ЗАТВЕРДЖУЮ
президент Державного університету
«Київський авіаційний інститут»
_____ Ксенія СЕМЕНОВА
«04» грудня 2025 року

ВИСНОВОК

Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» (далі – КАІ) про наукову новизну, теоретичне та практичне значення результатів дисертації Жигаревич Оксани Костянтинівни на тему: «Система корелювання подій та управління ІТ-інцидентами на об'єктах критичної інфраструктури» подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології»

ВИТЯГ

із протоколу №13 розширеного засідання науково-технічного семінару
кафедри комп'ютерних інформаційних технологій
Факультету комп'ютерних наук та технологій КАІ
від «03» грудня 2025 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;
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;
Толстікова Олена Володимирівна, к.т.н., доц., доцент кафедри;
Сидоренко Вікторія Миколаївна, к.т.н., доц., доцент кафедри;
Положенцев Артем Анатолійович, PhD, старший викладач кафедри;
Мельниченко Поліна Ігорівна, асистент кафедри;
Кравченко Микола Олексійович, асистент кафедри.

Присутні на засіданні науково-педагогічні працівники КАІ:

Гнатюк Сергій Олександрович – д.т.н., професор, проректор з наукових досліджень та трансферу технологій.

Фесенко Андрій Олексійович – к.т.н., доцент, декан факультету комп'ютерних наук та технологій (ФКНТ).

Охріменко Тетяна Олександрівна – к.т.н., ст. дослідник, заступник декана з наукової роботи ФКНТ.

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

Павленко Петро Миколайович, д.т.н., проф., професор кафедри організації авіаційних перевезень.

Приставка Пилип Олександрович, д.т.н., проф., головний науковий співробітник науково-дослідної частини.

Ільєнко Анна Вадимівна – к.т.н., доцент, завідувач кафедри кібербезпеки.

Присутні на засіданні науково-педагогічні працівники з інших установ:

1. Смірнов О.А. д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнського національного технічного університету.

Серед присутніх 8 докторів технічних наук та 11 кандидатів технічних наук.

Порядок денний:

Обговорення дисертаційного дослідження здобувачки кафедри комп'ютерних інформаційних технологій КАІ Жигаревич Оксани Костянтинівни на тему «Система корелювання подій та управління ІТ-інцидентами на об'єктах критичної інфраструктури», поданої на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.06 – «Інформаційні технології».

Тему дисертаційного дослідження «Система корелювання подій та управління ІТ-інцидентами на об'єктах критичної інфраструктури» затверджено на засіданні вченої ради Факультету комп'ютерних наук та технологій (протокол № 11 від 18 листопада 2025 року).

Науковий керівник – кандидат технічних наук, доцент, доцент кафедри комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій КАІ Сидоренко Вікторія Миколаївна.

Слухали:

Доповідь здобувача Жигаревич Оксани Костянтинівни на тему «Система корелювання подій та управління ІТ-інцидентами на об'єктах критичної інфраструктури», поданої на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.06 – «Інформаційні технології».

Доповідачка представила 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 дослідженню та розробці моделей та системи корелювання подій та управління ІТ-інцидентами на об'єктах

критичної інфраструктури (ОКІ) держави. У роботі розглянуто актуальні проблеми забезпечення ефективного реагування на інциденти в умовах функціонування сучасних інформаційно-комунікаційних систем (ІКС), досліджено особливості використання SIEM-рішень, а також проведено детальний аналіз існуючих типів баз даних та інтеграційних шин даних. Визначено існуючі підходи, методології та стандарти у сфері управління ІТ-інцидентами, ідентифіковано основні недоліки та області для покращення.

У роботі проаналізовано сучасні підходи до виявлення аномалій у хмарних середовищах, досліджено типи баз даних та інтеграційних шин даних, систематизовано підходи, методології та стандарти у сфері управління ІТ-інцидентами. Проведено порівняльний аналіз 16 SIEM-систем за 18 критеріями, що дозволило формалізувати завдання дослідження та визначити напрями удосконалення існуючих рішень.

Дослідницею удосконалено структурно-аналітичну модель оброблення даних для інтелектуалізованого виявлення аномалій у хмарних ІКС.

Розроблено модель онтологіко-реляційного сховища даних для зберігання та оброблення великих масивів інформації.

Жигаревич О.К. удосконалено модель інтеграційної шини даних для розподілу навантаження та захищеного обміну даними.

Дослідницею на основі розроблених моделей розроблено систему корелювання подій та управління ІТ-інцидентами на ОКІ.

Авторкою створено методику зберігання та класифікації даних, яка дозволяє сервісу індексації отримувати доступ до зовнішніх сховищ даних, проводити масштабування, агрегацію, аналіз, збір закономірностей та забезпечувати високу швидкість пошуку.

Здобувачкою сформовано специфікацію реалізації SIEM-систем на ОКІ, у вигляді основних та додаткових вимог.

Авторкою розроблено спеціальний програмний застосунок, який можна використовувати для управління ІТ-інцидентами, які виникають в КІ і мають вплив на критично важливі ресурси (КВР).

Крім того, Жигаревич О.К. створено спеціалізоване програмне забезпечення та проведено верифікацію розроблених у роботі моделей та системи з метою підтвердження їх ефективності та придатності для практичного застосування.

Структура та обсяг дисертації зумовлені метою і логікою дослідження та складаються з анотації, вступу, чотирьох розділів, висновків, списку використаних джерел, додатків.

Після закінчення доповіді Жигаревич Оксани Костянтинівни присутніми на засіданні фахівцями поставлені наступні запитання:

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

Запитання: У науковій новизні зазначено, що вперше розроблено модель онтологіко-реляційного сховища даних. В чому суть моделі?

Відповідь: Дякую за запитання. Запропонована модель онтологіко-реляційного сховища даних, за рахунок попередньої індексації та синтезу двох різних баз даних (Elasticsearch та MongoDB) з відповідними характеристиками, дає можливість покращити зручність у зберіганні та класифікації даних, а також забезпечити високу швидкість пошуку та отримання великих обсягів інформації.

Запитання: Яким чином відбувається вибір необхідних баз даних для моделі онтологіко-реляційного сховища даних?

Відповідь: Дякую за запитання. Спочатку вводяться множини баз даних, чинникових ознак (критеріїв) та облікових задач. Після цього відбувається процедура визначення рангу найбільш ефективних баз даних. Результати вибору найбільш ефективних БД представляються у вигляді кортежу, який характеризує БД з найвищим значенням рангового показника, що відповідають визначеним критеріям ефективності та здатні забезпечити виконання множини необхідних облікових задач. В результаті експериментальних досліджень були обґрунтовано виділені бази даних: ElasticSearch та MongoDB.

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

Запитання: Ви удосконалили модель інтеграційної шини даних. Що таке інтеграційна шина, і для чого вона потрібна?

Відповідь: Дякую за запитання. Запропонована модель інтеграційної шини даних (ІШД) реалізується на основі сервіс-орієнтованої архітектури (SOA) та забезпечує інтеграцію програмних компонентів через стандартизовані сервісні інтерфейси. ІШД виступає шаблоном та центральним елементом ІКС, який забезпечує обмін даними між сервісами SIEM-системи та зовнішніми компонентами через сервісні інтерфейси і шлюзи доступу. Таким чином, модель інтеграційної шини даних, дозволяє розподілити навантаження на послуги та гарантує безперервність обміну даними для ефективного функціонування системи корелювання подій та управління ІТ-інцидентами.

Запитання: Запропонована вами модель забезпечує обмін даними між сервісами SIEM-системи. Що ви розумієте під визначенням «сервіси»?

Відповідь: Дякую за запитання. Встановлено, що для ефективного функціонування системи корелювання подій та управління ІТ-інцидентами на ОКІ необхідно забезпечити безперервне надання сервісів SIEM-систем. Під сервісами розуміються послуги, що надаються SIEM-системами. Основним завданням ІШД є визначення режимів функціонування сервісів і формування оптимального порядку їх оброблення з урахуванням рівня критичності, що дає змогу мінімізувати втрати часу на очікування обслуговування та простої каналів.

3. Павленко П.М., д.т.н., проф., професор кафедри організації авіаційних перевезень КАІ.

Запитання: У першому розділі дисертаційної роботи ви провели аналіз 16 SIEM-систем за 18 критеріями. Де були взяті критерії? І чи всім критеріям відповідає розроблена вами система?

Відповідь: Дякую за запитання. Так, у першому розділі систематизовано

та проведено детальний аналіз 16 SIEM-систем за 18 запропонованими авторськими критеріями. Зокрема розглянуто їх функціональні можливості, принципи роботи, а також виконано порівняльний аналіз переваг і недоліків використання та відповідності міжнародним стандартам і специфікаціям. Результати дослідження показали, що системи відповідають більшості визначених критеріїв, однак відрізняються за вартістю, рівнем підтримки хмарних середовищ та можливостями подальшої інтеграції. На основі проведеного аналізу доведено доцільність розроблення універсальної системи корелювання подій та управління ІТ-інцидентами, яка буде відповідати всім зазначеним критеріям і поєднувати переваги існуючих SIEM-рішень.

Запитання: Дисертаційна робота має назву «Системи корелювання подій та управління ІТ-інцидентами на ОКІ». Де саме в роботі відображено процес управління ІТ-інцидентами?

Відповідь: Дякую за запитання. Для формалізації процесів управління ІТ-інцидентами на ОКІ в 4 розділі роботи представлено інформаційну технологію управління ІТ-інцидентами, що базується на використанні структурно-аналітичної моделі оброблення даних, онтологіко-реляційного сховища даних та інтеграційної шини даних. Експериментальне дослідження реалізації зазначеної інформаційної технології в складі системи корелювання подій та управління ІТ-інцидентами на ОКІ підтвердило її відповідність вимогам, сформованим на основі аналізу міжнародних стандартів і найкращих світових практик створення систем управління ІТ-інцидентами.

4. Охріменко Т.О., к.т.н., ст. дослідник, заступник декана з наукової роботи ФКНТ КАІ.

Запитання: В моделі оброблення даних ви використовували базу NSL-KDD, чому саме її? Чи є аналоги?

Відповідь: Дякую за запитання. Датасет NSL-KDD було обрано, оскільки він є одним із найпоширеніших відкритих наборів даних для досліджень систем виявлення вторгнень. Він містить структуровані характеристики мережевого трафіку та різні типи атак, такі як DoS, U2R, R2L та Probe, що дозволяє ефективно навчати моделі для виявлення аномалій і краще відповідає завданням розроблюваної системи корелювання подій та управління ІТ-інцидентами. Крім того, цей датасет очищений від дубльованих записів, що підвищує якість навчання моделі. Існують також аналоги, наприклад, UNSW-NB15, CICIDS2017 та KDD Cup 1999, які містять інші набори мережевих атак і також використовуються для досліджень у сфері інформаційних технологій.

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

Запитання: В моделі інтеграційної шини даних є процедура визначення критичності сервісів. Що таке критичність сервісів?

Відповідь: Дякую за запитання. Критичність сервісів – це ступінь важливості сервісу для функціонування системи, яка визначає пріоритет його обробки та рівень впливу на систему у випадку відмови. Для цього на етапі 2-3 моделі, черга обслуговування сервісів визначається за рівнем їх критичності з використанням підходу FMECA.

Запитання: В темі дисертаційної роботи є управління ІТ-інцидентами на ОКІ. Що ви розумієте під поняттям ІТ-інциденту та як він відрізняється від поняття кіберінциденту?

Відповідь: Дякую за запитання. ІТ-інцидент – це подія в інформаційній системі, що спричиняє або може спричинити порушення роботи ІТ-сервісів та потребує оперативного виявлення і реагування для відновлення їх нормального функціонування. Це може бути: відмова сервера або мережевого обладнання, недоступність бази даних або веб-сервісу, перевищення часу відповіді системи, помилки конфігурації. Кіберінцидент є різновидом ІТ-інциденту, який виникає внаслідок кібератак або інших загроз інформаційній безпеці та впливає на конфіденційність, цілісність або доступність інформації. До них відносять: DoS або DDoS-атаки, несанкціонований доступ до системи, витік або модифікація даних.

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

Запитання: Розкажіть детально, в чому практична цінність дисертаційної роботи? Що саме реалізовано?

Відповідь: Дякую за запитання. Практична цінність роботи полягає у такому: 1) на основі дата сету NSL-KDD навчено нейронну мережу з точки зору виявлення аномалій типу DoS, U2R, R2L та Probe; 2) створено методику зберігання та класифікації даних, яка дозволяє сервісу індексації отримувати доступ до зовнішніх сховищ даних, проводити масштабування, агрегацію, аналіз, збір закономірностей та забезпечувати високу швидкість пошуку; 3) сформовано специфікацію реалізації SIEM-систем на ОКІ, у вигляді основних та додаткових вимог; 4) розроблено спеціальний програмний застосунок, який можна використовувати для управління ІТ-інцидентами, які виникають в КІ і мають вплив на критично важливі ресурси (КВР).

Запитання: Де саме можна використовувати ваші результати? Чи є відповідні акти впровадження?

Відповідь: Дякую за запитання. Результати дисертації впроваджені і використовуються у діяльності НДЛ протидії кіберзагрозам авіаційної галузі КАІ, а також у навчальному процесі кафедри комп'ютерних наук та кібербезпеки Волинського національного університету імені Лесі Українки для підвищення ефективності підготовки фахівців з ІТ. Крім того, отримані в дисертаційній роботі результати можуть бути використані в галузі інформаційних технологій для забезпечення стійкого функціонування хмарної інформаційної інфраструктури (у т.ч. критичної) в умовах деструктивних інформаційно-технічних впливів.

7. Смірнов О.А., д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнського національного технічного університету.

Запитання: Як у вас реалізована інформаційна технологія управління ІТ-інцидентами?

Відповідь: Дякую за запитання. Інформаційна технологія базується на використанні структурно-аналітичної моделі оброблення даних, онтологіко-реляційного сховища даних та інтеграційної шини даних. Вхідними даними

інформаційної технології є потоки подій безпеки (журнали, мережеві та системні повідомлення), параметри структурно-аналітичної моделі оброблення даних, множини баз даних і облікових задач (DB, TS), а також множина сервісів системи (SR). В процесі функціонування здійснюється збирання, індексація та зберігання подій, їх корелювання й аналітичне оброблення, розрахунок часових характеристик, визначення рангу критичності сервісів і формування керуючих впливів. Реалізація зазначених процесів забезпечується нейронною мережею для виявлення аномалій, методикою зберігання та класифікації даних, специфікацією побудови SIEM-системи та програмним застосунком управління IT-інцидентами. Результатом реалізації інформаційної технології є: виявлені IT-інциденти та аномалії, сформовані пріоритети їх оброблення, аналітичні звіти та візуалізовані результати моніторингу (дашборди), забезпечення взаємодії з CERT/CSIRT, практичні рекомендації щодо реагування та підвищення рівня захищеності ОКІ.

Висновок наукового керівника

Науковий керівник – **к.т.н., доцент, доцент кафедри комп'ютерних інформаційних технологій КАІ Сидоренко Вікторія Миколаївна**.

Науковий керівник охарактеризувала актуальність обраної теми дослідження, поставлені та виконані завдання для досягнення мети щодо проведеного наукового дослідження.

Наголосила, що дисертаційна робота є завершеним самостійним науковим дослідженням і готова до захисту. У процесі виконання дослідження здобувачка опрацювала значний обсяг вітчизняних і зарубіжних джерел, що дало змогу узагальнити сучасний світовий досвід у відповідній галузі.

У процесі дослідження здобувачкою сформульовано низку важливих наукових та практичних результатів. Зокрема, удосконалено структурно-аналітичну модель оброблення даних, розроблено модель онтологіко-реляційного сховища даних, удосконалено модель інтеграційної шини даних, а також запропоновано систему корелювання подій та управління IT-інцидентами, яка дає змогу формалізувати інформаційну технологію управління IT-інцидентами на ОКІ відповідно до вимог міжнародних стандартів та найкращих світових практик.

Практична цінність роботи полягає у навчанні нейронної мережі для виявлення кібератак, створенні методики зберігання та класифікації даних, формуванні специфікації реалізації SIEM-систем, а також розробці програмного застосунку для управління IT-інцидентами, які виникають в КІ і мають вплив на КВР.

Під час виконання роботи здобувачка продемонструвала достатній рівень теоретичної підготовки та наукової кваліфікації, здатність до самостійного розв'язання складних наукових завдань. Вона систематично підвищує свій освітній і професійний рівень, бере участь у науково-дослідних роботах, має публікації у фахових виданнях та доповіді на наукових конференціях.

Науковий керівник зазначила, що дисертаційна робота є завершеною

науковою працею, спрямованою на розв’язання актуальної наукової задачі, та запропонував затвердити позитивний висновок щодо наукової новизни і практичної значущості одержаних результатів, а також рекомендувати роботу до захисту на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології».

Обговорення дисертаційного дослідження

Під час обговорення виступили:

1. Нечипорук О.П., д.т.н., проф., завідувач кафедри інтелектуальних кібернетичних систем КАІ, відзначила високий рівень теоретичного узагальнення, представлений у дисертаційній роботі. У своєму виступі вона підкреслила актуальність дослідження, спрямованого на розроблення системи корелювання подій та управління ІТ-інцидентами на ОКІ, а також відзначила вдале поєднання методів оброблення даних, моделей інтеграційної шини та онтологіко-реляційного сховища даних в інформаційну технологію. Було наголошено, що запропоновані моделі можуть бути використані для підвищення ефективності виявлення аномалій та забезпечення надійності функціонування хмарних ІКС. З огляду на викладене, Нечипорук О.П. зазначила, що робота Жигаревич О.К. відповідає вимогам МОН України та може бути рекомендована до захисту на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології».

2. Павленко П.М. д.т.н., проф., професор кафедри організації авіаційних перевезень КАІ акцентував увагу на науковій новизні дисертації, зокрема на удосконаленні структурно-аналітичної моделі оброблення даних, розробленні моделі онтологіко-реляційного сховища даних, удосконаленні моделі інтеграційної шини даних, а також розробленні системи корелювання подій та управління ІТ-інцидентами. Зазначив, що запропонована система дозволяє формалізувати інформаційну технологію управління ІТ-інцидентами на об’єктах критичної інфраструктури відповідно до вимог міжнародних стандартів та найкращих світових практик. Крім того, Павленко П.М. зазначив, що дисертаційна робота Жигаревич О.К. відповідає вимогам МОН України та може бути рекомендована до захисту на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології».

3. Савченко А.С., д.т.н., проф., завідувачка кафедри комп’ютерних інформаційних технологій КАІ підкреслила, що дисертаційна робота вирізняється комплексним підходом до вирішення поставленої наукової задачі – від аналізу сучасних підходів до управління ІТ-інцидентами до розроблення моделей та загальної системи. Було відзначено, що проведені експериментальні дослідження підтверджують ефективність запропонованих рішень для підвищення якості оброблення даних та забезпечення безперервності функціонування систем управління ІТ-інцидентами на ОКІ. На основі вищенаведеного, Савченко А.С. зазначила, що дисертаційна робота Жигаревич О.К. є завершеним науковим дослідженням, відповідає вимогам МОН України та може бути рекомендована до захисту на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології».

4. Смірнов О.А., д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнського національного технічного університету, відзначив практичну цінність результатів дисертаційної роботи. Було зазначено, що в межах дослідження на основі датасету NSL-KDD навчено нейронну мережу для виявлення аномалій типів DoS, U2R, R2L та Probe, розроблено методику зберігання та класифікації даних, сформовано специфікацію реалізації SIEM-систем на ОКІ та створено програмний застосунок для управління ІТ-інцидентами, що впливають на критично важливі ресурси. Наголосив, що результати дисертації впроваджено у діяльність НДЛ протидії кіберзагрозам авіаційної галузі КАІ та використовуються у навчальному процесі Волинського національного університету імені Лесі Українки. Як висновок, Смірнов О.А. зазначив, що дисертаційна робота Жигаревич О.К. відповідає вимогам МОН України та може бути рекомендована до захисту на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології».

ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації Жигаревич Оксани Костянтинівни на тему «Система корелювання подій та управління ІТ-інцидентами на об'єктах критичної інфраструктури», поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології».

1. Актуальність теми дослідження. Сучасна інформаційна інфраструктура характеризується високою складністю, масштабністю та взаємопов'язаністю значної кількості апаратних і програмних компонентів, що потребують постійного моніторингу та контролю їх функціонування. Особливої уваги набуває забезпечення безперервності роботи та стабільного функціонування об'єктів критичної інфраструктури (ОКІ), до яких належать енергетичні системи, гідротехнічні споруди, транспортні вузли, аеродроми, хімічні виробництва та інші життєво важливі об'єкти. Порушення їх функціонування внаслідок збоїв інформаційно-комунікаційних систем (ІКС) або відхилень у роботі ІТ-сервісів може призвести до значних економічних втрат і критичних наслідків.

В умовах зростання складності ІКС особливого значення набувають процеси своєчасного виявлення, аналізу та управління ІТ-інцидентами, що виникають унаслідок порушення роботи сервісів, ресурсів або інформаційних процесів. Існуючі інструментальні рішення, зокрема SIEM-системи, забезпечують збирання та аналітичну обробку подій, проте не повною мірою враховують специфіку функціонування ОКІ, потреби масштабованості та адаптації до конкретних умов експлуатації.

Наявність значної кількості програмно-технічних засобів не забезпечує комплексного підходу до управління ІТ-інцидентами, що обумовлює необхідність розроблення інтегрованої системи корелювання подій та підтримки

прийняття управлінських рішень. Отже, розроблення системи корелювання подій та управління ІТ-інцидентами на ОКІ є актуальною науково-технічною задачею, що має важливе теоретичне та практичне значення.

2. Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційна робота є складовою частиною наукових досліджень, що проводяться в КАІ та спрямовані на розвиток інформаційних технологій моніторингу, аналізу подій та управління ІТ-інцидентами в ІКС ОКІ.

Теоретичні і практичні положення дисертаційної роботи були використані в науково-дослідній роботі (НДР), яка виконувались у КАІ, а саме: «Методи, моделі та програмні засоби управління інцидентами кібербезпеки в критичній інфраструктурі держави», номер держреєстрації (д.р. № 0125U000624, роки виконання 2025-2026).

У межах НДР здобувачкою було розроблено структурно-аналітичну модель оброблення даних для інтелектуалізованого виявлення аномалій та запропоновано модель інтеграційної шини даних для розподілу навантаження.

Дослідження виконано в межах наукового напряму, пов'язаного з розробленням моделей оброблення даних, інтелектуалізованих методів виявлення аномалій, побудови інтегрованих систем корелювання подій та підтримки прийняття управлінських рішень в умовах підвищених вимог до надійності, масштабованості та безперервності функціонування ІКС.

Отримані результати спрямовані на формування науково-методичного підґрунтя створення інтегрованих систем моніторингу та управління ІТ-інцидентами, що забезпечують підвищення стійкості та ефективності функціонування ІКС ОКІ.

3. Мета і завдання дослідження. Метою дисертаційного дослідження є забезпечення можливості управління ІТ-інцидентами на ОКІ на основі розроблення та удосконалення моделей і синтезу системи управління інцидентами.

Відповідно до мети в роботі було поставлено і вирішено такі завдання:

– провести аналіз сучасних підходів до управління ІТ-інцидентами на ОКІ для виявлення їх переваг та недоліків;

– удосконалити структурно-аналітичну модель оброблення даних для інтелектуалізованого виявлення аномалій у хмарних системах ІКС;

– розробити модель онтологіко-реляційного сховища даних для зберігання та оброблення великих масивів інформації;

– удосконалити модель інтеграційної шини даних для розподілу навантаження та захищеного обміну даними;

– на основі запропонованих моделей розробити систему корелювання подій та управління ІТ-інцидентами на ОКІ;

– створити спеціалізоване програмне забезпечення та провести верифікацію розроблених у роботі моделей та системи.

4. Об'єктом дослідження є процеси управління ІТ-інцидентами на ОКІ.

5. Предметом дослідження є моделі, системи і засоби управління ІТ-інцидентами на ОКІ.

6. Методи досліджень. Проведені дослідження базуються на сучасних методах: математичної логіки, на основі якої розроблено модель онтологіко-реляційного сховища даних; теорії множин, для формалізації сукупності різноманітних баз даних та чинникових ознак, у вигляді основних критеріїв відбору; теорії штучного інтелекту, на основі якої, відбувалось навчання нейронної мережі для виявлення аномалій дата сету NSL-KDD; теорії комп'ютерних мереж, для розробки моделі інтеграційної шини даних; теорії системного та структурного аналізу, для представлення моделі оброблення даних. та обробки результатів експериментів і верифікації ефективності розроблених моделей та системи.

7. Наукова новизна дослідження: полягає у розробленні моделей оброблення даних, онтологіко-реляційного зберігання інформації та інтеграційної шини даних, а також у створенні системи корелювання подій і управління ІТ-інцидентами на ОКІ, що забезпечує підвищення ефективності виявлення аномалій, оптимізацію зберігання й оброблення великих масивів даних, розподіл навантаження між сервісами та безперервність інформаційного обміну відповідно до вимог міжнародних стандартів управління ІТ-інцидентами. Наукові результати базуються на таких основних положеннях.

уперше:

– розроблено модель онтологіко-реляційного сховища даних, яка за рахунок попередньої індексації та синтезу двох різних баз даних (Elasticsearch та MongoDB) з відповідними характеристиками, дає можливість покращити зручність у зберіганні та класифікації даних, а також забезпечити високу швидкість пошуку та отримання великих обсягів інформації;

удосконалено:

– структурно-аналітичну модель оброблення даних, яка завдяки формулюванню команд для передачі керування програмному клієнту ІКТ, додатковій обробці метаданих у хмарній системі та інтелектуалізованому виявленню сигнатур, дозволяє підвищити ефективність виявлення аномалій в хмарних ІКС;

– модель інтеграційної шини даних, яка за рахунок декомпозиції функціональності сервісів (кожен з яких відповідає за окреме завдання і може працювати ізольовано від інших) та визначення критичності сервісів, дозволяє розподілити навантаження на послуги та гарантує безперервність обміну даними для ефективного функціонування системи корелювання подій та управління ІТ-інцидентами;

отримала подальший розвиток :

– система корелювання подій та управління ІТ-інцидентами, яка за рахунок використання розроблених моделей обробки даних, онтологіко-реляційного сховища даних та інтеграційної шини даних, дає змогу формалізувати інформаційну технологію, що реалізує процеси управління ІТ-інцидентами на ОКІ згідно вимог міжнародних стандартів та найкращих світових практик щодо створення систем управління ІТ-інцидентами.

8. 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 мети 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.

9. Теоретичне значення. Теоретичне значення роботи полягає у розвитку наукових положень щодо побудови моделей оброблення, зберігання та інтеграції даних у системах корелювання подій і управління ІТ-інцидентами на ОКІ. Отримані результати розширюють уявлення про організацію інформаційних процесів моніторингу та аналізу подій в розподілених ІКС, формують теоретичне підґрунтя для створення інтегрованих систем підтримки прийняття рішень у сфері управління ІТ-інцидентами та можуть бути використані при подальших дослідженнях у галузі інформаційних технологій.

10. Практичне значення та використання результатів дисертаційного дослідження. Отримані в дисертаційній роботі результати можуть бути використані в галузі інформаційних технологій для забезпечення стійкого функціонування хмарної інформаційної інфраструктури (у т.ч. критичної) в умовах деструктивних інформаційно-технічних впливів, зокрема у діяльності:

– ТОВ «AxxonSoft» у практичній діяльності підприємства використано розроблену систему корелювання подій та управління ІТ-інцидентами та апробовано розроблений спеціалізований програмний застосунок, який може використовуватися для управління ІТ-інцидентами, що виникають на ОКІ та впливають на КВР (акт про впровадження від 11.03.2026).

– НДЛ протидії кіберзагрозам авіаційної галузі КАІ (акт про впровадження від 12.02.2024),

– кафедрою комп'ютерних наук та кібербезпеки Волинського національного університету імені Лесі Українки у навчальному процесі при підвищенні ефективності підготовки фахівців з ІТ (акт про впровадження від 21.12.2023).

11. Особистий внесок здобувача. Дисертація «Система корелювання подій та управління ІТ-інцидентами на об’єктах критичної інфраструктури», Жигаревич Оксани Костянтинівни є самостійною науковою працею, в якій наведено теоретичні положення і висновки, власні ідеї та розробки автора, які дають змогу вирішити поставлені завдання. Усі висновки та практичні рекомендації, винесені на захист, розроблені дисертантом особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

12. Апробація результатів дослідження. Результати досліджень дисертаційної роботи доповідалися та обговорювалися на таких наукових конференціях: «Cybersecurity Providing in Information and Telecommunication Systems» (CPITS), (Kyiv, 2023-2024); «International Conference on Dependable Systems, Services and Technologies» DESSERT-2024 (Athens, Greece 2023), «International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» IDAACS-2023 (Dortmund, Germany, 2023); «International Conference on Conflict Management in Global Information Networks» CMiGiN, (Kyiv, 2022, 2025); «Information Technology and Implementation» IT&I, (Kyiv, 2022); «Системи та засоби штучного інтелекту» (Київ, 2021); «АВІА-2023» (Київ, 2023); «Кіберзахист особи, суспільства і держави» (с. Велятино, 2024) та ін.

13. Публікації. Основні положення дисертації опубліковано у 22 наукових працях, у тому числі: 19 наукових статтях, серед них 11 – у закордонних рецензованих виданнях, які входять до наукометричної бази даних Scopus, 8 – у вітчизняних фахових наукових журналах, а також 3 публікації у матеріалах конференцій різного рівня.

Список опублікованих праць за темою дисертації

Статті у наукових фахових виданнях України:

1. Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., Смірнова Т.В. Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2023. Т. 3. № 19. С. 176-196. DOI: https://doi.org/10.28925/2663-4023.2023.19.176196

Особистий внесок автора – теоретичне обґрунтування моделі онтологіко-реляційного сховища даних, моделі інтеграційної шини даних та системи корелювання подій та управління ІТ-інцидентами на ОКІ.

2. 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. DOI: https://doi.org/10.18372/2073-4751.75.18014

Особистий внесок автора – розроблення етапів реалізації моделі інтеграційної шини даних.

3. Жигаревич О.К., Бердибаєв Р.Ш., Сидоренко В.М., Положенцев А.А., Кримська А.О. Модель онтологіко-реляційного сховища даних для функціонування хмарної SIEM-системи. *Проблеми інформатизації та управління*. 2023. Т. 4. № 76. С. 17-27. DOI: https://doi.org/10.18372/2073-4751.76.18236.

Особистий внесок автора – розроблення основних етапів реалізації моделі онтологіко-реляційного сховища даних).

4. Дмитрук Я.В., Гришанович Т.О., Глинчук Л.Я., Жигаревич О.К. Кібервійна як різновид інформаційних війн. Захист кіберпростору України. *Кібербезпека: освіта, наука, техніка*. 2022. Т. 4. №16. С. 28-36. DOI:

https://doi.org/10.28925/2663-4023.2022.16.2836.

Особистий внесок автора – дослідження інформаційних систем як складової інформаційної війни для критичних об'єктів.

5. Жигаревич О.К., Медведєв М.В. Інформаційна система «Студент-ФКНІТ» засобами PHP. *Комп'терно-інтегровані технології: освіта, наука, виробництво*. 2017. № 26. С. 88-92.

Особистий внесок автора – розробка та впровадження інформаційної системи для освітніх потреб.

6. Жигаревич О.К., Котлярець В.В., Луць А.Р. Модель екосистеми навчального програмного забезпечення. *Комп'терно-інтегровані технології: освіта, наука, виробництво*. 2017. № 26. С. 167-177.

Особистий внесок автора – побудова структурної моделі екосистеми, що враховує взаємодію між різними типами інформаційних засобів.

7. Жигаревич О.К., Мельник В.М., Мельник К.В. Підтримка оголошеної/встановленої комунікації в мережі через стандартні сокети API. *Комп'терно-інтегровані технології: освіта, наука, виробництво*. 2015. № 19. С. 23-27.

Особистий внесок автора – дослідження методів підтримки мережевої комунікації між компонентами інформаційних систем.

8. Мельник К.В., Мельник В.М., Багнюк Н.В., Жигаревич О.К., Климюк М. Система попереднього відбору кандидатів на основі нечіткої логіки. *Комп'терно-інтегровані технології: освіта, наука, виробництво*. 2015. № 19. С. 114-120.

Особистий внесок автора – дослідження методів нечіткої логіки для розробки інформаційної системи попереднього відбору кандидатів.

Статті в іноземних виданнях:

9. Pobochenko L., Prokopieva A., Zhyharevych O., Gavrylko O., Panikar G., Gavrilko T. Risks of investing in FinTech at the global and national levels. CEUR Workshop Proceedings. Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2025), June 20 - 22, 2025, Kyiv, Ukraine, 2025. Vol. 4024. P. 468-478. URL: https://ceur-ws.org/Vol-4024/paper30.pdf. (Scopus) Q4, ISSN 1613-0073.

Особистий внесок автора – дослідження інформаційних ризиків на глобальному та національному рівнях ОКІ держави).

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. Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2024),* February 28, 2024, Kyiv, Ukraine, 2024. Vol. 3654. P. 343-354. URL: https://ceur-ws.org/Vol-3654/paper29.pdf (*Scopus*) Q4, ISSN 1613-0073.

Особистий внесок автора – розроблення основних етапів реалізації моделі онтологіко-реляційного сховища даних, формування множини сучасних баз даних, критеріїв та задач.).

11. Gnatyuk S., Berdibayev R., Aleksander M., Sydorenko V., Zhyharevych O., Polozhentsev A. Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure. *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*. 2024. Vol. 213. P. 247-269. Springer, Cham. DOI: https://doi.org/10.1007/978-3-031-62213-7_12. (*Scopus*) Q3, ISSN 2367-4512.

Особистий внесок автора – розроблення етапів реалізації системи корелювання подій та управління IT-інцидентами на ОКІ.

12. Zdolbitska N., Ostapchuk O., Lavrenchuk S., Terletskyi T., Kaidyk O., Zhyharevych O. Business information system for forecasting raw material stocks for the production of flexible packaging. *2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Athens, Greece, 2024, P. 1-8. doi: 10.1109/DESSERT65323.2024.11122240. (*Scopus*), Q4.

Особистий внесок автора – дослідження інформаційних систем прогнозування.

13. Polozhentsev A., Gnatyuk S., Berdibayev R., Sydorenko V., Zhyharevych O. Novel Cyber Incident Management System for 5G-based Critical Infrastructures. *IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 2023, P. 1037-1041. DOI: 10.1109/IDAACS58523.2023.10348645. (Scopus), Q4, ISSN 2770-4262.

Особистий внесок автора – розроблення етапів реалізації системи корелювання подій та управління IT-інцидентами на ОКІ.

14. 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, Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2023)*, February 28, 2023, Kyiv, 2023, Vol. 3421, P. 206-213. URL: https://ceur-ws.org/Vol-3421/short6.pdf (Scopus) Q4, ISSN 1613-0073.

Особистий внесок автора – розроблення структурно-аналітичої моделі оброблення даних в хмарних ІКС.

15. Gnatyuk S., Zhaksigulova D., Zhyharevych O., Ospanova D., Chuba I. Studies on WSN Models for IoT-based Monitoring Systems in the Critical Infrastructure of the State. *CEUR Workshop Proceedings, Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2023-II),* October 26, 2023, Kyiv, 2023, Vol. 3550, P. 167-180. URL: https://ceur-ws.org/Vol-3550/paper14.pdf (*Scopus*) Q4, ISSN 1613-0073.

Особистий внесок автора – дослідження моделей для систем моніторингу ОКІ держави.

16. Smirnov O., Sydorenko V., Aleksander M., Zhyharevych O., Yenchev S. Simulation of the cloud IoT-based monitoring system for critical infrastructures. *CEUR Workshop Proceedings, Proceedings of the 2nd International Conference on Conflict Management in Global Information Networks (CMiGiN 2022)*, November 30, 2022, Kyiv, 2023, Vol. 3530, P. 256-265. URL: https://ceur-ws.org/Vol-

3530/paper25.pdf (*Scopus*) Q4, ISSN 1613-0073.

Особистий внесок автора – дослідження хмарних систем моніторингу ОКІ на базі Інтернету речей.

17. 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*, Proceedings of the: Information Technology and Implementation (IT&I2022), November 30 - December 02, 2022, Kyiv, Ukraine, Vol. 3347, Paper 20, P.234-245. URL: https://ceur-ws.org/Vol-3347/Paper_20.pdf (*Scopus*) Q4, ISSN 1613-0073.

Особистий внесок автора – дослідження методик визначення рівня критичності галузевих ІКС.

18. Melnyk V., Bahnyuk N., Melnyk K., Zhyharevych O., Panasyuk N. Implementation of the simplified communication mechanism in the cloud of high performance computations. *East-European journal of Enterprise Technologies*. Kharkiv, 2017. No 2/2/86. P. 24-32. DOI: 10.15587/1729-4061.2017.98896 (*Scopus*) Q3, ISSN 1729-3774.

Особистий внесок автора – аналіз механізмів зв'язку в хмарних системах.

19. Melnyk V., Pekh P., Melnyk K., Bahnyuk N., Zhyharevych O. Design and implementation of interdomain communication mechanism for high performance data processing, *East-European journal of Enterprise Technologies*. Kharkiv, 2016. No 1(9). P. 10-15. DOI: 10.15587/1729-4061.2016.60629 (Scopus) Q3, ISSN 1729-3774.

Особистий внесок автора – аналіз моделей оброблення даних.

Публікації, які додатково відображають наукові результати дисертації:

20. Сидоренко В., Положенцев А., Юдін О., Жигаревич О. Функціональна модель визначення критичності галузевих інформаційно-телекомунікаційних систем. *ABIA-2023:* XVI міжнар. наук.-техніч. конф., 18-20 квітня 2023 р.: тези доп., Київ: НАУ, 2023. С. 16.14-16.17.

21. Здолбіцька Н.В., Ліщина Н.М., Лавренчук С.В., Давиденко Н.В., Жигаревич О.К. Інтелектуальна інформаційна система «робот-гід». Матеріали Міжнародної наукової молодіжної школи *«Системи та засоби штучного інтелекту»* 28.11.2021р. Київ, 2021. С. 19-21.

22. 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*: наук.-практ. конф., с. Велятино, 24-27 січня 2024 р.: тези доп., Київ: НАУ, 2024. С. 14-15.

14. Структура дисертації та її обсяг. Дисертація складається з анотації, вступу, чотирьох розділів, висновків, додатків, списку використаних джерел .

Загальний обсяг роботи 196 сторінок, із них – 153 сторінки основного тексту, 90 рисунків, 9 таблиць, 2 додатки. Список використаних джерел налічує 101 найменування.

15. Оцінка мови та стилю дисертації. Дисертація викладена науковим стилем сучасною українською мовою, із використанням усталеної термінології галузі «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 змісту дисертації спеціальності, за якою вона подається до захисту. Дисертація відповідає паспорту наукової спеціальності 05.13.06 «Інформаційні технології», за якою вона подається до захисту, а саме: П.2. Розроблення інформаційних технологій для аналізу та синтезу структурних, інформаційних і функціональних моделей об'єктів і процесів, що автоматизуються. П.4. Дослідження та побудова інформаційних технологій для розроблення та впровадження баз і сховищ даних, баз знань і систем комп'ютерної підтримки рішень в автоматизованих системах і мережах. П.6. Розроблення теоретичних і прикладних основ побудови інформаційних технологій для автоматизації функціональних завдань керування, аналізу й оцінювання ефективності автоматизованих систем переробки інформації й управління. Зміст дисертації, отримані наукові результати та запропоновані моделі відповідають зазначеним напрямам досліджень і спрямовані на розвиток інформаційних технологій оброблення даних, побудови сховищ даних та автоматизації процесів управління ІТ-інцидентами.

17. Характеристика особистості здобувача. Під час підготовки дисертаційної роботи Жегаревич О.К. проявила себе як творчий дослідник і науковець, здатний самостійно на високому науково-методичному рівні вирішувати наукові та практичні завдання. Вона у повній мірі володіє сучасними методами аналізу, має належний рівень теоретичної та практичної підготовки.

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

Жигаревич О.К. чітко 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 виданнях та впровадженням у практику.

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Жигаревич Оксани Костянтинівни на тему «Система корелювання подій та управління ІТ-інцидентами на об'єктах критичної інфраструктури».

2. Вважати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація

Жигаревич О.К. відповідає спеціальності 05.13.06 – «Інформаційні технології» та вимогам нормативних документів МОН України до кандидатських дисертацій (зокрема, пп. 9, 11, 12, 13, 14 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. №567 з подальшими змінами і доповненнями).

3. Рекомендувати дисертаційну роботу «Система корелювання подій та управління ІТ-інцидентами на об'єктах критичної інфраструктури», подану Жигаревич О.К. на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.06 – «Інформаційні технології», до захисту у спеціалізованій вченій раді Д 26.062.01 в КАІ.

4. Результати голосування присутніх на засіданні докторів наук та кандидатів наук:

– всього: «за» – 19, «проти» – немає, «утрималося» – немає; в тому числі за профілем поданої на розгляд дисертації: «за» – 19, серед них: 8 докторів наук та 11 кандидатів наук зі спеціальності.

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 Олена ТОЛСТІКОВА

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