ЗАТВЕРДЖУЮ
Проректор з наукової роботи
та інноваційної діяльності
Національного університету біоресурсів
і природокористування України
доктор сільськогосподарських наук,
професор
_____ Оксана ТОНХА
«24» 02 2026 р.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації
Штанька Вадима Ігоровича
на тему: **«Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак»**,
поданої на здобуття ступеня доктора філософії
зі спеціальності **122 «Комп'ютерні науки»**
галузі знань **12 «Інформаційні технології»**

Витяг з протоколу № 1 фахового семінару кафедри комп'ютерних систем, мереж та кібербезпеки факультету інформаційних технологій Національного університету біоресурсів і природокористування України від «12» лютого 2026 року.

Присутні члени фахового семінару кафедри комп'ютерних систем, мереж та кібербезпеки факультету інформаційних технологій Національного університету біоресурсів і природокористування України: О. Є. Коваленко, професор кафедри комп'ютерних систем, мереж та кібербезпеки, доктор технічних наук, професор, гарант освітньо-наукової програми «Інформаційні технології», голова фахового семінару; І. М. Болбот, декан факультету інформаційних технологій, доктор технічних наук, професор; Б. Л. Голуб, завідувач кафедри комп'ютерних наук, кандидат технічних наук, доцент; О. Г. Глазунова, проректор з науково-педагогічної роботи та цифрової трансформації, професор кафедри інформаційних систем і технологій, доктор педагогічних наук, професор; Д. Ю. Касаткін, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки, кандидат педагогічних наук, доцент; Н. А. Клименко, доцент кафедри економічної кібернетики, кандидат економічних наук, доцент; В. М. Кравченко, професор кафедри економічної кібернетики, доктор економічних наук, доцент; О. В. Криворучко, професор кафедри комп'ютерних систем, мереж та кібербезпеки, доктор технічних наук, професор, експертка; В. А. Лахно, професор кафедри комп'ютерних систем, мереж та кібербезпеки, доктор технічних наук, професор; С. М. Мамченко, професор кафедри комп'ютерних систем, мереж та кібербезпеки, доктор педагогічних наук, професор; М. В. Мокрієв, доцент кафедри інформаційних систем і технологій, кандидат економічних наук, доцент; Є. В. Нікітенко, доцент кафедри комп'ютерних систем, мереж та кібербезпеки, кандидат технічних наук, доцент, науковий керівник; А. В. Сагун, доцент кафедри комп'ютерних систем, мереж та кібербезпеки, кандидат технічних наук, доцент, експерт; В. М. Смолій, професор кафедри інформаційних систем і технологій, доктор технічних наук, професор; М. З. Швиденко, завідувач кафедри інформаційних систем і технологій, кандидат економічних наук, доцент; Т. В. Волошина, доцент кафедри інформаційних систем і технологій, кандидат педагогічних наук, доцент; В. В. Шкарупило, професор кафедри комп'ютерних систем, мереж та кібербезпеки, доктор технічних наук, доцент, експерт; Є. А. Лавров, професор кафедри інформаційних технологій Сумського державного університету, доктор технічних наук, професор.

Інші присутні на засіданні фахового семінару кафедри комп'ютерних систем, мереж та кібербезпеки факультету інформаційних технологій Національного університету біоресурсів і природокористування України: В. І. Штанько, здобувач ступеня доктора філософії.

Порядок денний: обговорення основних наукових результатів дисертації **Штанька Вадима Ігоровича** на тему: **«Інформаційна технологія та інструментальні засоби створення інтелектуальної діагностичної системи захисту інформації»**, поданої на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Тему дисертації затверджено науковою радою факультету інформаційних технологій Національного університету біоресурсів і природокористування України (протокол № 2 від 04 жовтня 2022 року).

Дисертацію виконано на кафедрі комп'ютерних систем, мереж та кібербезпеки факультету інформаційних технологій Національного університету біоресурсів і природокористування України.

Науковий керівник: кандидат фізико-математичних наук, доцент **Нікітенко Євгеній Васильович**, доцент кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України.

Слухали: доповідь здобувача В. І. Штанька про основні положення дисертації. Здобувач представив основні результати дослідження, розкрив зміст, мету та науково-практичну значущість дисертації. У доповіді обґрунтовано актуальність теми з огляду на зростання вимог до створення ефективних інформаційних технологій аналізу мережевого трафіку в умовах поширення кібератак та необхідність забезпечення адаптивності систем виявлення вторгнень до змінних умов функціонування інформаційно-комунікаційного середовища.

Метою дисертації визначено розроблення та обґрунтування інформаційної технології дворівневої інтелектуальної системи аналізу мережевих атак, методів адаптивної обробки мережевого трафіку в умовах варіативної зміни його характеристик, а також моделей машинного навчання для підвищення ефективності виявлення та класифікації мережевих атак. У науковій новизні підкреслено, що вперше розроблено інформаційну технологію аналізу мережевих атак у віртуалізованому середовищі, яка реалізує замкнений цикл «генерація – маркування – класифікація» та забезпечує формування верифікованих навчальних наборів даних без евристичної розмітки. Удосконалено метод виявлення вторгнень на основі адаптивного налаштування порогів класифікації з використанням мінімізації баєсівського ризику та оцінки зсуву домену за зваженою дивергенцією Кульбака-Лейблера, що дозволяє автоматично коригувати чутливість системи до змін характеристик трафіку. Методологічну основу дослідження становлять методи системного аналізу та проєктування, баєсівський підхід до прийняття рішень, методи аналізу даних і статистичного моделювання, а також об'єктно-орієнтований підхід до програмної реалізації. Обґрунтовано дворівневу архітектуру системи виявлення атак і механізм адаптивного налаштування порогів на основі оцінки статистичного зсуву мережевого трафіку. Емпіричною базою слугували експериментальні дані, отримані в ізольованому віртуальному середовищі, що забезпечило безпечну емуляцію мережевих атак і перевірку ефективності запропонованих рішень за результатами експериментального та синхронного віконного аналізу. Основні результати роботи полягають у розробленні архітектури інформаційної технології дворівневої інтелектуальної системи аналізу мережевих атак, орієнтованої на адаптивне функціонування та інтеграцію з існуючими засобами моніторингу мережевої безпеки. Створено алгоритми потокової обробки та класифікації мережевого трафіку, що забезпечують автоматичне виявлення атак і визначення їх типу в умовах статистичної нестабільності даних. Сформовано дворівневу ієрархічну модель на основі наївного баєсівського класифікатора та випадкового лісу з механізмом відмови від рішення, що дозволяє досягти балансу між обчислювальною ефективністю та точністю атрибуції атак. Реалізовано механізм адаптивного налаштування

порогів прийняття рішень на основі оцінки зсуву домену, що забезпечує стабільність функціонування системи без необхідності повного перенавчання моделей. Розроблення та впровадження запропонованої інформаційної технології має безпосереднє практичне значення для організацій, що прагнуть підвищити рівень автоматизації та надійності систем виявлення вторгнень. Запропонований підхід забезпечує зменшення кількості помилкових рішень, підвищення стійкості до зміни характеристик трафіку та можливість масштабування під нові типи кіберзагроз. Практичне застосування результатів у складі програмних комплексів аналізу мережевого трафіку та систем IDS/IPS робить дослідження придатним до впровадження в реальних інформаційно-комунікаційних середовищах.

Здобувачеві було поставлено 15 запитань, на які він надав обґрунтовані відповіді та пояснення.

Виступили:

Науковий керівник – кандидат фізико-математичних наук, доцент Є. В. Нікітенко, який відзначив актуальність теми дисертації В. І. Штанька, що присвячена розробленню інформаційної технології дворівневої інтелектуальної системи аналізу мережевих атак в умовах варіативної зміни характеристик трафіку. У своєму виступі науковий керівник наголосив, що здобувач продемонстрував глибокі теоретичні знання у галузі систем виявлення вторгнень, теорії ймовірностей та машинного навчання, володіння сучасними методами аналізу даних і проєктування програмних систем, а також уміння комплексно поєднувати математичні підходи з експериментальним моделюванням для вирішення прикладних завдань кібербезпеки. Було підкреслено, що результати дослідження мають суттєву наукову новизну, зокрема вперше розроблено інформаційну технологію аналізу мережевих атак із замкненим циклом «генерація – маркування – класифікація», у межах якої поєднано три ключові компоненти: бінарну фільтрацію трафіку на основі наївного баєсівського підходу, багатокласову атрибуцію атак із використанням моделі випадкового лісу та механізм адаптивного налаштування порогів прийняття рішень на основі оцінки зсуву домену. Таке поєднання забезпечило зниження вартості помилкових рішень, підвищення стійкості до статистичної нестабільності мережевого трафіку та створило основу для побудови адаптивних систем виявлення вторгнень нового покоління. Також зазначено, що здобувач повною мірою виконав освітньо-наукову програму «Інформаційні технології», успішно опанував навчальні дисципліни, продемонстрував високий рівень аналітичного мислення, самостійності та відповідальності під час виконання наукового дослідження. У процесі підготовки дисертації В. І. Штанько зарекомендував себе як ініціативний та цілеспрямований дослідник, здатний формулювати складні наукові завдання у сфері інформаційної безпеки, обґрунтовано їх вирішувати та чітко презентувати отримані результати на наукових семінарах. Отримані результати є самостійним науковим здобутком, що має теоретичне та практичне значення для розвитку інтелектуальних систем аналізу мережевого трафіку та сучасних технологій кіберзахисту.

Експерти:

Криворучко О. В., доктор технічних наук, професор, позитивно оцінила дисертацію здобувача та підтвердила, що вона відповідає всім вимогам до досліджень на здобуття ступеня доктора філософії зі спеціальності 122 «Комп’ютерні науки». У рецензії відзначено високий рівень наукової обґрунтованості та завершеності дослідження, достатню кількість і якість публікацій, а також належну апробацію результатів на конференціях. Експертка підкреслила, що робота є самостійною науковою працею, виконаною без порушень принципів академічної доброчесності, з чіткою структурою та логічним викладом матеріалу. Серед зауважень експертка відзначила необхідність більш детального обґрунтування вибору розміру вікна агрегації мережевого трафіку та аналізу його впливу на швидкість детекції й стабільність функціонування системи. Також було рекомендовано стисло й більш структуровано подати інтерпретацію графіків і таблиць, зокрема у частині пояснення різкого зниження показників ефективності при переході між різними наборами даних. Окрему увагу звернуто на доцільність додаткового роз’яснення впливу порогів першого рівня класифікації

на подальшу каскадну перевірку, з метою чіткого демонстрування механізму контролю над помилковими відсівами на етапі первинної фільтрації. Водночас було підкреслено, що зазначені зауваження мають уточнювальний характер і не знижують наукової та практичної цінності дисертації, яка вирізняється актуальністю, системністю викладу та комплексним підходом до розв'язання задач адаптивного виявлення та класифікації мережевих атак.

На основі проведеного аналізу дисертації експерткою запропоновано дати їй загальну позитивну оцінку, як такій, що відповідає вимогам 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 № 44 від 12 січня 2022 року, та рекомендувати дисертацію для подання до розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Сагун А. В., кандидат технічних наук, доцент, у своєму виступі наголосив на високій актуальності обраної тематики, зумовленій зростанням складності кіберзагроз та необхідністю створення адаптивних систем виявлення атак, здатних функціонувати в умовах нестабільності мережевого середовища. Було відзначено, що розроблення інформаційних технологій, орієнтованих на поєднання математично обґрунтованих методів прийняття рішень із експериментально верифікованими моделями машинного навчання, відповідає сучасним тенденціям розвитку систем кіберзахисту та має значний прикладний потенціал. Водночас основне зауваження стосувалося недостатньо розгорнутого порівняльного аналізу запропонованої системи з існуючими рішеннями IDS, зокрема щодо архітектурних підходів, механізмів адаптації до зміни трафіку та показників ефективності в реальних умовах експлуатації. Експерт звернув увагу на доцільність представлення систематизованого зіставлення функціональних можливостей, принципів прийняття рішень і стратегій обробки невизначеності з відомими відкритими та комерційними рішеннями, що дозволило б чіткіше окреслити конкурентні переваги запропонованої інформаційної технології.

На основі проведеного аналізу дисертації експертом запропоновано дати їй загальну позитивну оцінку, як такій, що відповідає вимогам 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 № 44 від 12 січня 2022 року, та рекомендувати дисертацію для подання до розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

В обговоренні результатів дисертації взяли участь: доктор технічних наук, професор І. М. Болбот; доктор технічних наук, професор О. Є. Коваленко; доктор технічних наук, професор В. А. Лахно; кандидат педагогічних наук, доцент Д. Ю. Касаткін; кандидат фізико-математичних наук, доцент Є. В. Нікітенко.

Виступаючі зазначили, що дисертацію В. І. Штанька виконано на важливу тему, робота містить значну кількість нових наукових даних, має наукову новизну, актуальність, важливе теоретичне та практичне значення, відповідає вимогам наказу Міністерства освіти і науки України № 40 від 12 січня 2017 року «Про затвердження вимог до оформлення дисертації», 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 № 44 від 12 січня 2022 року.

Було запропоновано уточнити формулювання теми дисертації з метою більш чіткого відображення її предметної спрямованості та наукової новизни, затвердити її в такій редакції: «Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак» та підтримано пропозицію експертів про рекомендацію дисертації В. І. Штанька

для подання до розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Постановили: заслухавши та обговоривши дисертацію **Штанька Вадима Ігоровича** на тему: **«Інформаційна технологія та інструментальні засоби створення інтелектуальної діагностичної системи захисту інформації»**, члени фахового семінару кафедри комп'ютерних систем, мереж та кібербезпеки факультету інформаційних технологій Національного університету біоресурсів і природокористування України ухвалили:

1. Актуальність теми дисертації. Дисертацію В. І. Штанька присвячено розробленню інформаційної технології дворівневої інтелектуальної системи аналізу мережевих атак. Актуальність дослідження зумовлена зростанням кількості та складності кіберзагроз, а також необхідністю створення адаптивних систем виявлення вторгнень, здатних ефективно функціонувати в умовах варіативної зміни характеристик мережевого трафіку. Сучасні інформаційно-комунікаційні системи працюють у середовищі постійної еволюції атак, що ускладнює застосування традиційних сигнатурних або статичних методів детекції. Існуючі підходи часто демонструють зниження ефективності при зміні статистичного профілю трафіку та потребують регулярного перенавчання моделей або ручного налаштування параметрів. Розвиток технологій машинного навчання, а також можливості створення контрольованих віртуалізованих середовищ для моделювання атак відкривають передумови для впровадження інтелектуальних систем аналізу трафіку з механізмами адаптації до зсуву домену. Запропонована у роботі інформаційна технологія поєднує математично обґрунтовані методи прийняття рішень із експериментально верифікованими моделями машинного навчання, що забезпечує підвищення надійності виявлення та класифікації мережевих атак. Дослідження є актуальним як з наукового, так і з практичного погляду, оскільки спрямоване на розвиток адаптивних інтелектуальних систем кіберзахисту та може бути використане для вдосконалення сучасних рішень у сфері мережевої безпеки.

2. Зв'язок теми дисертації з державними програмами, науковими напрямами Університету та кафедри. Тема дисертації відповідає пріоритетним тематичним напрямам наукових досліджень, визначеним постановою Кабінету Міністрів України № 476-2024-п. Дослідження належить до напрямів «Інформаційні та комунікаційні технології», «Системи штучного інтелекту», «Інтелектуальні інтерактивні інформаційно-аналітичні системи», а також «Інформаційно-комунікаційні системи та мережі», оскільки спрямоване на розроблення програмно-алгоритмічних засобів аналізу мережевого трафіку з використанням методів машинного навчання. Запропонована інформаційна технологія реалізує сучасні підходи до обробки даних, адаптивного прийняття рішень та побудови інтелектуальних інформаційних систем, що узгоджується з державними пріоритетами розвитку цифрових технологій та штучного інтелекту. Тема дисертації повністю відповідає науковим напрямам факультету інформаційних технологій та кафедри комп'ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України, які охоплюють дослідження у галузі інтелектуальних інформаційних систем, обробки великих масивів даних, машинного навчання, систем підтримки прийняття рішень.

3. Особистий внесок здобувача в отриманні наукових результатів та вирішенні конкретного наукового завдання. Здобувачем самостійно проведено аналіз наукових джерел, нормативно-правової бази та сучасних підходів до побудови систем виявлення вторгнень, а також здійснено оцінку стану існуючих методів аналізу мережевого трафіку на основі машинного навчання. Розроблено архітектуру інформаційної технології дворівневої інтелектуальної системи аналізу мережевих атак, що об'єднує підсистеми захоплення та агрегації потоків, бінарної фільтрації та багатокласової атрибуції з механізмом відмови від рішення. Самостійно сформовано математичну модель адаптивного налаштування порогів прийняття рішень на основі мінімізації баєсівського ризику та оцінки зсуву домену

із використанням дивергенції Кульбака-Лейблера. Реалізовано алгоритми дворівневої класифікації з використанням наївного баєсівського підходу та моделі випадкового лісу, а також розроблено експериментальне віртуалізоване середовище для безпечної емуляції сценаріїв атак і формування верифікованих наборів даних. Здобувач особисто розробив програмні модулі системи, зокрема компоненти перехоплення потоків, навчання та застосування моделей, а також реалізував повний цикл оброблення даних від захоплення сирого трафіку до дворівневої класифікації. Інтерпретацію результатів, формулювання висновків і практичних рекомендацій здійснено під науковим консультуванням керівника, при цьому всі основні положення дисертації, що виносяться на захист, є самостійним науковим здобутком здобувача. Особистий внесок у публікаціях, виконаних у співавторстві, чітко визначено у списку наукових праць.

4. Достовірність і обґрунтованість отриманих результатів і запропонованих автором рішень, висновків, рекомендацій. Результати дисертаційного дослідження здобувача є достовірними, відтворюваними та науково обґрунтованими, що забезпечено належним методичним рівнем виконаних досліджень і використанням сучасного програмно-аналітичного інструментарію. У процесі роботи застосовано загальнонаукові та спеціальні методи дослідження, зокрема системний аналіз, об’єктно-орієнтоване проєктування, методи теорії ймовірностей і математичної статистики, баєсівський підхід до прийняття рішень, алгоритми машинного навчання (наївний баєсівський класифікатор, випадковий ліс), а також методи кількісної оцінки статистичного зсуву на основі дивергенції Кульбака-Лейблера. Достовірність отриманих висновків підтверджено результатами експериментальних досліджень, проведених у контрольованому віртуалізованому середовищі, а також аналізом ефективності моделей за сукупністю показників якості класифікації. Проведений синхронний віконний аналіз дозволив оцінити стабільність функціонування системи в умовах зміни статистичного профілю трафіку. Практичну цінність запропонованих рішень підтверджено їх програмною реалізацією та можливістю відтворення експериментів у створеному середовищі емуляції мережевих атак.

5. Наукова новизна основних результатів дослідження. Наукова новизна дисертації ґрунтується на комплексному використанні методів машинного навчання та теорії прийняття рішень для побудови адаптивної системи аналізу мережевих атак і полягає у такому: уперше розроблено інформаційну технологію виявлення атак у віртуалізованому середовищі із замкненим циклом «генерація – маркування – потокова класифікація», що забезпечує формування верифікованих навчальних наборів без евристичної розмітки. Запропоновано модель адаптивного налаштування порогів класифікації на основі мінімізації баєсівського ризику та оцінки зсуву домену за допомогою зваженої дивергенції Кульбака-Лейблера, що дозволяє автоматично коригувати чутливість системи до змін трафіку. Набув подальшого розвитку метод оцінювання ефективності IDS через застосування синхронного віконного аналізу замість статичних метрик, що дає змогу виявляти деградацію якості моделей при зміні статистичного профілю даних. Удосконалено архітектурний підхід до побудови систем виявлення вторгнень шляхом впровадження дворівневої ієрархічної структури на основі наївного баєсівського класифікатора та випадкового лісу з механізмом відмови від рішення, що забезпечує баланс між обчислювальною ефективністю та точністю атрибуції атак.

Зазначені елементи новизни демонструють, що дисертація містить оригінальні наукові результати.

6. Практична цінність результатів дослідження та їх впровадження. Практична цінність дисертації здобувача полягає у створенні інформаційної технології дворівневої інтелектуальної системи аналізу мережевих атак, розроблення та впровадження якої має безпосереднє практичне значення для організацій, що використовують інформаційно-комунікаційні системи та прагнуть підвищити ефективність моніторингу мережевого трафіку. Запропонований підхід забезпечує підвищення точності виявлення та класифікації

атак за рахунок адаптивного налаштування порогів прийняття рішень, зменшення кількості помилкових спрацювань і збереження стабільності роботи системи в умовах зміни статистичних характеристик трафіку. Практичне застосування результатів у складі програмних комплексів аналізу мережевого трафіку, систем IDS/IPS або інших засобів моніторингу мереж дозволяє автоматизувати процес виявлення загроз і підвищити надійність функціонування інформаційних систем. Реалізація розробленої технології у вигляді програмного засобу та створення віртуалізованого середовища для тестування забезпечують можливість її впровадження та адаптації до реальних умов експлуатації.

7. Перелік наукових праць, які відображають основні результати дисертації. Основні положення виконаного В. І. Штаньком дослідження опубліковано у 7 наукових працях, з яких стаття у науковому виданні, включеному до міжнародних наукометричних баз даних Scopus та/або Web of Science Core Collection, стаття у наукових виданнях, включеному до Переліку наукових фахових видань України, 5 тез наукових доповідей.

Стаття у науковому виданні,
включеному до міжнародних наукометричних баз даних
Scopus та/або Web of Science Core Collection

1. Konyrbaev N., Nikitenko Ye., **Shtanko V.**, Lakhno V., Baishemirov Z., Ibadulla S., Galymzhankyzy A., Myrzabek E. Evaluation and Optimization of the Naive Bayes Algorithm for Intrusion Detection Systems Using the USB-IDS-1 Dataset. Eastern-European Journal of Enterprise Technologies. 2024. Vol. 6. No. 2 (132). P. 74–82. *(Konyrbaev N. сформульовано концепцію дослідження та визначено загальну постановку задачі оцінювання ефективності алгоритму Naive Bayes в IDS. Nikitenko Y. визначено наукову гіпотезу щодо залежності ефективності моделі від кількості записів і кількості класів та забезпечено методологічне керівництво дослідженням. Shtanko V. реалізовано модель Gaussian Naive Bayes у середовищі Python, виконано підготовку та оброблення даних USB-IDS-1, сформульовано експериментальний протокол із двома групами розрахунків (залежність від обсягу даних та від кількості класів), здійснено обчислення accuracy та precision, проведено регресійний аналіз отриманих результатів і сформульовано висновки щодо обмежень алгоритму у багатокласовому режимі. Lakhno V. здійснено інтерпретацію результатів дослідження в контексті практичного застосування систем виявлення вторгнень. Myrzabek E визначено структуру експериментального дизайну та організацію ітераційних обчислень. Ibadulla S. забезпечено формалізацію структури вхідних даних та підготовку наборів для експериментального аналізу. Galymzhankyzy A. виконано статистичну обробку експериментальних результатів та підготовлено графічну інтерпретації залежностей. Baishemirov Z. здійснено узагальнення результатів дослідження та підготовку матеріалів до публікації)*.

Стаття у науковому виданні,
включеному до Переліку наукових фахових видань України

2. **Штанько В.**, Нікітенко Є. Проєктування та реалізація віртуального середовища для аналізу мережевого трафіку. Наука і техніка сьогодні. 2025. № 7 (48). С. 2028–2045. *(Штанько В. спроєктовано архітектуру ізольованого віртуального середовища на базі GNS3 та VirtualBox, реалізовано мережеву топологію з використанням маршрутизатора Cisco 2600, налаштовано IP-адресацію, маршрутизацію та сегментацію підмереж, розгорнуто вузол-«зловмисник» на Kali Linux та вузли-«жертви» на Debian Linux, забезпечено повну ізоляцію віртуальної мережі від зовнішнього середовища, виконано верифікацію топології за допомогою ping, traceroute та аналізу ICMP-пакетів у Wireshark, а також здійснено експериментальну перевірку коректності маршрутизації та мережевої ізоляції. Нікітенко Є. сформульовано концептуальні засади побудови ізольованого дослідницького середовища для аналізу мережевих атак, визначено методологічні вимоги до контрольованості та відтворюваності експериментальної платформи, а також здійснено науковий супровід і редакційне опрацювання матеріалів)*.

Тези наукових доповідей

3. **Штанько В. І.**, Нікітенко Є. В. Актуальні методи побудови систем виявлення вторгнень. Теоретичні та прикладні аспекти розробки комп'ютерних систем '2023': V Всеукраїнська науково-практична конференція студентів і аспірантів, м. Київ, 26 квітня 2023 року: тези доповіді. Київ, 2023. С. 180–181. *(Штаньком В. І. здійснено огляд наявних методів побудови систем виявлення вторгнень, виконано аналіз класифікації IDS за методами розгортання та способами виявлення атак, узагальнено переваги й обмеження сигнатурних та аномалійних підходів, а також сформульовано висновки щодо доцільності використання сучасних методів у системах захисту інформації. Нікітенком Є. В. визначено концептуальні засади дослідження та здійснено наукове керівництво підготовкою тез)*.

4. Штанько В. І. Порівняльний аналіз навчальних наборів даних для машинного навчання систем виявлення вторгнень. Інформаційні технології: економіка, техніка, освіта '2023': XIV Міжнародна науково-практична конференція молодих вчених, м. Київ, 26–27 жовтня 2023 року: тези доповіді. Київ, 2023. С. 244–245.

5. Штанько В. І. Використання аналізаторів трафіку для побудови систем виявлення вторгнень. Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2024': XII Міжнародна науково-практична конференція, м. Київ, 21–22 листопада 2024 року: тези доповіді. Київ, 2024. С. 97–99.

6. Штанько В. І. Швидкодія моделі Naive Bayes з відбором ознак для набору USB-IDS-1. Теоретичні та прикладні аспекти розробки комп'ютерних систем '2025': VII Всеукраїнська науково-практична конференція студентів і аспірантів, м. Київ, 24 квітня 2025 року: тези доповіді. Київ, 2025. С. 375–376.

7. Vadym Shtanko. Usage of GNS3 for cybersecurity research. Achievements of Science and Education in the Modern World. Achievements of Science and Education in the Modern World: 2nd International Scientific Conference, Birmingham, United Kingdom, 14 June 2025: Conference Paper. Birmingham, United Kingdom, 2025. P. 128–130.

8. Апробація основних результатів дослідження. Основні наукові положення, результати та висновки дисертаційного дослідження В. І. Штанька пройшли апробацію на: V Всеукраїнській науково-практичній конференції студентів і аспірантів «Теоретичні та прикладні аспекти розробки комп'ютерних систем 2023» (м. Київ, 2023 р.); XIV Міжнародній науково-практичній конференції молодих вчених «Інформаційні технології: економіка, техніка, освіта '2023» (м. Київ, 2023 р.); XII Міжнародній науково-практичній конференції «Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2024» (м. Київ, 2024 р.); VII Всеукраїнській науково-практичній конференції студентів і аспірантів «Теоретичні та прикладні аспекти розробки комп'ютерних систем '2025» (м. Київ, 2025 р.); 2nd International Scientific Conference Achievements of Science and Education in the Modern World (м. Бірмінгем, Велика Британія, 2025 р.).

Ухвалили:

Внести зміни до теми дисертації та затвердити її у такій редакції: «Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак».

Дисертація здобувача ступеня доктора філософії Штанька Вадима Ігоровича на тему: «Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак» є завершеною кваліфікаційною науковою працею, у якій вирішено актуальне наукове завдання щодо створення інтелектуальної інформаційної технології для генерації персональних рекомендацій та супроводу процедури вибору дисциплін для забезпечення індивідуалізації навчання, що має істотне значення для галузі знань 12 «Інформаційні технології».

Дисертація відповідає вимогам наказу Міністерства освіти і науки України № 40 від 12 січня 2017 року «Про затвердження вимог до оформлення дисертації», 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 № 44 від 12 січня 2022 року.

З урахуванням наукової зрілості та професійних якостей здобувача Штанька Вадима Ігоровича дисертація на тему: «Інформаційна технологія дворівневої інтелектуальної системи аналізу мережевих атак» рекомендується для подання розгляду та захисту у разовій спеціалізованій вченій раді на здобуття ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Рішення прийнято одноголосно.

Головуючий на засіданні фахового семінару
кафедри інформаційних систем і технологій
факультету інформаційних технологій
Національного університету біоресурсів
і природокористування України
професор кафедри комп'ютерних систем,
мереж та кібербезпеки,
доктор технічних наук, професор **Олексій КОВАЛЕНКО**

Експерти:
Професор кафедри комп'ютерних систем,
мереж та кібербезпеки
Національного університету біоресурсів
і природокористування України,
доктор технічних наук, професор **Олена КРИВОРУЧКО**

Доцент кафедри комп'ютерних систем,
мереж та кібербезпеки
Національного університету біоресурсів
і природокористування України
кандидат технічних наук, доцент **Андрій САГУН**

Відповідальний за атестацію здобувачів
вищої освіти ступеня доктора філософії **Сергій БОЯРЧУК**