності систем захисту інформації, що циркулює в інформаційних системах, за запропонованими когнітивними моделями дослідження захищеності комп'ютерної мережі, системи захисту інформації та об'єкта критичної інфраструктури.

3. На основі множинного регресійного аналізу доведено достовірність впливу загроз на рівень захищеності комп'ютерної мережі, системи захисту інформації та об'єкта критичної інфраструктури, визначеного за результатами когнітивного моделювання. Отримані результати надають можливість спрогнозувати розвиток ситуації для прийняття вчасних та ефективних управлінських рішень, спрямованих на підвищення захищеності досліджуваних систем захисту інформації, що циркулює в інформаційних системах.

4. Проведено динамічний часовий аналіз впливу факторів загроз на рівень захищеності об'єкта критичної інфраструктури, результати якого дозволяють визначити та



порівняти рівні впливу досліджуваних загроз на захищеність даного об'єкта у різні моменти часу.

5. Здійснено симпліціальний аналіз структури когнітивної моделі для дослідження захищеності об'єкта критичної інфраструктури, у результаті якого було сформовано множину управляючих для всієї системи концептів та встановлено взаємозв'язні вершини, вплив на які всередині кожного блоку дозволить за найменших зусиль підвищити рівень захищеності досліджуваного об'єкта.

6. Досліджено розвиток у часі когнітивної моделі для визначення зміни рівня захищеності системи захисту інформації, шляхом введення імпульсних впливів у концепти когнітивної карти. Це дослідження надало змогу прослідкувати еволюційний розвиток системи, що сприятиме підвищенню ефективності прогнозування розвитку ситуацій у разі впливу ймовірних загроз.

Отримані на основі наукових досліджень практичні результати впроваджено при розробці комплексних систем захисту інформації в автоматизованих системах: Хмельницького зонального відділу Військової служби правопорядку (16.11.2020 р.), відокремленого підрозділу «Південно-Західна електроенергетична система» ПАТ «Національна енергетична компанія «Укренерго»» (20.11.2020 р.), головного управління Пенсійного фонду України у Вінницькій області (01.10.2020 р.) та в навчальному процесі Вінницького національного технічного університету (16.11.2020 р.), що підтверджено відповідними актами впровадження, які містяться у додатках до дисертаційної роботи.

#### **4.10. Оцінка структури дисертації, її мови та стилю викладення**

Дисертаційна робота викладена на 208 сторінках та складається з анотації, змісту, переліку скорочень, вступу, чотирьох основних розділів, в яких міститься 30 рисунків та 21 таблиця, списку використаних джерел з 125 найменування, а також 5 додатків. За структурою, мовою та стилем викладення дисертація відповідає вимогам МОН України. Робота написана грамотною українською мовою з використанням сучасної наукової термінології, а стиль викладення матеріалу є послідовним та логічним.

**У ході обговорення дисертації до неї не було висунуто жодних зауважень щодо самої суті роботи.**

5. З урахуванням зазначеного,

#### **На фаховому семінарі кафедри захисту інформації ухвалили:**

5.1. Дисертація Салієвої Ольги Володимирівни «Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання» є завершеною науковою працею, у якій розв'язано конкретне наукове завдання підвищення захищеності систем захисту інформації, що циркулює в інформаційних системах, створенням функціональних когнітивних моделей для оцінювання рівня їхньої захищеності, що має важливе значення для галузі знань 12 «Інформаційні технології».

5.2. У 18 наукових публікаціях повністю відображені основні результати дисертації, з них 10 статей у наукових фахових виданнях України, 1 стаття у науковому періодичному виданні іншої держави, яке включено до міжнародної наукометричної бази (Scopus) та 7 – у матеріалах і тезах конференцій.

5.3. Дисертація відповідає вимогам наказу МОН України № 40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації», Порядку проведення експерименту з присудження ступеня доктора філософії (Постанова Кабінету Міністрів України від 6 березня 2019 р. № 167).



5.4. З урахуванням наукової зрілості та професійних якостей Салієвої Ольги Володимирівни дисертація «Моделі та засоби оцінювання рівня захищеності систем захисту інформації на основі когнітивного моделювання» рекомендується для подання до розгляду та захисту у спеціалізованій вченій раді.

За затвердження висновку проголосували:

за	-	(двадцять шість)
проти	-	(немає)
утримались	-	(немає)

Головуючий на засіданні фахового семінару, професор кафедри захисту інформації, д.т.н., професор

Пархуць Л.Т.

Рецензенти:

д.т.н., професор, професор кафедри захисту інформації

Хома В.В.

д.т.н., доцент, професор кафедри захисту інформації

Опирський І.Р.

Відповідальний у ІКТА за атестацію PhD

д.т.н., професор, професор кафедри захисту інформації

Пархуць Л.Т.

"01" 03 2021 р.