**«ЗАТВЕРДЖУЮ»**
проректор з наукової роботи
Хмельницького національного університету,
_____ д.т.н., доцент
О.М.Синюк
«20» січня 2020 р.

# В И Т Я Г

**з протоколу № 6 розширеного засідання**
**кафедри комп'ютерної інженерії та системного програмування**
**Хмельницького національного університету**
**від 17 січня 2020 р.**
**по розгляду дисертаційної роботи**
**к.т.н., доцента Лисенка Сергія Миколайовича**
**на тему: «Методологічні основи та інформаційна технологія забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз»**
**на здобуття наукового ступеня доктора технічних наук**
**за спеціальністю 05.13.06 – інформаційні технології.**

**Головуючий на засіданні кафедри:**
Говорущенко Т.О. – д.т.н., професор, завідувач кафедри комп'ютерної інженерії та системного програмування Хмельницького національного університету.

**Секретар засідань кафедри:**
Нічепорук А.О. – доцент кафедри комп'ютерної інженерії та системного програмування Хмельницького національного університету.

**1. ПРИСУТНІ:** 15 із 18 науково-педагогічних працівників кафедри комп'ютерної інженерії та системного програмування, а саме:

1. Говорущенко Т.О., завідувач кафедри, д.т.н., професор;
2. Савенко О.С., декан факультету програмування та комп'ютерних і телекомунікаційних систем, професор кафедри, к.т.н., професор;
3. Мартинюк В.В., д.т.н., доцент, завідувач кафедри телекомунікацій і комп'ютерно-інтегрованих технологій Хмельницького національного університету;
4. Медзатий Д.М., доцент кафедри, к.т.н., доцент;
5. Лисенко С.М., доцент кафедри, к.т.н., доцент;
6. Гнатчук Є.Г., доцент кафедри, к.т.н., доцент;
7. Кисіль Т.М., доцент кафедри, к. ф.-м.н., доцент;

8. Ковтун Л.О., доцент кафедри, к.т.н., доцент;
9. Стецюк В.М., старший викладач кафедри;
10. Бобровнікова К.Ю., доцент кафедри, к.т.н.;
11. Нічепорук А.О., доцент кафедри, к.т.н.
12. Гурман І.В., доцент, к.т.н.;
13. Красовский М.В., асистент;
14. Грибинчук В. І., асистент;
15. Денисюк Д.О., асистент.

**На засідання кафедри запрошені:**

1. Сорокатий Р.В., д.т.н., професор, завідувач кафедри комп'ютерних наук та інформаційних технологій Хмельницького національного університету;
2. Бойко Ю.М., д.т.н., професор, професора кафедри телекомунікацій та радіотехніки Хмельницького національного університету;
3. Бармак О.В. – д.т.н., професор, професор кафедри комп'ютерних наук та інформаційних технологій Хмельницького національного університету.

З 18 присутніх – 5 докторів наук та 8 кандидатів наук – фахівці за профілем представленої дисертації.

Головуючим на засіданні кафедри була обрана завідувач кафедри комп'ютерної інженерії та системного програмування Хмельницького національного університету. д.т.н., професор Говорущенко Т.О.

**2. СЛУХАЛИ**:

Доповідь доцента кафедри комп'ютерної інженерії та системного програмування Лисенко Сергія Миколайовича за матеріалами дисертації: «Методологічні основи та інформаційна технологія забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз», представленої на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 – інформаційні технології.

Науковий консультант – доктор технічних наук, професор Харченко В.С., завідувач кафедри комп'ютерних систем, мереж та кібербезпеки Національного аеро-космічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» (призначено на засіданні Вченої ради Хмельницького національного університету, протокол №5 від 24.12.2015).

Тему дисертації Лисенка С.М. затверджено 24 грудня 2015 року на засіданні Вченої ради Хмельницького національного університету, протокол №5.

Робота виконана на кафедрі комп’ютерної інженерії та системного програмування Хмельницького національного університету.

У своїй доповіді Лисенка С.М. виклав зміст дисертаційної роботи та визначив її суть і основні наукові та практичні результати.

Доповідачеві було задано 23 запитання, на які він дав правильні та обґрунтовані відповіді. Питання задавали:

- Бармак О.В., професор кафедри комп’ютерних наук та інформаційних технологій, д.т.н., професор;
- Бойко Ю.М., д.т.н., професор, професора кафедри телекомунікацій та радіотехніки Хмельницького національного університету;
- Сорокатий Р.В., завідувач кафедри комп’ютерних наук та інформаційних технологій, д.т.н., професор;
- Мартинюк В.В., завідувач кафедри телекомунікацій і комп'ютерно-інтегрованих технологій, д.т.н., доцент;
- Говорущенко Т.О., завідувач кафедри комп’ютерної інженерії та системного програмування Хмельницького національного університету, д.т.н., професор;
- Савенко О.С., декан факультету програмування та комп’ютерних і телекомунікаційних систем, професор кафедри комп’ютерної інженерії та системного програмування, к.т.н., професор;
- Медзатий Д.М., доцент кафедри комп’ютерної інженерії та системного програмування, к.т.н., доцент;
- Гнатчук Є.Г., доцент кафедри комп’ютерної інженерії та системного програмування, к.т.н., доцент;
- Кисіль Т.М., доцент кафедри комп’ютерної інженерії та системного програмування, к.ф.-м.н., доцент;
- Ковтун Л.О., доцент кафедри комп’ютерної інженерії та системного програмування, к.т.н., доцент;
- Бобровнікова К.Ю., доцент кафедри комп’ютерної інженерії та системного програмування, к.т.н.;
- Нічепорук А.О., доцент кафедри комп’ютерної інженерії та системного програмування, к.т.н.

## 3. ВИСТУПИ ПРИСУТНІХ:

З оцінкою дисертаційної роботи виступили рецензенти:

- Говорущенко Т.О., завідувач кафедри комп’ютерної інженерії та системного програмування Хмельницького національного університету, д.т.н., професор;
- Бармак О.В., професор кафедри комп’терних наук та інформаційних технологій, д.т.н., професор;
- Мартинюк В.В., завідувач кафедри телекомунікацій і комп'ютерно-інтегрованих технологій, д.т.н., доцент,

які зазначили актуальність теми дисертації, відзначили цілісність роботи, новизну отриманих наукових результатів та практичну цінність дисертаційного

дослідження. Наголосили, що представлена дисертаційна робота відповідає паспорту спеціальності 05.13.06 – інформаційні технології. Відзначили важливість роботи дисертанта з підвищення рівня інформаційної безпеки комп'ютерних систем, що відображено в представлених актах впровадження результатів дисертаційної роботи. Рекомендували представляти дисертаційну роботу у спеціалізовану вчену раду за спеціальністю 05.13.06 – інформаційні технології.

З оцінкою дисертаційної роботи також виступили присутні на розширеному засіданні кафедри:

– Сорокатий Р.В., завідувач кафедри комп'ютерних наук та інформаційних технологій, д.т.н., професор – позитивно оцінив дисертаційну роботу і зазначив актуальність теми дисертації, присвяченої підвищенню резильєнтності комп'ютерних систем шляхом розроблення та практичного впровадження методологічних основ та інформаційної технології забезпечення резильєнтності комп'ютерних систем на основі принципів проактивного виявлення атак та адаптивної реконфігурації систем в умовах кіберзагроз. Відзначив цілісність роботи та наукову новизну і практичну цінність отриманих результатів. Рекомендував представляти дисертаційну роботу у спеціалізовану вчену раду за спеціальністю 05.13.06 – інформаційні технології;

– Савенко О.С., декан факультету програмування та комп'ютерних і телекомунікаційних систем, професор кафедри комп'ютерної інженерії та системного програмування, к.т.н., професор – позитивно оцінив дисертаційну роботу. Окремо наголосив, що всі наукові результати роботи Лисенка С.М. опубліковані в співавторстві ним з іншими викладачами, що захистились з нашої кафедри, розділені між співавторами і частка яка належить йому точно відображає його науковий результат в представленій роботі та не належить іншим і в інших роботах не представлена як наукова новизна тих робіт. Доповідач також сказав, що представлена дисертаційна робота відповідає паспорту спеціальності 05.13.06 – інформаційні технології. Рекомендував подавати дисертаційну роботу до спеціалізованої вченої ради за спеціальністю 05.13.06 – інформаційні технології;

– Медзатий Д.М., доцент кафедри комп'ютерної інженерії та системного програмування, к.т.н., доцент – підтримав роботу і рекомендував представляти роботу у спеціалізовану вчену раду за спеціальністю 05.13.06 – інформаційні технології;

– Гнатчук Є.Г., доцент кафедри комп'ютерної інженерії та системного програмування, к.т.н., доцент – відзначила важливість роботи дисертанта з реальними специфікаціями вимог до програмного забезпечення. Рекомендувала представляти роботу у спеціалізовану вчену раду за спеціальністю 05.13.06 – інформаційні технології;

– Бобровнікова К.Ю., доцент кафедри комп'ютерної інженерії та системного програмування, к.т.н. – відзначила актуальність та важливість роботи, наголосив на відповідності роботи паспорту спеціальності 05.13.06 і

рекомендував представляти роботу у спеціалізовану вчену раду за спеціальністю 05.13.06 – інформаційні технології;

– Кисіль Т.М., доцент кафедри комп'ютерної інженерії та системного програмування, к.ф.-м.н., доцент – дала позитивну оцінку дисертаційній роботі. Вказала на цікавість та актуальність роботи, підкреслив важливість досвіду роботи доповідача в області теми дисертації. Рекомендувала подавати дисертаційну роботу до спеціалізованої вченої ради за спеціальністю 05.13.06 – інформаційні технології.

Всі виступаючі підтвердили актуальність вирішеної наукової проблеми розроблення теоретичних та прикладних засад інформаційної технології оцінювання забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз, а також наукову новизну отриманих результатів, відзначили практичну цінність проведених досліджень та результатів дисертації, відповідність дисертації встановленим вимогам.

Загальна характеристика дисертаційної роботи Лисенка С.М. на здобуття наукового ступеня доктора технічних наук – позитивна.

З характеристикою наукової зрілості та особистісних якостей здобувача виступила завідувач кафедри комп'ютерної інженерії та системного програмування Хмельницького національного університету д.т.н., професор, Говорущенко Т.О., яка відзначила, що Лисенко Сергій Миколайович пройшов довгий шлях дослідника до представлення такої роботи - докторської дисертації. У 2005 році з відзнакою закінчив Хмельницького національного університету за спеціальністю «Комп'ютерні системи та мережі» і здобув фах магістра комп'ютерної інженерії. З 1 вересня 2004 року працює в Хмельницькому національному університеті на кафедрі системного програмування (з 1.12.2016 – кафедра комп'ютерної інженерії та системного програмування).

В січні 2011 він захистив кандидатську дисертацію на тему «Адаптивна інформаційна технологія діагностування комп'ютерних систем на наявність троянських програм» за спеціальністю 05.13.06 – інформаційні технології у Тернопільському національному економічному університеті, і наполегливо зразу почав працювати над наступною своєю дисертацією. У 2013 році здобув вчене звання доцента за кафедрою системного програмування.

За час підготовки своєї роботи, за ці 9 років, він допомагав трьом аспірантам корисним консультуванням, чим набув досвіду і здобув авторитет серед колег не тільки на кафедрі але і в нашому університеті. Здобувач має важливі публікації в Scopus та WoS. За актуальністю та науковими результатами представлена робота відповідає вимогам.

Виступаючий відзначив, що Лисенко С.М. є автором та співавтором 10 навчально-методичних робіт, в тому числі навчального посібника. Виступаючий наголосила, що Лисенко С.М. є автором понад 80 наукових публікацій; брав активну участь у виконанні держбюджетних науково-дослідних робіт (зокрема, держбюджетної НДР Хмельницького національного університету №2Б-2011 «Методологія інтелектуального автоматизованого оцінювання відповідності програмного забезпечення систем критичного

застосування вимогам» та №1Б-2019 «Агентно-орієнтована система підвищення безпеки та якості програмного забезпечення комп'ютерних систем» (номер державної реєстрації 0119U100662), а також міжнародних проектів Хмельницького національного університету TEMPUS SAFEGUARD «National Safeware Engineering Network of Centers of Innovative Academia-Industry Handshaking» (№158886-TEMPUS-2009-UK-JPCR, 2010-2012 рр.) та TEMPUS SEREIN (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR, 2014-2017 рр.) «Модернізація післядипломної освіти у галузі безпеки та стійких інформаційних систем для індустрії»). Виступаючий відзначила важливість значного досвіду роботи здобувача за темою дисертаційної роботи і наголосила, що здобувач за час роботи на кафедрі проявив себе як відповідальний, обов'язковий, принциповий та вимогливий викладач, гарний організатор. Науковий консультант зазначила також, що за час роботи над дисертацією Лисенко С.М. проявив себе цілеспрямованим і активним науковцем, здатним вирішувати складні наукові проблеми.

**4. Заслухавши та обговоривши доповідь Лисенка Сергія Миколайовича, а також за результатами попередньої експертизи представленої дисертації, на засіданні кафедри комп'ютерної інженерії та системного програмування Хмельницького національного університету**, прийнято наступні висновки щодо дисертаційної роботи: «Методологічні основи та інформаційна технологія забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз», поданої на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.06 – інформаційні технології.

**Висновок**
**розширеного засідання кафедри комп'ютерної інженерії та системного програмування Хмельницького національного університету**
**про наукову та практичну цінність дисертаційної роботи**
«Методологічні основи та інформаційна технологія забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз»
***здобувача наукового ступеня*** доктора технічних наук
за спеціальністю 05.13.06 – інформаційні технології

## 4.1. Актуальність теми дисертації

Сьогодні кіберзлочинці знаходять нові способів отримати прибутку від підприємств, які є об'єктом вимагання та прибутковим джерелом доходу для організованих злочинних груп через приватну інформацію, що зберігається та обробляється цими установами. Різні види кіберзагроз є потужним інструментом, які використовуються кіберзлочинцями для вчинення зловмисних дій.

Стрімкий розвиток інформаційних технологій призвели до значного розширення можливостей кіберзагроз при запуску атак на відмову в обслуговуванні, інфікування мільйонів комп'ютерних систем (КС) шкідливим кодом, викраденні конфіденційних даних, масштабний спам, шантаж і вимагання. Кіберзагрози можуть використовувати комбінації декількох атак, що використовують відомі та невідомі вразливості кінцевих пристроїв.

Кіберзлочинці розробляють нові способи уникнути сучасних методів виявлення атак, тому існуючі підходи не в змозі протистояти зростаючій загрозі атак. Тим часом наслідки кібератаки стають все більш небезпечними та руйнівними.

За наявності кібератак важливим завданням є вжиття заходів, які дозволять послабити такі атаки та забезпечити стабільне функціонування мережі, тобто резильєнтність мережі.

Описана ситуація активізує розробку нових підходів, здатних виявляти, запобігати та пом'якшувати кібератаки на мережі. Крім того, дуже важливо забезпечити стабільне функціонування КС в умовах атак. Одним із способів вирішити цю проблему є побудова резильєнтних систем, які здатні швидко відновлюватися та продовжувати функціонувати в умовах здійснення атак.

З точки зору кібербезпеки резильєнтність - це здатність передбачати, протистояти, відновлюватись та пристосовуватися до несприятливих умов, зовнішніх впливів, атак чи порушення нормального функціонування системи.

Для забезпечення резильєнтності КС в умовах необхідним є створення моделей методів та інформаційних технологій, які б надали таким системам здатності передбачати кібератаки, протистояти їм та мати здатність до відновлення після здійснення атак.

Існуючі методи та засоби не розглядають в комплексі усі принципи забезпечення резильєнтності комп'ютерних систем, зокрема проактивність, адаптивність, резильєнтність до втручань, диверсність, еластичність, керована

деградація, захист в глибину, здатність до еволюції, і не пропонують єдиного системного підходу до її оцінки, що є необхідною умовою забезпечення резильєнтного функціонування КС в умовах здійснення нових і невідомих атак.

Таким чином, *актуальною науково-прикладною проблемою* є створення резильєнтних комп'ютерних систем, яка полягає у вирішенні об'єктивного **протиріччя** між існуванням комп'ютерних мереж, хостів мереж і програмного забезпечення хостів, що надають розподілені послуги обробки інформації, технологій, що забезпечують можливість взаємодії цих компонентів, але не гарантують їх резильєнтного функціонування в умовах кіберзагроз різного типу, а також зростаючими вимогами фізичних і корпоративних користувачів до захищеності даних та оперативності надання інформаційно-обчислювальних послуг в Інтернет-середовищі, з одного боку, і відсутністю методологічних основ для ефективного створення резильєнтних комп'ютерних систем, здатних проактивно реагувати на нові та невідомі кібератаки, протистояти їм та мати здатність до відновлення після атак, а також еволюціонувати в процесі свого функціонування, - з іншого боку.

### 4.2. Зв'язок теми дисертації з державними програмами, планами, темами університету та кафедри

Дисертаційну роботу виконано відповідно до державних науково-технічних програм, що сформульовані в Законах України «Про наукову і науково–технічну діяльність», «Про національну програму інформатизації», а також планам найважливіших науково–технічних програм Міністерства освіти і науки України: 6 – Інформатика, автоматизація та приладобудування; 6.2.1 – Інтелектуалізація процесів прийняття рішень; 6.2.2 – Перспективні інформаційні технології і системи.

Представлені в дисертації дослідження проводились в рамках держбюджетних НДР Хмельницького національного університету № 2Б-2011 «Методологія інтелектуального автоматизованого оцінювання відповідності програмного забезпечення систем критичного застосування вимогам» (номер держреєстрації 0111U002294), № 1Б-2019 «Агентно-орієнтована система підвищення безпеки та якості програмного забезпечення комп'ютерних систем» (номер державної реєстрації 0119U100662), а також в рамках Міжнародних проектів Хмельницького національного університету TEMPUS SAFEGUARD «National Safeware Engineering Network of Centers of Innovative Academia-Industry Handshaking» (№158886-TEMPUS-2009-UK-JPCR, 2010-2012 рр.) та TEMPUS SEREIN (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR, 2014-2017 рр.) «Модернізація післядипломної освіти у галузі безпеки та стійких інформаційних систем для індустрії».

Роль автора в цих НДР і проектах, в яких дисертант був безпосереднім виконавцем, полягає в розробці методології, принципів, моделей, методів та інформаційних технологій забезпечення резильєнтності комп'ютерних систем.

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

У друкованих працях, опублікованих у співавторстві, автору дисертації належать:

[1-10, 13, 15-21, 27-32, 37, 40, 45, 46] – дослідження особливостей функціонування кібератак мережного типу в комп'ютерних мережах;

[11,12, 33, 41] - метод забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз на основі самоадаптивності;

[11] - інформаційна технологія забезпечення резильєнтності комп'ютерних систем;

[11, 14] - метод оцінювання резильєнтності комп'ютерних систем в умовах кіберзагроз;

[22] - оцінка ефективності засобів антивірусного діагностування комп'ютерних систем;

[34] - метод виявлення кібер-загроз на основі еволюційних алгоритмів

[35] - метод виявлення шкідливих програмних засобів на основі алгоритму найближчих сусідів;

[43,44] - моделі кібератак мережного та хостового типу;

[41] - модель формального опису резильєнтних КС в умовах кіберзагроз;

[38, 45] - метод виявлення кібератак на основі протоколу DNS;

[36,47] - метод виявлення ШПЗ хостового типу на основі алгоритму клонального відбору;

[39] - метод виявлення повільних атак на основі самоподібності мережного трафіку;

[41, 42] - методологія та принципи створення резильєнтних комп'ютерних систем в умовах здійснення кібератак;

[15-33, 16, 23, 45,46] – обґрунтування актуальності проблеми побудови ефективних методів виявлення шкідливого програмного забезпечення та кібератак в комп'ютерних системах;

[1-6, 19] – аналіз сучасного стану інформаційної безпеки комп'ютерних систем;

[11, 14, 27] – реалізація інформаційної технології забезпечення резильєнтності комп'ютерних систем.

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

Наукові положення, висновки та рекомендації, що містяться в дисертації, є достовірними і обґрунтованими, оскільки вони відповідають фундаментальним теоретичним принципам, узгоджуються з даними з науково-технічної літератури, а також підтверджуються результатами обчислювальних експериментів та математичного моделювання.

**Ступінь наукової новизни основних результатів дисертаційної роботи**

***Одержано такі наукові результати*:**

*вперше розроблено:*

1) методологію створення резильєнтних комп'ютерних систем, яка, на відміну від відомих, базується на принципах проактивного виявлення кібератак, адаптивності, забезпечення стійкості до втручань, диверсності та керованої деградації продуктивності КС, а також захисту в глибину разом зі здатністю до еволюції та адаптації, що дозволяє надавати інформаційно-обчислювальні послуги та сервіси комп'ютерними системами в умовах здійснення кібератак;

2) метод забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз на основі самоадаптивності, який, на відміну від інших, дозволяє здійснювати реконфігурування компонентів КС шляхом застосування сценаріїв безпеки та забезпечує здатність системи її стійкого функціонування в ситуації наявності кібератак, а також реалізує принципи адаптивності та здатності до еволюції КС в умовах кібератак;

3) структурну модель інформаційної технології забезпечення резильєнтності комп'ютерних систем, яка відображає рух інформаційних потоків при опрацюванні інформації щодо мережного вхідного та вихідного трафіку та поведінки ПЗ КС і дозволяє отримати висновок про присутність відомих та невідомих кібератак, шкідливого мережного трафіку, шкідливого програмного забезпечення мережного та хостового типу, а також про застосування необхідного сценарію безпеки в умовах здійснення атак;

*одержали подальший розвиток:*

4) моделі кібератак мережного та хостового типу, які на відміну від відомих, враховують не тільки особливості їх поведінки, але й архітектурні особливості, що дозволило створити базу поведінок атак мережного та хостового типу для їх використання в процесі виявлення атак;

5) модель формального опису резильєнтних КС в умовах кіберзагроз, яка відрізняється від відомих тим, що дозволяє описувати процес функціонування КС в умовах кібератак з урахування етапів нормального функціонування, деградації та відновлення системи після здійснення атаки;

6) метод виявлення кібератак на основі протоколу DNS шляхом аналізу мережних запитів, який на відміну від інших враховує не лише характеристики запитів, але й ентропію доменних імен, що дозволяє підвищити достовірність та ефективність процесу виявлення кібератак мережного типу та реалізує принцип проактивності для забезпечення резильєнтності КС в умовах кібератак;

7) метод виявлення ШПЗ хостового типу на основі алгоритму клонального відбору, який здійснює виявлення ШПЗ в КС на основі аналізу поведінки ПЗ в КС, і у якому на відміну від відомих методів, поведінкова сигнатура ШПЗ формується у вигляді множини антигенів шляхом застосування штучних імунних систем, а також реалізує принципи

адаптивності та проактивності для забезпечення резильєнтності КС в умовах кібератак;

8) метод виявлення повільних атак на основі самоподібності мережного трафіку, який дозволяє виявляти повільні розподілені атаки на відмову в обслуговуванні шляхом аналізу мережного трафіку, і який на відміну від інших методів забезпечує визначення ступеня його схожості з попередньо зібраним трафіком повільної атаки, де в якості критерію схожості використовується значення ступенів самоподібності трафіку на різних часових відрізках у різних часових масштабах, які визначаються за допомогою коефіцієнта Херста, що забезпечує підвищення достовірність та ефективність процесу виявлення повільних кібератаки в комп'ютерних мережах, а також реалізує принципи проактивності для забезпечення резильєнтності КС в умовах кібератак;

9) метод оцінювання резильєнтності комп'ютерних систем в умовах кіберзагроз, який дозволяє одержати інтегрований показник резильєнтності, і, який на відміну від інших, враховує усі етапи операційного циклу КС: підготовки (прогнозування, попередження) до функціонування системи в умовах кібератак; захисту системи, виявлення атаки, поглинання атаки, відповіді на атаку, відновлення системи після здійснення кібератаки, адаптації на основі знань про попередні атаки.

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

Результати дисертаційної роботи повною мірою відображені у 67 наукових працях, з яких 19 статей у зарубіжних виданнях, індексованих у наукометричних базах (в тому числі 14 статті у періодичних зарубіжних виданнях), індексованих у наукометричній базі Scopus); 29 статей у наукових фахових виданнях України; опубліковано 3 патенти на корисну модель, 1 свідоцтво про реєстрацію авторського права на твір; 15 статей та тез доповідей у збірниках праць конференцій.

Нижче наведений перелік основних опублікованих праць за темою дисертації.

#### Статті у періодичних зарубіжних виданнях, індексованих у наукометричних базах

1) Savenko O. Multi-agent based approach of botnet detection in computer systems / O. Savenko, **S. Lysenko**, A. Kryschuk // Communications in Computer and Information Science, ISSN: 1865-0929 (Scopus, Web of Science). – 2012. – Vol. 291. – Pp. 171–180.

2) Pomorova O. Multi-Agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic / O. Pomorova, O. Savenko, **S. Lysenko**, A. Kryshchuk // Communications in Computer and Information Science, ISSN: 1865–0929 (Scopus, Web of Science). – 2013. – Vol. 370. – Pp. 146–156.
3) Pomorova O. A Technique for detection of bots which are using polymorphic code / O. Pomorova, O. Savenko, **S. Lysenko**, A. Kryshchuk, A. Nicheporuk // Communications in Computer and Information Science, ISSN: 1865–0929 (Scopus, Web of Science). – 2014. – Vol. 431. – Pp. 265–276.
4) Pomorova O. A Technique for the Botnet Detection Based on DNS-Traffic Analysis / O. Pomorova, O. Savenko, **S. Lysenko**, A. Kryshchuk, K. Bobrovnikova // Communications in Computer and Information Science, ISSN: 1865-0929 (Scopus, Web of Science). – 2015. – Vol. 522. – Pp. 127–138.
5) Pomorova O. Anti-evasion Technique for the Botnets Detection Based on the Passive DNS Monitoring and Active DNS Probing / O. Pomorova, O. Savenko, S**. Lysenko,** A. Kryshchuk, K. Bobrovnikova // Communications in Computer and Information Science ISSN: 1865-0929 (Scopus, Web of Science). – Brunów, 2016 – Vol. 608. – Pp. 83–95.
6) Oksana Pomorova, Oleg Savenko, **Sergii Lysenko**, Andrii Nicheporuk Metamorphic Viruses Detection Technique Based on the Modified Emulators // CEUR- WS, ISSN: 1613–0073 (Scopus). – 2016. – Vol-1614. – Pp. 375-383
7) Savenko O. Metamorphic Viruses' Detection Technique Based on the Equivalent Functional Block Search / O. Savenko, S. Lysenko, A. Nicheporuk, B. Savenko // CEUR- WS, ISSN: 1613–0073 (Scopus). – 2017. – Vol. 1844. – Pp. 555–569.
8) **Lysenko S**. Information technology for botnets detection based on their behaviour in the corporate area network / **S. Lysenko**, O. Savenko, K. Bobrovnikova, A. Kryshchuk, B. Savenko // Communications in Computer and Information Science, ISSN: 1865–0929 (Scopus, Web of Science). – 2017. – Vol. 718. – Pp. 166–181.
9) **Sergii Lysenko**, Oleg Savenko, Kira Bobrovnikova. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering / CEUR-WS, ISSN: 1613–0073 (Scopus). – 2018. - vol.2104, pp. 688-695.
10) Markowsky G. The technique for metamorphic viruses' detection based on its obfuscation features analysis / G. Markowsky, O. Savenko, **S. Lysenko**, A. Nicheporuk // CEUR-WS, ISSN: 1613–0073 (Scopus). – 2018. – Vol. 2104. – Pp. 680–687.
11) **S. Lysenko**, O. Savenko, K. Bobrovnikova, A. Kryshchuk. Self-adaptive system for the corporate area network resilience in the presence of botnet cyberattacks / Communications in Computer and Information Science, ISSN: 1865-0929 (Scopus, Web of Science). - 2018. - pp 385-401.
12) **Sergii Lysenko**, Kira Bobrovnikova, Andrii Nicheporuk, Roman Shchuka SVM-based Technique for Mobile Malware Detection // CEUR-WS, ISSN: 1613–0073 (Scopus). – 2019. – Vol-2353. – Pp. 85-97.

13) Savenko O. / Dynamic signature-based malware detection technique based on API call tracing / Savenko, O., Nicheporuk, A., Hurman, I., **Lysenko, S**. - CEUR-WS: ISSN: 1613–0073 (Scopus). – 2019. – Vol. Vol-2393. – P. 633-643.
14) Lysenko S., Bobrovnikova K., Savenko O., Kryshchuk A. BotGRABBER: SVM-Based Self-Adaptive System for the Network Resilience Against the Botnets' Cyberattacks. / Communications in Computer and Information Science, Springer, Cham ISSN: 1865-0929 (Scopus, Web of Science). – 2019. - pp. 127-143.

## Статті у наукових фахових виданнях України

15) Савенко О. Діагностування комп'ютерних систем на наявність шкідливого програмного забезпечення на основі антивірусної мультиагентної системи / О. Савенко, А. Крищук, **С. Лисенко** // Вісник Нац. ун-ту "Львів. політехніка". - 2011. - № 717. - С. 147-152.
16) **Лисенко, С. М.** Побудова процесу виявлення троянських програм [Текст] / **С. М. Лисенко**, А. В. Красій, В. В. Мельник // Вісник Хмельницького національного університету. Технічні науки. – 2012. – № 2. – С. 164-171.
17) Savenko O.S. Multi-agent based approach of botnet detection / O.S. Savenko, **S.M. Lysenko,** A.F. Kryshchuk // Радіоелектронні і комп'ютерні системи. – 2012. – №5. – С.56-61.
18) Савенко О.С. Графічна модель ботнет мереж. / О.С. Савенко, С.М. **Лисенко С.М**., А.Ф. Крищук // Науковий вісник Чернівецького національного університету імені Юрія Федьковича. Серія: Комп'ютерні системи та компоненти. Том 4, Вип.2.- 2013. - С. 25-30.
19) Савенко О. С., **Лисенко С. М**., Крищук А. Ф. Модель ботнет-мереж, *Вісник Вінницького політехнічного інституту*, № 3, с. 76-81, 1.
20) Savenko O. Model of the computer system diagnosis process for botnet presence in corporate area network / O. Savenko, **S. Lysenko**, A. Kryshchuk // Радіоелектронні і комп'ютерні системи. – 2013. – №5. – с.342-347.
21) Савенко О.С. Процес діагностування комп'ютерних систем на наявність ботнер-мереж на основі мультиагентних технологій / О.С. Савенко, **С.М. Лисенко**, А.Ф. Крищук // Комп'ютерно-інтегровані технології : освіта, наука, виробництво: наук. журн. – 2013. — №11. – С.72–81.
22) **Лисенко С. М.** Оцінка ефективності засобів антивірусного діагностування комп'ютерних систем [Текст] / **С. М. Лисенко** // Вісник Хмельницького національного університету. Технічні науки. – 2013. – № 2. – С. 196-201.
23) Савенко О. С. Модель ботнет-мереж [Електронний ресурс] / О. С. Савенко, С**. М. Лисенко**, А. Ф. Крищук // Вісник Вінницького політехнічного інституту. - 2013. - № 3. - С. 76-81. - Режим доступу: http://nbuv.gov.ua/UJRN/vvpi_2013_3_17
24) **Лисенко, С. М.** Дослідження методу опорних векторів як засобу ідентифікації шкідливого програмного забезпечення [Текст] / С. М. Лисенко,

М. П. Южека // Вісник Хмельницького національного університету. Технічні науки. – 2013. – № 6. – С. 194-201.
25) **Лисенко С. М.** Метод виявлення поліморфного коду ботів ботнет-мереж / С. М. Лисенко, О. С. Савенко, А. О. Нічепорук // Радіоелектрон. і комп'ют. системи. - 2014. - № 5. - С. 129-134.
26) Савенко О. С. Ефективність діагностування комп'ютерних систем на наявність бот-мереж антивірусною мультиагентною системою / О.С. Савенко, **С.М. Лисенко**, А.Ф.Крищук // Компютерно-інтегровані технології: освіта, наука, виробництво: наук. журн. - 2014.- №14. - С.109-114.
27) Савенко О. С. DNS-метод виявлення бот-мереж / О. С. Савенко, **С. М. Лисенко**, К. Ю. Бобровнікова // Інформаційні технології та комп'ютерна інженерія. – 2014. – № 3. – С. 39-45.
28) Савенко О. С. Модель процесу діагностування комп’ютерних систем на наявність поліморфного та метаморфного програмного коду / О. С. Савенко, **С. М. Лисенко**, А. О. Нічепорук // Інформаційні технології та комп'ютерна інженерія. - 2014. - № 3. - С. 46-51. - Режим доступу: http://nbuv.gov.ua/UJRN/Itki_2014_3_9.
29) Савенко О., **Лисенко С**., Нічепорук А. Моделі рівнів поліморфних комп’ютерних вірусів, Вісник Вінницького політехнічного інституту, № 2, с. 75-83, Бер 2015.
30) Савенко О.С. Метод виявлення бот-мереж, що використовують технології ухилення на основі DNS / О.С. Савенко, **С.М. Лисенко**, К.Ю. Бобровнікова // Комп’ютерно-інтегровані технології: освіта, наука, виробництво. – 2015. – № 19. – С. 71-78.
31) Савенко О. С. Інформаційна технологія виявлення бот-мереж на основі аналізу DNS-трафіка / О. С. Савенко, **С. М. Лисенко**, К. Ю. Бобровнікова // Радіоелектронні і комп’ютерні системи. - 2016. - №5. - С. 38–42. - Режим доступу: http://nbuv.gov.ua/UJRN/recs_2016_5_8.
32) Савенко О.С., **Лисенко С.М**., Нічепорук А.О. Інформаційна технологія діагностування комп’ютерних систем на наявність поліморфного програмного коду, Вісник Вінницького політехнічного інституту, № 6, с. 53-58, Лют 2017.
33) **Лисенко С. М**. Метод забезпечення живучості комп'ютерних систем в корпоративних мережах на основі самоадаптивності [Текст] / **С. М. Лисенко**, К. Ю. Бобровнікова, В. І. Дмитрук, А. С. Адаменко // Вісник Хмельницького національного університету. Технічні науки. – 2017. – № 3. – С. 196-201.
34) **Лисенко, С.М.** Метод виявлення кібер-загроз на основі еволюційних алгоритмів [Текст] / **С. М. Лисенко**, Д. І. Стопчак, В. В. Самотес // Вісник Хмельницького національного університету. Технічні науки. – 2017. – № 6. – С. 81-88.
35) **Лисенко, С.М.** Метод виявлення шкідливих програмних засобів на основі алгоритму найближчих сусідів [Текст] / **С. М. Лисенко**, В. В. Гуменюк // Вісник Хмельницького національного університету. Технічні науки. – 2017. – № 6. – С. 96-101.
36) **Лисенко С. М.** Метод та програмні засоби виявлення шкідливого програмного забезпечення типу backdoor на основі використання алгоритму

клонального відбору [Текст] / **С. М. Лисенко**, О. І. Шевчук // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2018. – № 2. – С. 73-79.
37) С.М. Лисенко Метод виявлення троянських програм на основі апарату нечіткої кластеризації / **С.М. Лисенко**, Ю.О. Гайбура, В.М. Стецюк // Комп'ютерно-інтегровані технології : освіта, наука, виробництво: наук. журн. – 2018. — №30-31. – С.75-82, http://ki.lutsk-ntu.com.ua/node/138/section/25
38) Лисенко, С.М. Метод та програмне забезпечення виявлення шкідливих запитів в комп'ютерних мережах на основі протоколу DNS [Текст] / **С. М. Лисенко**, В. О. Лісовий // Вісник Хмельницького національного університету. Технічні науки. – 2019. – №3. – С. 173-179.
39) Лисенко, С.М. Метод та програмні засоби виявлення кібератаки типу R.U.D.Y. на основі використання алгоритму визначення самоподібності трафіку [Текст] / **С. М. Лисенко**, В. А. Ткачук // Вісник Хмельницького національного університету. Технічні науки. – 2019. – №3. – С. 180-187.
40) **Лисенко С.М**. Методи виявлення бот-мереж в комп'ютерних системах. / **С.М.Лисенко**., К.Ю.Бобровнікова, В.С.Харченко // Сучасні інформаційні системи. - 2019. - Т.3, №4. - С.87-95.
41) **Лисенко С. М**. Метод забезпечення резильєнтності комп’ютерних систем в умовах кібер-загроз на основі самоадаптивності / **С. М. Лисенко** // Радіоелектронні і комп’ютерні системи. - 2019. - №4. - С. 4-16.
42) **Лисенко С. М**. Резильєнтність комп’ютерних систем в умовах кіберзагроз: Онтологія та таксономії / **С. М. Лисенко**, В.С. Харченко, К.Ю. Бобровнікова, Р. Щука // Радіоелектронні і комп’ютерні системи. - 2020. - №1. - С. 55–65.
43) **Лисенко С. М.** Моделі опису здійснення кібер-атак на інформаційно-комунікаційні системи [Текст] / **С. М. Лисенко** // ВОТТП. – 2019. – №2. – С. 173-179.

## Статті у матеріалах зарубіжних та українських конференцій, що індексуються у наукометричних базах Scopus та Web of Science

44) **Lysenko S**. Botnet detection technique for corporate area network / **Lysenko S.**, Savenko O., A. Kryshchuk, Y. Klyots // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Berlin, DE, IEEE, 2013, p. 315-320, ISBN 978-1-4799-1426-5 Видання, що входить до бази IEEE *Xplore* Digital Library та до бази SCOPUS та Web of Science
45) **Sergii Lysenko**. DNS-based Anti-evasion Technique for Botnets Detection / **Sergii Lysenko**, Oksana Pomorova, Oleg Savenko, Andrii Kryshchuk and Kira Bobrovnikova // Proceedings of the 2015 IEEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IDAAACS’2015, Warsaw, Poland, September 24-26, 2015, Vol.1, pp.453-458. Видання, що входить до баз SCOPUS, Web of Science.
46) Savenko O. Approach for the Unknown Metamorphic Virus Detection / O. Savenko, **S. Lysenko**, A. Nicheporuk, B. Savenko // The 9-th IEEEE International

Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, September 21-23, 2017: Proceedings. – Bucharest (Romania), 2017 – PP. 453-458. Видання, що входить до баз SCOPUS, Web of Science.

47) **Sergii Lysenko**, Kira Bobrovnikova and Oleg Savenko. A Botnet Detection Approach Based on The Clonal Selection Algorithm // Proceedings of 2018 IEEE 9th International Conference on Dpendable Systems, Services and Technologies (DeSSerT-2018, Kyiv, Ukraine, May 24-27, 2018) – pp. 424-428

48) **Lysenko Sergiy**, Oleg Savenko. Software for Computer Systems Trojans Detection as a Safety-Case Tool. // Information & Security : An International Journal 28, no. 1 (2012): 121-132. ISSN 0861-5160, Зміст за посиланням: http://www.procon.bg/?q=volume28.

**Патенти та авторські свідоцтва**

49) Пат. на корисну модель 108238 Україна, МПК G06F 21/55 Мультиагентний спосіб локалізації бот-мереж у корпоративних комп'ютерних мережах / О. В. Поморова, О. С. Савенко, А. Ф. Крищук, **С. М. Лисенко**, К. Ю. Бобровнікова, А. О. Нічепорук; заявник і патентовласник Хмельницький національний університет. – № u201600127; заявл. 04.01.2016; опубл. 11.07.2016, Бюл. № 13/2016.

50) Пат. на корисну модель 118456 Україна, МПК G06F 21/55 Спосіб виявлення метаморфних вірусів на основі статистичних метрик для визначення еквівалентних функціональних програмних блоків / О. С. Савенко, **С. М. Лисенко**, К. Ю. Бобровнікова, А. О. Нічепорук, Б. О. Савенко; заявник і патентовласник Хмельницький національний університет. – № u201701743; заявл. 23.02.2017; опубл. 10.08.2017, Бюл. № 15/2017.

51) Пат. на корисну модель 118663 Україна, МПК G06F 21/55 Спосіб ідентифікації бот-мереж у корпоративних комп'ютерних мережах на основі аналізу DNS-трафіку / О. С. Савенко, **С. М. Лисенко**, К. Ю. Бобровнікова, А. О. Нічепорук, Б. О. Савенко; заявник і патентовласник Хмельницький національний університет. – № u201612041; заявл. 28.11.2016; опубл. 28.08.2017, Бюл. № 16/2017.

52) А. с. 80223 Україна. Комп'ютерна програма пошуку та визначення еквівалентних функціональних блоків у виконуваних файлах для ідентифікації ознак метаморфних вірусів в локальних комп'ютерних мережах / А. О. Нічепорук, О. С. Савенко, **С. М. Лисенко**. 2018.

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

Основні результати дисертаційного дослідження неодноразово доповідалися та обговорювалися на 30 міжнародних та всеукраїнських

конференціях, а саме 6-th, 7-th, 8-th, 9-th IEEE Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications IDAACS'2011 (Prague, Chech Republic, 2011), IDAACS'2013 (Berlin, Germany, 2013), IDAACS'2015 (Warszawa, Poland, 2015), IDAACS'2017 (Bucharest, Romania, 2017) IDAACS'2019 (Metz, France, 2019); 19-th, 20-th, 21-th, 22-th, 23-th, 24-th, 25-th, 26-th International Conference on Computer Networks: CN'2012 (Szczyrk, Poland, 2012), CN'2013 (Lwówek Slaski, Poland, 2013), CN'2014 (Brunów, Poland, 2014), CN'2015 (Brunów, Poland, 2015), CN'2016 (Brunów, Poland, 2016), CN'2017 (Brunów, Poland, 2017), CN'2018 (Gliwice, Poland, 2018), CN'2019 (Sanctuary of St. Jack, Kamień Śląski, Poland, 2019); 7-th International Scientific and Technical Conference on Computer Science and Information Technologies: CSIT (Lviv, Ukraine, 2012); International Conference Advanced Computer Systems and Networks: Design and Application ACSN (Lviv, Ukraine, 2011); 1-st International Academic Conference on Science and Education in Australia, America and Eurasia: Fundamental and Applied Science (Melbourne, Australia, 2014); Міжнародній науково-практичній конференції «Сучасні інформаційні і електронні технології (CIET)» (Одеса, 2011, 2012, 2013); Проблемно-науково-міжгалузевій конференції «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління (ПНМК)» (Бучач – Яремча, 2011, 2014); Міжнародній конференції «Контроль і управління в складних системах (КУСС)» (Вінниця, 2012, 2014); Міжнародній науково-технічній конференції «Захист інформації і безпека інформаційних систем» (Львів, 2012); International Workshop «Critical infrastructure safety and security (CrlSS-DESSERT'11)» (Kirovograd, 2011, 2013); Міжнародній конференції «Інтелектуальний аналіз інформації (IAI)» (Київ, 2013); щорічних наукових конференціях професорсько-викладацького складу Хмельницького національного університету. Наведений перелік конференцій підтверджує достатньо високий рівень апробації наукових результатів дисертації.

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

У дисертаційній роботі вирішена актуальна науково-прикладна проблема створення резильєнтних комп'ютерних систем, яка дозволяє вирішити об'єктивне протиріччя між існуванням комп'ютерних мереж, хостів мереж і програмного забезпечення хостів, що надають розподілені послуги обробки інформації, технологій, що забезпечують можливість взаємодії цих компонентів, але не гарантують їх резильєнтного функціонування в умовах кіберзагроз різного типу, а також зростаючими вимогами фізичних і корпоративних користувачів до захищеності даних та оперативності надання інформаційно-обчислювальних послуг в Інтернет-середовищі, з одного боку, і

відсутністю методологічних основ для ефективного створення резильєнтних комп'ютерних систем, здатних проактивно реагувати на нові та невідомі кібератаки, протистояти їм та мати здатність до відновлення після атак, а також еволюціонувати в процесі свого функціонування, - з іншого боку.

Отримані в дисертаційній роботі результати можуть бути застосовані в усіх галузях, де використовуються комп'ютерні системи і гостро стоїть питання забезпечення інформаційної безпеки комп'ютерних систем.

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

Практичне значення отриманих результатів визначається тим, що розроблені методологія, моделі і методи є науково-методологічною основою для створення інформаційної технології створення складних сервіс-орієнтованих систем з необхідними характеристиками резильєнтності в умовах здійснення кібератак. Доведені до рівня інженерних методик, алгоритмів та інструментальних засобів вони дозволяють:

- отримати висновок про присутність відомих та невідомих повільних атак та розподілених атака на відмову в обслуговуванні шляхом аналізу інформації щодо вхідного та вихідного мережного трафіку на предмет самоподібності, що реалізує принцип проактивного виявлення кіберзагроз щодо КС;
- отримати висновок щодо присутності кіберзагроз в умовах недостатності інформації шляхом аналізу інформації щодо поведінки програмного забезпечення в КС для реалізації принципів проактивного виявлення кіберзагроз, захисту в глибину та адаптивного функціонування КС та здатності до еволюції комп'ютерних систем в умовах кіберзагроз;
- отримати висновок щодо присутності шкідливого мережного трафіку шляхом його аналізу інформації щодо DNS запитів вхідного для забезпечення принципів проактивного виявлення кіберзагроз та забезпечення стійкості до втручань в КС;
- отримати висновок щодо присутності шкідливого програмного забезпечення мережного та хостового типу шляхом аналізу інформація щодо вихідного мережного трафіку та поведінки ПЗ в КС для реалізації принципів проактивного виявлення кіберзагроз, адаптивного функціонування КС та здатності до еволюції КС в умовах кіберзагроз;
- отримати числову поточну оцінку резильєнтності КС в умовах здійснення кібератак з метою забезпечення принципів еластичності та керованої деградація комп'ютерної системи;
- отримати інформацію про застосування необхідного сценарію безпеки шляхом опрацювання інформації щодо наявної кібератаки на комп'ютерну

систему з метою забезпечення принципів адаптивного функціонування КС, стійкості до втручань в КС, забезпечення захисту в глибину, керованої деградація, а також диверсності компонентів КС в умовах здійснення атак.

Результати дисертаційної роботи Лисенка С.М. в даний час використовуються як система забезпечення резильєнтності КС, яка складається з модулів моніторингу мережі та хостів у вигляді програмного забезпечення – BotGRABBER.

Система здатна ефективно виявляти присутність шкідливого мережного трафіку мережного та хостового типу, а також застосувати необхідні сценарії безпеки в залежності від типу атаки з метою підвищення рівня інформаційної безпеки в компаніях м. Хмельницького різного профілю.

### 4.10. Реалізація та впровадження результатів роботи

Результати дисертаційної роботи впроваджено у навчальному процесі Хмельницького національного університету (акт впровадження від 11.12.2019 р.), Національної академії Державної прикордонної служби України ім. Б. Хмельницького (акт впровадження від 13.12.2019 р.), Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» (акт впровадження від 18.12.2019 р.).

Розроблені методологію та інформаційну технологію забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз: для ПЗ системи обліку та білінгу надання послуг доступу до мережі Інтернет на підприємстві *ТОВ «ІТТ»* (акт впровадження від 20.01.2020 р.), де вона дала можливість підвищити ефективність виявлення кіберзагроз на рівні 94,54% при хибному виявленні 2,21%; для інфраструктури підприємства *ТОВ «Гілея»* (акт впровадження від 31.01.2020 р.), де вона дала можливість забезпечення резильєнтності комп'ютерних систем і підвищила ефективність інформаційної безпеки до 98,42%; для локальної мережі на підприємстві *ТОВ «Деймос»* (акт впровадження від 03.01.2020 р.), де вона дала можливість отримання висновку щодо присутності кіберзагроз в умовах недостатності інформації шляхом аналізу інформації щодо поведінки програмного забезпечення в КС для реалізації принципів проактивного виявлення кіберзагроз; для комп'ютерної мережі хостів інфраструктури ГО «IT cluster Хмельницький» (акт впровадження від 24.12.2019 р.), де вона дала можливість підвищити ефективність інформаційної безпеки інфраструктури ГО «*IT cluster Хмельницький*» до 98,42%, для комп'ютерних систем підприємства *ООО GM Host* (акт впровадження від 20.12.2019 р.), у якій застосування інформаційної технології підвищило достовірність виявлення повільних DNS атак до 97,24%.

### 4.11. Оцінка структури дисертації, її мови та стилю викладення

Дисертаційна робота має логічну структуру і складається з анотації, вступу, семи розділів, висновків, списку використаних джерел та 5 додатків. Ці складові частини в сукупності вирішують поставлену проблему. Дисертаційна робота за обсягом, структурою, мовою та стилем викладення відповідає вимогам МОН України до дисертацій на здобуття наукового ступеня доктора технічних наук.

**4.12. Відповідність дисертації паспорту спеціальності, за якою вона представляється до захисту**

Дисертація відповідає формулі та 7 пунктам паспорту спеціальності 05.13.06 – інформаційні технології, зокрема, п.1 «Розроблення наукових і методологічних основ створення і застосування інформаційних технологій та інформаційних систем для автоматизованої переробки інформації і управління», п.2 «Розроблення інформаційних технологій для аналізу та синтезу структурних, інформаційних і функціональних моделей об'єктів і процесів, що автоматизуються», п.8 «Побудова інформаційних технологій для ефективного розроблення програмного забезпечення комп'ютерних мереж і систем розподіленої обробки даних», п.9 «Створення інформаційних технологій для розроблення моделей і методів контролю, класифікації, кодування та забезпечення достовірності інформації», п.10 «Моделювання предметних галузей інформаційних систем (аналітичне, імітаційне, інфологічне, об'єктно-орієнтоване, тощо) на підґрунті створення і застосування відповідних інформаційних технологій», п.11 «Розроблення інформаційно-пошукових і експертних систем обробки інформації для прийняття рішень, а також знанняорієнтованих систем підтримки рішень в умовах ризику та невизначеності як інтелектуальних інформаційних технологій», п.14 «Розроблення й дослідження моделей і методів оцінювання якості і підвищення надійності, функціональної безпеки і живучості інформаційних та інформаційно-управляючих систем, а також інформаційних технологій для створення гарантоздатних автоматизованих систем переробки інформації та управління критичного застосування»

У ході обговорення дисертаційної роботи до неї не було висунуто жодних зауважень, що стосуються самої суті роботи.

**4.13. Ступінь використання матеріалів кандидатської дисертації**

У дисертації на здобуття наукового ступеня доктора технічних наук Лисенка С. М. не використовував матеріалів своєї дисертації на здобуття наукового ступеня кандидата технічних наук на тему «Адаптивна інформаційна технологія діагностування комп'ютерних систем на наявність троянських програм», захищеної у 2013 році в НУ «Львівська політехніка» за спеціальністю 05.13.06 – Інформаційні **технології.**

**5. З врахуванням вищевикладеного,**

**УХВАЛИЛИ:**

**5.1.** Дисертаційна робота Лисенка Сергія Миколайовича «Методологічні основи та інформаційна технологія забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз» є завершеною науковою працею, в якій вирішено актуальну наукову проблему розроблення методологічних

основ та інформаційної технології забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз, які підвищує резильєнтності комп'ютерних систем на основі принципів проактивного виявлення атак та адаптивної реконфігурації систем в умовах кіберзагроз, і дозволяє отримання інформації про застосування необхідного сценарію безпеки шляхом опрацювання інформації щодо наявної кібератаки на комп'ютерну систему.

**5.2.** Основні результати дисертаційної роботи повністю викладені у 61 наукові праці, з них: 18 статей у зарубіжних виданнях, індексованих у наукометричних базах (в тому числі 14 статей у періодичних зарубіжних виданнях), індексованих у наукометричній базі Scopus); 29 статей у наукових фахових виданнях України; опубліковано 3 патенти на корисну модель, 1 свідоцтво про реєстрацію авторського права на твір; 9 статей та тез доповідей у збірниках праць конференцій.

**5.3.** Дисертаційна робота Лисенка Сергія Миколайовича «Методологічні основи та інформаційна технологія забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз» відповідає паспорту спеціальності 05.13.06 – інформаційні технології, а також вимогам «Порядку присудження наукових ступенів.

**5.4.** Враховуючи наукову зрілість та професійні якості дисертанта, рекомендувати дисертаційну роботу Лисенка Сергія Миколайовича «Методологічні основи та інформаційна технологія забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз» до подання до розгляду у спеціалізовану вчену раду за спеціальністю 05.13.06 – «Інформаційні технології».

За затвердження висновку проголосували:
за – 18 (вісімнадцять)
проти – немає
утримались – немає

Головуючий на засіданні,
завідувач кафедри комп'ютерної інженерії
та системного програмування
Хмельницького національного
університету,
д.т.н., професор Т.О. Говорущенко

Секретар засідання,
доцент кафедри комп'ютерної інженерії
та системного програмування
Хмельницького національного
університету А. О. Нічепорук

17 січня 2020 р.