ЗАТВЕРДЖУЮ
В.о. ректора Національного авіаційного університету
_____ Ксенія СЕМЕНОВА
«25» 06 2024 р.

ВИСНОВОК

Національного авіаційного університету (далі – НАУ) про наукову новизну, теоретичне та практичне значення результатів дисертації Положенцева Артема Анатолійовича на здобуття ступеня доктора філософії з галузі знань 12 "Інформаційні технології" за спеціальністю 122 "Комп'ютерні науки" на тему: "Методи та засоби управління ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури"

ВИТЯГ

із протоколу № 10 розширеного засідання
кафедри комп'ютерних інформаційних технологій
Національного авіаційного університету від 29 травня 2024 року

Присутні на засіданні науково-педагогічні працівники кафедри комп'ютерних інформаційних технологій:

Савченко А.І., д.т.н, професор, завідувач кафедри;
Віноградов М.А., д.т.н., професор кафедри;
Воронін А.М., д.т.н., професор кафедри;
Зіатдінов Ю.К., д.т.н., професор кафедри;
Гнатюк С.О., д.т.н., професор кафедри;
Василенко В.А., к.т.н., доцент кафедри;
Харченко О.Г., к.т.н., доцент кафедри;
Моденов Ю.Б., к.т.н., доцент кафедри;
Райчев І.Е., к.т.н., доцент кафедри;
Холявкіна Т.В., к.т.н., доцент кафедри;
Климова А.С., к.т.н., доцент кафедри;
Чуба І.В., к.т.н. доцент кафедри;
Колісник О.В., к.т.н. доцент кафедри;
Зудов О.М., к.т.н., доцент кафедри;
Прокопенко К.І., к.т.н., доцент кафедри;
Сінько Ю.І., к.пед.н., доцент кафедри;
Толстікова О.В., к.т.н., доцент кафедри;
Сидоренко В.М., к.т.н., доцент кафедри;

Водоп’янов С.В., к.т.н., доцент кафедри;

Охріменко Т.О., к.т.н., ст. дослідник, п.н.с. НДЛ протидії кіберзагрозам в авіаційній галузі;

Єрмачков Ю.О старший викладач кафедри;

Остапенко О.С., старший викладач кафедри;

Шевченко О.П., старший викладач кафедри;

Горіна В.В., старший викладач кафедри;

Рибасова Н.О., старший викладач кафедри;

Охремчук О.С., асистент кафедри;

Мельниченко П.І., асистент кафедри.

Присутні на засіданні науково-педагогічні працівники інших кафедр НАУ:

Одарченко Р.С. д.т.н., професор, в.о. декана факультету аеронавігації, електроніки та телекомунікацій НАУ;

Нечипорук О.П., д.т.н., професор, професор кафедри комп’ютеризованих систем управління НАУ;

Павленко П.М., д.т.н., професор, професор кафедри організації авіаційних перевезень НАУ.

Слухали:

Доповідь аспіранта кафедри комп’ютерних інформаційних технологій Національного авіаційного університету Положенцева Артема Анатолійовича на тему: “Методи та засоби управління ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури”, поданої на здобуття ступеня доктора філософії з галузі знань 12 “Інформаційні технології”, за спеціальністю 122 “Комп’ютерні науки”.

Тему дисертаційного дослідження “Методи та засоби управління ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури”, затверджено на засіданні Вченої ради Факультету комп’ютерних наук та технологій 11 грудня 2023 року, протокол №8.

Науковий керівник – Сидоренко В.М., к.т.н., доцент, доцент кафедри комп’ютерних інформаційних технологій Національного авіаційного університету.

Доповідач обґрунтував актуальність обраної теми, визначив мету, завдання, методи дослідження, охарактеризував об’єкт та предмет дисертації, виклав основні наукові положення та висновки, що виносяться на захист, вказав науково-практичну значущість роботи, зазначив про впровадження результатів дослідження.

Автором проведено аналіз сучасних підходів до управління ІТ-інцидентами на об’єктах критичної інфраструктури держави. Дослідником визначено існуючі методології та стандарти в сфері ІТ-безпеки, ідентифіковано основні недоліки та області для покращення.

Дослідником удосконалено метод визначення рівня захищеності, а також розроблені відповідні рекомендації щодо оптимізації захисту об’єктів критичної інформаційної інфраструктури для визначення стану їх захищеності та управління захистом від ІТ-інцидентів.

Автором удосконалено метод визначення пріоритетів ІТ-інцидентів для кількісного визначення пріоритетів та управління ними.

Положенцевим А.А. було розроблено метод управління ІТ-загрозами, для ідентифікації, оцінки та пріоритизації ІТ-загроз для оптимального розподілу ресурсів захисту критичної інфраструктури держави.

Дослідником створено спеціальне програмне забезпечення, яке автоматизує процес оцінки стану захищеності об'єктів критичної інформаційної інфраструктури, забезпечуючи структурний підхід до збору даних, проведення оцінювання рівня захищеності та надання конкретних рекомендацій для покращення безпеки.

Автором створено спеціалізоване програмне забезпечення для визначення пріоритетів ІТ-інцидентів, що дозволяє ефективно ідентифікувати та пріоритизувати ІТ-інциденти, оптимізуючи розподіл ресурсів і забезпечуючи надійність та стійкість критичних інформаційних систем.

Дослідником проведено верифікацію розроблених методів з використанням розробленого програмного забезпечення з метою підтвердження їх ефективності та придатності для практичного застосування.

Структура та обсяг дисертації зумовлена метою і логікою дослідження та складається з анотації, вступу, чотирьох розділів, які об'єднують 20 підрозділів, висновків, списку використаних джерел, додатків.

Запитання до здобувача:

1. **Гнатюк С.О.,** д.т.н., професор, професор кафедри КІТ.

Запитання: У чому полягає власне процес управління інцидентами? З представлених Вами рисунків та слайдів це не зрозуміло.

Відповідь: Дякую за запитання. Процес управління інцидентами складається з декількох етапів. Розроблені методи допомагають визначити тип інцидентів та їх пріоритети на основі впливу та ймовірності реалізації, що позитивно вплине на загальний процес управління.

2. **Гнатюк С.О.,** д.т.н., професор, професор кафедри КІТ

Запитання: Яка практична цінність дисертаційної роботи? Які програмні застосунки було розроблено?

Відповідь: Дякую за запитання. Практична цінність дисертаційної роботи полягає у створенні методології та інструментів для ефективного управління ІТ-загрозами на ОКІІ. Було розроблено два програмні застосунки: застосунок для оцінки стану захищеності ОКІІ, який автоматизує процес збору даних, проведення оцінювання та надання рекомендацій для покращення безпеки та застосунок для визначення пріоритетів ІТ-загроз, що дозволяє ефективно ідентифікувати, оцінювати та пріоритизувати ІТ-загрози, оптимізуючи розподіл ресурсів.

3. **Гнатюк С.О.,** д.т.н., професор, професор кафедри КІТ

Запитання: Яким чином було визначено поняття ІТ-інциденти та ІТ-загрози? Що було взято за основу при виділенні цих термінів?

Відповідь: Дякую за запитання. Поняття ІТ-інциденти та ІТ-загрози були визначені на основі стандартів та рекомендацій міжнародних організацій, таких як ITIL та NIST.

4. **Гнатюк С.О.,** д.т.н., професор, професор кафедри КІТ

Запитання: Які кількісні, або якісні показники були використанні у роботі? Як вимірювали покращення ефективності?

Відповідь: Дякую за запитання. У роботі використовувалися як кількісні, так і якісні показники. До кількісних показників відносяться, наприклад, Індикатори ІТ-безпеки, Рівень цифрової трансформації, а до якісних – Оцінка рівня захищеності.

Покращення ефективності вимірювалося шляхом порівняння показників до та після впровадження розроблених методів та застосунків, а також через проведення постінцидентного аналізу та верифікацію результатів у реальних умовах.

5. **Нечипорук О.П.,** д.т.н., професор, професор кафедри комп'ютеризованих систем управління НАУ.

Запитання: Що мається на увазі під поняттям ОКІІ? Чи входить в цей перелік ІКС, чи інші системи?

Відповідь: Дякую за запитання. Під поняттям ОКІІ маються на увазі всі інформаційні системи, які є життєво важливими для функціонування держави. ІКС, а також інші системи, такі як системи енергетики, транспорту, фінансів входять до цього переліку.

6. **Нечипорук О.П.,** д.т.н., професор, професор кафедри комп'ютеризованих систем управління НАУ.

Запитання: Яке практичне застосування розроблених методів? Чи було отримано акт впровадження застосування методів?

Відповідь: Дякую за запитання. Практичне застосування розроблених методів полягає у їх використанні для оцінки та підвищення рівня захищеності ОКІІ, а також для ефективного управління ІТ-інцидентами та загрозами. На даний момент результати впроваджені і використовуються у НДЛ протидії кіберзагрозам в авіаційній галузі, а також завершується процес отримання акту впровадження у ДержНДІ технологій кібербезпеки та захисту інформації.

7. **Нечипорук О.П.,** д.т.н., професор, професор кафедри комп'ютеризованих систем управління НАУ.

Запитання: Як Ваша робота стосується процесу управління?

Відповідь: Дякую за запитання. Дисертація спрямована на розробку методів для управління ІТ-інцидентами в ОКІІ. Тобто, це включає розробку методів для оцінки стану захищеності, пріоритизації та реагування на інциденти, а також створення програмного забезпечення, яке автоматизує ці процеси, забезпечуючи більш ефективне управління ресурсами та покращення захищеності ОКІІ в умовах реалізації загроз та обмежених ресурсів захисту.

8. **Нечипорук О.П.,** д.т.н., професор, професор кафедри комп'ютеризованих систем управління НАУ.

Запитання: Що отримує користувач на виході після застосування програмного застосунку?

Відповідь: Дякую за запитання. Після застосування програмних застосунків користувач отримує звіт про стан захищеності ОКІІ, рекомендації щодо покращення захисту, а також перелік пріоритизованих ІТ-інцидентів.

9. **Нечипорук О.П.,** д.т.н., професор, професор кафедри комп'ютеризованих

систем управління НАУ.

Запитання: Які дані будуть отримані після застосування розроблених методів?

Відповідь: Дякую за запитання. Після застосування розроблених методів та програмних застосунків, користувач отримає наступні дані: оцінку стану захищеності ОКІІ та рекомендації щодо отриманих результатів, пріоритизацію наданих ІТ-інцидентів та рівень критичності ідентифікованих ІТ-загроз.

10. **Нечипорук О.П.,** д.т.н., професор, професор кафедри комп'ютеризованих систем управління НАУ.

Запитання: Чи є в дисертаційній роботі прогнозування результатів?

Відповідь: Дякую за запитання. Так, у роботі прогнозування дозволяє визначити, як впроваджені заходи покращать захищеність ОКІІ та мінімізують ризики. Наприклад, першочергові дії при настанні ІТ-інцидентів.

11. **Нечипорук О.П.,** д.т.н., професор, професор кафедри комп'ютеризованих систем управління НАУ.

Запитання: Що таке ефективність управління? Що відноситься до якості?

Відповідь: Дякую за запитання. Ефективність управління означає, наскільки добре система виконує свої завдання, досягаючи поставлених цілей і при яких витратах ресурсів, таких як час, наприклад.

12. **Нечипорук О.П.,** д.т.н., професор, професор кафедри комп'ютеризованих систем управління НАУ.

Запитання: Що мається на увазі під поняттям стан захищеності? Для чого використовується на практиці?

Відповідь: Дякую за запитання. Під станом захищеності мається на увазі рівень захисту ОКІІ від ІТ-загроз та інцидентів. На практиці стан захищеності використовується для оцінки поточного рівня безпеки, визначення пріоритетів для покращення та планування заходів для мінімізації ризиків та підвищення стійкості системи.

13. **Павленко П.М., д.т.н., професор, професор кафедри організації авіаційних перевезень НАУ.**

Запитання: У Вашій роботі Ви вказуєте, що розробили методи управління. У чому саме полягає управління?

Відповідь: Дякую за запитання. Управління в моїй роботі полягає у систематичному підході до ідентифікації, оцінці, пріоритизації та надання рекомендацій щодо реагування на ІТ-інциденти та загрози.

14. **Павленко П.М., д.т.н., професор, професор кафедри організації авіаційних перевезень НАУ.**

Запитання: Яка науково-технічна задача Вашої роботи?

Відповідь: Дякую за запитання. Науково-технічна задача моєї роботи полягає у забезпеченні безперервного управління ІТ-інцидентами на ОКІІ за рахунок розроблення відповідних методів і засобів оцінювання рівня захищеності, визначення пріоритетів і управління ІТ-загрозами.

15. **Павленко П.М., д.т.н., професор, професор кафедри організації авіаційних перевезень НАУ.**

Запитання: Яка різниця у поняттях метод та методика?

Відповідь: Дякую за запитання. На мою думку, метод – це спосіб досягнення поставленої мети, за допомогою певних кроків, а методика – конкретний набір інструкцій для реалізації підходів на практиці.

16. **Павленко П.М., д.т.н., професор, професор кафедри організації авіаційних перевезень НАУ.**

Запитання: Розглянемо поняття ефективності, яке було розглянуто у дисертаційній роботі. Що саме покращують розроблені методи, як це вимірюється?

Відповідь: Дякую за запитання. Розроблені методи підвищують ефективність у таких аспектах як, наприклад, точність ідентифікації загроз та інцидентів, своєчасність реагування на інциденти, пріоритизація загроз та оцінювання стану захищеності ОКІІ.

17. **Одарченко Р.С. д.т.н., професор, в.о. декана факультету аеронавігації, електроніки та телекомунікацій НАУ.**

Запитання: Які наукові принципи лежать в основі розроблених вами методів управління ІТ-інцидентами?

Відповідь: Дякую за запитання. В роботі були використані такі наукові принципи: системний аналіз, теорія множин, методи багатокритеріального прийняття рішень та моделювання загроз.

18. **Одарченко Р.С. д.т.н., професор, в.о. декана факультету аеронавігації, електроніки та телекомунікацій НАУ.**

Запитання: Як застосування багатокритеріального аналізу впливає на точність оцінки загроз у вашій роботі?

Відповідь: Дякую за запитання. Застосування методу TODIM дозволило враховувати різні аспекти ІТ-загроз, такі як ймовірність реалізації, потенційний збиток та складність нейтралізації, що значно підвищує точність оцінки, оскільки дозволяє комплексно оцінити кожну загрозу з урахуванням потрібних характеристик.

19. **Савченко А.І., д.т.н, професор, завідувач кафедри**.

Запитання: Чи можете показати схематично, як розроблені методи вирішують завдання з управління?

Відповідь: Дякую за запитання. Розроблені методи вирішують завдання управління ІТ-інцидентами шляхом надання комплексних рішень, які дозволяють користувачам приймати своєчасні управлінські рішення. На слайдах схематично зображено застосування розроблених методів.

20. **Савченко А.І., д.т.н, професор, завідувач кафедри**.

Запитання: Як розроблені методи покращують ефективність? Які оцінки використовуються?

Відповідь: Дякую за запитання. Розроблені методи покращують ефективність управління ІТ-інцидентами та загрозами наступним чином: підвищують точність виявлення ІТ-загроз, зменшують час від виявлення до реагування на інцидент, забезпечують більш ефективний розподіл ресурсів шляхом визначення пріоритетів ІТ-загроз за допомогою багатокритеріального аналізу, а також допомагають швидко визначити стан захищеності ОКІІ.

Положенцев А.А. докладно відповів на всі поставлені запитання, обґрунтувавши свою авторську позицію.

Висновок наукового керівника.

Після відповідей на запитання було озвучено висновок наукового керівника Сидоренко Вікторії Миколаївни, к.т.н., доцента, доцента кафедри комп'ютерних інформаційних технологій Національного авіаційного університету.

Зазначено, що дисертант успішно виконав індивідуальний план наукової роботи та індивідуальний навчальний план. Підготовлена дисертація готова до захисту. У роботі опрацьовано досить багато різноманітного матеріалу, дуже багато наукових праць – англомовні видання, які дозволили узагальнити досить широкий світовий досвід.

У процесі виконання роботи дисертант показав необхідну кваліфікацію для самостійного вирішення поставлених наукових задач, постійно працює над підвищенням свого освітнього і професійного рівня. Вміє проводити наукові дослідження, приймає участь у науково-дослідних роботах, має наукові публікації та доповіді у наукових конференціях.

Положенцев Артем Анатолійович працює над питаннями критичної інфраструктури протягом усього періоду навчання в Національному авіаційному університеті з 2015 року. За цей час продемонстрував себе як старанний та цілеспрямований здобувач, а наукові результати висвітлено та обговорено під час численних доповідей на науково-практичних конференціях та наукових форумах, отримав дипломи ступеня бакалавр та магістр з відзнакою.

Дисертаційна робота є завершеною науковою працею, яка націлена на вирішення актуальної наукової задачі, відповідає спеціальності 122 "Комп'ютерні науки", а її автор Положенцев Артем Анатолійович заслуговує присудження ступеня доктора філософії, на підставі Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, який затверджено Постановою Кабінету Міністрів України № 44 від 12 січня 2022 року.

Науковий керівник запропонував затвердити позитивний висновок про наукову новизну, теоретичне та практичне значення результатів зазначеної дисертації та рекомендувати до захисту на здобуття ступеня доктора філософії з галузі знань 12 "Інформаційні технології", за спеціальністю 122 "Комп'ютерні науки".

Обговорення дисертаційного дослідження.

Нечипорук О.П., д.т.н., професор, професор кафедри комп'ютеризованих систем управління НАУ.

Звернула увагу, що необхідно додати схему, яка б описала процес управління. Також варто краще висвітлити вхідні та вихідні дані розроблених програмних застосунків. Крім цього, звернути увагу на поняття ефективності та доречності його застосування. Зазначила, що доповідь дисертанта та власне дослідження свідчать про його високий рівень як науковця. Підтримала дисертаційне дослідження з урахуванням виправлення озвучених зауважень і пропозицій.

Гнатюк С.О., д.т.н., професор, професор кафедри КІТ.

Зазначив, що необхідно додати схему, яка б описала процес управління інцидентами і отримати акти впровадження результатів. Також Гнатюк С.О. Підтримав роботу і побажав виходити на захист дисертації.

Павленко П.М., д.т.н., професор, професор кафедри організації авіаційних перевезень НАУ.

Наголосив на актуальності дисертаційного дослідження, зазначив, що робота має цікаві ідеї, які підходи, а розроблені методи вирішують потрібні завдання. Зауважив, що дисертанту варто розібратись з поняттями ефективності та управління та їх застосування у роботі. Підтримав роботу і побажав виходити на захист дисертації.

Одарченко Р.С. д.т.н., професор, в.о. декана факультету аеронавігації, електроніки та телекомунікацій НАУ.

Робота є актуальною, комплексною, структурованою, містить цікаві, доречні пропозиції. З урахуванням виправлення озвучених зауважень і пропозицій, підтримую роботу і бажаю успіхів дисертанту.

Савченко А.І., д.т.н, професор, завідувач кафедри.

Зазначила, що дисертаційна робота дійсно є актуальною та необхідною.

Зауважила, що необхідно доопрацювати схеми, рисунки та формули, які були висвітлені у презентації. Підтримала дисертаційне дослідження з урахуванням виправлення озвучених зауважень і пропозицій.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації на тему: “Методи та засоби управління ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури”, поданої на здобуття ступеня доктора філософії з галузі знань 12 “Інформаційні технології” за спеціальністю 122 “Комп’ютерні науки”

Актуальність теми дослідження та її зв’язок із планами науково-дослідних робіт.

В умовах швидкого розвитку інформаційних технологій та цифрової трансформації всіх сфер суспільного життя, захист ІТ-систем стає однією з ключових складових національної безпеки будь-якої держави. Питання захисту критичної інфраструктури (КІ) є важливими, оскільки від надійності цих систем залежить стабільне функціонування економіки, громадського порядку, охорони здоров'я та інших життєво важливих секторів.

КІ держави включає енергетичні, транспортні, фінансові, промислові, цифрові системи та інші важливі сектори, які, у разі порушення їх роботи, можуть призвести до серйозних наслідків для суспільства та держави в цілому. Зростаюча кількість та складність ІТ-загроз вимагає розробки нових підходів до оцінювання стану захищеності та управління ІТ-інцидентами для забезпечення надійного функціонування критичної інформаційної інфраструктури (КІІ).

КІІ держави є особливо вразливою до ІТ-інцидентів та загроз. Відсутність належного захисту КІІ може призвести до зупинки критичних функцій держави, що, в свою чергу, може мати катастрофічні наслідки для економіки та безпеки країни.

Важливість дослідження зумовлена необхідністю створення ефективних методів для управління та пріоритизації ІТ-загроз, що дозволить оптимально

розподіляти ресурси для їх нейтралізації. Сучасні методи оцінювання стану ІТ-систем повинні враховувати не лише технічні аспекти, але й рівень цифрової трансформації, а також бути адаптованими до постійно змінюваного ландшафту загроз.

Питаннями захисту КІІ держави, зокрема від ІТ-інцидентів, займаються такі вітчизняні та закордонні вчені: К. Маклафлін, Р. Хан, Д. Лаверті, С. Сезер, А.Б. Качинський, В.С. Харченко, В.В. Мохор, Ю.І. Хлапонін, О.Ю. Юдін, С.Ф. Гончар, П.М. Складанний, та ін.

Теоретична база дослідження питань оцінювання стану ІТ-систем та управління ІТ-загрозами є достатньо розвиненою, однак розробки щодо їх практичної реалізації в сучасних умовах майже відсутні. Більшість досліджень фокусуються на питаннях кібербезпеки, тоді як дослідження ІТ-інцидентів має свої особливості та відрізняється від загальних питань інформаційної безпеки.

Дослідження ІТ-інцидентів є важливим, оскільки вони безпосередньо впливають на працездатність та стабільність інформаційних систем. ІТ-інциденти можуть включати як зовнішні атаки, так і внутрішні помилки, збоїв в програмному забезпеченні та інші непередбачувані події, які можуть призвести до втрати даних, зупинки сервісів та інших негативних наслідків. Важливо швидко ідентифікувати та оцінювати ці інциденти для мінімізації їхнього впливу та забезпечення безперервності роботи систем.

Ця тематика відрізняється від загальних питань інформаційної безпеки тим, що вона охоплює не лише захист від зовнішніх загроз, але й управління внутрішніми ризиками та відновлення після інцидентів. В той час як інформаційної безпеки здебільшого фокусується на превентивних заходах, дослідження ІТ-інцидентів включає також реактивні та відновлювальні процеси, що є критично важливими для збереження функціональності інформаційних систем у випадку інциденту.

Таким чином, питання захисту КІ та КІІ є надзвичайно актуальними в сучасному світі, де інформаційні системи стають все більш інтегрованими та залежними від технологій, що створює нові виклики та ризики, які необхідно враховувати та активно управляти.

З огляду на зазначене, розроблення методів управління ІТ-інцидентами на ОКІ є актуальною науково-технічною задачею, що має теоретичне і практичне значення.

Тема дисертації відповідає освітньо-науковій програмі “Комп’ютерні науки” за спеціальністю 122 “Комп’ютерні науки” галузі знань 12 “Інформаційні технології” в Національному авіаційному університеті.

Формулювання наукового завдання, вирішення якого отримано в дисертації.

Метою дисертаційної роботи є удосконалення системи управління ІТ-інцидентами на об’єктах критичної інформаційної інфраструктури в умовах реалізації загроз та обмежених ресурсів захисту.

Для цього сформульовано комплекс наступних науково-технічних задач:

1. Провести аналіз сучасних підходів до управління ІТ-інцидентами на об’єктах критичної інфраструктури держави;
2. Удосконалити метод оцінювання рівня захищеності та розробити відповідні рекомендації щодо оптимізації захисту об’єктів критичної інформаційної

інфраструктури для визначення стану їх захищеності та управління захистом від ІТ-інцидентів.

3. Удосконалити метод визначення пріоритетів ІТ-інцидентів для кількісного визначення пріоритетів та управління ними.

4. Розробити метод оцінювання ІТ-загроз, для ідентифікації, оцінки та пріоритизації ІТ-загроз для оптимального розподілу ресурсів захисту критичної інформаційної інфраструктури.

5. Провести верифікацію розроблених методів з використанням розробленого програмного забезпечення з метою підтвердження їх ефективності та придатності для практичного застосування.

Об'єкт дослідження – процеси управління ІТ-інцидентами на об’єктах критичної інформаційної інфраструктури.

Предмет дослідження – методи та засоби управління інцидентами на об'єктах критичної інформаційної інфраструктури в умовах реалізації загроз та обмежених ресурсів захисту.

У дисертаційній роботі вирішено науково-прикладну задачу щодо розроблення нових та удосконалення існуючих методів управління ІТ-інцидентами на ОКІ.

Наукові положення, розроблені особисто здобувачем, та їх новизна полягають у тому, що:

вперше

- розроблено метод управління ІТ-загрозами, який за рахунок синтезу методів багатокритеріального прийняття рішень, моделювання загроз та функції перспективної цінності, дає змогу ідентифікувати, оцінювати та пріоритизувати ІТ-загрози для оптимального розподілу ресурсів захисту критичної інфраструктури держави.

удосконалено

- метод визначення пріоритетів ІТ-інцидентів, який за рахунок представлення ієрархічних структур елементів потенційних загроз та розрахунку ймовірності їх реалізації, дозволяє кількісно оцінити пріоритети ІТ-інцидентів та управляти ними для забезпечення необхідного рівня захисту життєво важливих інтересів громадян, суспільства, держави та правопорядку;

отримав подальшого розвитку

- метод оцінювання рівня захищеності, який за рахунок використання нових індикаторів ІТ-безпеки та рівня цифрової трансформації, а також розроблених рекомендацій для оптимізації захисту дає змогу визначити стан захищеності об’єктів критичної інфраструктури (сектору/підсектору чи держави в цілому), а також управляти захистом зазначених об’єктів в умовах виникнення ІТ-інцидентів;

Обґрунтованість і достовірність наукових положень, висновків, рекомендацій, які захищаються.

Наукові положення, висновки й рекомендації, сформульовані в дисертації, відповідають вимогам до такого виду досліджень. Високий рівень обґрунтованості наукових положень, висновків, рекомендацій сформульованих у дисертації, їхня достовірність забезпечені:

– професійним вирішенням автором низки наукових завдань, що сприяло реалізації поставленої мсти дослідження, та адекватністю структурно-логічної схеми дослідження визначеній меті: кожен наступний розділ чи підрозділ органічно пов’язаний із попереднім і доповнює його;

– використанням широкої бази наукових джерел за темою дисертації й достатнім масивом аналітичних даних.

Наукове значення роботи полягає у вирішенні актуальної наукової задачі щодо управління ІТ-інцидентами на ОКІІ.

Практичне значення та використання результатів дисертаційного дослідження полягає у тому, що отримані результати можуть бути використані відповідними органами для ефективного оцінювання стану захищеності сектуру/підсектору КІІ, або управління ІТ-загрозами, крім цього було:

- реалізовано програмний застосунок, який автоматизує процес оцінки стану захищеності об’єктів критичної інформаційної інфраструктури, для забезпечення структурованого підходу до збору даних, проведення оцінювання рівня захищеності та надає конкретні рекомендації для покращення безпеки критичної інформаційної інфраструктури.
- реалізовано методику, яку можна використовувати для визначення пріоритетів ІТ-інцидентів, що дозволяє ефективно ідентифікувати та пріоритизувати інциденти на ОКІІ та оптимізувати розподіл ресурсів, забезпечуючи надійність та стійкість критичних інформаційних систем.
- реалізовано програмний застосунок для управління ІТ-загрозами критичної інформаційної інфраструктури, який шляхом синтезу багатокритеріального методу прийняття рішень TODIM та моделлю загроз STRIDE, дозволяє ефективно ідентифікувати, оцінювати та пріоритизувати загрози, враховуючи їхню ймовірність, потенційний збиток та складність реалізації.
- теоретичні результати дисертації та результати експериментальних досліджень впроваджені і використовуються у науково-дослідній діяльності НДЛ протидії кіберзагрозам авіаційної галузі НАУ (акт впровадження від 11.12.2023), а також у ДержНДІ технологій кібербезпеки та захисту інформації для підвищення ефективності підготовки фахівців з ІТ та забезпечення захисту ОКІ (акт впровадження від 14.06.2024).

Повнота викладення матеріалів дисертації в публікаціях та особистий внесок у них автора. Дисертація “Методи та засоби управління ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури” Положенцева Артема Анатолійовича є самостійною науковою працею, в якій наведено теоретичні і практичні положення, висновки, власні ідеї та розробки автора, які дають змогу вирішити поставлені завдання. Усі висновки та практичні рекомендації, винесені на захист, розроблені дисертантом особисто.

Найважливіші ідеї, висновки, рекомендації, отримані в дисертації, оприлюднені на наукових та науково-практичних конференціях, у тому числі міжнародних, всеукраїнських та за міжнародною участю: «12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems:Technology and Applications» (м. Дортмунд, 2023), «1st International Workshop on Social Communication and Information Activity in Digital Humanities» (м.

Львів, 2022), «VIII International conference “Information Technology and Implementation» (м. Київ, 2021), «The 3rd International Workshop on Intelligent Information Technologies & Systems of Information Security» (м. Хмельницький, 2022), «Перспективні напрямки захисту інформації», (м. Одеса, 2021).

Основні наукові результати дисертаційної роботи опубліковано у 26 наукових публікаціях, із них: 0.5 розділу у колективній монографії, 3 наукові статті надруковані у вітчизняних фахових наукових виданнях, 15 публікацій включені до міжнародної наукометричної бази Scopus, а також 7.5 тез доповідей на науково-практичних конференціях.

Праці, в яких опубліковані основні наукові результати дисертації:

Розділ у колективній монографії:

1. Polozhentsev A., Fesenko A., Gnatyuk V, (2017) Method for CSIRT performance evaluation, *Project interdyscyplinarny projektem XXI wieku, Tom 2* (263-269).

Особистий внесок автора: проведено оцінку ефективності роботи команди реагування на інциденти комп'ютерної безпеки.

Особистий внесок Фесенка А.О.: визначено ключові показники ефективності, побудована панель індикаторів.

Особистий внесок Гнатюка В.О.: розроблено метод оцінки ефективності роботи команди реагування на інциденти комп'ютерної безпеки.

Статті у наукових фахових виданнях:

1. Положенцев А. А., Сидоренко В. М. Метод управління ІТ-загрозами на об’єктах критичної інформаційної інфраструктури. *Наукоємні технології*. 2024. Т. 2, № 62. С. 121–133.

Особистий внесок автора: розроблено метод управління ІТ-загрозами для ОКІІ.

Особистий внесок Сидоренко В.М.: проведено експериментальне дослідження методу управління ІТ-загрозами.

2. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів ІТ-інцидентів на об’єктах критичної інформаційної інфраструктури держави. *Проблеми інформатизації та управління*. 2024. Т. 2. №78. С. 68-80.

Особистий внесок автора: розроблено етапи методу визначення пріоритетів ІТ-інцидентів.

Особистий внесок Сидоренко В.М.: проведено експериментальне дослідження методу визначення пріоритетів ІТ-інцидентів.

Особистий внесок Сидоренко С.Ю.: проведено верифікацію розробленого методу.

Особистий внесок Скуратівського А.А.: проведено аналіз підходів до визначення пріоритетів ІТ-інцидентів;

3. Сидоренко В.М., Положенцев А.А., Гнатюк С.О. Метод оцінювання рівня кібербезпеки галузі критичної інформаційної інфраструктури держави. *Вісник інженерної академії України*. 2017. № 42. С. 81–89.

Особистий внесок автора: проведено аналіз підходів оцінювання рівня

кібербезпеки об'єктів критичної інфраструктури держави.

Особистий внесок Сидоренко В.М.: розроблено етапи методу оцінювання рівня кібербезпеки галузі критичної інформаційної інфраструктури.

Особистий внесок Гнатюка С.О.: досліджено питання кібербезпеки галузі критичної інформаційної інфраструктури держави.

4. Гнатюк С.О., Бердибаєв Р.Ш., Богун А.М., Сидоренко В.М., Положенцев А.А., Жигаревич О.К. Інтеграційна шина даних для ефективного функціонування системи управління подіями інформаційної безпеки. *Проблеми інформатизації та управління*. 2023. Т. 3. № 75. С. 29-40.

Особистий внесок автора: проаналізовано найпопулярніші сучасні рішення для побудови інтеграційної шини даних.

Особистий внесок Гнатюка С.О.: визначено основні концепцій і підходи до побудови інтеграційної шини даних.

Особистий внесок Бердибаєва Р.Ш.: проведено огляду літератури та аналіз існуючих рішень в області інтеграційних шин даних.

Особистий внесок Богуна А.М.: проведено оптимізацію алгоритмів, тестування на відповідність.

Особистий внесок Сидоренко В.М.: здійснено експериментальне дослідження та тестування запропонованої моделі.

Особистий внесок Жигаревич О.К.: розроблено основні етапи реалізації моделі інтеграційної шини даних.

5. Жигаревич О.К., Бердибаєв Р.Ш., Сидоренко В.М., Положенцев А.А., Кримська А.О. Модель онтоголіко-реляційного сховища даних для функціонування хмарної SIEM-системи. *Проблеми інформатизації та управління*. 2023. Т. 4. № 76. С. 17-27.

Особистий внесок автора: проведено аналіз використання хмарних SIEM-систем.

Особистий внесок Жигаревич О.К.: розроблено основні етапи реалізації моделі онтоголіко-реляційного сховища даних.

Особистий внесок Бердибаєва Р.Ш.: розробка методології дослідження, побудова математичних моделей та алгоритмів.

Особистий внесок Сидоренко В.М.: здійснено експериментальне дослідження та тестування запропонованої моделі.

Особистий внесок Кримської А.О.: проведено аналіз результатів дослідження, підготовка візуалізацій та графічних матеріалів.

Статті у виданнях, які включено до міжнародних наукометричних баз:

1. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., Fesenko, A., Akatayev, N., Zhilkishbayeva, G. Method of cybersecurity level determining for the critical information infrastructure of the state. *CEUR Workshop Proceedings*. 2020. Vol. 2616. P. 332-341. URL: https://ceur-ws.org/Vol-2616/paper28.pdf

Особистий внесок автора: представлено метод визначення рівня кібербезпеки об'єктів критичної інформаційної інфраструктури держави.

2. Gnatyuk, S., Sydorenko, V., Polozhentsev, A., Sotnichenko, Y. Experimental Cybersecurity Level Determination in the Civil Aviation Critical

Infrastructure. *IEEE International Conference on Problems of Infocommunications Science and Technology*. 2021. P. 757-764. DOI: https://doi.org/10.1109/PICST51311.2020.9467987.

Особистий внесок автора: визначено переваги та недоліки відомих підходів визначення рівня кібербпезки галузі цивільної авіації.

3. Gnatyuk, S., Yudin, O., Sydorenko, V., Smirnova, T., Polozhentsev, A. The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems. *CEUR Workshop Proceedings*, 2022. Vol. 3156. P. 390-399. URL: https://ceur-ws.org/Vol-3156/paper29.pdf

Особистий внесок автора: проведено аналіз існуючих методів та моделей оцінки рівня критичності ІТС.

4. Polozhentsev, A., Gnatyuk, S., Berdibayev, R., Sydorenko, V., Zhyharevych, O. Novel Cyber Incident Management System for 5G-based Critical Infrastructures. *IDAACS*. 2023, P. 1037-1041. DOI: https://doi.org/10.1109/IDAACS58523.2023.10348645.

Особистий внесок автора: досліджено універсальну систему кореляції подій та управління інцидентами кібербезпеки для мереж 5G.

5. Lutskyi, M., Sydorenko, V., Polozhentsev, A., Apenko, N., Sydorenko, S. Model for Assessing the Effectiveness of Information Security Systems of Interdependent Critical Infrastructures. *CEUR Workshop Proceedings*. 2023. Vol. 3421. P. 214-222. URL: https://ceur-ws.org/Vol-3421/short7.pdf

Особистий внесок автора: досліджено основні підходи до оцінки ефективності систем захисту інформації.

6. Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., Brzhanov, R. Method of Forming the Functional Security Profile for the Sectoral Information and Telecommunication Systems. *CEUR Workshop Proceedings*. 2021. Vol. 3179. P. 272-283. URL: https://ceur-ws.org/Vol-3179/Paper_25.pdf

Особистий внесок автора: проведено аналіз існуючих методів визначення функціонального профілю безпеки підсистеми галузевої ІТС.

7. Yarotskiy, S., Sydorenko, V., Lelechenko, A., Kolisnyk, O., Polozhentsev, A. Method of Determining the Importance Factor of IT Security Projects Investment Attractiveness in Critical Infrastructures. *CEUR Workshop Proceedings*. 2023. Vol. 3550. P. 181-190. URL: https://ceur-ws.org/Vol-3550/paper15.pdf

Особистий внесок автора: обґрунтовано, що оцінка ступеня інвестиційної привабливості об'єкта експертизи отримується за допомогою мультиплікативної функції агрегування, яка враховує нормовані коефіцієнти важливості.

8. Gnatyuk, S., Sydorenko, V., Yudin, O., Zhyharevych, O., Polozhentsev, A. Method for Calculating the Criticality Level of Sectoral Information and Telecommunication Systems. *CEUR Workshop Proceedings*. 2022. Vol. 3347. P. 234-245. URL: https://ceur-ws.org/Vol-3347/Paper_20.pdf

Особистий внесок автора: проаналізовано перелік переваг та недоліків підходів до розрахунку рівня критичності галузевих ІТС.

9. Gnatyuk, S., Sydorenko, V., Polozhentsev, A. Method for Cybersecurity Level Evaluation in the Civil Aviation Critical Infrastructure. *Lecture Notes in Networks and Systems*. 2023. Vol. 736. P. 206-218, DOI: https://doi.org/10.1007/978-3-031-38082-2_16.

Особистий внесок автора: представлено метод визначення рівня кібербезпеки ОКІІ.

10. Sydorenko, V., Zhyharevych, O., Berdybaev, R., Polozhentsev, A., Fesenko, A. Ontological-Relational Data Store Model for a Cloud-based SIEM System Development. *CEUR Workshop Proceedings*. 2024. Vol. 3654. P. 343-354. URL: https://ceur-ws.org/Vol-3654/paper29.pdf

Особистий внесок автора: проведено аналіз сучасних типів баз даних, для обґрунтування вибору найбільш ефективних підходів.

11. Gnatyuk, S., Satybaldiyeva, F., Sydorenko, V., Zhyharevych, O., Polozhentsev, A. Model of Information Technology for Efficient Data Processing in Cloud-based Malware Detection Systems of Critical Information Infrastructure. *CEUR Workshop Proceedings*. 2023. Vol. 3421. P. 206-213. URL: https://ceur-ws.org/Vol-3421/short6.pdf

Особистий внесок автора: проведено дослідження імовірнісних та часових характеристик алгоритмів і програм генерації та обробки метаданих у хмарній системі виявлення шкідливого програмного забезпечення.

12. Lutskyi, M., Gnatyuk, S., Sydorenko, V., Yarotskiy, S., Polozhentsev, A. Study on the Evaluating the Degree of Investment Attractiveness of IT-Projects. *DESSERT*. 2023. P 1-7. DOI: https://doi.org/10.1109/DESSERT61349.2023.10416440

Особистий внесок автора: проведено аналіз групових систем переваг експертів за комплексом характерних особливостей інвестиційної привабливості оцінювання IT-проектів.

13. Semenchenko, A., Gurkovskyi, V., Romanenko, Y., Sydorenko, V., Kudrenko, S., Polozhentsev, A. Ukraine on the Road to the European Digital Market: Status and Tools for Implementing the European Digital Economy and Society Index in Ukraine. *CEUR Workshop Proceedings*. 2022. Vol. 3296. P. 18-28. URL: https://ceur-ws.org/Vol-3296/paper2.pdf

Особистий внесок автора: обґрунтовано актуальність та необхідність впровадження індексу цифрової економіки та суспільства в Україні.

14. Lutskyi, M., Gnatyuk, S., Verkhovets, O., Polozhentsev, A. Information Flows Formalization for BSD Family Operating Systems Security Against Unauthorized Investigation. Lect*ure Notes on Data Engineering and Communications Technologies*. 2023. Vol. 178. P. 235-246. DOI: https://doi.org/10.1007/978-3-031-35467-0_16.

Особистий внесок автора: проведено моделювання інформаційних потоків в операційних системах, що дозволяє більш ефективно виявляти загрози інформаційній безпеці.

15. Gnatyuk, S., Berdibayev, R., Sydorenko, V., Polozhentsev, A., Ryabyy, M. Enterprise Service Bus Construction in SOA Architecture for SIEM Implementation in Critical Information Infrastructure. *CEUR Workshop Proceedings*. 2022. Vol. 3288. P. 11-20. URL: https://ceur-ws.org/Vol-3288/paper2.pdf

Особистий внесок автора: проаналізовано найпопулярніші сучасні рішення для побудови корпоративних сервісних шин.

Наукові праці, які додатково відображають наукові результати дисертації:

1. Сидоренко В.М., Положенцев А.А., Юдін О.К., Жигаревич О.К. Функціональна модель визначення критичності галузевих інформаційно-телекомунікаційних систем. *АВІА-2023* : матеріали XVI міжнар. наук.-техніч. конф., м. Київ, 18-20 квітня 2023 р. м. Київ, 2023. С. 16.14-16.17.

Особистий внесок автора: розглянуто питання критичних галузевих інформаційно-телекомунікаційних систем.

Особистий внесок Сидоренко В.М.: проведено аналіз існуючих моделей та методик визначення критичності.

Особистий внесок Юдін О.Ю.: розробка концептуальної моделі для визначення критичності інформаційно-телекомунікаційних систем.

Особистий внесок Жигаревич О.К.: розробка математичних моделей та алгоритмів.

2. Жигаревич О.К., Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю. Модель онтологіко-реляційного сховища даних для функціонування хмарної SIEM-системи. *Кіберзахист особи, суспільства і держави* : матеріали наук.-практ. конф., с. Велятино, 24-27 січня 2024 р. м. Київ. 2024. С. 14-15.

Особистий внесок автора: проведено аналіз використання хмарних SIEM-систем.

Особистий внесок Жигаревич О.К.: розробка концептуальної моделі онтологіко-реляційного сховища даних.

Особистий внесок Сидоренко В.М.: експериментальне дослідження запропонованої моделі онтологіко-реляційного сховища даних.

Особистий внесок Сидоренко С.Ю.: проведення аналізу існуючих моделей сховищ даних, участь у розробці методології дослідження.

3. Положенцев А.А., Сидоренко В.М. Метод визначення рівня кібербезпеки об’єктів критичної інфраструктури держави. *ПОЛІТ-2018. Сучасні проблеми науки* : матеріали XVIII міжнар. наук.-практ. конф. молодих учених і студентів, м. Київ, 4-6 квітня 2018 р. м. Київ, 2018. С. 102-103.

Особистий внесок автора: представлено метод визначення рівня кібербезпеки.

Особистий внесок Сидоренко В.: розробка методологічних підходів до оцінки кібербезпеки галузі критичної інфраструктури.

4. Гнатюк С.О., Сидоренко В.М., Положенцев А.А. Визначення показників рівня кібербезпеки об’єктів критичної інфраструктури авіаційної галузі. *Перспективні напрямки захисту інформації* : матеріали VII Всеукр. наук.-практ. конф., м. Одеса, 30 серпня-03 вересня 2021 р. м. Одеса. 2021. С. 150-153.

Особистий внесок автора: проведено аналіз підходів визначення рівня кібербезпеки.

Особистий внесок Гнатюк С.О.: визначення основних показників рівня кібербезпеки для об’єктів критичної інфраструктури авіаційної галузі.

Особистий внесок Сидоренко В.М.: розробка методологічних підходів до оцінки кібербезпеки.

5. Алімсеітова Ж., Положенцев А.А. Аналіз підходів до визначення терміну критична інфраструктура у різних країнах світу. *ITSEC* : матеріали VI Міжн. наук.-практ. конф., м. Київ, 17-19 травня 2016. м. Київ, 2016. С. 62.

Особистий внесок автора: проведено аналіз підходів до визначення терміну «критична інфраструктура».

Особистий внесок Алімсеітова Ж.: проведення огляду літератури та аналізу існуючих підходів до визначення терміну «критична інфраструктура».

6. Положенцев А.А. Методи ведення кібервійни як потенційна загроза критичним авіаційним інформаційним системам. *Проблеми та перспективи розвитку авіації та космонавтики* : матеріали IV Всеукр. наук.-практ. конф. молодих учених і студентів з міжнародною участю. м. Київ, 28-29 жовтня 2015. м. Київ, 2015. С. 106.

Особистий внесок автора: висвітлено питання кібервійни як загрози критичним авіаційним інформаційним системам.

7. Положенцев А.А. Поняття кібервійни та їх прояв у сучасному світі. *Перспективні напрями захисту інформації* : матеріали наук.-практ. конф., м. Одеса, 7-8 вересня 2015р., м. Одеса, 2015. С. 79-80.

Особистий внесок автора: висвітлено поняття кібервійни та її прояв у сучасному світі.

8. Положенцев А.А. Інформаційна війна. *Політ. Сучасні проблеми науки* : матеріали XV Міжн. наук.-практ. конф. молодих учених і студентів., м.Київ, 8-9 квітня 2015р. м. Київ, 2015. С. 139.

Особистий внесок автора: проведено аналіз підходів до визначення поняття інформаційної війни.

9. Гнатюк В.О., Положенцев А.А. Метод оцінки ефективності роботи груп реагування на кіберінциденти. *Перспективні напрями захисту інформації :* матеріали II Всеукр. наук.-пр. конф., м. Одеса, 03-07 вересня 2016р. м. Одеса, 2016. С. 56-58.

Особистий внесок автора: проведено аналіз підходів реагування на кіберінциденти.

Особистий внесок Гнатюк В.О. представлено Метод оцінки ефективності роботи груп реагування на кіберінциденти.

Структура та обсяг дисертації. Дисертація складається із анотації, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел до кожного розділу. Загальний обсяг дисертації складає 180 сторінок тексту, із них 151 сторінок основного тексту. Робота включає 30 рисунків, 38 таблиць, 3 додатків. Список використаних джерел налічує 125 найменувань.

Оцінка мови та стилю дисертації. Текст дисертації викладено грамотною мовою, логічно та послідовно. Матеріали дослідження викладені з дотриманням вимог наукового стилю. Дисертація оформлена згідно з вимогами Міністерства освіти і науки України.

Характеристика особистості здобувача. Під час підготовки дисертаційної роботи здобувач проявив себе як висококваліфікований та творчий дослідник, здатний самостійно вирішувати наукові та практичні завдання. Він володіє сучасними методами аналізу та має глибокі знання у своїй галузі дослідження. Здобувач відповідальний, дисциплінований, активно бере участь у наукових заходах і демонструє високий рівень аналітичного мислення та комунікативних навичок.

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Положенцева Артема Анатолійовича на тему "Методи та засоби управління ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури".

2. Вважати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Положенцева Артема Анатолійовича відповідає спеціальності 122 "Комп'ютерні науки" та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року. № 261 (зі змінами і доповненнями від 03 квітня 2019 року № 283), вимогам пп. 6, 7, 8, 9 "Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії", затвердженому постановою Кабінету Міністрів України від 12 січня 2022 року № 44.

3. Рекомендувати дисертаційну роботу "Методи та засоби управління ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури", подану Положенцевим Артемом Анатолійовичем на здобуття ступеня доктора філософії з галузі знань 12 "Інформаційні технології", за спеціальністю 122 "Комп'ютерні науки" до захисту у разовій спеціалізованій вченій раді.

4. Рекомендувати Вченій раді НАУ клопотати про призначення:

Головою разової спеціалізованої вченої ради:

Одарченка Романа Сергійовича, д.т.н., професора, в.о. декана Факультету аеронавігації, електроніки та телекомунікацій НАУ.

Рецензентами:

Савченко Аліну Станіславівну, д.т.н., професора, завідувача кафедри комп'ютерних інформаційних технологій НАУ;

Охріменко Тетяну Олександрівну, к.т.н., ст. дослідника, п.н.с. НДЛ протидії кіберзагрозам в авіаційній галузі.

Офіційними опонентами:

Смірнова Олексія Анатолійовича, д.т.н., професора, завідувача кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету України;

Мартинюк Ганну Вадимівну, к.т.н., доцент, в.о. завідувача кафедри системного аналізу та інформаційних технологій Маріупольського державного університету.

Головуючий на засіданні:
доктор технічних наук, професор,
завідувач кафедри комп'ютерних
інформаційних технологій НАУ Аліна САВЧЕНКО

Секретар засідання:
кандидат технічних наук, ст. дослідник,
п.н.с. НДЛ протидії кіберзагрозам
в авіаційній галузі НАУ Тетяна ОХРІМЕНКО

ПОГОДЖЕНО:
доктор технічних наук, професор,
в.о проректора з наукової роботи НАУ Сергій ГНАТЮК