“ЗАТВЕРДЖУЮ”
В.о. ректора, перший проректор
Національного технічного університету
«Дніпровська політехніка»
_____Артем ПАВЛИЧЕНКО
“23” червня 2026 р.

ВИСНОВОК

Національного технічного університету «Дніпровська політехніка» щодо дисертації **МЄШКОВА Вадима Ігоровича** на тему: **«Інформаційна технологія інтелектуального моніторингу трафіку комп’ютерної мережі для систем виявлення атак»** на здобуття наукового ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп’ютерні науки». Тема дисертації затверджена на засіданні Вченої ради Національного технічного університету «Дніпровська політехніка» (протокол № 11 від 29.11.2022 р.).

ВИТЯГ

з протоколу №14 засідання кафедри
програмного забезпечення комп’ютерних систем
факультету інформаційних технологій
навчально-наукового інституту електроенергетики
від «23» червня 2026 року

ПРИСУТНІ:

головуючий на засіданні д.т.н., проф., проф. кафедри програмного забезпечення комп’ютерних систем Мороз Б.І.; д.т.н., проф., завідувач кафедри програмного забезпечення комп’ютерних систем Алексєєв М.О.; д.т.н., проф., завідувач кафедри безпеки інформації та телекомунікацій Корнієнко В.І., д.т.н., проф., проф. кафедри програмного забезпечення комп’ютерних систем Мещеряков Л.І.; д.т.н., проф., проф. кафедри програмного забезпечення комп’ютерних систем Швачич Г.Г.; д.т.н., проф., проф. кафедри програмного забезпечення комп’ютерних систем Лактіонов І.С.; д.т.н., доц., проф. кафедри програмного забезпечення комп’ютерних систем Бердник М.Г.; к.т.н., доц., доц. кафедри програмного забезпечення комп’ютерних систем Ширін А.Л.; к.т.н., доц., доц. кафедри програмного забезпечення комп’ютерних систем Кабак Л.В.; к.т.н., доц., доц. кафедри програмного забезпечення комп’ютерних систем Спірінцев В.В.; к.т.н., доц., доц. кафедри програмного забезпечення комп’ютерних систем Приходченко С.Д.; к.т.н., доц., доц. кафедри програмного забезпечення комп’ютерних систем Горбова О.В.; к.т.н., доц., доц. кафедри

програмного забезпечення комп'ютерних систем Клименко А.В.; к.т.н., доц., доц. кафедри безпеки інформації та телекомунікацій Герасіна О.В.; PhD, доц. кафедри програмного забезпечення комп'ютерних систем Мартиненко А.А.; PhD, доц. кафедри програмного забезпечення комп'ютерних систем Мороз Д.М.; PhD, доц. кафедри програмного забезпечення комп'ютерних систем Шевцова О.С.; PhD, доц. кафедри програмного забезпечення комп'ютерних систем Голінько О.В.; асистент кафедри програмного забезпечення комп'ютерних систем Щербина П.О.; асистент кафедри програмного забезпечення комп'ютерних систем Рулікова В.В.

Серед присутніх 7 докторів технічних наук, 7 кандидатів технічних наук і 4 доктори філософії – фахівці зі спеціальності, з якої виконувалась дисертація та за напрямом досліджень здобувача.

ПОРЯДОК ДЕННИЙ:

1. Обговорення результатів дисертаційного дослідження здобувача кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка» **МЄШКОВА Вадима Ігоровича** на тему: **«Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак»**, поданого на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки», щодо її рекомендації для попереднього розгляду та захисту у разовій спеціалізованій вченій раді.

Науковий керівник – доктор технічних наук, професор, завідувач кафедри безпеки інформації та телекомунікацій КОРНІЄНКО Валерій Іванович.

Дисертація виконувалась на кафедрі програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка» з урахуванням наукових напрямків роботи кафедри та сучасних досягнень у галузі створення й дослідження прикладних комп'ютерних технологій.

Тема дисертації затверджена на засіданні Вченої ради НТУ «Дніпровська політехніка» (протокол № 11 від 29.11.2022 р.).

СЛУХАЛИ:

1. Повідомлення голови семінару – **МОРОЗ Б.І.,** д.т.н., проф., проф. кафедри програмного забезпечення комп'ютерних систем, за матеріалами дисертаційної роботи МЄШКОВА Вадима Ігоровича на тему: «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак», поданої на здобуття наукового ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Тема дисертації затверджена на засіданні Вченої ради НТУ «Дніпровська політехніка» (протокол № 11 від 29.11.2022 р.).

Науковий керівник – доктор технічних наук, професор, завідувач кафедри безпеки інформації та телекомунікацій КОРНІЄНКО Валерій Іванович.

2. Доповідь здобувача ступеня доктора філософії МЄШКОВА Вадима Ігоровича на тему: «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак», поданої на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Під час доповіді здобувачем МЄШКОВИМ В.І. було розкрито актуальність обраної теми, об'єкт, предмет, мету, завдання, наукову новизну та методи дослідження, основні наукові положення та висновки, що виносяться на захист, підкреслено науково-практичну значущість роботи, а також надано інформацію про впровадження результатів дослідження.

3. Запитання до здобувача. Запитання по матеріалам дисертації ставили:

1. д.т.н., проф., Лактіонов Іван Сергійович

Питання 1.

Який тип мають вхідні дані, що використовувалися у дослідженні: лише числовий чи також категоріальний? Чи містить набір даних категоріальні змінні, наприклад ознаки джерела даних?

Відповідь.

У дослідженні використовувався підготовлений набір даних CIC-IDS2017, у якому основні вхідні ознаки мережевого трафіку подані у числовому вигляді. Це статистичні характеристики потоків і пакетів мережевого трафіку. Категоріальні змінні як окремі вхідні ознаки не використовувалися. Останній стовпець набору даних є цільовою міткою класу, яка визначає тип трафіку: нормальний трафік або відповідний тип атаки.

Питання 2.

Наскільки коректно називати отримані результати саме інформаційною технологією, якщо в роботі продемонстровано переважно програмні компоненти та моделі машинного навчання?

Відповідь.

Термін «інформаційна технологія» у роботі використано коректно, оскільки запропоноване рішення не обмежується лише окремою програмною реалізацією або однією моделлю машинного навчання. Воно включає послідовність взаємопов'язаних процедур: підготовку та очищення даних, уніфікацію ознак, стандартизацію, аналіз кореляції, зниження розмірності за допомогою PCA, формування збалансованих вибірок, навчання моделей, оцінювання якості класифікації та інтерпретацію отриманих результатів. Програмні компоненти є засобом реалізації цієї технології, а сама інформаційна технологія охоплює методи, алгоритми, етапи обробки та порядок використання моделей для інтелектуального моніторингу мережевого трафіку в IDS.

Питання 3.

Чи виконувалася перевірка пояснюваності моделей машинного навчання, тобто аналіз того, які ознаки або компоненти найбільше впливають на результат класифікації?

Відповідь.

Окремі методи пояснюваного штучного інтелекту, наприклад SHAP або LIME, у межах цієї роботи не застосовувалися. Водночас у роботі виконано аналіз ознак на етапі попередньої обробки даних. Зокрема, було проведено кореляційний аналіз за коефіцієнтом Пірсона для виявлення надмірно пов'язаних ознак, а також застосовано метод головних компонент PCA. У результаті початковий простір ознак було зменшено до 35 головних компонент, які використовувалися для навчання моделей. Це дозволило знизити надмірність даних і зберегти основну інформативність вхідного простору.

Питання 4.

Чи перевірялася робота моделей на нових даних, які можуть надходити в режимі інференсу, а не лише на тестовій частині вихідного набору даних?

Відповідь.

У роботі перевірка моделей виконувалася на сформованих навчальних і тестових вибірках із набору CIC-IDS2017 із використанням кросвалідації. Також здійснювалося повторне навчання моделей на різних випадково сформованих вибірках, що дозволило оцінити стабільність результатів. Отримані відхилення основних метрик якості були незначними. Разом із тим застосування моделей до повністю нових потоків трафіку в реальному середовищі потребує додаткового тестування та подальшого донавчання моделей на актуальних даних.

2. д.т.н., проф. Алексєєв Михайло Олександрович

Питання.

Як запропонована модель буде реагувати на новий або видозмінений тип атаки? Чи зможе вона його виявити, чи така атака буде проігнорована?

Відповідь.

Модель навчалася на визначеному переліку типів атак, представлених у наборі даних CIC-IDS2017, зокрема Brute Force, DoS, DDoS, Web Attack, Botnet, PortScan, Infiltration та Heartbleed. Якщо нова атака має подібні статистичні характеристики до вже відомих типів атак, модель може віднести її до одного з наявних класів, але точність такої ідентифікації може бути нижчою. Якщо ж атака має принципово нову структуру ознак, для її коректного розпізнавання необхідно доповнювати набір даних новими прикладами та виконувати донавчання або перенавчання моделі.

3. д.т.н., доц., проф. каф. ПЗКС Бердник Михайло Генадійович

Питання 1.

Чи залежить обробка даних від протоколу мережевого трафіку?

Відповідь.

Так, характеристики мережевого трафіку певною мірою залежать від протоколу, оскільки різні протоколи мають різні особливості передавання даних,

типові порти, структуру пакетів, розміри повідомлень, наявність або відсутність шифрування та службові параметри взаємодії. У наборі CIC-IDS2017 представлені різні типи мережевої активності, пов’язані, зокрема, з протоколами HTTP, HTTPS, FTP, SSH та поштовими протоколами.

Питання 2.

У чому полягають основні відмінності під час обробки трафіку різних протоколів?

Відповідь.

Відмінності пов’язані з тим, що різні протоколи формують різні статистичні характеристики трафіку: кількість і розмір пакетів, тривалість з’єднання, напрям передавання, частоту запитів, обсяг службової інформації, а також особливості шифрування. У межах запропонованого підходу ці відмінності враховуються не через ручне налаштування окремої обробки для кожного протоколу, а через числові ознаки потоків трафіку, які надалі проходять стандартизацію, зниження розмірності та класифікацію моделями машинного навчання.

4. д.т.н., проф. Мороз Борис Іванович

Питання 1.

Чи не є проблемою те, що моделі навчаються на застарілих даних, тоді як у реальних мережах можуть з’являтися нові характеристики трафіку та нові типи атак?

Відповідь.

Використання історичних наборів даних має певні обмеження, оскільки з часом можуть з’являтися нові типи атак або змінюватися характеристики мережевого трафіку. Разом із тим багато атак зберігають спільні структурні та поведінкові ознаки, наприклад підвищену інтенсивність запитів, аномальні розміри пакетів, нетипову тривалість з’єднань або характерні співвідношення між потоками. Тому моделі можуть бути ефективними для виявлення атак, подібних до тих, на яких вони навчалися. Для підтримання актуальності системи в реальних умовах необхідно періодично оновлювати навчальні дані та виконувати донавчання моделей.

Питання 2.

Як система може працювати в реальному масштабі часу, якщо атака вже починає впливати на мережевий трафік до моменту її виявлення?

Відповідь.

Запропонована інформаційна технологія орієнтована на моніторинг поточного мережевого трафіку та швидке виявлення ознак атаки за статистичними характеристиками потоків. Після надходження ознак трафіку на вхід навченої моделі виконується класифікація, і в разі виявлення атаки система може передати результат до IDS/IPS або іншого захисного компонента. Подальші дії – блокування з’єднання, обмеження трафіку, ізоляція сегмента мережі або формування сповіщення – визначаються політиками безпеки конкретної системи. Тобто завдання роботи полягає саме у виявленні та класифікації атаки, а не у безпосередньому виконанні всіх захисних дій.

Питання 3.

Чи здійснюється у роботі прогнозування атак на майбутні періоди?

Відповідь.

Ні, у роботі не розв’язувалася задача прогнозування майбутніх атак. Основна увага приділялася виявленню наявності атаки в мережевому трафіку та розпізнаванню її типу на основі вже сформованих ознак поточного або зафіксованого трафіку. Тому запропонований підхід належить до задач класифікації мережевого трафіку, а не до задач прогнозування появи атак у майбутньому.

4. Виступи та обговорення щодо дисертаційної роботи. В обговоренні дисертації взяли участь:

У дискусії виступив д.т.н., проф. Швачич Геннадій Григорович, який зазначив, що загалом погоджується з висловленими рецензентами оцінками та підтримує представлену роботу. Водночас він звернув увагу здобувача на необхідність уточнення окремих формулювань у презентації та тексті роботи.

Зокрема, було зазначено, що формулювання об’єкта дослідження як «моніторинг трафіку» потребує коригування, оскільки об’єктом дослідження доцільно визначати процес або явище. Було запропоновано сформулювати об’єкт дослідження як процеси моніторингу та аналізу мережевого трафіку в структурі системи виявлення атак.

Також д.т.н, проф. Швачич Геннадій Григорович звернув увагу на перший пункт наукової новизни, зазначивши, що його необхідно подати більш переконливо. На його думку, у чинному формулюванні переважно відображено інтеграцію відомих методів, тоді як потрібно чіткіше показати власний науковий результат здобувача. Було рекомендовано акцентувати увагу на тому, що запропонований підхід відрізняється дворівневою архітектурою послідовного бінарного та багатокласового аналізу мережевого трафіку, що забезпечує підвищення точності виявлення атак порівняно з існуючими підходами.

У підсумку д.т.н., проф. Швачич Геннадій Григорович зазначив, що висловлені зауваження мають змістовний і стилістичний характер та спрямовані на покращення подання результатів дослідження. Він підкреслив, що робота є достойною, підтримав її та рекомендував колегам також підтримати дисертаційне дослідження.

У дискусії також виступив д.т.н., проф. Лактіонов Іван Сергійович, який зазначив, що підтримує роботу, оскільки здобувач добре орієнтується в її змісті, розуміє поставлену задачу, використані методи та отримані результати. Він підкреслив, що висловлені ним міркування мають рекомендаційний характер і спрямовані на покращення роботи.

Д.т.н., проф. Лактіонов Іван Сергійович звернув увагу на необхідність більш чіткого розкриття поняття інформаційної технології в межах дисертаційного дослідження. Було рекомендовано детальніше показати складові запропонованої інформаційної технології, зокрема вхідні дані, етапи їх обробки, програмні компоненти, моделі машинного навчання та логіку їх взаємодії. Це

дозволило б повніше обґрунтувати, що отриманий результат є не лише набором окремих моделей або програмних процедур, а саме інформаційною технологією інтелектуального моніторингу мережевого трафіку.

Д.т.н., проф. Мороз Борис Іванович у своєму виступі підтримав думку щодо необхідності детальнішого представлення структурних елементів запропонованого рішення. Зокрема, він рекомендував чіткіше описати, що саме є мережевим трафіком як вхідними даними для моделі, як виглядає модель, які вона має входи та виходи, які параметри використовуються для класифікації, а також яким чином модель включається до загальної структурної схеми обробки даних.

Було зазначено, що за умови більш формалізованого опису моделі та її місця в загальній структурі обробки даних запропоноване рішення можна переконливіше представити як інформаційну технологію. Д.т.н., проф. Мороз Борис Іванович наголосив, що його зауваження мають рекомендаційний характер.

У підсумку д.т.н., проф. Мороз Борис Іванович зазначив, що дисертаційна робота є актуальною, містить нові рішення, а автор підібрав відповідний інструментарій для розв'язання поставленої задачі, обґрунтував вибір вхідних даних і провів експериментальну перевірку працездатності моделей. Він підтримав роботу та зазначив, що вважає можливим рекомендувати її до подальшого розгляду.

За результатами дискусії учасники семінару загалом підтримали дисертаційну роботу Мєшкова Вадима Ігоровича, відзначили її актуальність, практичну спрямованість і наявність отриманих результатів. Висловлені зауваження та рекомендації стосувалися переважно уточнення формулювань об'єкта дослідження, наукової новизни, а також більш детального представлення інформаційної технології, структури моделей і їх місця в загальній схемі інтелектуального моніторингу мережевого трафіку.

Науковий керівник здобувача – доктор технічних наук, професор КОРНІЄНКО Валерій Іванович

Науковий керівник здобувача – д.т.н., проф. КОРНІЄНКО Валерій Іванович – представив автора дисертації та зазначив, що висновок про роботу над дисертацією та виконання індивідуального навчального плану МЄШКОВА Вадима Ігоровича, який здобуває науковий ступінь доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки», є позитивним. Здобувач МЄШКОВ В.І. виконав усі вимоги індивідуального плану наукової роботи та індивідуального навчального плану, а представлене ним дослідження відповідає всім формальним вимогам щодо підготовки дисертації.

Як науковий керівник здобувача ступеня доктора філософії МЄШКОВА Вадима Ігоровича, Валерій Іванович КОРНІЄНКО зазначив, що дисертаційна робота на тему: «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак» є самостійним,

завершеним і актуальним науковим дослідженням, виконаним на належному науково-методичному рівні. Робота спрямована на розв'язання важливої науково-прикладної задачі підвищення ефективності виявлення атак і розпізнавання їх типів у комп'ютерних мережах шляхом розроблення інформаційної технології інтелектуального моніторингу мережевого трафіку для систем виявлення атак.

У період навчання в аспірантурі МЄШКОВ Вадим Ігорович зарекомендував себе як відповідальний, дисциплінований, наполегливий і самостійний дослідник, здатний до критичного аналізу сучасних науково-технічних рішень, постановки та розв'язання науково-прикладних задач, планування експериментальних досліджень і практичної реалізації отриманих результатів. Здобувач послідовно опрацьовував наукові джерела з проблематики інтелектуального моніторингу трафіку комп'ютерної мережі, систем виявлення атак, методів машинного навчання та аналізу великих масивів даних.

Науковий керівник підкреслив, що дисертаційна робота має логічну, цілісну та завершену структуру, а її зміст послідовно розкриває шлях від аналізу сучасного стану проблеми й постановки задачі до розроблення методу, інформаційної технології, програмної реалізації та експериментального підтвердження ефективності отриманих результатів.

Загалом науковий керівник зазначив, що дисертаційна робота МЄШКОВА Вадима Ігоровича за змістом, об'єктом, предметом, метою, завданнями, методами дослідження, науковою новизною та практичним значенням повністю відповідає спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології». Робота виконана державною мовою, відповідає встановленим вимогам до дисертацій на здобуття ступеня доктора філософії та може бути рекомендована до проходження попередньої експертизи й подальшого захисту в разовій спеціалізованій вченій раді.

Рецензенти дисертаційної роботи, які наголосили на позитивних аспектах дослідження та висловили свої побажання й рекомендації.

Доктор технічних наук, професор АЛЕКСЄЄВ Михайло Олександрович

Детально проаналізувавши дисертаційну роботу здобувача МЄШКОВА Вадима Ігоровича на тему: «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак», хотів би зазначити, що вона є актуальним, завершеним і самостійним науковим дослідженням, спрямованим на розв'язання важливої науково-прикладної задачі у галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Актуальність дисертаційної роботи не викликає сумнівів, оскільки сучасні комп'ютерні мережі функціонують в умовах постійного зростання кількості, складності та динамічності кіберзагроз. Традиційні сигнатурні методи виявлення атак не завжди забезпечують достатню ефективність під час розпізнавання

нових, модифікованих або малопоширених загроз. У зв’язку з цим особливого значення набуває розроблення інформаційних технологій інтелектуального моніторингу мережевого трафіку, що базуються на методах машинного навчання та здатні забезпечувати як первинне виявлення атакувальної активності, так і подальше розпізнавання типів атак.

Наукова новизна роботи полягає у розробленні інформаційної технології інтелектуального моніторингу трафіку комп’ютерної мережі для систем виявлення атак, яка забезпечує повний цикл обробки даних мережевого трафіку: від завантаження, очищення, уніфікації та стандартизації даних до формування ознакового простору, балансування вибірок, навчання моделей машинного навчання та комплексного оцінювання результатів. Особливої уваги заслуговує те, що автор розглядає задачу не лише у бінарній постановці, тобто як відокремлення нормального трафіку від атакувального, а й у багатокласовій постановці, що передбачає розпізнавання конкретних типів атак. Такий підхід підвищує практичну цінність дослідження для побудови сучасних інтелектуальних компонентів систем виявлення атак.

Позитивним аспектом дисертації є її чітка методична структура. Автор обґрунтував вибір набору даних CIC-IDS2017, визначив вимоги до підготовки мережевого трафіку, реалізував процедури очищення даних, обробки пропущених і некоректних значень, стандартизації числових ознак, аналізу кореляційних залежностей і зниження розмірності ознакового простору. Важливим є також використання процедур балансування даних, що має принципове значення для задач виявлення атак, оскільки реальні та експериментальні набори мережевого трафіку зазвичай характеризуються суттєвою нерівномірністю представлення класів.

Практичне значення одержаних результатів полягає у створенні програмної реалізації інформаційної технології, яка об’єднує основні етапи інтелектуального аналізу мережевого трафіку в єдиний програмний модуль. У роботі реалізовано й досліджено моделі машинного навчання для бінарної та багатокласової класифікації, зокрема логістичну регресію, метод опорних векторів, дерево рішень, випадковий ліс і метод k-найближчих сусідів. Застосування системи взаємодоповнювальних метрик, таких як accuracy, precision, recall, F1-score, ROC-AUC, Precision–Recall-криві, матриці помилок і п’ятикратна перехресна перевірка, свідчить про належний рівень організації експериментального дослідження.

Як побажання до подальшого розвитку роботи, хотів би звернути увагу на доцільність більш детального аналізу продуктивності запропонованої інформаційної технології в умовах наближеного до реального часу моніторингу мережевого трафіку, зокрема щодо обчислювальної складності окремих етапів, часу навчання моделей, часу класифікації та можливостей масштабування програмної реалізації для великих корпоративних мереж. Крім того, перспективним напрямом подальших досліджень може бути порівняння запропонованого підходу з сучасними глибинними моделями машинного навчання та перевірка його стійкості на інших наборах даних мережевих атак.

Загалом вважаю, що дисертаційна робота МЄШКОВА Вадима Ігоровича є добре структурованою, логічно викладеною, виконаною на належному науковому рівні та має як теоретичне, так і практичне значення. Отримані результати є обґрунтованими, пройшли апробацію та відображені у наукових публікаціях здобувача. Незважаючи на окремі дискусійні положення, які не знижують загальної позитивної оцінки роботи, вважаю, що дисертація відповідає вимогам, які висуваються до дисертацій на здобуття ступеня доктора філософії, і може бути рекомендована до захисту.

Кандидат технічних наук, доцент ГЕРАСІНА Олександра Володимирівна

На підставі детального ознайомлення з дисертаційною роботою МЄШКОВА Вадима Ігоровича можу зазначити, що представлене дослідження є актуальним, цілісним і завершеним. Робота присвячена розробленню інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак, що є важливим напрямом розвитку сучасних інформаційних технологій, комп'ютерних наук і кібербезпеки.

Актуальність теми визначається потребою у підвищенні ефективності виявлення атак у комп'ютерних мережах, де обсяги мережевого трафіку постійно зростають, а характер кіберзагроз ускладнюється. Особливо важливим є те, що автор розглядає мережевий трафік як джерело даних для інтелектуального аналізу та формування класифікаційних рішень. Застосування методів машинного навчання у такому контексті є обґрунтованим, оскільки ці методи дають змогу виявляти статистичні закономірності у високовимірному просторі ознак і підвищувати результативність систем виявлення атак.

Наукова новизна дисертаційної роботи полягає в комплексному поєднанні процедур підготовки даних, аналізу ознак, зниження розмірності, формування та балансування вибірок, навчання моделей машинного навчання й оцінювання їх якості. На мою думку, важливим результатом є удосконалений метод підготовки даних, класифікації та оцінювання мережевого трафіку, який дозволяє забезпечити методично коректне розв'язання задач бінарного виявлення атак і багатокласового розпізнавання їх типів. Такий підхід свідчить про системність виконаного дослідження та його відповідність сучасним вимогам до побудови інтелектуальних інформаційних технологій.

Слід позитивно відзначити, що автор не обмежився лише побудовою окремих класифікаційних моделей, а розробив узгоджену технологічну схему, яка охоплює повний цикл роботи з даними мережевого трафіку. У дисертації обґрунтовано вибір набору даних CIC-IDS2017, розглянуто особливості його використання для експериментального дослідження, сформовано вибірки для двох режимів класифікації, реалізовано процедури балансування та проведено порівняльне оцінювання моделей. Така організація дослідження забезпечує відтворюваність результатів і дає змогу об'єктивно порівнювати ефективність різних алгоритмів машинного навчання.

Практична значущість роботи полягає у тому, що запропонована інформаційна технологія та її програмна реалізація можуть бути використані як основа для побудови інтелектуальних компонентів систем виявлення атак у комп'ютерних мережах. Результати дослідження можуть бути корисними для автоматизованого аналізу мережевого трафіку, виявлення атакувальної активності, подальшої деталізації інцидентів за типами атак, а також для підтримки прийняття рішень фахівцями з кібербезпеки. Окремо слід відзначити можливість використання отриманих результатів у науково-дослідній та освітній діяльності під час підготовки фахівців у галузі комп'ютерних наук і кібербезпеки.

Як рекомендацію щодо подальшого вдосконалення роботи, вважаю доцільним у майбутніх дослідженнях розширити інтерпретацію впливу окремих ознак мережевого трафіку та головних компонент на результати класифікації. Також корисним було б провести додатковий аналіз стійкості моделей до змін структури вхідних даних, появи нових типів атак і зміни співвідношення класів у навчальних вибірках. Це дозволило б ще повніше оцінити придатність запропонованої інформаційної технології до використання в реальних умовах функціонування систем виявлення атак.

Проте зазначені побажання мають рекомендаційний характер і не знижують загальної позитивної оцінки дисертаційної роботи. Вважаю, що дисертація Мєшкова Вадима Ігоровича написана на належному науковому рівні, має логічну структуру, містить обґрунтовані наукові результати та практично значущі положення. Основні результати роботи пройшли апробацію, опубліковані у наукових працях і відповідають темі дисертаційного дослідження. За змістом, обсягом, рівнем наукової новизни та практичним значенням робота відповідає вимогам до дисертацій на здобуття ступеня доктора філософії та може бути рекомендована до захисту.

Члени семінару зазначили:

Дисертація відповідає вимогам законодавства про авторське право і суміжні права. У роботі використано наукові положення, ідеї, результати та висновки, сформовані й отримані здобувачем особисто. У разі використання положень, результатів і текстів інших авторів у дисертації наведено відповідні посилання на джерела їх опублікування. Щодо наукових праць, опублікованих здобувачем у співавторстві, у роботі чітко зазначено особистий внесок МЄШКОВА В.І. та конкретизовано зміст виконаних ним досліджень і розробок. За результатами аналізу тексту дисертації та списку використаних джерел ознак порушення академічної доброчесності не виявлено.

Після розкриття здобувачем основних положень дисертаційної роботи науковці відзначили, що дослідження є актуальним, виконаним на належному науковому рівні, має завершений і самостійний характер та містить нові науково обґрунтовані результати, спрямовані на розв'язання актуальної науково-прикладної задачі у галузі знань 12 «Інформаційні технології». Зазначена задача полягає у підвищенні ефективності виявлення атак і розпізнавання їх типів у комп'ютерних мережах шляхом розроблення інформаційної технології

інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак, що базується на методах машинного навчання та забезпечує функціонування у бінарному і багатокласовому режимах аналізу.

Члени семінару зазначили, що отримані МЄШКОВИМ В.І. наукові результати достатньо повно опубліковані у наукових працях та пройшли апробацію на міжнародних і всеукраїнських науково-технічних та науково-практичних заходах. Також було відзначено, що основні теоретичні, методичні та практичні положення дисертації доведені до рівня прикладної інформаційної технології, програмної реалізації, алгоритмічних процедур і практичних рекомендацій. Запропоновані результати можуть бути використані для побудови інтелектуальних компонентів сучасних систем виявлення атак, автоматизованої обробки мережевого трафіку, формування ознакового простору, бінарного виявлення атакувальної активності, багатокласового розпізнавання типів атак і підтримки прийняття рішень у сфері кібербезпеки.

Під час виступів науковці висловили єдину думку, що дисертаційна робота МЄШКОВА Вадима Ігоровича на тему: «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак», подана на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки», відповідає встановленим вимогам до підготовки дисертації та може бути рекомендована до подальшого проходження і захисту в разовій спеціалізованій вченій раді до завершення терміну навчання в аспірантурі.

ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації МЄШКОВА Вадима Ігоровича на тему: «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак» на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології»

Обґрунтування вибору теми дослідження. Сучасні комп'ютерні мережі є критично важливою складовою інформаційної інфраструктури підприємств, установ і організацій, а їх функціонування супроводжується постійним зростанням кількості та складності кіберзагроз. Умови цифровізації, розширення мережевих сервісів, збільшення обсягів передаваних даних і підвищення інтенсивності мережевих взаємодій зумовлюють необхідність удосконалення методів і засобів моніторингу мережевого середовища та своєчасного виявлення ознак атак. У таких умовах мережевий трафік виступає одним із найбільш інформативних джерел даних для виявлення атакувальної активності, оскільки відображає взаємодії між компонентами мережі та дає змогу фіксувати як явні, так і приховані ознаки кіберзагроз.

Традиційні системи виявлення атак, що базуються переважно на сигнатурних механізмах, залишаються ефективними для розпізнавання відомих

шаблонів загроз, проте виявляються недостатньо гнучкими у випадках нових, модифікованих або малопоширених атак. Це знижує їхню результативність у сучасному мережевому середовищі, де атакувальна активність постійно еволюціонує, а характеристики трафіку змінюються динамічно. Саме тому одним із перспективних напрямів розвитку систем виявлення атак є застосування інтелектуальних методів аналізу даних, заснованих на машинному навчанні, які дають змогу виявляти статистичні закономірності у високовимірному просторі ознак мережевого трафіку та формувати класифікаційні рішення щодо наявності атакувальної активності.

Разом із тим ефективність інтелектуального виявлення атак визначається не лише вибором конкретної моделі машинного навчання, а й якістю підготовки даних, коректністю формування ознакового простору, урахуванням дисбалансу класів, зменшенням надлишковості ознак і дотриманням методично коректної процедури оцінювання результатів. Для мережевого трафіку характерні пропущені та некоректні значення, дубльовані записи, істотні відмінності у масштабах числових характеристик, висока корельованість ознак і нерівномірність представлення класів, що безпосередньо впливає на здатність моделей до узагальнення. У зв'язку з цим постає потреба не лише в побудові окремих класифікаційних моделей, а в розробленні цілісної інформаційної технології, яка інтегрує всі етапи обробки мережевого трафіку: від формування підготовлених вибірок до навчання моделей і комплексного оцінювання їх ефективності.

Особливої актуальності набуває побудова такої інформаційної технології для двох взаємопов'язаних постановок задачі: бінарного виявлення атак, коли необхідно швидко відокремити нормальний трафік від атакувального, та багатокласового розпізнавання, коли важливо визначити конкретний тип атаки для подальшого реагування на інцидент. Реалізація двох режимів аналізу в межах єдиної інформаційної технології дозволяє поєднати функції первинного виявлення атакувальної активності з її детальнішою інтерпретацією, що підвищує практичну цінність результатів дослідження для систем виявлення атак у комп'ютерних мережах.

Для проведення дослідження доцільним є використання сучасного репрезентативного набору даних, придатного для відтворюваного експериментального аналізу. У роботі таким набором обрано CIC-IDS2017, який містить описи мережевих потоків нормального та атакувального трафіку, охоплює кілька категорій атак і дозволяє досліджувати задачу виявлення атак як у бінарній, так і в багатокласовій постановках. Використання цього набору даних створює основу для методично коректного порівняння моделей машинного навчання та побудови відтворюваного експериментального конвеєра.

Відтак, вибір теми дисертаційного дослідження зумовлений практичною потребою у підвищенні ефективності виявлення атак у комп'ютерних мережах та науковою необхідністю розроблення інформаційної технології інтелектуального моніторингу мережевого трафіку, яка забезпечує методично коректну підготовку даних, підтримує бінарний і багатокласовий режими

класифікації, а також дозволяє підвищити достовірність і відтворюваність результатів функціонування систем виявлення атак.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано в Національному технічному університеті «Дніпровська політехніка» відповідно до плану науково-дослідних робіт кафедри безпеки інформації та телекомунікацій у межах науково-дослідної роботи «Інтелектуальні методи моделювання процесів в інформаційно-телекомунікаційних системах критичної інфраструктури» (державний обліковий номер 0225U004731, дата реєстрації 17.12.2025, термін виконання етапу: 01.2024–12.2025). У межах зазначеної науково-дослідної роботи автором виконано дослідження, пов'язані з розробленням інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак, підготовкою даних мережевого трафіку, побудовою моделей машинного навчання та експериментальним оцінюванням їх ефективності.

Мета і завдання дослідження. Метою роботи є розв'язання актуальної науково-прикладної задачі підвищення ефективності виявлення атак і розпізнавання їх типів у комп'ютерних мережах шляхом розроблення інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак (СВА), що базується на методах машинного навчання та забезпечує функціонування в бінарному і багатокласовому режимах аналізу.

Для досягнення поставленої мети в роботі сформульовано такі завдання:

– проаналізувати сучасні методи та засоби моніторингу мережевого трафіку та виявлення атак, класифікацію систем IDS/IPS, а також методи машинного навчання, що застосовуються в задачах інтелектуального аналізу мережевого трафіку;

– обґрунтувати вибір набору даних для проведення дослідження та визначити вимоги до підготовки даних мережевого трафіку для задач інтелектуального виявлення атак;

– розробити метод підготовки даних, класифікації та оцінювання мережевого трафіку для систем виявлення атак;

– сформувати вибірки для бінарного виявлення атак і багатокласового розпізнавання їх типів, а також реалізувати процедури балансування даних для підвищення коректності навчання моделей;

– розробити архітектуру інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для СВА, яка передбачає послідовну обробку мережевого трафіку, формування ознакового простору, навчання моделей машинного навчання та оцінювання результатів;

– розробити програмну реалізацію інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі, що об'єднує етапи підготовки даних, формування ознакового простору, навчання моделей машинного навчання та оцінювання результатів;

– реалізувати та дослідити моделі машинного навчання для бінарної класифікації мережевого трафіку і багатокласового розпізнавання типів атак;

– провести експериментальне дослідження ефективності розробленої інформаційної технології на основі набору даних CIC-IDS2017 із використанням системи взаємодоповнювальних метрик оцінювання;

– оцінити придатність розробленої інформаційної технології для використання як основи побудови інтелектуальних компонентів систем виявлення атак у комп'ютерних мережах.

Об'єкт дослідження – моніторинг трафіку комп'ютерної мережі в системах виявлення атак.

Предмет дослідження – методи, моделі та засоби побудови інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак.

Методи дослідження.

Теоретичний аналіз – вивчення наукової літератури, публікацій і сучасних науково-технічних рішень у сфері моніторингу мережевого трафіку, виявлення атак, класифікації систем IDS/IPS та застосування методів машинного навчання в задачах кібербезпеки; системний аналіз – використано для формування структури інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі, визначення взаємозв'язків між етапами підготовки даних, побудови моделей та оцінювання результатів; статистичний аналіз – застосовано для дослідження набору даних CIC-IDS2017, виявлення пропущених, нескінченних і дубльованих значень, аналізу розподілів ознак, кореляційних залежностей та оцінювання репрезентативності вибірок; методи попередньої обробки даних – використано для очищення даних, уніфікації структури ознак, заповнення пропущених значень, стандартизації числових характеристик, зменшення надлишковості ознак і зниження розмірності ознакового простору; методи машинного навчання – застосовано для аналізу та класифікації мережевого трафіку. Для бінарного виявлення атак використано логістичну регресію та метод опорних векторів, а для багатокласового розпізнавання типів атак – випадковий ліс, дерево рішень і метод k-найближчих сусідів; методи балансування даних – використано для усунення дисбалансу класів у вибірках, зокрема випадкове зменшення класу більшості для бінарної класифікації та метод SMOTE (Synthetic Minority Over-sampling Technique) для багатокласового розпізнавання типів атак, що дало змогу підвищити коректність навчання моделей машинного навчання; експериментальний метод – застосовано для перевірки ефективності розробленої інформаційної технології в умовах бінарної та багатокласової класифікації мережевого трафіку; методи оцінювання якості моделей – використано для аналізу результатів класифікації за допомогою показників accuracy, precision, recall, F1-score, ROC-AUC, Precision–Recall-кривих, матриць помилок і перехресної перевірки; методи візуалізації даних – застосовано для графічного подання результатів аналізу даних, кореляційної структури ознак, матриць помилок і порівняння ефективності моделей.

Наукова новизна одержаних результатів

вперше розроблено інформаційну технологію інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак, яка, на відміну від існуючих науково-технічних рішень, забезпечує в межах єдиного

програмного модуля повний цикл підготовки даних мережевого трафіку, формування ознакового простору, побудови вибірок, балансування, навчання моделей машинного навчання та комплексного оцінювання результатів для двох взаємопов'язаних постановок задачі – бінарного виявлення атак і багатокласового розпізнавання їх типів;

удосконалено метод підготовки даних, класифікації та оцінювання мережевого трафіку для систем виявлення атак, який відрізняється інтегрованим поєднанням процедур попередньої обробки даних, аналізу та зниження розмірності ознакового простору, формування й балансування вибірок, навчання моделей машинного навчання та оцінювання їх якості, що забезпечує підвищення ефективності підготовки даних і розв'язання задач бінарного виявлення атак та багатокласового розпізнавання їх типів;

набули подальшого розвитку методичні положення комплексного оцінювання ефективності моделей машинного навчання в задачах моніторингу мережевого трафіку, які відрізняються уніфікованим поєднанням покласових метрик якості класифікації, ROC-AUC, Precision–Recall-кривих, матриць помилок і п'ятикратної перехресної перевірки та дають змогу визначати ефективні конфігурації моделей для двох режимів функціонування інформаційної технології: первинного бінарного виявлення атак і подальшого багатокласового розпізнавання їх типів.

Практичне значення одержаних результатів.

Практичне значення одержаних результатів полягає у розробці програмної реалізації інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі, яка може бути використана як основа для побудови інтелектуальних компонентів сучасних систем виявлення атак. Запропонована інформаційна технологія забезпечує автоматизований аналіз мережевого трафіку, підготовку вхідних даних до класифікації, виявлення атакувальної активності в бінарному режимі та розпізнавання типів атак у багатокласовому режимі, що підвищує ефективність підтримки прийняття рішень у сфері кібербезпеки.

Практична цінність результатів дослідження полягає також у можливості використання розробленого програмного модуля для проведення експериментальних досліджень у задачах інтелектуального моніторингу мережевого трафіку, порівняльного аналізу моделей машинного навчання та оцінювання їх ефективності на основі набору даних CIC-IDS2017. Реалізована інформаційна технологія дозволяє відтворювати повний цикл обробки даних мережевого трафіку – від їх інтеграції, очищення, стандартизації та формування ознакового простору до навчання моделей і комплексного оцінювання результатів.

Одержані результати можуть бути використані в діяльності фахівців з кібербезпеки, під час розроблення та вдосконалення систем виявлення атак, а також у науково-дослідній та освітній діяльності закладів вищої освіти для підготовки здобувачів за спеціальностями, пов'язаними з комп'ютерними науками та кібербезпекою.

Впровадження одержаних результатів.

Результати дисертаційної роботи впроваджено в діяльність ТОВ «Центум-Д» для підвищення рівня кібербезпеки корпоративної мережі та інформаційних сервісів підприємства. У межах упровадження використано розроблені методичні положення, алгоритмічні та програмні рішення для інтелектуального моніторингу мережевого трафіку, виявлення аномальної активності, первинної класифікації інцидентів і підтримки прийняття рішень щодо реагування на кіберзагрози. Зазначені рішення інтегровано з наявними засобами захисту, журналювання та моніторингу. Факт упровадження підтверджується актом, наведеним у додатках до дисертації.

Результати дисертаційного дослідження впроваджено в навчальний процес Національного технічного університету «Дніпровська політехніка» та використано під час викладання дисциплін «Кіберзахист» для підготовки здобувачів вищої освіти за спеціальністю 125 Кібербезпека (2022 рік вступу), 125 Кібербезпека та захист інформації (2023 рік вступу). Факт упровадження підтверджується актом, наведеним у додатках до дисертації.

Особистий внесок здобувача.

Дисертаційна робота є самостійно виконаним науковим дослідженням. Усі основні наукові положення, результати, висновки та рекомендації, що виносяться на захист, отримані здобувачем особисто.

У наукових працях (фахові статті категорії Б), опублікованих одноосібно, автору належать: аналіз сучасних систем інтелектуального моніторингу трафіку комп’ютерної мережі для систем виявлення атак; розроблення методу попередньої обробки даних для створення інформаційних моделей в інтелектуальних системах виявлення атак; дослідження методів машинного навчання для бінарної та багатокласової класифікації мережевого трафіку у системах виявлення атак; обґрунтування архітектури інформаційної технології інтелектуального моніторингу мережевого трафіку; аналіз кореляційної матриці показників набору даних CIC-IDS2017; аналіз наборів даних мережевого трафіку для систем виявлення атак; дослідження сучасних систем моніторингу трафіку в комп’ютерній мережі.

У фаховій статті, опублікованій у співавторстві з О. Сафаровим, В. Корнієнком та В. Горєвим, автору належать аналіз вразливостей електронних комунікаційних систем медичного призначення, узагальнення загроз для персональної медичної інформації та участь в обґрунтуванні програмних методів забезпечення кібербезпеки таких систем. Результати цієї публікації використано для поглиблення теоретичних положень дисертаційної роботи щодо кіберзагроз, вразливостей інформаційних систем і комплексного захисту даних.

У наукових працях (тези доповіді на конференціях), опублікованих у співавторстві, особистий внесок здобувача полягає в такому: у роботі, виконаній спільно з Корнієнком В. І., здобувачеві належать аналіз методів і засобів ідентифікації та прогнозування трафіку комп’ютерної мережі для систем виявлення атак, постановка задачі дослідження та узагальнення отриманих результатів; у праці, присвяченій розробці інформаційної технології інтелектуального моніторингу трафіку комп’ютерної мережі для систем

виявлення атак, здобувачеві належать формування основних положень дослідження, обґрунтування структури інформаційної технології та підготовка матеріалів до публікації; у роботі, опублікованій у співавторстві з I. Mamuzić, здобувачеві належать аналіз перспективних напрямів моніторингу трафіку комп'ютерної мережі для систем виявлення атак, узагальнення методів, моделей і засобів інтелектуального виявлення загроз та підготовка основної частини матеріалів.

Матеріали й результати дисертаційного дослідження пройшли апробацію на міжнародних і всеукраїнських науково-технічних та науково-практичних конференціях. Ідеї, положення та результати, що належать співавторам опублікованих праць, у дисертації використано лише з відповідними посиланнями.

Апробація результатів роботи.

Основні положення, результати та висновки дисертаційної роботи доповідалися, обговорювалися та пройшли апробацію на міжнародних і всеукраїнських науково-технічних та науково-практичних конференціях, а саме:

– XIV Міжнародній науково-технічній конференції «ITSec: Безпека інформаційних технологій» (Тернопіль, 22-24 травня 2025 р.) / Західноукраїнський національний університет – Державний університет інформаційно-комунікаційних технологій;

– XII Міжнародній науково-технічній конференції студентів, аспірантів та молодих вчених «Молодь: наука та інновації» (Дніпро, 13-15 листопада 2024 р.) / Національний технічний університет «Дніпровська політехніка»;

– 17th International Symposium of Croatian Metallurgical Society "Materials and Metallurgy" (SHMD 2024) (Загреб, Хорватія, 18-19 квітня 2024 р.) / Zagreb: Hrvatsko metalurško društvo / ISSN 0543-5846;

– I (VII) Міжнародній науково-практичній конференції здобувачів вищої освіти і молодих учених «Інформаційні технології: теорія і практика» (Дніпро, 20-22 березня 2024 р.) / Національний технічний університет «Дніпровська політехніка»;

– XIII Всеукраїнській науково-практичній конференції здобувачів вищої освіти і молодих учених «Молоді вчені 2023 – від теорії до практики» (Дніпро, 23 березня 2023 р.) / Український державний університет науки і технологій;

– XIII Міжнародній науково-технічній конференції студентів, аспірантів та молодих вчених «Наукова весна» (Дніпро, 1-3 березня 2023 р.) / Національний технічний університет «Дніпровська політехніка»;

– XIV Всеукраїнській науково-практичній конференції «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 30 березня 2023 р.) / Національна академія служби безпеки України.

Публікації. За матеріалами дисертації опубліковано 11 робіт, з яких 4 статті включено до переліку фахових видань (категорія Б), затверджених МОН України за спеціальністю дисертації, та 7 – публікації у матеріалах конференцій/симпозіумів (у тому числі 5 міжнародних).

Структура та обсяг дисертації. Повний обсяг дисертації становить 230 сторінок, з яких 190 сторінок основного тексту. Дисертаційна робота складається

зі вступу, чотирьох розділів, висновків, списку використаних джерел (150 найменувань) та додатків. Робота містить 47 рисунків, 13 таблиць та 5 додатків.

Список публікацій здобувача на тему дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації

Публікації у фахових виданнях України:

1. Мєшков, В. (2025). Методи машинного навчання для бінарної та багатокласової класифікації мережевого трафіку у системах виявлення атак. Таврійський науковий вісник. Серія: Технічні науки. 2025, Т. 1, № 4. С. 182-196. DOI: https://doi.org/10.32782/tnv-tech.2025.4.1.20, URL: https://journals.ksauniv.ks.ua/index.php/tech/article/view/1064/977 (Фаховий (категорія Б)).

2. Мєшков, В. (2025). Метод попередньої обробки даних для створення інформаційних моделей в інтелектуальних системах виявлення атак. Information Technology: Computer Science, Software Engineering and Cyber Security, 2025, №2. С. 108-114, DOI: https://doi.org/10.32782/IT/2025-2-11, URL: https://journals.politehnica.dp.ua/index.php/it/article/view/825/742 (Фаховий (категорія Б)).

3. Сафаров, О., Корнієнко, В., Горєв, В., Мєшков, В. (2024). Підвищення кібербезпеки електронних комунікаційних систем медичного призначення. // Information Technology: Computer Science, Software Engineering and Cyber Security, 2024, № 2, С. 128-133, DOI: https://doi.org/10.32782/IT/2024-2-16, URL: https://journals.politehnica.dp.ua/index.php/it/article/view/595/527 (Фаховий (категорія Б)).

4. Мєшков, В. (2023). Аналіз систем інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. // Information Technology: Computer Science, Software Engineering and Cyber Security, 2023, № 1, С. 85-92, DOI: https://doi.org/10.32782/IT/2023-1-11, URL: https://journals.politehnica.dp.ua/index.php/it/article/view/262/233 (Фаховий (категорія Б)).

Наукові праці, які засвідчують апробацію матеріалів дисертації

Матеріали конференцій та тези доповідей:

1. Мєшков В. І. Архітектура інформаційної технології інтелектуального моніторингу мережевого трафіку. // ITSec: Безпека інформаційних технологій: матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. 243с.

2. Мєшков В. І. Аналіз кореляційної матриці для показників набору даних CSE-CIC-IDS2017. // XII Міжнародна науково-технічна конференція студентів, аспірантів та молодих вчених «Молодь: наука та інновації», Дніпро, 13-15 листопада 2024 року (у 3-х томах) / Національний технічний університет «Дніпровська політехніка» – Дніпро: НТУ «ДП», 2024. Том 2. 291с.

3. V.I. Mieshkov, I. Mamuzić. Promising directions of computer network traffic monitoring for intrusion detection systems // 17th International Symposium of Croatian Metallurgical Society „Materials and Metallurgy", SHMD ´2024. Materials And Metallurgy. Book Of Abstracts, Zagreb, Croatia: 2024, April, 18-19, С. 319.

4. Мєшков В. І. Аналіз наборів даних мережевого трафіку для систем виявлення атак // І (VII) міжнародна науково-практична конференція здобувачів вищої освіти і молодих учених «Інформаційні технології: теорія і практика», Дніпро, 20-22 березня 2024 року / Національний технічний університет «Дніпровська політехніка» – Дніпро: НТУ «ДП», 2024, С. 281-285.

5. Мєшков В. І. Сучасні системи моніторингу трафіку в комп'ютерній мережі // XIII Міжнародна науково-технічна конференція студентів, аспірантів та молодих вчених «Наукова весна», Дніпро, 1-3 березня 2023 року / Національний технічний університет «Дніпровська політехніка» – Дніпро: НТУ «ДП», 2023. С. 183-186.

6. Мєшков В. І., Корнієнко В. І. Ідентифікація та прогнозування трафіку комп'ютерної мережі для систем виявлення атак // XIII Всеукраїнська науково-практична конференція здобувачів вищої освіти і молодих учених «Молоді вчені 2023 - від теорії до практики»: Матеріали. Електронне видання. – Дніпро, Журфонд, 2023. С. 164-169.

7. Мєшков В. І., Корнієнко В. І. Розробка інформаційної технології інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак // XIV Всеукраїнська науково-практична конференція «Актуальні проблеми управляння інформаційною безпекою держави», – Київ, 30 березня 2023, / Національна академія Служби безпеки України, Матеріали конференції, 2023. С. 294-298.

Характеристика особистості здобувача

Здобувач ступеня доктора філософії МЄШКОВ Вадим Ігорович народився 04 листопада 1984 р. у м. Дніпро. У 2006 році закінчив Національний гірничий університет, факультет інформаційних технологій, за спеціальністю «Захист інформації в комп'ютерних системах та мережах», отримав диплом магістра НР 30448548 (дата видачі 30.06.2006) та професійну кваліфікацію: інженера з інформаційної безпеки комп'ютерних систем з дослідницьким рівнем діяльності, викладача вищого навчального закладу. Наразі є здобувачем ступеня доктора філософії вечірньої форми навчання, спеціальності 122 Комп'ютерні науки, Національного технічного університету «Дніпровська політехніка», термін навчання: 2022-2026 роки.

У період навчання в аспірантурі здобувач зарекомендував себе як відповідальний, дисциплінований і наполегливий дослідник, здатний до самостійного наукового пошуку, критичного аналізу сучасних науково-технічних рішень і практичної реалізації результатів дослідження. Під час виконання дисертації МЄШКОВ Вадим Ігорович послідовно опрацьовував наукові джерела з проблематики інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак, методів машинного навчання та аналізу великих масивів даних.

Здобувач ступеня доктора філософії виявив належний рівень професійної підготовки, ініціативність, самостійність у постановці та розв'язанні науково-прикладних задач, уміння планувати експериментальні дослідження, працювати з сучасними програмними засобами аналізу даних і вірно інтерпретувати отримані результати. У спілкуванні з науково-педагогічними працівниками

кафедри та колегами проявив доброзичливість, коректність, академічну доброчесність і відповідальне ставлення до виконання індивідуального плану.

МЄШКОВ Вадим Ігорович має науково-педагогічний стаж понад 19 років. У період роботи на кафедрі безпеки інформації та телекомунікацій викладав такі навчальні дисципліни: «Кіберзахист», «Комп'ютерні мережі», «Захист економічної інформації», «Захист інформації в банківських та комерційних системах», «Аналіз безпеки програмного забезпечення» та інші. Здійснював керівництво навчальною і виробничою практиками здобувачів вищої освіти, а також активно залучав студентів до науково-дослідної роботи.

Оцінка мови та стилю дисертації

Матеріали дисертації викладено українською мовою, послідовно, у формально-логічний спосіб, з дотриманням наукового стилю викладення. Оцінка змісту дисертації, її завершеності та відповідності встановленим вимогам позитивна. Анотація відображає основний зміст та результати дослідження. Робота має належну візуалізацію, містить аналітичні матеріали, коректну статистичну інформацію.

Відповідно до п.15 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 р. № 44 (зі змінами № 507 від 03.05.2024 р.), пропонується такий **склад разової спеціалізованої вченої ради:**

Голова ради:

МОРОЗ Борис Іванович, д.т.н., професор, професор кафедри програмного забезпечення комп'ютерних систем, Національного технічного університету «Дніпровська політехніка», м. Дніпро.

Рецензенти:

1. АЛЕКСЄЄВ Михайло Олександрович, д.т.н., професор, завідувач кафедри програмного забезпечення комп'ютерних систем, Національного технічного університету «Дніпровська політехніка», м. Дніпро.

2. ГЕРАСІНА Олександра Володимирівна, к.т.н., доцент, доцент кафедри безпеки інформації та телекомунікацій, Національного технічного університету «Дніпровська політехніка», м. Дніпро.

Офіційні опоненти:

1. ГУЛАК Геннадій Миколайович, д.т.н., професор, професор кафедри інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка, Київського столичного університету імені Бориса Грінченка, м. Київ.

2. СМІРНОВА Тетяна Віталіївна, к.т.ню, доцент, ст. викладач кафедри автоматизації виробничих процесів, Центральноукраїнського національного технічного університету, м. Кропивницький.

За результатами обговорення результатів дисертаційного дослідження здобувача кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка» МЄШКОВА Вадима Ігоровича

УХВАЛИЛИ:

1. Констатувати, що робота є самостійним, завершеним науковим дослідженням, яке за своєю актуальністю, ступенем новизни, обґрунтованості, наукової та практичної цінності здобутих результатів відповідає галузі знань 12 «Інформаційні технології» та спеціальності 122 «Комп'ютерні науки», вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 р. № 261, пп. 6, 7, 8 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 р. № 44.

2. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації МЄШКОВА Вадима Ігоровича на тему: «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак».

3. Рекомендувати дисертаційну роботу МЄШКОВА Вадима Ігоровича на тему: «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак» до захисту на здобуття ступеня доктора філософії у разовій спеціалізованій вченій раді за спеціальністю 122 «Комп'ютерні науки».

4. Рекомендувати Вченій раді Національного технічного університету «Дніпровська політехніка» затвердити склад разової спеціалізованої вченої ради:

Голова ради:

МОРОЗ Борис Іванович, д.т.н., професор, професор кафедри програмного забезпечення комп'ютерних систем, Національного технічного університету «Дніпровська політехніка», м. Дніпро.

Рецензенти:

1. АЛЕКСЄЄВ Михайло Олександрович, д.т.н., професор, завідувач кафедри програмного забезпечення комп'ютерних систем, Національного технічного університету «Дніпровська політехніка», м. Дніпро.

2. ГЕРАСІНА Олександра Володимирівна, к.т.н., доцент, доцент кафедри безпеки інформації та телекомунікацій, Національного технічного університету «Дніпровська політехніка», м. Дніпро.

Офіційні опоненти:

1. ГУЛАК Геннадій Миколайович, д.т.н., професор, професор кафедри інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка, Київського столичного університету імені Бориса Грінченка, м. Київ.

2. СМІРНОВА Тетяна Віталіївна, к.т.н., доцент, ст. викладач кафедри автоматизації виробничих процесів, Центральноукраїнського національного технічного університету, м. Кропивницький.

Результати голосування щодо рекомендації дисертації МЄШКОВА Вадима Ігоровича на тему: «Інформаційна технологія інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак» до

захисту на здобуття ступеня доктора філософії у разовій спеціалізованій вченій раді за спеціальністю 122 «Комп'ютерні науки» присутніх на засіданні:

за – 20 осіб, проти – немає, утримался – немає.

Презентація МЄШКОВА В.І. на 31 стор. додається.

Головуючий на засіданні
Гарант ОНП 122 Комп'ютерні науки, 3 рівня
д.т.н., проф., проф. ПЗКС Борис МОРОЗ

Секретар засідання
асистент кафедри ПЗКС Валерія РУЛІКОВА