ЗАТВЕРДЖУЮ
президент Державного університету
«Київський авіаційний інститут»

Ксенія СЕМЕНОВА

«2» квітня 2026 року

ВИСНОВОК

Державного університету «Київський авіаційний інститут» (далі – КАІ) про наукову новизну, теоретичне та практичне значення результатів дисертації Скуратівського Анатолія Анатолійовича на тему «Методи та інструментальні засоби управління вимогами кібербезпеки при впровадженні програмного забезпечення в бізнесі», поданої на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки»

Витяг
із протоколу № 2 розширеного засідання
кафедри комп'ютерних інформаційних технологій КАІ
від «2» квітня 2026 року

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

Савченко Аліна Станіславівна, д.т.н, проф., завідувач кафедри;
Віноградов Микола Анатолійович, д.т.н.,проф., професор кафедри;
Воронін Альбер Миколайович, д.т.н., проф., професор кафедри;
Гнатюк Сергій Олександрович, д.т.н., проф., професор кафедри;
Райчев Ігор Едуардович, к.т.н., доц., доцент кафедри;
Климова Асія Сабирівна, к.т.н., доц., доцент кафедри;
Чуба Ірина Вікторівна, к.т.н., доц., доцент кафедри;
Колісник Олена Василівна, к.т.н., доц., доцент кафедри;
Зудов Олег Миколайович, к.т.н., доцент кафедри;
Прокопенко Костянтин Ігорович, к.т.н., доц., доцент кафедри;
Толстікова Олена Володимирівна, к.т.н., доц., доцент кафедри;
Сидоренко Вікторія Миколаївна, к.т.н., доц., доцент кафедри;
Положенцев Артем Анатолійович, PhD, доцент кафедри.

Присутні на засіданні науково-педагогічні працівники КАІ:

Нечипорук Олена Петрівна, д.т.н., проф., завідувач кафедри інтелектуальних кібернетичних систем;

Ахрамович Володимир Миколайович, д.т.н., проф., професор кафедри кібербезпеки;

Лукашенко Вікторія Вікторівна, д.т.н., проф., професор кафедри комп'ютерних систем та мереж;

Ільєнко Анна Вадимівна, к.т.н., доц., завідувач кафедри кібербезпеки;

Охріменко Тетяна Олександрівна, к.т.н., ст. дослідник, заступник декана Факультету комп'ютерних наук та технологій;

Фесенко Андрій Олексійович, к.т.н., доцент, декан Факультету комп'ютерних наук та технологій.

Порядок денний:

Обговорення дисертаційного дослідження аспірантка кафедри комп'ютерних інформаційних технологій КАІ Скуратівського Анатолія Анатолійовича на тему «Методи та інструментальні засоби управління вимогами кібербезпеки при впровадженні програмного забезпечення в бізнесі», поданої на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології», за спеціальністю 122 «Комп'ютерні науки».

Дисертація виконувалася на кафедрі комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій КАІ. Тема дисертації затверджена на засіданні Вченої ради Факультету комп'ютерних наук та технологій (протокол № 9 від 28 листопада 2022 року).

Науковий керівник – д.т.н., професор, професор кафедри комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій КАІ Гнатюк Сергій Олександрович.

Виступили:

Здобувач Скуратівський Анатолій Анатолійович представив результати свого дослідження, обґрунтувавши актуальність обраної теми, мету, завдання, методи дослідження, охарактеризувавши об'єкт та предмет дисертаційного дослідження, виклала основні наукові положення та висновки, що виносяться на захист, вказала науково-практичну значимість роботи, зазначила про впровадження результатів дослідження.

Дисертаційна робота присвячена підвищенню ефективності процесу впровадження ПЗ в бізнесі шляхом розроблення методів та інструментальних засобів управління вимогами кібербезпеки, які забезпечують їх формалізовану інтеграцію, трасованість, адаптацію до змін середовища загроз і ресурсних обмежень, а також узгодженість з функціональними та нефункціональними вимогами інформаційних систем.

Аналіз сучасних наукових підходів до управління вимогами кібербезпеки показав, що сучасні підходи до управління вимогами кібербезпеки зосереджуються на необхідності вдосконалення нормативно-правової бази, впровадження галузево специфічних фреймворків, інтеграції управління кіберризиками та стандартизації процесів безпеки.

Основний недолік відомих підходів імплементації вимог в життєвий цикл розроблення ПЗ – це відсутність формалізованої, динамічної та трасованої інтеграції вимог кібербезпеки у всі етапи життєвого циклу розроблення ПЗ, що призводить до фрагментарного врахування загроз, запізнілого впровадження контролів та підвищення рівня ризику.

Математичну модель управління вимогами кібербезпеки при впровадженні ПЗ дозволяє визначити пріоритети серед вимог кібербезпеки, врахувати невизначеності та ймовірність ризиків, а також оптимально розподілити

ресурси між вимогами з урахуванням обмежень бюджету та мінімізації ризиків, забезпечуючи комплексне управління вимогами кібербезпеки під час впровадження ПЗ з урахуванням міжнародних стандартів і сучасних методів оцінки ризиків. На основі розробленої моделі управління вимогами кібербезпеки при впровадженні ПЗ було проведено практичні симуляції з використанням фреймворків міжнародних стандартів і рекомендованих практик (NIST 800-53, ISO 22316, MITRE ATT&CK).

Метод динамічного управління вимогами кібербезпеки дає змогу регулярно оновлювати пріоритети, врахувати нові вимоги кібербезпеки при впровадженні ПЗ, а також забезпечити адаптацію системи до зміни ресурсних або нормативних умов. Формалізовано адаптивний механізм управління вимогами кібербезпеки, який забезпечує обґрунтований вибір пріоритетів, оптимальний розподіл ресурсів та підвищення системної стійкості ІКС, у вигляді псевдокоду, що може бути реалізований у системах підтримки прийняття рішень; програмних засобах управління кіберризиками; корпоративних GRC-платформах; автоматизованих системах планування тощо.

Уніфікована модель SDLC дозволяє представити відомі моделі життєвого циклу розроблення ПЗ у зручній формі для інтегрування й імплементування вимог. На основі цієї моделі було формалізовано відомі моделі життєвого циклу розроблення ПЗ, зокрема класичну каскадну модель, V-модель, інкрементальну модель, спіральну модель, Agile, DevOps та DevSecOps, що може бути використано при проєктуванні захищених ІКС; аудиті процесів безпечної розробки ПЗ згідно стандартів ISO/IEC, NIST, PCI DSS, PSD2, GDPR, MITRE ATT&CK; створенні політик secure SDLC; впровадженні DevSecOps у державних та корпоративних ІТ-системах тощо.

Метод інтегрування вимог кібербезпеки в SDLC на базі уніфікованої моделі дозволяє інтегрувати вимоги кібербезпеки в конкретну фазу (pipeline) життєвого циклу розроблення ПЗ, а також дає можливість формалізованої оптимізації вибору контролів кібербезпеки залежно від контексту системи та ресурсних обмежень.

Результати дисертаційної роботи впроваджені у навчальний процес кафедри комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій Державного університету «Київський авіаційний інститут» і діяльність Наукової асоціації кібербезпеки України.

Після закінчення презентації Скуратівського А.А. присутніми на захисті фахівцями були поставлені наступні запитання:

Запитання до здобувача:

1. **Ахрамович В.М.,** д.т.н., проф., професор кафедри кібербезпеки КАІ.

Запитання: На вашу думку, у чому полягає новизна Вашого дослідження? Тільки коротко – основна суть, найголовніше.

Відповідь: Дякую за запитання. Наукова новизна полягає у розробленні математичної моделі управління вимогами кібербезпеки, яка інтегрує метод аналізу ієрархій, нечітку логіку та байєсові мережі для врахування невизначеностей і ризиків, а також забезпечує оптимальний розподіл ресурсів з урахуванням бюджетних обмежень. Додатково запропоновано метод динамічного управління вимогами та метод інтегрування вимог кібербезпеки у

SDLC, що формалізує DevSecOps-підхід та забезпечує їх трасованість і адаптивність.

2. **Савченко А.С.,** д.т.н., проф., завідувач кафедри комп'ютерних інформаційних технологій КАІ.

Запитання: Яку основну проблему в галузі ІТ ви вирішуєте у дисертації?

Відповідь: Дякую за запитання. Основною проблемою є відсутність формалізованого, системного та динамічного підходу до управління вимогами кібербезпеки при впровадженні програмного забезпечення, що призводить до фрагментарного врахування загроз, запізнілого впровадження контролів і підвищення ризиків. Запропоновані в роботі моделі та методи дозволяють усунути ці недоліки шляхом інтеграції вимог у всі етапи життєвого циклу програмного забезпечення.

3. **Ільєнко А.В.,** к.т.н., доц., завідувач кафедри кібербезпеки КАІ.

Запитання: Які математичні методи, крім теорії множин, використані в роботі?

Відповідь: Дякую за запитання. У дисертації застосовано комплекс математичних методів, зокрема теорію множин (з елементами нечіткої логіки), теорію графів, метод аналізу ієрархій (AHP), байєсові мережі та методи оптимізації. Такий міждисциплінарний підхід дозволяє формалізувати процес управління вимогами, враховувати невизначеність і забезпечувати обґрунтоване прийняття рішень.

4. **Нечипорук О.П.,** д.т.н., проф., завідувач кафедри інтелектуальних кібернетичних систем КАІ.

Запитання: У чому перевага запропонованої моделі над існуючими підходами?

Відповідь: Дякую за запитання. Перевага полягає у комплексності та адаптивності моделі, яка враховує не лише пріоритетність вимог, але й ризики, невизначеності та ресурсні обмеження. На відміну від існуючих підходів, вона забезпечує динамічне оновлення вимог, їх трасованість та інтеграцію у всі фази SDLC, що значно підвищує ефективність управління кібербезпекою.

5. **Лукашенко В.В.,** д.т.н., проф., професор кафедри комп'ютерних систем та мереж КАІ.

Запитання: Як реалізується динамічне управління вимогами кібербезпеки?

Відповідь: Динамічне управління реалізується через ітераційний процес, який включає ініціалізацію вимог відповідно до стандартів, визначення тригерів змін, моніторинг середовища та загроз, переоцінювання вимог і ризиків, оптимізацію ресурсів та формування зворотного зв'язку. Це дозволяє системі адаптуватися до змін у реальному часі та підтримувати актуальність вимог кібербезпеки.

6. **Ільєнко А.В.,** к.т.н., доц., завідувач кафедри кібербезпеки КАІ.

Запитання: Які стандарти кібербезпеки враховано у дослідженні?

Відповідь: Дякую за запитання. У роботі враховано міжнародні стандарти та фреймворки, зокрема NIST 800-53, ISO 22316 та MITRE ATT&CK та інші. На їх основі проведено моделювання та експериментальні дослідження, що підтвердили ефективність запропонованих підходів щодо мінімізації ризиків і оптимізації ресурсів.

7. **Савченко А.С.,** д.т.н., проф., завідувач кафедри комп'ютерних інформаційних технологій КАІ.

Запитання: У чому полягає практична цінність результатів?

Відповідь: Дякую за запитання. Практична цінність полягає у створенні формалізованого механізму управління вимогами кібербезпеки, який може бути реалізований у системах підтримки прийняття рішень, GRC-платформах та DevSecOps pipeline. Це дозволяє підвищити автоматизацію контролів, зменшити витрати на усунення вразливостей та підвищити загальний рівень кіберстійкості організацій.

8. **Сидоренко В.М.,** к.т.н., доц., доцент кафедри комп'ютерних інформаційних технологій КАІ.

Запитання: Як інтегруються вимоги кібербезпеки у SDLC?

Відповідь: Дякую за запитання. Інтеграція здійснюється через формалізацію життєвого циклу розроблення програмного забезпечення у вигляді системи множин та відображень, що дозволяє впроваджувати вимоги кібербезпеки у конкретні фази pipeline. Запропонований метод забезпечує автоматизований контроль виконання вимог і оптимізацію вибору засобів захисту залежно від контексту системи.

9. **Фесенко А.О.,** к.т.н., доц., декан ФКНТ КАІ.

Запитання: Які результати експериментальної перевірки отримано?

Відповідь: Дякую за запитання. Експериментальні дослідження показали, що запропонована модель дозволяє мінімізувати ризики при дотриманні бюджетних обмежень, забезпечити баланс між важливістю вимог і ресурсами, а також ефективно враховувати вимоги різних стандартів. Це підтверджує її застосовність у реальних умовах впровадження ПЗ.

10. **Фесенко А.О.,** к.т.н., доц., декан ФКНТ КАІ.

Запитання: Де можуть бути застосовані результати дисертації?

Відповідь: Дякую за запитання. Результати можуть бути застосовані у проєктуванні захищених ІКС, аудиті безпечної розробки ПЗ, впровадженні DevSecOps у державних і корпоративних IT-системах, а також у критичній інфраструктурі та хмарних середовищах. Вони також впроваджені в освітній процес і діяльність профільних організацій.

11. **Охріменко Т.О.,** к.т.н., ст. дослідник, заступник декана ФКНТ.

Запитання: Чому у дисертації значна увага приділена кібербезпеці, хоча спеціальність «Комп'ютерні науки»?

Відповідь: Дякую за запитання. Попри те, що робота фокусується на кібербезпеці, вона повністю відповідає спеціальності «Комп'ютерні науки», оскільки базується на розробленні математичних моделей, алгоритмів і методів прийняття рішень для управління вимогами в складних інформаційних системах. Кібербезпека у даному випадку виступає прикладною областю, у межах якої застосовано інструментарій комп'ютерних наук. Запропоновані моделі є універсальними і можуть бути адаптовані до інших предметних областей, де існує необхідність управління вимогами в умовах невизначеності та ресурсних обмежень. Вимоги авіаційної безпеки, техногенної безпеки тощо.

Крім того, сучасні тенденції розвитку комп'ютерних наук передбачають інтеграцію з кібербезпекою, особливо у контексті DevSecOps, хмарних технологій, критичної інфраструктури та AI-систем. У дисертації досліджуються саме обчислювальні та алгоритмічні аспекти управління вимогами, а не лише прикладні заходи захисту, що підтверджує її належність до галузі комп'ютерних наук. Таким чином, кібербезпека виступає як предметна область застосування, тоді як основний науковий внесок полягає у розвитку методів, моделей та інструментальних засобів комп'ютерних наук.

Після відповідей на запитання виступили:

Науковий керівник – д.т.н., професор, професор кафедри комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій КАІ Гнатюк Сергій Олександрович.

Гнатюк С.О.: Доброго дня, шановні колеги! Скуратівський Анатолій Анатолійович є випускником бакалаврату та магістратури Національного авіаційного університету (нині - Київський авіаційний інститут), де з перших років навчання зарекомендував себе як відповідальний, дисциплінований і мотивований студент із глибоким інтересом до комп'ютерних наук та інженерії. У процесі навчання він продемонстрував високий рівень академічної підготовки, аналітичне мислення та здатність до самостійного опрацювання складних наукових і прикладних завдань. Важливо відзначити його активну участь у науковому житті університету, прагнення до професійного розвитку та постійне вдосконалення власних компетентностей.

Як науковець, здобувач характеризується системністю мислення, наполегливістю та високою працездатністю. Він відповідально ставиться до виконання наукових завдань, вміє чітко формулювати проблеми, знаходити оптимальні шляхи їх вирішення та аргументовано відстоювати власну позицію. У процесі роботи над дисертацією здобувач проявив здатність до критичного аналізу наукових джерел, узагальнення отриманих результатів і формулювання обґрунтованих висновків. Окремо слід підкреслити його вміння поєднувати теоретичні дослідження з практичними аспектами, що значною мірою підвищує цінність отриманих результатів.

Професійна діяльність здобувача в міжнародній IT-компанії EPAM свідчить про його високий рівень компетентності та затребуваність у сучасній індустрії. Він успішно застосовує отримані знання на практиці, бере участь у реалізації складних технологічних проєктів та демонструє здатність працювати в команді, приймати відповідальні рішення і досягати поставлених цілей. Такий

досвід позитивно вплинув на формування його як фахівця і науковця, забезпечивши тісний зв'язок між наукою та практикою.

Як особистість, здобувач є порядною, відповідальною та цілеспрямованою людиною з активною громадянською позицією. Він усвідомлює значення своєї професійної діяльності для розвитку держави, особливо в умовах сучасних викликів, та прагне застосовувати свої знання і навички на благо суспільства. Йому притаманні такі якості, як доброчесність, комунікабельність, здатність до саморозвитку та прагнення до досягнення високих результатів.

Дисертаційна робота А. Скуратівського виконана на належному науковому рівні, має логічну структуру, чітко сформульовані мету, завдання та висновки. Отримані результати є обґрунтованими, достовірними та мають як теоретичне, так і практичне значення. Здобувач виявив себе як сформований науковець, здатний до проведення самостійних досліджень і вирішення складних науково-прикладних задач.

Вважаю, що дисертаційна робота відповідає вимогам, встановленим для здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», а її автор Анатолій Скуратівський сформувався як кваліфікований фахівець і зрілий науковець, здатний до самостійного вирішення складних науково-прикладних задач у галузі комп'ютерних наук. Вважаю, що за рівнем підготовки, професійними та особистими якостями повністю відповідає вимогам до здобувачів ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» та заслуговує на його присудження.

Рецензенти дисертаційної роботи, які наголосили на позитивних аспектах дослідження та висловили свої побажання та зауваження:

Ахрамович Володимир Миколайович, д.т.н., проф., професор кафедри кібербезпеки КАІ.

Детально ознайомився з дисертаційною роботою здобувача, проаналізував її структуру, зміст та отримані результати. Хочу відзначити актуальність обраної тематики, високий рівень теоретичного опрацювання матеріалу та логічність викладення. Отримані результати є обґрунтованими, а використані методи - сучасними та коректно застосованими. Особливо позитивно оцінюю практичну спрямованість роботи та можливість використання запропонованих підходів у реальних ІТ-системах. Як і будь-які роботи, вона містить дрібні помилки і неточності, але загалом враження дуже позитивне. Вважаю, що дисертація відповідає вимогам до наукових робіт за спеціальністю 122 «Комп'ютерні науки», а її автор заслуговує на присудження ступеня доктора філософії.

Ільєнко Анна Вадимівна, к.т.н., доц., завідувач кафедри кібербезпеки КАІ.

Я також ознайомилася з дисертаційною роботою здобувача та можу підтвердити її високий науковий і прикладний рівень. Робота вирізняється системністю підходу, чіткістю постановки задач та аргументованістю висновків. Важливо, що автору вдалося поєднати теоретичні дослідження з практичними аспектами, що підвищує значущість отриманих результатів. Окремо хочу відзначити професійний рівень підготовки здобувача, його

старанність, здатність до самостійної наукової роботи. Загалом підтримую подану дисертацію та вважаю за доцільне рекомендувати її до захисту з подальшим присудженням ступеня доктора філософії.

В **обговоренні** дисертаційного дослідження взяли участь:

Нечипорук О.П., д.т.н., проф., завідувач кафедри інтелектуальних кібернетичних систем КАІ. Відзначила високу практичну спрямованість дисертаційної роботи. Запропоновані автором моделі та методи управління вимогами кібербезпеки мають чітку орієнтацію на впровадження у реальні процеси розроблення програмного забезпечення, зокрема в середовищах DevSecOps, хмарних інфраструктурах та корпоративних IT-системах. Важливо, що результати дослідження можуть бути безпосередньо використані у системах підтримки прийняття рішень, інструментах управління кіберризиками та GRC-платформах, що значно підвищує їх цінність для бізнесу та критичної інфраструктури. Вважаю, що така орієнтація на практичне застосування є суттєвою перевагою роботи та відповідає сучасним вимогам до досліджень у галузі комп'ютерних наук.

Савченко А.С., д.т.н., проф., завідувач кафедри комп'ютерних інформаційних технологій КАІ. Автору вдалося поєднати різні методологічні інструменти – теорію множин, нечітку логіку, байєсові мережі та метод аналізу ієрархій – у єдину узгоджену модель управління вимогами кібербезпеки. Така інтеграція дозволяє враховувати як формалізовані, так і невизначені аспекти задачі, що є суттєвою перевагою порівняно з існуючими підходами. Особливо цінним є запропонований механізм динамічного оновлення вимог, який забезпечує адаптивність системи до змін у середовищі загроз і ресурсних обмежень. Вважаю, що саме цей комплексний та міждисциплінарний підхід формує наукову новизну роботи та відкриває перспективи для подальших досліджень у даній галузі.

Сидоренко В.М., к.т.н., доц., доцент кафедри комп'ютерних інформаційних технологій КАІ. Відзначила ґрунтовне опрацювання здобувачем міжнародних стандартів і фреймворків у сфері кібербезпеки. У дисертації коректно використано та проаналізовано підходи, закладені у NIST 800-53, ISO 22316 та MITRE ATT&CK, що свідчить про високий рівень орієнтації автора у сучасних нормативних і методичних основах кіберзахисту. Особливо цінним є те, що ці стандарти не просто наведені для огляду, а інтегровані у запропоновані моделі та методи, що забезпечує їх практичну релевантність і відповідність міжнародним вимогам. Вважаю, що такий підхід значно підсилює наукову і прикладну цінність роботи та демонструє здатність здобувача працювати на рівні сучасних глобальних IT-практик.

Фесенко А.О., к.т.н., доц., декан Факультету комп'ютерних наук та технологій КАІ. Запропоновані здобувачем моделі та методи управління вимогами кібербезпеки є вкрай актуальними в умовах широкого використання хмарних технологій, мікросервісної архітектури та DevSecOps-підходів. Вони

дозволяють підвищити рівень автоматизації процесів безпеки, забезпечити узгодженість вимог на всіх етапах розроблення програмного забезпечення та зменшити ризики виникнення вразливостей. Особливо важливо, що результати роботи мають прикладний характер і можуть бути інтегровані у сучасні інструменти розроблення та управління ІТ-проєктами. Вважаю, що це робить дослідження значущим не лише з наукової, а й з практичної точки зору для розвитку ІТ-індустрії.

Лукашенко В.В., д.т.н., проф., професор кафедри комп'ютерних систем та мереж КАІ. Відзначила, що здобувачем охоплено різні домени кібербезпеки, що свідчить про комплексність і глибину проведеного дослідження. У роботі враховано аспекти безпеки на рівні мереж, додатків, даних, управління доступом, а також організаційні та процесні компоненти, зокрема інтеграцію вимог у DevSecOps і SDLC. Такий міждоменний підхід дозволяє розглядати кібербезпеку не фрагментарно, а як цілісну систему, де взаємодіють технічні, управлінські та нормативні складові. Вважаю, що це є суттєвою перевагою роботи, оскільки забезпечує її універсальність і можливість застосування в різних типах інформаційних систем – від корпоративних до об'єктів критичної інфраструктури.

Охріменко Т.О., к.т.н., ст. досл., заступник декана ФКНТ КАІ. Важливою перевагою дисертаційної роботи є орієнтація на кількісне оцінювання вимог кібербезпеки та рівня їх реалізації. Здобувачем запропоновано підходи, які дозволяють формалізувати процес прийняття рішень, використовуючи метрики, вагові коефіцієнти та оцінки ризиків, що значно підвищує об'єктивність і обґрунтованість управління кібербезпекою. Використання методів багатокритеріальної оцінки, нечіткої логіки та оптимізаційних моделей дає змогу перейти від якісних експертних оцінок до кількісно вимірюваних показників, що є особливо важливим для сучасних ІТ-систем і бізнес-середовищ. Вважаю, що такий підхід суттєво підвищує наукову цінність роботи та створює передумови для її практичного впровадження у системах підтримки прийняття рішень.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Скуратівського Анатолія Анатолійовича на тему «Методи та інструментальні засоби управління вимогами кібербезпеки при впровадженні програмного забезпечення в бізнесі», поданої на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології», за спеціальністю 122 «Комп'ютерні науки»

1. Обґрунтування вибору теми дослідження. Вибір теми дисертаційної роботи Скуратівського Анатолія Анатолійовича зумовлений сучасними викликами оскільки стрімка цифровізація бізнесу, активне використання хмарних сервісів, IoT, AI та DevOps/DevSecOps-підходів призводять до зростання кількості кіберзагроз і ускладнення забезпечення безпеки програмного забезпечення на всіх етапах його впровадження. При цьому існуючі підходи управління вимогами кібербезпеки часто є фрагментарними,

несистемними та слабо інтегрованими у процеси життєвого циклу розроблення програмного забезпечення, що ускладнює своєчасне виявлення вразливостей, підвищує ризик інцидентів та збільшує витрати на їх усунення.

Сучасний бізнес потребує ефективних методів і інструментальних засобів, що дозволяють інтегрувати вимоги кібербезпеки у процеси розроблення та впровадження ПЗ без зниження швидкості інновацій та time-to-market. Особливої важливості набуває забезпечення трасованості вимог кібербезпеки, автоматизації контролів у DevOps/DevSecOps-процесах, зниження операційних ризиків та оптимізації витрат на забезпечення кіберстійкості інформаційних систем, що безпосередньо впливає на безперервність бізнес-процесів, а також довіру клієнтів та конкурентоспроможність організацій.

Водночас сучасні підприємства активно впроваджують складні програмні системи, що базуються на мікросервісній архітектурі, хмарних платформах, API інтеграціях, CI/CD pipeline та Agile-методологіях, що значно підвищує динамічність змін у ПЗ та ускладнює управління вимогами протягом життєвого циклу ПЗ. Часті оновлення, інтеграція сторонніх сервісів, використання відкритих бібліотек та швидке масштабування ІТ-рішень формують потребу у методах, які дозволяють системно управляти вимогами під час проєктування, розроблення, тестування, розгортання та супроводу ПЗ, забезпечуючи узгодженість функціональних, нефункціональних і технологічних вимог у складних ІТ-середовищах.

Таким чином, розроблення методів та інструментальних засобів управління вимогами кібербезпеки при впровадженні ПЗ є актуальним науково-технічним завданням, спрямованим на підвищення загального рівня резильєнтності інформаційних систем бізнесу, забезпечення їх стійкості та відповідності сучасним стандартам і рекомендованим практикам в галузі ІТ та кібербезпеки.

2. Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційна робота є складовою частиною досліджень, що проводяться в КАІ. Тема дисертаційної роботи корелює з Глобальною інноваційною стратегією України WinWin2030, що визначає ключові напрямки, цілі та принципи державної політики у сфері цифрового розвитку інноваційної діяльності. Зокрема, в контексті досягнення Стратегічної цілі 15 «Створення умов для розробки та застосування продуктів у сфері кібербезпеки», що включає в себе розробку та безпечне використання ІТ-технологій і продуктів у сфері кібербезпеки, удосконалення нормативно-правового та технічного регулювання у сфері кібербезпеки та кіберзахисту, проведення заходів із виявлення вразливостей, загроз, оперативного та комплексного реагування на кіберінциденти та кібератаки. При цьому доцільним є використання досвіду країн ЄС (рекомендацій ENISA, NIST, CISA тощо) та інформації для реалізації зазначених напрямів для досягнення кінцевої мети – забезпечення кібербезпеки та кіберстійкості держави, її критичної інфраструктури, оборонної сфери, електронних послуг тощо.

Тема дисертації відповідає освітньої-науковій програмі «Комп'ютерні науки» за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» в КАІ (зокрема, ОК 1.3.3, ОК 1.3.4 та ОК 1.3.5).

3. Мета і завдання дослідження. Мета дисертаційного дослідження полягає в підвищенні ефективності процесу впровадження ПЗ в бізнесі шляхом розроблення методів та інструментальних засобів управління вимогами кібербезпеки, які забезпечують їх формалізовану інтеграцію, трасованість, адаптацію до змін середовища загроз і ресурсних обмежень, а також узгодженість з функціональними та нефункціональними вимогами інформаційних систем.

Для досягнення поставленої мети необхідно розв'язати такі задачі:

1) Провести аналіз сучасних підходів до управління вимогами кібербезпеки при розробленні і впровадженні ПЗ, для виявлення їх недоліків, вибору найбільш ефективних математичних методів і підходів та формалізації завдання дослідження;

2) Розробити та дослідити математичну модель управління вимогами кібербезпеки при впровадженні ПЗ на основі міжнародних стандартів для забезпечення ефективного управління вимогами кібербезпеки під час впровадження ПЗ в бізнесі (визначати пріоритетні вимоги, оптимально розподіляти ресурси з урахуванням обмежень тощо);

3) Розробити метод динамічного управління вимогами кібербезпеки для врахування нових вимог кібербезпеки при впровадженні ПЗ, а також забезпечення адаптації системи до зміни ресурсних або нормативних умов;

4) Розробити уніфіковану модель SDLC та на її базі метод інтегрування вимог кібербезпеки в SDLC для інтегрування вимог кібербезпеки в конкретну фазу життєвого циклу розроблення ПЗ та оптимізації вибору контролів кібербезпеки залежно від контексту системи та ресурсних обмежень;

5) Провести експериментальне дослідження розроблених моделей і методів з використанням розроблених інструментальних засобів (псевдокоди, симуляційні моделі та фреймворки).

4. Об'єктом дослідження – процес управління вимогами кібербезпеки.

5. Предметом дослідження – методи, моделі та інструментальні засоби управління вимогами кібербезпеки при впровадженні ПЗ в бізнесі.

6. Методи дослідження. Для вирішення поставленої наукового завдання в дисертаційній роботі використані такі методи: теорію множин (у тому числі, з елементами нечіткої логіки), теорію графів, метод аналізу ієрархій (Analytic Hierarchy Process, AHP), теорію байєсових мереж, методи оптимізації та неформальне представлення алгоритмів програмування за допомогою псевдокодів, симуляційні моделі та фреймворки.

7. Наукова новизна дослідження: полягає в розробленні нових і удосконалених методів та моделей для формалізації процесу управління вимогами кібербезпеки при впровадженні ПЗ в бізнесі, зокрема:

уперше:

– розроблено математичну модель управління вимогами кібербезпеки при впровадженні ПЗ, що за рахунок створення графу залежностей вимог, використання методу AHP для пріоритезації вимог, застосування нечіткої логіки для оцінки рівня відповідності вимогам, моделювання ризиків за допомогою Байєсової мережі та оптимізації ресурсів за допомогою математичного програмування, дозволяє дозволяє визначити пріоритети серед вимог кібербезпеки, врахувати невизначеності та ймовірність ризиків, а також оптимально розподілити ресурси між вимогами з урахуванням обмежень бюджету та мінімізації ризиків, забезпечуючи комплексне управління вимогами кібербезпеки під час впровадження ПЗ з урахуванням міжнародних стандартів і сучасних методів оцінки ризиків.

– розроблено метод динамічного управління вимогами кібербезпеки, який за рахунок ініціалізації вимог кібербезпеки відповідно до нормативних документів і стандартів, визначення тригерів динамічного оновлення вимог кібербезпеки, моніторингу змін у середовищі впровадження ПЗ та актуальних загроз, кореляції та переоцінювання вимог кібербезпеки з урахуванням виявлених змін і оновлень ризиків, оптимізації розподілу ресурсів між вимогами кібербезпеки з урахуванням оновлених пріоритетів і обмежень, формування зворотного зв'язку та ініціації наступного циклу управління вимогами, дає змогу регулярно оновлювати пріоритети, врахувати нові вимоги кібербезпеки при впровадженні ПЗ, а також забезпечити адаптацію системи до зміни ресурсних або нормативних умов.

удосконалено:

– метод інтегрування вимог кібербезпеки в SDLC, що за рахунок формалізації моделі DevSecOps (на базі уніфікованої моделі SDLC), ідентифікації вимог кібербезпеки, трансформації вимог у контрольні механізми, інтегрування контрольних механізмів у SDLC, верифікування та моніторингу виконання вимог кібербезпеки у вигляді системи множин та відображень, дозволяє інтегрувати вимоги кібербезпеки в конкретну фазу (pipeline) життєвого циклу розроблення ПЗ, а також дає можливість формалізованої оптимізації вибору контролів кібербезпеки залежно від контексту системи та ресурсних обмежень;

отримала подальший розвиток:

– уніфікована модель SDLC, яка за рахунок формалізованого відображення множин фаз життєвого циклу розроблення ПЗ, відношень між фазами та функцій, дозволяє представити відомі моделі життєвого циклу розроблення ПЗ у зручній формі для інтегрування й імплементування вимог.

8. Теоретичне значення. Теоретичне значення дисертаційної роботи полягає у розвитку наукових положень щодо підвищення ефективності процесу впровадження ПЗ в бізнесі шляхом розроблення методів, моделей та інструментальних засобів управління вимогами кібербезпеки, орієнтованих на забезпечення їх інтеграції, трасованості, адаптації до змін середовища загроз і ресурсних обмежень, а також аспектів узгодженості з функціональними та нефункціональними вимогами сучасних інформаційних систем. Отримані результати є основою для подальших досліджень у галузі інформаційних

технологій, зокрема в напрямку впровадження вимог кібербезпеки на різних рівнях розроблення ПЗ.

9. Практичне значення та використання результатів дисертаційного дослідження. Практичні результати можна звести до наступних пунктів:

1) на основі розробленої моделі управління вимогами кібербезпеки при впровадженні ПЗ було проведено практичні симуляції з використанням фреймворків міжнародних стандартів і рекомендованих практик, зокрема досліджено:

- розроблену модель на основі стандарту NIST 800-53, що забезпечило мінімізацію ризиків при дотриманні обмежень бюджету та пріоритетності вимог кібербезпеки згідно з вимогами стандарту NIST;
- розроблену модель на основі стандарту ISO 22316, що забезпечило досягнення балансу між важливістю вимог, мінімізацією ризиків і наявними ресурсами, відповідно вимогам ISO 22316 для забезпечення стійкості організації;
- розроблену модель на основі стандарту MITRE ATT&CK, що забезпечило виконання критичних вимог MITRE ATT&CK і мінімізацію загальних ризиків при дотриманні бюджету.

2) формалізовано адаптивний механізм управління вимогами кібербезпеки, який забезпечує обґрунтований вибір пріоритетів, оптимальний розподіл ресурсів та підвищення системної стійкості ІКС у вигляді псевдокоду, що та може бути реалізований у системах підтримки прийняття рішень; програмних засобах управління кіберризиками; корпоративних GRC-платформах; автоматизованих системах планування тощо;

3) на основі уніфікованої моделі SDLC було формалізовано відомі моделі життєвого циклу розроблення ПЗ, зокрема класичну каскадну модель, V-модель, інкрементальну модель, спіральну модель, Agile, DevOps та DevSecOps, що може бути використано при проєктуванні захищених ІКС; аудиті процесів безпечної розробки ПЗ згідно стандартів ISO/IEC, NIST, PCI DSS, PSD2, GDPR, MITRE ATT&CK; створенні політик secure SDLC; впровадженні DevSecOps у державних та корпоративних ІТ-системах тощо;

4) практична цінність методу інтегрування вимог кібербезпеки в SDLC полягає у можливості його використання для системного інтегрування вимог кібербезпеки в процеси розроблення ПЗ в організаціях, що створюють або експлуатують інформаційні системи критичної інфраструктури, хмарні сервіси та корпоративні ІКС. Застосування цього методу дозволяє: забезпечити узгодженість вимог кібербезпеки на всіх етапах SDLC; підвищити рівень автоматизації контролю кібербезпеки у DevSecOps pipeline; зменшити ризик пропуску критичних вимог кібербезпеки під час швидких ітерацій розроблення; підвищити обґрунтованість вибору засобів захисту інформації; скоротити витрати на усунення вразливостей за рахунок їх виявлення на ранніх етапах SDLC; забезпечити можливість кількісного оцінювання рівня реалізації вимог кібербезпеки за допомогою метрик кібербезпеки; створити інструментальні засоби підтримки прийняття рішень у процесах DevSecOps;

5). Проведені в дисертаційній роботі дослідження реалізовані й впроваджені: в навчальному процесі кафедри комп'ютерних інформаційних

технологій. (Акт про впровадження результатів від 18.02.2026року); в діяльність Наукової асоціації кібербезпеки України. (Акт про впровадження результатів від 17.12.2025 року).

10. Особистий внесок здобувача. Дисертація «Методи та інструментальні засоби управління вимогами кібербезпеки при впровадженні програмного забезпечення в бізнесі», Скуратівського Анатолія Анатолійовича є самостійною науковою працею, в якій наведено теоретичні положення і висновки, власні ідеї та розробки автора, які дають змогу вирішити поставлені завдання. У дисертації наукові ідеї та розробки співавторів не використовувалися. Усі сформульовані положення, висновки та пропозиції обґрунтовані на основі особистих досліджень автора.

11. Апробація результатів дослідження. Наукові результати та основні положення дисертаційної роботи доповідались, обговорювались на всеукраїнських, міжнародних семінарах та конференціях, а саме: «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (м. Дотмунд, Німеччина, 07-09 вересня 2023 р); «Cyber Hygiene and Conflict Management in Global Information Networks» (м. Київ, 24-27 січня 2024 р.), «Advanced Technologies in Cyber Resilience» (м. Київ, 20-22 червня 2025 р.).

12. Публікації. Основні положення та результати дисертаційного дослідження викладено в 3 наукових публікаціях, серед них 2 публікації у наукових фахових виданнях України категорії Б, 1 у виданні, проіндексованому в базі даних *Scopus*, а також автор має 2 праці апробаційного характеру, що включено до бази даних *Scopus* .

Список опублікованих праць за темою дисертації

Статті у наукових фахових виданнях України:

1. Гнатюк С.О., Сидоренко В.М., Скуратівський А.А. Модель управління вимогами кібербезпеки при впровадженні програмного забезпечення. Кібербезпека: освіта, наука, техніка, 2025, Т.4, № 28, с. 25-37. DOI: https://doi.org/10.28925/2663-4023.2025.28.841

Здобувачу належить розроблення та формалізований опис моделі управління вимогами кібербезпеки при впровадженні ПЗ. Гнатюку С.О. належить постановка завдання наукового дослідження, Сидоренко В.М. – вибір стандартів кібербезпеки і формалізація компонентів моделі.

2. Гнатюк, С.О., Сидоренко В.М., Скуратівський А.А. Аналіз сучасних підходів до управління вимогами кібербезпеки при впровадженні програмного забезпечення, Проблеми інформатизації та управління, 2025, Т.2, № 82, с. 5-18, https://doi.org/10.18372/2073-4751.82.20363

Здобувачу належить визначення критеріїв і проведення аналізу, а також дослідження актуальних наукових публікацій за напрямком досліджень. Гнатюку С.О. належить вибір підходів для аналізу, а Сидоренко В.М. – категоризація і класифікація підходів.

3. Сидоренко В.М., Положенцев А.А., Сидоренко С.Ю., Скуратівський А.А. Метод визначення пріоритетів IT-інцидентів на об'єктах критичної інформаційної інфраструктури держави. Проблеми інформатизації та управління, 2024, Т. 2, №°78, С. 104-114, https://doi.org/10.18372/2073-4751.78.18967

Здобувачу належать дослідження вимог міжнародних стандартів ISO/IEC 20000 та NIST Cybersecurity Framework в контексті теми дисертації, Сидоренко В.М. належить постановка завдання і висновки, Положенцеву А.А. – попарне порівняння і пріоритезація інцидентів, а Сидоренку С.Ю. – дослідження вимог стандартів ITIL та COBIT.

4. Гнатюк В.О., Батрак О.Г., Скуратівський А.А., Кудренко С.О., Метод оптимізації роботи системи масового обслуговування з використанням віртуального асистента на базі штучного інтелекту, Проблеми інформатизації та управління, 2025, Т.3. № 75, с. 21-28, https://doi.org/10.18372/2073-4751.75.18013

Здобувачу належить дослідження оптимізації безпеки систем масового обслуговування як прикладу ПЗ, до якого застосовуються вимоги кібербезпеки, Гнатюку В.О. належить постановка завдання у цьому дослідженні, а Батраку О.Г. – практичні аспекти застосування алгоритмів штучного інтелекту.

Статті в іноземних виданнях:

5. Dorozhynskyi S., Zakutynskyi I., Ryabyy M., Skurativskyi A. Maximizing Security and Efficiency in 5G Networks by Means of Quantum Cryptography and Network Slicing Concepts, Proceedings of the IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems Technology and Applications, 2023, pp. 1031-1036, 10.1109/IDAACS58523.2023.10348871, ISSN 2770-4262

Здобувачу належить дослідження практичних аспектів безпеки сучасних програмних систем і контролю виконання вимог кібербезпеки.

6. Gnatyuk S., Sydorenko V., Polozhentsev A., Skurativskyi A., Kluczewska-Chmielarz K., Shuitenov G. Modern approaches to cybersecurity requirements management for software implementation, CEUR Workshop Proceedings, 2025, Vol. 4024, pp. 186-200.

Здобувачу належать визначення критеріїв та проведення порівняльного аналізу методів управління вимогами при впровадженні ПЗ в бізнесі.

7. Odarchenko R., Pinchuk A., Polihenko O., Skurativskyi A. A comparative analysis of cyber threat intelligence models, CEUR Workshop Proceedings, 2025, Vol. 3925, pp. 3-12.

Здобувачу належить дослідження моделей threat intelligence в контексті вимог кібербезпеки до розроблюваного ПЗ.

13. Структура та обсяг дисертації. Дисертація складається з основної частини (анотації, вступу, чотирьох розділів та висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 121 сторінку, з яких 102 сторінки основного тексту. Список використаних джерел складається з 101 найменування і займає 15 сторінок, додатки викладено на 2 сторінках.

14. Характеристика особистості здобувача. Під час підготовки дисертації Скуратівський Анатолій Анатолійович проявив себе як ініціативний і наполегливий дослідник, здатний комплексно поєднувати теоретичні знання та практичні навички. Здобувач продемонстрував високий рівень самостійності, креативності у постановці та вирішенні завдань, уміння систематизувати й аналізувати великий обсяг наукової інформації. Здобувач вільно володіє англійською мовою, що дозволяє йому бути в курсі останніх досліджень і трендів у галузі інформаційних технологій, а також отримувати вагомі результати як теоретичного, так і прикладного характеру. Під час роботи над дисертацією Анатолій Скуратівський проявив здатність ефективно планувати дослідницьку діяльність, дотримуватися термінів виконання етапів дослідження та інтегрувати отримані результати у навчальний процес і практику.

15. Оцінка мови та стилю дисертації. Дисертація викладена науковим стилем сучасною українською мовою, із використанням усталеної термінології спеціальності «Комп'ютерні науки». Виклад матеріалу відзначається чіткістю, логічною послідовністю та аргументованістю.

Структура тексту відповідає вимогам Міністерства освіти і науки України щодо дисертаційних робіт, усі положення та результати подані в академічно коректній формі.

16. Відповідність принципам академічної доброчесності.

Дисертація відповідає чинному законодавству та сучасним принципам академічної доброчесності. У роботі відсутні ознаки плагіату чи безпідставних запозичень. Усі використані наукові результати, підходи, методи та твердження супроводжуються відповідними бібліографічними посиланнями.

Автор відокремлює власні наукові здобутки від результатів попередніх досліджень інших учених. Представлені результати є достовірними та перевіреними, що підтверджено експериментальною перевіркою, апробацією на наукових конференціях, публікаціями у фахових і міжнародних виданнях та впровадженням у навчальний процес і практичну діяльність.

17. Рецензенти рекомендують: відповідно до **пп. 15, 16** Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44, ***пропонується такий склад разової ради:***

Голова ради:

ЛУКАШЕНКО Вікторія Вікторівна, д.т.н., проф., професор кафедри комп'ютерних систем та мереж Факультету комп'ютерних наук та технологій КАІ.

Рецензенти:

АХРАМОВИЧ Володимир Миколайович, д.т.н., проф., професор кафедри кібербезпеки Факультету комп'ютерних наук та технологій КАІ.

ІЛЬЄНКО Анна Вадимівна, к.т.н., доц., завідувач кафедри кібербезпеки Факультету комп'ютерних наук та технологій КАІ.

Офіційні опоненти:

ЄВДОКИМЕНКО Марина Олександрівна, д.т.н., проф., професор кафедри інфокомунікаційної інженерії ім. В.В. Поповського Харківського національного університету радіоелетроніки.

МИРУТЕНКО Лариса Вікторівна, к.т.н., доц., доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Усі члени разової спеціалізованої вченої ради не мають реального чи потенційного конфлікту інтересів щодо здобувача Скуратівського Анатолія Анатолійовича (зокрема, не є його близькою особою) та/або його наукового керівника.

У результаті попередньої експертизи дисертації Скуратівського Анатолія Анатолійовича повноти публікації основних результатів дослідження

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Скуратівського Анатолія Анатолійовича на тему «Методи та інструментальні засоби управління вимогами кібербезпеки при впровадженні програмного забезпечення в бізнесі».

2. Вважати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Скуратівського Анатолія 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 23.03.2016. № 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 інструментальні засоби управління вимогами кібербезпеки при впровадженні програмного забезпечення в бізнесі», подану Скуратівським Анатолієм 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 затвердити склад разової спеціалізованої вченої ради:

Головою спеціалізованої вченої ради:

ЛУКАШЕНКО Вікторію Вікторівну, д.т.н., проф., професора кафедри комп'ютерних систем та мереж Факультету комп'ютерних наук та технологій КАІ.

Рецензентами:

АХРАМОВИЧА Володимира Миколайовича, д.т.н., проф., професора кафедри кібербезпеки Факультету комп'ютерних наук та технологій КАІ.

ІЛЬЄНКО Анну Вадимівну, к.т.н., доц., завідувача кафедри кібербезпеки Факультету комп'ютерних наук та технологій КАІ.

Офіційними опонентами:

ЄВДОКИМЕНКО Марину Олександрівну, д.т.н., проф., професора кафедри інфокомунікаційної інженерії ім. В.В. Поповського Харківського національного університету радіоелетроніки.

МИРУТЕНКО Ларису Вікторівну, к.т.н., доц., доцента кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Результати голосування щодо рекомендації до захисту дисертації Скуратівського Анатолія Анатолійовича:

«за» – 10.

«проти» – немає.

«утримались» – немає.

Головуючий на засіданні:
завідувачка кафедри комп'ютерних інформаційних технологій КАІ, д.т.н., професор — Аліна САВЧЕНКО

Секретар засідання:
доцент кафедри комп'ютерних інформаційних технологій КАІ, к.т.н., доцент — Вікторія СИДОРЕНКО

ПОГОДЖЕНО:
проректор з наукових досліджень та трансферу технологій КАІ, д.т.н., професор — Сергій ГНАТЮК