ЗАТВЕРДЖУЮ:
в.о. президента Державного університету «Київський авіаційний інститут»

_____Ксенія СЕМЕНОВА

«__» _травня_ 2025 року

ВИСНОВОК

Державного університету «Київський авіаційний інститут» (далі – КАІ) про наукову новизну, теоретичне та практичне значення результатів дисертації Петляк Наталії Сергіївни на тему: «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах», поданої на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека»

ВИТЯГ

із протоколу № 8 розширеного засідання кафедри кібербезпеки КАІ від 08 травня 2025 року

Присутні на засіданні науково-педагогічні працівники кафедри кібербезпеки:

Ахрамович Володимир Миколайович – д.т.н., професор, професор кафедри.

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

Петренко Андрій Борисович – к.т.н., доцент, доцент кафедри.

Толбатов Андрій Володимирович – к.т.н., доцент, доцент.

Петрик Валентин Михайлович – к.держ. управл., доцент, доцент кафедри.

Гулак Наталія Костянтинівна – к.т.н., доцент кафедри.

Висоцька Олена Олександрівна – к.т.н., доцент, доцент кафедри.

Коваленко Юлія Борисівна – к.пед.н., доцент, доцент кафедри.

Лозова Ірина Леонідівна – старший викладач кафедри.

Прокопенко Олена Володимирівна – старший викладач кафедри.

Бурбела Ольга Олександрівна – старший викладач кафедри.

Вишневська Наталія Сергіївна – старший викладач кафедри.

Мазур Яна Сергіївна – асистент кафедри.

Якимчук Євгеній Анатолійович – асистент кафедри.

Терейковський Олег Ігорович – аспірант кафедри.

Марченко Ярослав Володимирович– асистент кафедри.

Самофалов Дмитро Валентинович – асистент кафедри.

Присутні на засіданні науково-педагогічні працівники інших кафедр КАІ:

Гнатюк Сергій Олександрович – д.т.н., професор, професор кафедри комп'ютерних інформаційних технологій.

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

Головуючий на засіданні: Міщенко Андрій Віталійович – д.т.н., професор, професор кафедри технічного захисту інформації, гарант освітньо-наукової програми 125 «Кібербезпека».

Козловський Валерій Валерійович– д.т.н., професор, завідувач кафедри технічного захисту інформації.

Одарченко Роман Сергійович – д.т.н., проф., декан факультету аеронавігації, електроніки та телекомунікацій.

Лазаренко Сергій Володимирович – д.т.н., професор, професор кафедри технічного захисту інформації.

Іванченко Ігор Сергійович – к.т.н., доцент, доцент кафедри технічного захисту інформації.

Скворцов Сергій Олександрович – к.т.н., доцент, доцент кафедри технічного захисту інформації.

Щербак Тетяна Леонідівна – к.т.н., доцент, доцент кафедри технічного захисту інформації.

Рябова Любов Володимирівна – асистент кафедри технічного захисту інформації.

Присутні на засіданні науково-педагогічні працівники інших закладів освіти:

Кльоц Юрій Павлович – к.т.н., доцент, завідувач кафедри кібербезпеки Хмельницького національного університету.

Корченко Олександр Григорович – д.т.н., професор, перший проректор Державного університету інформаційно-комунікаційних технологій.

Терейковський Ігор Анатолійович – д.т.н., професор, професор кафедри системного програмування і спеціалізованих комп'ютерних систем факультету прикладної математики КПІ ім. Ігоря Сікорського.

Терейковська Людмила Олексіївна – д.т.н., професор, професор кафедри інформаційних технологій проєктування та прикладної математики Київського національного університету будівництва і архітектури.

Лаптєв Олександр Анатолійович – д.т.н., старший науковий співробітник, доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Порядок денний:

Обговорення дисертаційного дослідження аспірантки кафедри кібербезпеки КАІ ПЕТЛЯК Наталії Сергіївни на тему «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах», поданої на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології», за спеціальністю 125 «Кібербезпека».

Дисертація виконувалась на кафедрі кібербезпеки Факультету комп'ютерних наук та технологій КАІ. Тема дисертації «Методи та засоби виявлення аномального трафіку у загальнодоступних комп'ютерних мережах» затверджена на засіданні Вченої ради Факультету кібербезпеки, комп'ютерної та програмної інженерії (протокол № 9, від 28 листопада 2022 року). Уточнену редакцію теми «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах» дисертаційного дослідження затверджено на засіданні Вченої ради Факультету комп'ютерних наук та технологій (протокол №2, від 12 лютого 2025 року).

Наукові керівники: ЛАЗАРЕНКО Сергій Володимирович, д.т.н., професор, професор кафедри технічного захисту інформації Факультету комп'ютерних наук та технологій Державного університету «Київський авіаційний інститут»; КЛЬОЦ Юрій Павлович, к.т.н., доцент, завідувач кафедри кібербезпеки Факультету інформаційних технологій Хмельницького національного університету (на громадських засадах).

Виступили:

Доповідач Петляк Наталія Сергіївна 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 на підприємстві.

Автором здійснено всебічний аналіз сучасного стану безпеки інформаційно-комунікаційних систем в умовах зростання кількості та складності кіберзагроз. Особливу увагу приділено аналізу актуальних викликів, пов'язаних з виявленням аномалій у мережевому трафіку, які все частіше стають індикатором складних кібератак, зокрема таких, що здійснюються через вихідний трафік.

Аспіранткою проведено детальне дослідження існуючих моделей виявлення аномалій, серед яких розглянуто статистичні, поведінкові,

кластеризаційні моделі та моделі на основі машинного навчання. Виявлено їх обмеження щодо точності виявлення, чутливості до змін характеристик трафіку та неспроможності реагувати на нові загрози. На основі аналізу сучасного стану було визначено, що більшість існуючих підходів зосереджені на моніторингу вхідного трафіку, тоді як вихідний трафік залишається недостатньо дослідженим, попри його важливу роль у виявленні внутрішніх загроз, зокрема ботнет-активності та організації DDoS-атак. Тому актуальною задачею є розробка відповідних – моделі, методу, структурної системи, алгоритмічного забезпечення та програмного застосунку для ефективного виявлення аномального трафіку в інформаційно-комунікаційних системах, з акцентом на аналіз вихідного трафіку як одного з основних джерел внутрішніх загроз і потенційної зловмисної активності.

У дисертаційній роботі було проведено аналіз сучасних методів та моделей виявлення аномального трафіку в інформаційно-комунікаційних системах і моделей типового користувача та потенційного порушника, що стало відправною точкою в початку вдосконалення моделі сигнатури пакету з урахуванням інформативності полів заголовку та пакету щодо визначення їх аномальності, моделі процесу визначення аномального трафіку на основі самоподібності з урахуванням потенційних загроз та особливостей трафіку в інформаційно-комунікаційних системах, моделі процесу нечіткого визначення аномального трафіку, що враховує поведінку типового користувача та потенційного порушника.

Автором вперше розроблено гібридний метод виявлення аномального трафіку в інформаційно-комунікаційних системах в якому за рахунок інтеграції методу класифікації трафіку за ознаками, методу самоподібності та розробленої моделі процесу нечіткого виявлення дозволило динамічно формувати множини сигнатур при класифікації трафіку за ознаками та підвищити показники виявлення аномального трафіку.

На основі розроблених моделей та методу автор удосконалив структурну модель системи виявлення аномального трафіку в інформаційно-комунікаційних системах, що за рахунок інтегрування розробленого гібридного методу виявлення аномального трафіку в інформаційно-комунікаційних системах та динамічного варіювання множиною дозволених та заборонених з'єднань у режимі реального часу дозволило зменшити навантаження на процесор.

У дисертаційній роботі представлено програмний застосунок, що базується на вдосконалених моделях, розробленому гібридному методі та структурі системи виявлення аномального трафіку в інформаційно-комунікаційних системах. Програмний продукт забезпечує повний цикл обробки мережевого трафіку — від його захоплення до прийняття рішення щодо безпечності

з'єднання. Реалізоване програмне забезпечення дозволяє проводити глибокий аналіз вихідного трафіку в режимі реального часу.

Автором представлено, що розроблене програмне забезпечення було впроваджено в ТОВ «X-CITY», що підтверджується актом впровадження.

Структура та обсяг дисертації зумовлена метою і логікою дослідження та складається з анотації державною та англійською мовами, вступу, чотирьох розділів, які об'єднують 18 підрозділів, висновків, списку використаних джерел, додатків.

Запитання до здобувачки:

1. **АХРАМОВИЧ В. М.** д.т.н., професор, професор кафедри кібербезпеки.

Запитання: Чи розглядали ви інші методи аналізу трафіку, до прикладу машинне навчання?

Відповідь: Дякую за запитання. Машинне навчання потребує попереднього навчання та тестування, що потребує висококваліфікованих фахівців та обчислювальних ресурсів, використання застарілих наборів даних для навчання та тестування не завжди відображають реальні умови застосування. Саме тому використання таких методів недоцільне для аналізу трафіку публічних мереж.

Запитання: Чи враховували мертві зони інформаційно-комунікаційної мережі?

Відповідь: Дякую за запитання. Мертва зона не є критичною для аналізу вихідного мережевого трафіку, оскільки вона стосується фізичного рівня доступу до мережі, а не самого трафіку, що вже передається мережею.

2. **ТЕРЕЙКОВСЬКИЙ І. А.** д.т.н., професор, професор кафедри системного програмування і спеціалізованих комп'ютерних систем факультету прикладної математики КПІ ім. Ігоря Сікорського.

Запитання: Яким методом визначалась міра самоподібності трафіку?

Відповідь: Дякую за запитання. Для оцінки використовувався кореляційний метод оцінювання показника Херста. Виконується покомпонентний аналіз подібності сигнатур. Після оцінки окремих компонентів проводиться узагальнення отриманих результатів для всього набору. Результатом є загальна числова оцінка, що відображає ступінь самоподібності сигнатур в аналізованому інтервалі, причому більш високі значення свідчать про більшу подібність сигнатур. З отриманою оцінкою проводиться порівняння з встановленим пороговим значенням.

Запитання: Як саме проводився експеримент?

Відповідь: Дякую за запитання. Експеримент проводився в ізольованому сегменті мережі з реальним навантаженням. Все обладнання мало однакову апаратну конфігурацію. Кожен ПК відповідав за іншу IDPS систему. Було реалізовано чотири типи атак: масове вивантаження файлів, атака підбору

паролю, сканування портів, розсилка повідомлень у месенджерах. Маршрутизатор віддзеркалював трафік на всі системи одночасно. Під час експерименту аналізувалося навантаження на процесори пристроїв.

Запитання: Як формувалась тестова вибірка і який її розмір?

Відповідь: Дякую за запитання. Вибірка формувалась у локальному захищеному середовищі. Типовий дозволений трафік генерувався стандартними програмами імітуючи типового користувача. Аномальний трафік моделювався через імітацію атак, зокрема активна розвідка, підбір паролю, сканування. Загальний обсяг вибірки становив близько 1,5 млн записів, де близько 20% становив аномальний трафік.

3. **ФЕСЕНКО А. О.** к.т.н., доцент, декан ФКНТ КАІ.

Запитання: Який саме набір даних використовувався для оцінки роботи методу?

Відповідь: Дякую за запитання. Використовувався власний набір даних, сформований у контрольованому середовищі без впливу зовнішніх факторів. Дані збиралися за допомогою сніфера Snort, а елементи маркувалися як дозволені або аномальні.

Запитання: Які обмеження є в запропонованого методу?

Відповідь: Дякую за запитання. Метод орієнтований на аналіз трафіку публічних мереж. Зазвичай в таких мережах до 100-200 користувачів, тому перевірка на більших кількостях не проводилась.

Запитання: Чи можна цей метод застосувати для аналізу трафіку в стільникових мережах?

Відповідь: Дякую за запитання. Метод не було проаналізовано в стільниковій мережі. Однак, метод потенційно придатний для стільникових мереж. Оскільки принципи виявлення засновані на сигнатурах можуть бути адаптовані під трафік мобільного зв'язку.

4. **ІЛЬЄНКО А. В.** к.т.н., доцент, завідувач кафедри кібербезпеки.

Запитання: Які значення часових інтервалів використовували для визначення міри самоподібності?

Відповідь: Дякую за запитання. Часовий інтервал t_1-t_2 становить 120 с, який призначений для першої оцінки міри Херста. Часовий інтервал t_2-t_3 становить 12 с, як наступний інтервал для порівняння рівня подібності.

Після відповідей на запитання виступили:

Науковий керівник – д.т.н., професор, професор кафедри технічного захисту інформації ФКНТ, КАІ Лазаренко Сергій Володимирович,

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

Наголосив, що аспірант успішно виконав індивідуальний план наукової роботи та індивідуальний навчальний план. Підготовлена дисертація готова до захисту. У роботі опрацьовано досить багато різноманітного матеріалу, є достатня кількість наукових праць, які дозволили узагальнити широкий світовий досвід.

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

Дисертаційна робота є завершеною науковою працею, яка націлена на вирішення актуальної наукової задачі, що відповідає спеціальності 125 «Кібербезпека», а її автор, Петляк Наталія Сергіївна, заслуговує присудження ступеня доктора філософії, на підставі Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, який затверджено Постановою Кабінету Міністрів України № 44 від 12 січня 2022 року.

Науковий керівник (*на громадських засадах*) – к.т.н., доцент, завідувач кафедри кібербезпеки Факультету інформаційних технологій Хмельницького національного університету Кльоц Юрій Павлович

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

Аспірант успішно виконав індивідуальний план наукової роботи та індивідуальний навчальний план, а підготовлена дисертація відповідає вимогам і може бути рекомендована до захисту. У межах дослідження було опрацьовано значний обсяг різнопланового матеріалу, а також підготовлено достатню кількість публікацій, що засвідчують обґрунтованість узагальнень та врахування світового досвіду у сфері дослідження.

У процесі виконання наукової роботи здобувач продемонстрував належний рівень наукової компетентності та здатність до самостійного вирішення складних наукових завдань. Постійно працює над підвищенням свого освітнього й професійного рівня, активно займається науковими дослідженнями, бере участь у виконанні науково-дослідних проєктів, має наукові публікації та виступи на наукових конференціях.

Дисертаційна робота є завершеною науковою працею, яка націлена на вирішення актуальної наукової задачі, що відповідає спеціальності 125 «Кібербезпека», а її автор, Петляк Наталія Сергіївна, заслуговує присудження ступеня доктора філософії, на підставі Порядку присудження ступеня доктора

філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, який затверджено Постановою Кабінету Міністрів України № 44 від 12 січня 2022 року.

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

ІЛЬЄНКО А.В., к.т.н., доц., завідувач кафедри кібербезпеки КАІ. Дисертаційна робота аспірантки кафедри кібербезпеки КАІ Петляк Наталії Сергіївни на тему «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах» присвячена актуальному науково-прикладному завданню, що напряму пов'язане з удосконаленням інструментів виявлення кіберзагроз, зокрема тих, що проявляються у вигляді аномалій у мережевому трафіку. Авторкою запропоновано інноваційний гібридний підхід до виявлення аномального трафіку з орієнтацією на вихідні потоки — важливий аспект, який дотепер залишався малодослідженим у вітчизняній та світовій науковій практиці. Особливої уваги заслуговує інтеграція методу самоподібності, нечіткого моделювання та класифікації за ознаками у межах однієї архітектури, що дозволяє адаптуватися до змін середовища у режимі реального часу. Це рішення є надзвичайно практичним та перспективним у контексті сучасної кібербезпеки. Програмне забезпечення, створене за результатами дослідження, уже впроваджено у виробничу практику, що свідчить про прикладну цінність результатів. Дисертація логічно структурована, науково обґрунтована, містить достатню кількість публікацій у фахових виданнях та апробацію результатів на конференціях. Обсяг і зміст роботи відповідають вимогам до наукових досліджень такого рівня.

На основі вищезазначеного, вважаю, що дисертаційна робота Петляк Наталії Сергіївни є завершеним науковим дослідженням, відповідає спеціальності 125 «Кібербезпека» та вимогам до дисертацій на здобуття наукового ступеня доктора філософії, а її автор заслуговує на присудження відповідного наукового ступеня.

ОДАРЧЕНКО Р.С., д.т.н., проф., декан факультету аеронавігації, електроніки та телекомунікацій. Дисертаційна робота Петляк Наталії Сергіївни є вагомим внеском у розвиток науково-практичних засад кібербезпеки, зокрема, в напряму виявлення аномального трафіку в інформаційно-комунікаційних системах. Робота характеризується актуальністю, інноваційним підходом, високим рівнем теоретичної і прикладної розробки. Запропоновані моделі й методи засвідчують наукову новизну та здатність авторки до проведення самостійних досліджень. Дисертація відповідає вимогам до наукових кваліфікаційних робіт і заслуговує позитивної оцінки.

Обговорення дисертаційного дослідження.

АХРАМОВИЧ В. М. д.т.н., професор, професор кафедри кібербезпеки.

Відзначив що в роботі детально описані моделі та методи, а поставлені у роботі завдання ґрунтовно вирішені. Відмітив достатній обсяг матеріалу. Підтримав роботу.

ТЕРЕЙКОВСЬКИЙ І. А. д.т.н., професор, професор кафедри системного програмування і спеціалізованих комп'ютерних систем факультету прикладної математики КПІ ім. Ігоря Сікорського.

Відзначив високу актуальність теми дисертації в умовах зростання складності сучасних кібератак. Наголосив на важливості орієнтації на аналіз вихідного трафіку, який традиційно недооцінюється. Позитивно оцінив практичну реалізованість запропонованого гібридного методу та можливість його застосування. Підтримав роботу.

ФЕСЕНКО А. О. к.т.н., доц., декан ФКНТ КАІ.

Зазначив, що тематика дисертаційної роботи повністю відповідає сучасним викликам у галузі кібербезпеки. Відзначив практичну спрямованість дослідження та наявність результатів впровадження. Оцінив чітку структуру та логіку викладення матеріалу. Підтримав роботу.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Петляк Наталії Сергіївни на тему «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах», поданої на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека»

1. Обґрунтування вибору теми дослідження. У сучасному цифровому середовищі традиційні методи виявлення кіберзагроз виявляються малоефективними проти нових чи модифікованих атак. Особливою проблемою є недостатнє охоплення вихідного трафіку, який може свідчити про внутрішні загрози або використання системи як плацдарму для зовнішніх атак. Актуальність посилюється зростанням кількості інцидентів і збитків, завданих саме такими типами атак.

Тому розробка гібридного методу виявлення аномального трафіку в інформаційно-комунікаційних системах із фокусом на вихідний трафік, який враховує поведінкові особливості користувачів і порушників, а також здатен адаптуватися до невизначеності та змін середовища, забезпечуючи високу точність і надійність виявлення сучасних кіберзагроз є актуальною науковою задачею.

2. Зв'язок роботи з науковими програмами, планами, темами, грантами.

Дисертаційна робота проводилась в межах науково-дослідної роботи, яка велася в Національному авіаційному університеті за темою: «Моделі кіберзахисту інформаційних систем» (Державний реєстраційний номер: 0122U201817).

Тема дисертації відповідає освітньо-науковій програмі «Кібербезпека» за спеціальністю за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» в КАІ (зокрема, ОК 6, ОК 7, ОК 8).

3. Мета і завдання дослідження.

Метою дослідження роботи є підвищення достовірності виявлення аномального трафіку в інформаційно-комунікаційних системах шляхом розроблення гібридного методу, який враховує поведінкові характеристики користувачів і порушників. Для досягнення поставленої мети необхідно вирішити ***задачі***:

- Провести аналіз сучасних методів та моделей виявлення аномального трафіку в інформаційно-комунікаційних системах і моделей типового користувача та потенційного порушника.
- Вдосконалити модель сигнатури пакету з урахуванням інформативності полів заголовку та пакету щодо визначення їх аномальності.
- Вдосконалити модель процесу визначення аномального трафіку на основі самоподібності з урахуванням потенційних загроз та особливостей трафіку в інформаційно-комунікаційних системах.
- Вдосконалити модель процесу нечіткого визначення аномального трафіку, що враховує поведінку типового користувача та потенційного порушника.
- Розробити гібридний метод визначення аномального трафіку на основі нечіткого аналізу, визначеного як не самоподібний та імплементувати його в архітектуру системи захисту мережі.
- Розробити структурну модель системи виявлення аномального трафіку в інформаційно-комунікаційних системах.
- Розробити алгоритмічне та програмне забезпечення системи виявлення аномального трафіку та провести експериментальні дослідження.

4. Об'єктом дослідження є процес виявлення аномального трафіку в інформаційно-комунікаційних системах.

5. Предметом дослідження є моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах.

6. Методи дослідження. Для розв'язання поставлених задач використовуються основні положення методів аналізу даних, нечіткої логіки, теорії графів, теоретико-множинний підхід, статистичного аналізу даних, експертні оцінки, теорії множин та теорії комп'ютерних мереж.

7. Наукова новизна дослідження, полягає у наступному:

уперше:

- розроблено гібридний метод виявлення аномального трафіку в інформаційно-комунікаційних системах в якому за рахунок інтеграції методу класифікації трафіку за ознаками, методу самоподібності та розробленої моделі процесу нечіткого виявлення дозволило динамічно формувати множини сигнатур при класифікації трафіку за ознаками та підвищити показники виявлення аномального трафіку;

удосконалено:

- модель сигнатури пакету для пошуку аномального трафіку, що за рахунок виключення з параметрів сигнатури розміру заголовка, контрольної суми заголовку, корисного розміру пакета, мітки потоку, пріоритету пакету, контрольної суми пакету за принципом Парето, забезпечило зменшення часу аналізу трафіку.
- модель процесу нечіткого виявлення аномального трафіку, в якій за рахунок використання експертного підходу сформована множина правил та набір відповідних лінгвістичних змінних, що дозволило розробити нові підходи до виявлення аномального трафіку в інформаційно-комунікаційних системах.
- структурну модель системи виявлення аномального трафіку в інформаційно-комунікаційних системах, що за рахунок інтегрування розробленого гібридного методу виявлення аномального трафіку в інформаційно-комунікаційних системах та динамічного варіювання множиною дозволених та заборонених з'єднань у режимі реального часу дозволило зменшити навантаження на процесор.

8. Теоретичне значення.

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. Практичне значення та використання результатів дисертаційного дослідження полягає в тому, що:

- розроблено алгоритмічне забезпечення системи виявлення аномального трафіку в інформаційно-комунікаційних системах, що реалізує гібридний метод, його складові метод класифікації трафіку за ознаками, метод самоподібності, нечіткий метод та моделі, що в них використовуються;

- на основі алгоритму розроблено програмний застосунок, що дозволяє проводити аналіз трафіку в інформаційно-комунікаційних системах;
- можливість практичного використання розробленого програмного застосунку сумісно з маршрутизаторами в інформаційно-комунікаційній системі.

Результати дисертаційної роботи впроваджено:

- компанією ТОВ «X-CITY» (м. Хмельницький) для аналізу трафіку абонентів за допомогою гібридного методу в інформаційно-комунікаційні системі, що дозволило без зміни архітектури інформаційно-комунікаційної системи ТОВ «X-CITY» та апаратного забезпечення зменшити аномальний трафік, звернення провайдерів вищого рівня про атаки, що надходять з інформаційно-комунікаційної системи ТОВ «X-CITY» (*акт про впровадження від 10.04.2025).*
- у навчальному процесі кафедри кібербезпеки Хмельницького національного університету під час викладання дисциплін «Технології виявлення вразливостей та вторгнень», «Безпека безпроводових мереж та інтернет речей» та «Моніторинг та менеджмент інформаційної безпеки» (*акт про впровадження від 25.03.2025).*

10. Особистий внесок здобувача.

Дисертація «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах» Петляк Наталії Сергіївни є самостійною науковою працею, в якій наведено теоретичні положення та висновки, власні ідеї та розробки авторки, які дають змогу повною мірою вирішити поставлені завдання. Усі висновки та практичні рекомендації, винесені на захист, розроблені дисертанткою особисто.

11. Апробація результатів дослідження.

Найважливіші ідеї, висновки, рекомендації, отримані в дисертації, оприлюднені на міжнародних наукових та науково-практичних конференціях, у тому числі: «Інформаційна, функційна та кібербезпека» (м. Харків, 2022), «The International Workshop on Intelligent Information Technologies & Systems of Information Security» (м. Хмельницький, 2022), «Інформаційна безпека та комп'ютерні технології» (м. Кропивницький, 2023), «ITSec: Безпека інформаційних технологій» (м. Ужгород, 2023), «Захист інформації і безпека інформаційних систем» (м. Львів, 2023), «13th International Conference on Dependable Systems, Services and Technologies» (Athens, 2023), «ITSec: Безпека інформаційних технологій» (м. Львів, 2024), «4the International Workshop on Intelligent Information Technologies & Systems of Information Security» (м. Хмельницький, 2024), «1st International Workshop on Advanced Applied Information Technologies» (Khmelnytskyi, 2024), «1st International Workshop on Intelligent and CyberPhysical Systems» (Khmelnytskyi, 2024), «2nd International Workshop on Computer Information Technologies in Industry 4.0» (Ternopil, 2024).

12. Публікації. Основні наукові результати дисертаційної роботи опубліковано в 16 наукових публікаціях, із них: 5 статей у наукових фахових виданнях України, 6 – у виданнях, проіндексованих у наукометричній базі даних Scopus, а також 5 тез доповідей на міжнародних і науково-практичних конференціях різного рівня.

Список опублікованих праць за темою дисертації

Статті у наукових фахових виданнях України:

1. Тітова В.Ю., Кльоц Ю.П., Петляк Н.С., Капустян М.В. Fuzzy inference subsystem for classifying threats to computer information. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2022. № 1. С. 57-61. DOI: https://doi.org/10.31891/2219-9365-2022-69-1-8

Особистий внесок Петляк Н.С.: описано підсистему логічного виведення результатів для реалізації набору правил.

Особистий внесок Тітової В.Ю.: класифіковано загрози за їх атрибутами, визначено зв'язки між класами загроз, атрибутами та відповідними методами та інструментами безпеки

Особистий внесок Кльоца Ю.П.: описано математичну модель проблеми класифікації комп'ютерних загроз

Особистий внесок Капустян М.В.: проаналізовано загрози комп'ютерним даним в комп'ютерних системах

2. Кльоц Ю.П., Петляк Н.С. Виявлення аномального трафіку у загальнодоступних комп'ютерних мережах. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2022. № 3. С. 79-86. DOI: https://doi.org/10.31891/2219-9365-2022-71-3-9

Особистий внесок Петляк Н.С.: проведено аналіз статистики кіберінцидентів та запропоновано структуру ІКС з використанням системи виявлення вихідного аномального трафіку

Особистий внесок Кльоца Ю.П.: описано типи атак, які найчастіше виходять із загальнодоступних комп'ютерних мереж, для атак на третіх осіб

3. Мостовий С.В., Петляк Н.С., Голота І.О. Дослідження ефективності інструментів виявлення і запобігання вторгнень на вузли в корпоративних мережах. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2023. № 2. С. 5-8. DOI: https://doi.org/10.31891/2219-9365-2023-74-1

Особистий внесок Петляк Н.С.: налаштування тестового середовища та порівняння результатів роботи систем Snort та Suricata, що дозволило обрати оптимальний варіант для інтегрування розробленого гібридного методу.

Особистий внесок Мостового С.В.: проведено аналіз наявних досліджень та публікацій щодо сучасних підходів до виявлення та прогнозування атак

Особистий внесок Голоти І.О.: запуск атак та контроль мережевого трафіку під час тестування

4. Petliak N., Khokhlachova Yu. Method of analysis of outgoing traffic package signatures. *Захист інформації*. 2024. № 1. С. 179-187. DOI: https://doi.org/10.18372/2410-7840.26.18841

Особистий внесок Петляк Н.С.: описано вдосконалені модель сигнатури пакету для пошуку аномального трафіку за принципом Парето та модель процесу нечіткого виявлення аномального трафіку

Особистий внесок Хохлачової Ю.Є.: проведення розрахунків за результатами експерименту.

5. Петляк Н.С. Аналіз моделей виявлення аномалій трафіку в сучасних інформаційно-комунікаційних системах та мережах. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2025. № 1. С. 180-186. DOI: https://doi.org/10.31891/2219-9365-2025-81-21

6. Петляк Н.С. Гібридний метод та система виявлення аномального трафіку в інформаційно-комунікаційних системах. *Вісник Хмельницького національного університету. Серія: Технічні науки*. 2025. №2. С. 561-569. Режим доступу: https://doi.org/10.31891/2307-5732-2025-349-82.

Статті в іноземних виданнях:

1. Klots Y., Titova V., Petliak N., Cheshun V., Salem A.-B.M. Research of the Neural Network Module for Detecting Anomalies in Network Traffic. *CEUR Workshop Proceedings*. 2022. Vol. 3156. P. 378-389. URL: https://ceur-ws.org/Vol-3156/paper28.pdf (*Scopus*) Q4

ISSN 16130073

Особистий внесок автора: запропоновано модифікацію системи виявлення вторгнень Snort для можливості аналізу вихідного трафіку

2. Petliak N., Klots Y., Titova V., Cheshun V., Boyarchuk A. Signature-based Approach to Detecting Malicious Outgoing Traffic. *CEUR Workshop Proceedings*, 2023. Vol. 3373. P. 486-506. URL: https://ceur-ws.org/Vol-3373/paper33.pdf (Scopus) Q4

ISSN 16130073

Особистий внесок автора: вдосконалено модель сигнатури пакету для пошуку аномального трафіку з оптимізацією параметрів за принципом Парето

3. Klots Y., Petliak N., Titova V. Evaluation of the efficiency of the system for detecting malicious outgoing traffic in public networks. *DESSERT 2023: 13th International Conference on Dependable Systems, Services and Technologies*. 2023. URL: https://ieeexplore.ieee.org/document/10416502 (Scopus)

ISBN 979-835039611-9
DOI 10.1109/DESSERT61349.2023.10416502

Особистий внесок автора: виконано моделювання процесу нечіткого виявлення аномального трафіку

4. Klots Y., Petliak N., Martsenko S., Tymoshchuk V., Bondarenko I. Machine Learning system for detecting malicious traffic generated by IoT devices. *CEUR Workshop Proceedings*. 2024. Vol. 3742. P. 97-110. URL: https://ceur-ws.org/Vol-3742/paper7.pdf (Scopus) Q4

ISSN 16130073

Особистий внесок автора: запропоновано рішення аналізу вихідного трафіку для пошуку ботів та проведено аналіз наявних наборів даних

5. Titova V., Klots Y., Petliak N., Cheshun V., Salem A.-B.M. Detection of network attacks in cyber-physical systems using a rule-based logical neural network. *CEUR Workshop Proceedings*. 2024. Vol. 3736. P. 255-268. URL: https://ceur-ws.org/Vol-3736/paper19.pdf (Scopus) Q4

ISSN 16130073

Особистий внесок автора: запропоновано метод виявлення мережевих атак в локальній мережі та проведено розрахунок достовірності пропонованого рішення

6. Petliak N., Klots Y., Titova V., Salem A.-B.M. Attack detection system based on network traffic analysis by means of fuzzy inference. *CEUR Workshop Proceedings*. 2025. Vol. 3899. P. 201-213. URL: https://ceur-ws.org/Vol-3899/paper18.pdf (Scopus) Q4

ISSN 16130073

Особистий внесок автора: виконано моделювання процесу нечіткого виявлення аномального трафіку

Наукові праці, які додатково відображають наукові результати дисертації:

1. Петляк Н.С., Кльоц Ю.П., Хохлачова Ю.Є. Виявлення аномального трафіку у загальнодоступних комп'ютерних мережах. *Інформаційна, функційна і кібербезпека.* 30 листопада – 1 грудня 2022. Харків. С. 45-46. URL: http://dx.doi.org/10.13140/RG.2.2.29592.67844/1

2. Петляк Н.С., Кльоц Ю.П. Підхід до аналізу вихідного трафіку на основі сигнатур. Інформаційна безпека та комп'ютерні технології. 20-21 квітня 2023. Кропивницький. С. 3-4. URL: https://dspace.kntu.kr.ua/handle/123456789/12768

3. Петляк Н.С., Кльоц Ю.П., Хохлачова Ю.Є. Підхід до аналізу вихідного трафіку. *ITSec-2023: Безпека інформаційних технологій.* 2-4 травня 2023. Ужгород. С. 97-99. URL: http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf

4. Петляк Н.С., Кльоц Ю.П., Тітова В.Ю., Чешун В.М. Виявлення зловмисного вихідного трафіку мережі на основі нечіткого логічного висновку.

Захист інформації і безпека інформаційних систем. 25-26 травня 2023. Львів. С. 33-35.

5. Петляк Н.С., Кльоц Ю.П. Метод ідентифікації вторгнень на основі алгоритму визначення самоподібності трафіку та алгоритмів нечіткої логіки. *ITSec-2024: Безпека інформаційних технологій*. 9-11 травня 2024. Львів. С. 117-119.

13. Структура та обсяг дисертації. Дисертація складається із анотацій, вступу, чотирьох розділів, висновків, додатків, списку використаних джерел. Повний обсяг роботи становить 153 сторінки, із них122 сторінки основного тексту. Список використаних джерел налічує 104 найменування. Дисертація містить 45 рисунків та 14 таблиць.

14. Характеристика особистості здобувача. Під час підготовки дисертаційної роботи Петляк Н.С. 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.

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

16. Відповідність принципам академічної доброчесності.

Дисертація не містить необґрунтованих запозичень та плагіату. У роботі дотримано правила посилання на джерела інформації у випадку використання підходів, положень, тверджень, відомостей. Надано достовірну інформацію про результати досліджень, джерела використаної інформації.

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, ***такий склад разової ради:***

Голова ради:

ГНАТЮК Сергій Олександрович, д.т.н, професор, професор кафедри комп'ютерних інформаційних технологій КАІ.

Рецензенти:

ОДАРЧЕНКО Роман Сергійович, д.т.н, професор, декан факультету аеронавігації, електроніки та телекомунікацій КАІ.

ІЛЬЄНКО Анна Вадимівна, к.т.н., доцент, завідувач кафедри кібербезпеки КАІ.

Офіційні опоненти:

КАЗМІРЧУК Світлана Володимирівна, д.т.н., професор, професор кафедри систем та технологій кібербезпеки Державного університету інформаційно-комунікаційних технологій.

КОРЧЕНКО Анна Олександрівна д.т.н., професор, професор кафедри безпеки інформації та телекомунікацій Національного технічного університету «Дніпровська політехніка».

Усі члени разової спеціалізованої вченої ради не мають реальний чи потенційний конфлікт інтересів щодо здобувача Петляк Наталії Сергіївни (зокрема, є його близькою особою) та/або його наукового керівника.

У результаті попередньої експертизи дисертації Петляк Наталії Сергіївни і повноти публікації основних результатів дослідження.

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Петляк Наталії Сергіївни на тему «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах»

2. Вважати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Петляк Наталії Сергіївни відповідає спеціальності 125 «Кібербезпека» та вимогам «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах)», затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року. № 261 (зі змінами і доповненнями від 03 квітня 2019 року № 283), вимогам пп. 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 року № 44.

3. Рекомендувати дисертаційну роботу «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах», подану Петляк Наталією Сергіївною на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології», за спеціальності 125 «Кібербезпека» до захисту у разовій спеціалізованій вченій раді.

4. Рекомендувати Вченій раді КАІ клопотати про призначення:

Головою спеціалізованої вченої ради:

ГНАТЮКА Сергія Олександровича, д.т.н, професора, професора кафедри комп'ютерних інформаційних технологій КАІ.

Рецензентами:

ОДАРЧЕНКА Романа Сергійовича, д.т.н, професора, декана факультету аеронавігації, електроніки та телекомунікацій КАІ.

ІЛЬЄНКО Анну Вадимівну, к.т.н., доцента, завідувача кафедри кібербезпеки КАІ.

Офіційними опонентами:

КАЗМІРЧУК Світлану Володимирівну, д.т.н., професора, професора кафедри систем та технологій кібербезпеки Державного університету інформаційно-комунікаційних технологій.

КОРЧЕНКО Анну Олександрівну, д.т.н., професора, професора кафедри безпеки інформації та телекомунікацій Національного технічного університету «Дніпровська політехніка».

Результати голосування щодо рекомендації до захисту дисертації Петляк Наталії Сергіївни:

«за» – 12.

«проти» – немає.

«утримались» – немає.

Головуючий на засіданні:
професор кафедри технічного захисту
інформації ФКНТ КАІ,
д.т.н., професор Андрій МІЩЕНКО

Секретар засідання:
завідувач кафедри кібербезпеки ФКНТ
КАІ, к.т.н., доцент Анна ІЛЬЄНКО

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