



ЗАТВЕРДЖУЮ

**Ректор Національного університету
«Одеська юридична академія»**

Олег ТОДОЩАК

2026 року

ВИСНОВОК

Національного університету «Одеська юридична академія» щодо дисертації Дикої Анастасії Іванівни на тему: «Методи машинного навчання в тестуванні безпеки веборієнтованого програмного забезпечення», поданої на здобуття ступеня доктора філософії в галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки» (тема затверджена Вченою радою Національного університету «Одеська юридична академія» 25 листопада 2024 року, протокол № 3)

Витяг

**з протоколу розширеного засідання кафедри програмної інженерії
Національного університету «Одеська юридична академія»
№ 3 від 30 березня 2026 року**

Присутні:

кафедра програмної інженерії: в.о. завідувача кафедри, кандидат педагогічних наук, доцент Логінова Н.І. (головуюча); доцент кафедри, кандидат технічних наук, доцент Трофименко О.Г. (науковий керівник); доцент кафедри, кандидат технічних наук, доцент Манаков С.Ю.; доцент кафедри, кандидат педагогічних наук, доцент Лобода Ю.Г.; доцент кафедри, кандидат юридичних наук, доцент Чанишев Р.І.; доцент кафедри, кандидат технічних наук, доцент Чикунов П.О.; доцент кафедри, кандидат технічних наук, доцент Щербина Ю.В.; асистент кафедри Дика А.І. (здобувачка); асистент кафедри Литвин О.С.

кафедра кібербезпеки: в.о. завідувача кафедри, доктор технічних наук, професор Соколов А.В.; доцент кафедри, кандидат технічних наук, доцент Ахмаметьєва Г.В.; доцент кафедри, кандидат технічних наук, доцент Бойко В.Д.; доцент кафедри, кандидат технічних наук, доцент Кухаренко С.В.; доцент кафедри, кандидат фізико-математичних наук, доцент Чепурна О.Є.; асистент кафедри, доктор філософії в галузі права Слатвінська В.М.; доцент кафедри, кандидат юридичних наук, доцент, декан Факультету кібербезпеки та інформаційних технологій Дикий О.В.; професор кафедри, доктор технічних наук, професор Казакова Н.Ф.; асистент кафедри Рачук В.О.

кафедра штучного інтелекту та математичного моделювання: в.о. завідувача кафедри, доктор економічних наук, професор Горбаченко С.А.; доцент кафедри, кандидат технічних наук Гура В.І.; доцент кафедри, кандидат технічних наук, доцент Задерейко О.В.; доцент кафедри, кандидат економічних наук, доцент Куклінова Т.В.; доцент кафедри, кандидат фізико-математичних наук, доцент Черевко Є.В.; старший викладач кафедри Баландіна Н.М.; асистент кафедри Овчинников М.Ю.; асистент кафедри Разінкін Н.С.; асистент кафедри Скідан В.С.; асистент кафедри Толокнов А.А.

Порядок денний:

Обговорення дисертаційного дослідження Дикої Анастасії Іванівни на тему: «Методи машинного навчання в тестуванні безпеки веборієнтованого програмного забезпечення», поданого на здобуття ступеня вищої освіти доктора філософії за спеціальністю 122 «Комп'ютерні науки» щодо рекомендації до разового публічного захисту дисертації у спеціалізованій вченій раді.

Слухали:

Доповідь здобувачки ступеня вищої освіти доктора філософії Дикої А.І. на тему: «Методи машинного навчання в тестуванні безпеки веборієнтованого програмного забезпечення», поданої на здобуття вищої освіти доктора філософії за спеціальністю 122 «Комп'ютерні науки».

Доповідачка обґрунтувала актуальність обраної теми, визначила мету, завдання, методологію дисертаційного дослідження, охарактеризувала його об'єкт та предмет, виклала науково-практичну значимість роботи, надала відомості щодо впровадження результатів дослідження.

Вибір теми дослідження зумовлений науковими інтересами здобувачки у сфері тестування безпеки вебзастосунків, штучного інтелекту та стеганоаналізу, а також практичним досвідом у галузі забезпечення якості програмного забезпечення. У процесі наукової та професійної діяльності було виявлено наявність недостатньо досліджених аспектів щодо виявлення прихованих каналів і фішингових атак у середовищі вебзастосунків, що й визначило доцільність поглибленого дослідження саме цієї проблематики та формування комплексного підходу до її розв'язання.

Актуальність теми дисертаційного дослідження зумовлена стрімкою цифровізацією суспільства та зростанням ролі вебзастосунків як складової критичної інформаційної інфраструктури держави. В умовах постійного збільшення кількості та складності кібератак, зокрема фішингових кампаній і використання прихованих каналів передавання інформації, традиційні засоби тестування безпеки (SAST, DAST, IAST, SCA) не забезпечують належного рівня виявлення сучасних загроз. Особливої гостроти проблема набуває у контексті впровадження CI/CD та концепції DevSecOps, де безпека повинна інтегруватися у всі етапи життєвого циклу програмного забезпечення.

Дисертаційна робота спрямована на розв'язання актуального науково-прикладного завдання – підвищення ефективності тестування безпеки

вебзастосунків шляхом розроблення теоретично обґрунтованих та практично придатних методів виявлення фішингових атак і стеганографічних загроз на основі перетворення Уолша-Адамара та методів машинного навчання. Запропоновані підходи відповідають сучасним викликам кібербезпеки, мають значення для розвитку наукових засад стеганоаналізу та інтелектуального тестування безпеки й можуть бути інтегровані у процеси DevSecOps та Runtime Security веборієнтованого програмного забезпечення.

Аналіз наукових джерел свідчить, що питання інтеграції безпеки у життєвий цикл розробки програмного забезпечення та впровадження практик DevSecOps ґрунтовно досліджені в працях Kuhrmann M., Prates L., Pereira R., Sinan M., Shahin M., Gondal I. Значну увагу приділено також автоматизованому тестуванню вебзастосунків, зокрема методам SAST, DAST та SCA (Li K., Croft R., Albahar M., Imtiaz N., Zhao L.). Водночас проблематика стеганоаналізу активно розвивалася у межах просторових і частотних підходів (DCT, DWT, SVD) у роботах Holub V., Fridrich J., Setiadi D.R.I.M., Shehab D.A., Alhaddad M.J., а також вітчизняних дослідників (Кобозева А.А., Шелест М.Є., Соколов А.В., Костирка О.В.). Методи машинного навчання для задач класифікації загроз, включаючи фішинг і стеганоаналіз, широко представлені у працях Jain A.K., Gupta B.B., Catal C. та інших авторів.

Разом із тим, в науковій літературі відсутній комплексний підхід до виявлення прихованих стеганографічних каналів саме у вебзастосунках із використанням спектральних характеристик перетворення Уолша-Адамара та їх подальшої інтеграції у процеси тестування безпеки в межах DevSecOps і Runtime Security. Більшість наявних досліджень розглядають стеганоаналіз ізольовано від специфіки функціонування вебсередовища або без урахування вимог реального часу та масштабованості.

Аналогічно, попри значну кількість робіт, присвячених виявленню фішингових атак, переважна їх частина орієнтована на клієнтські механізми захисту або аналіз текстового контенту, тоді як питання інтеграції інтелектуальних методів виявлення фішингового контенту безпосередньо у серверну логіку вебзастосунків та процедури автоматизованого тестування безпеки залишаються недостатньо дослідженими. Таким чином, формування теоретично обґрунтованого базису виявлення прихованих каналів у поєднанні з розробленням адаптивних методів протидії фішингу на основі машинного навчання становить невирішене науково-прикладне завдання, що й зумовлює наукову новизну та доцільність виконаного дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами, грантами. По-перше, дослідження узгоджується зі Стратегією національної безпеки України (Указ Президента України від 14 вересня 2020 р. № 392/2020, з урахуванням змін, внесених Указом Президента від 6 січня 2025 р. № 16/2025), де у п. 52 Розділу III визначено ключове завдання розвитку системи кібербезпеки – «гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації». По-друге, дисертація відповідає «Концепції розвитку штучного інтелекту в Україні»

(схвалена Розпорядженням Кабінету Міністрів України від 2.12.2020 № 1556-р), Розпорядженню Кабінету Міністрів України «Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки» від 12.05.2021 р. № 438-р, Постанові Верховної Ради України «Про затвердження завдань Національної програми інформатизації на 2022-2024 роки» від 8.07.2022 № 2360-IX, Постанові Кабінету Міністрів України «Про затвердження Національної економічної стратегії на період до 2030 року» від 3.03.2021 р. № 179. По-третє, результати дисертаційної роботи пов'язані з положеннями Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 р. № 447/2021 (на підставі рішення РНБО від 14 травня 2021 р.). У документі визначено оновлені стратегічні цілі та завдання держави у сфері кібербезпеки, серед яких – розвиток національної спроможності з виявлення та протидії кібератакам, захист критичної інформаційної інфраструктури, інтеграція інноваційних підходів і технологій, у тому числі на основі штучного інтелекту.

Мета і завдання дослідження. Метою роботи є підвищення ефективності виявлення фішингових атак та прихованих стеганографічних каналів у вебзастосунках шляхом розроблення теоретичних моделей, алгоритмів і методів тестування безпеки на основі перетворення Уолша-Адамара та методів машинного навчання, придатних для інтеграції у CI/CD-середовище.

Для досягнення поставленої мети необхідно розв'язати такі задачі:

1. Аналіз сучасного стану проблеми щодо вразливостей вебзастосунків, зокрема загроз фішингових атак та створення прихованих каналів передачі інформації засобами стеганографії в контексті життєвого циклу розробки ПЗ (CI/CD) та процесів тестування безпеки.
2. Розробка теоретичного базису для виявлення прихованих каналів, побудованих на основі концепції кодового управління, шляхом аналізу статистичних властивостей трансформант перетворення Уолша-Адамара.
3. Узагальнення розробленого теоретичного базису виявлення прихованих каналів у просторі перетворення Уолша-Адамара на випадок каналів, створених за допомогою SVD UV-методів, через аналіз характерних зсувів у їх спектрі.
4. Розробка методів стеганоаналізу на основі машинного навчання для виявлення стеганографічних повідомлень, сформованих сучасними методами (зокрема з кодовим управлінням та SVD UV), орієнтованих на роботу у реальному часі та інтеграцію у Runtime Security вебзастосунків для тестування мультимедійної інформації, що надходить від користувачів.
5. Формування ансамблевих підходів до стеганоаналізу сучасних стеганоалгоритмів шляхом інтеграції розроблених теоретичних засад та сучасних алгоритмів машинного навчання, з подальшим дослідженням їхньої точності, стійкості та швидкодії при виявленні прихованих каналів у вебзастосунках.
6. Інтеграція алгоритмів штучного інтелекту та машинного навчання у процедури автоматизованого тестування безпеки вебзастосунків з метою

створення адаптивних методів виявлення фішингу з високою точністю детектування.

7. Проведення порівняльного аналізу ефективності запропонованих методів із відомими аналогами за базовими критеріями у контексті тестування безпеки вебзастосунків.

8. Розробка підходів до інтеграції запропонованих стеганоаналітичних методів і методу захисту від фішингу у життєвий цикл вебзастосунків у межах концепції DevSecOps.

Об'єктом дослідження є процеси забезпечення інформаційної безпеки вебзастосунків у життєвому циклі розробки програмного забезпечення та його експлуатації.

Предметом дослідження є теоретичні основи та методи виявлення прихованих каналів і фішингових атак у вебзастосунках.

Методи дослідження. Для розробки теоретичної бази захисту від прихованих каналів у вебзастосунках використовувалися ЗПАІС, методи матричного аналізу, спектрального та сингулярного розкладу, теорії інформації та кодування, теорії досконалих алгебраїчних конструкцій. Для створення стеганоаналітичних методів виявлення прихованих каналів, зокрема на основі трансформант дискретного косинусного перетворення, сингулярного розкладу та перетворення Уолша-Адамара, застосовувалися методи теорії сигналів, статистичного аналізу та машинного навчання. Для побудови моделей виявлення фішингових атак і адаптивних методів безпеки вебзастосунків використовувалися методи машинного навчання та штучного інтелекту. Для оцінки якісних і кількісних характеристик запропонованих методів застосовувалися методи математичного моделювання, теорія алгоритмів і методи статистичної оцінки стохастичної якості.

Наукова новизна одержаних результатів.

1. Вперше на основі ЗПАІС встановлено та строго доведено твердження щодо модальностей і зсувів статистичних характеристик коефіцієнтів перетворення Уолша-Адамара у контейнерах мультимедійних даних, що на відміну від існуючих підходів, що ґрунтуються переважно на евристичному аналізі просторових або DCT/SVD-представлень, дало можливість обґрунтувати ефективність використання цього перетворення як математичного апарату для побудови теоретичного базису виявлення прихованих каналів у вебзастосунках.

2. Вперше на основі доведених тверджень щодо статистичних характеристик трансформант перетворення Уолша-Адамара запропоновано теоретичний базис для виявлення прихованих каналів, побудованих на основі концепції кодового управління та SVD UV-методів, що на відміну від наявних рішень, що розглядають зазначені методи ізольовано або без формалізованого спектрального узагальнення, дозволило закласти основу створення ефективних методів стеганоаналізу для виявлення прихованих каналів у вебзастосунках.

3. Подальшого розвитку за рахунок застосування розробленого теоретичного базису набула технологія виявлення прихованих каналів у

вебзастосунках, у межах якої запропоновано нові методи стеганоаналізу стеганоповідомлень на основі кодового управління та SVD UV-методів, які забезпечують підвищену ефективність і швидкодію, порівняно з наявними аналогами.

4. Подальшого розвитку отримала технологія автоматизованого виявлення фішингових сторінок у вебзастосунках за рахунок використання методів обробки контенту та машинного навчання, що дозволило, на відміну від наявних аналогів, враховувати структурні й семантичні ознаки у реальному часі.

5. Удосконалено підхід до інтеграції методів тестування та забезпечення безпеки вебзастосунків у життєвий цикл розробки ПЗ, що дозволило поєднати традиційні засоби SAST/DAST/IAST із розробленими у дисертації інтелектуальними методами стеганоаналізу й виявлення фішингових атак, на відміну від наявних сучасних аналогів, які не забезпечують комплексної інтеграції у процеси CI/CD та DevSecOps.

Після завершення доповіді Дика А.І. відповідала присутніми поставлені такі запитання:

Професор кафедри кібербезпеки, доктор технічних наук, професор Казакова Н.Ф. запитала, у чому полягає принципова наукова новизна використання перетворення Уолша-Адамара для виявлення прихованих каналів порівняно з класичними частотними методами, такими як DCT або SVD?

Дика А.І. відповіла, що якщо говорити про наукову новизну, то вона полягає не просто у використанні перетворення Уолша-Адамара, а у формуванні на його основі строгого теоретичного базису стеганоаналізу. У роботі доведено, що при вбудовуванні додаткової інформації відбуваються характерні зміни модальностей і зсуви статистичних характеристик трансформант Уолша-Адамара.

На відміну від класичних підходів, які здебільшого базуються на евристичному аналізі DCT або SVD-представлень, у дисертації спочатку сформульовано математичні твердження, а вже потім підтверджено їх експериментально.

Крім того, саме перетворення Уолша-Адамара має низьку обчислювальну складність, що робить його придатним для застосування у вебсередовищі в режимі реального часу. Таким чином, новизна полягає у поєднанні строгого спектрального обґрунтування та практичної орієнтації.

Доцент кафедри програмної інженерії, кандидат технічних наук, доцент Манаков С.Ю. запитав, які обмеження мають запропоновані методи стеганоаналізу та виявлення фішингу, і в яких умовах їх ефективність може знижуватися?

Дика А.І. відповіла, що будь-який метод аналізу має межі застосовності, і в дисертації це питання не ігнорується. По-перше, якщо йдеться про стеганоаналіз, то ефективність знижується у випадках надзвичайно малого обсягу вбудованої інформації, коли зміни статистичних характеристик

контейнера наближаються до рівня природного шуму. У такій ситуації спектральні зсуви стають менш вираженими.

По-друге, якщо зломисник застосовує комбіновані методи приховування з попереднім додаванням адаптивного шуму або складною постобробкою, це може зменшувати контрастність виявлюваних ознак.

Щодо виявлення фішингу, потенційним обмеженням є використання повністю легітимних шаблонів або компрометація реальних ресурсів, коли шкідливий контент мінімально відрізняється структурно. Однак навіть у таких випадках побайтова візуалізація дозволяє фіксувати мікроструктурні особливості HTML-коду.

Таким чином, методи не претендують на абсолютність, але вони демонструють високу стійкість у більшості практичних сценаріїв, що підтверджено експериментально.

В.о. завідувача кафедри кібербезпеки, доктор технічних наук, професор Соколов А.В. запитав, яким чином запропоновані методи протидіють еволюції стеганографічних алгоритмів та сучасних фішингових технік?

Дика А.І. відповіла, що у роботі зроблено акцент на виявленні не конкретного алгоритму приховування, а структурних порушень статистичних закономірностей контейнера. Навіть при зміні параметрів вбудовування або застосуванні нових модифікацій стеганографічних алгоритмів зберігаються характерні спектральні зсуви.

У задачі виявлення фішингу використано підхід побайтової візуалізації HTML-коду, що дозволяє аналізувати структурні особливості сторінки незалежно від мови тексту чи семантичної маскувальної складової.

Це підвищує стійкість методів до адаптивних змін атак.

Доцент кафедри кібербезпеки, кандидат технічних наук, доцент Бойко В.Д., запитав, чому для класифікації було обрано SVM, MLP та ансамблі CNN, а не більш сучасні глибокі архітектури, наприклад, трансформери?

Дика А.І. відповіла, що вибір моделей був обумовлений не лише прагненням до максимальної точності, а й вимогами до обчислювальної ефективності та можливості інтеграції у вебсередовище.

Трансформерні архітектури демонструють високу результативність у задачах обробки природної мови або великих зображень, однак вони потребують значних обчислювальних ресурсів і мають складну процедуру навчання та розгортання.

У межах дисертаційного дослідження стояло завдання створити методи, придатні для роботи в умовах реального часу, з мінімальним впливом на серверну інфраструктуру. Саме тому було обрано: SVM, як стабільний та добре інтерпретований класифікатор для задач із чітко сформованими ознаками; MLP, як компактну нейронну модель із високою швидкістю; ансамблі CNN для підвищення стійкості до варіативності даних.

Таким чином, вибір моделей є усвідомленим компромісом між точністю, швидкістю та можливістю масштабування.

В.о. завідувача кафедри штучного інтелекту та математичного моделювання, доктор економічних наук, професор Горбаченко С.А. запитав, як оцінюється інтерпретованість отриманих моделей? Чи можна пояснити, на основі яких саме ознак модель приймає рішення?

Дика А.І. відповіла, що на відміну від «чорних скриньок» глибокого навчання, у роботі значна частина ознак має фізичну та математичну інтерпретацію, це спектральні коефіцієнти, статистичні моменти, характеристики розподілу.

Для SVM можливо чітко простежити ваги та вплив ознак на формування роздільної гіперплощини. У випадку ансамблів CNN інтерпретованість є менш прямою, однак використання попередньо сформованого спектрального представлення вже обмежує простір рішень фізично обґрунтованими характеристиками.

Таким чином, модель не є повністю «непрозорою», її рішення спираються на математично осмислені ознаки.

В.о. завідувача кафедри програмної інженерії, кандидат педагогічних наук, доцент Логінова Н.І. зазначила, що у роботі поєднуються строгі математичні доведення та прикладні експерименти, та запитала, що, є домінуючим внеском – теоретичний чи прикладний?

Дика А.І. відповіла, що робота має збалансований характер, однак її фундаментальність полягає саме у формуванні теоретичного підґрунтя.

Практичні експерименти демонструють ефективність методів, але вони є логічним наслідком математичного аналізу. Без доведених спектральних закономірностей це були б лише інженерні рішення.

Водночас саме прикладна реалізація підтверджує життєздатність теорії та її готовність до впровадження.

Тому робота розглядається як така, що формує міст між теоретичними дослідженнями у сфері спектрального аналізу та практичними задачами кібербезпеки вебзастосунків.

Доцент кафедри штучного інтелекту та математичного моделювання, кандидат технічних наук Гура В.І. запитав, якщо припустити, що зловмисник знає про використання спектрального аналізу Уолша-Адамара, чи може він адаптувати алгоритм так, щоб нейтралізувати виявлені Вами ознаки?

Дика А.І. відповіла, що теоретично, так, якщо зловмисник має повну інформацію про метод детекції, він може намагатися компенсувати спектральні зсуви.

Однак тут виникає компроміс: щоб зберегти статистичні характеристики контейнера, потрібно суттєво зменшити потужність вбудовування або застосувати складну корекцію після модифікації. Це, у свою чергу, або знижує

пропускну здатність прихованого каналу, або різко підвищує обчислювальну складність атаки.

Фактично ми переводимо атаку в економічно та технічно менш доцільну площину.

Крім того, в роботі використано ансамблевий підхід і багатовимірний простір ознак, що ускладнює повну компенсацію всіх статистичних змін одночасно.

Після відповідей на запитання виступи **науковий керівник** – доцент кафедри програмної інженерії, кандидат технічних наук, доцент Трофименко О.Г.

Науковий керівник зазначила, що дисертаційна робота Дикої Анастасії Іванівни присвячена вирішенню актуальної науково-прикладної проблеми підвищення ефективності тестування безпеки вебзастосунків шляхом розроблення теоретично обґрунтованих і практично орієнтованих методів виявлення фішингових атак та прихованих стеганографічних каналів на основі перетворення Уолша-Адамара та технологій машинного навчання.

Актуальність обраної теми зумовлена стрімким розвитком веборієнтованих інформаційних систем та зростанням кількості складних кіберзагроз, що використовують адаптивні механізми маскування та соціальної інженерії. Традиційні методи тестування безпеки (SAST, DAST, IAST, SCA) не забезпечують достатнього рівня ефективності щодо виявлення сучасних стеганографічних методів приховування інформації та інтелектуалізованих фішингових механізмів. У цьому контексті запропонований у дисертації комплексний підхід, орієнтований на інтеграцію інтелектуальних методів у процеси DevSecOps та CI/CD, є своєчасним і науково обґрунтованим.

Наукова новизна одержаних результатів полягає у формуванні теоретичного базису виявлення прихованих каналів у вебзастосунках на основі аналізу статистичних характеристик трансформант перетворення Уолша-Адамара, встановленні закономірностей зсувів їхніх модальностей під впливом кодового управління та SVD UV-методів, а також у розробленні нових інтелектуальних методів стеганоаналізу та виявлення фішингового контенту. Запропоновані підходи забезпечують поєднання високої точності детектування з відносно низькою обчислювальною складністю, що є принципово важливим для їх застосування в умовах реального часу.

Практичне значення роботи підтверджується реалізацією розроблених методів у вигляді програмних прототипів, можливістю їх інтеграції в серверні та клієнтські модулі вебзастосунків, а також впровадженням результатів у діяльність ІТ-компанії та освітній процес факультету кібербезпеки та інформаційних технологій університету. Отримані показники точності (precision, recall, F1-score понад 0,94-0,97 для задач стеганоаналізу та понад 0,92 для задач виявлення фішингового контенту) підтверджують

конкурентоспроможність запропонованих рішень порівняно з наявними аналогами.

Дисертація має логічну структуру, складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Матеріал викладено послідовно, з чітким формулюванням мети, завдань, об'єкта та предмета дослідження. Результати експериментальних досліджень є достатньо обґрунтованими, підтверджені статистичним аналізом та апробовані на наукових конференціях різного рівня.

Особистий внесок здобувачки є визначальним. Усі основні теоретичні положення, алгоритмічні рішення та експериментальні дослідження виконані нею самостійно. У спільних публікаціях Дика А.І. відповідала за формування методології досліджень, розроблення алгоритмів та програмну реалізацію моделей.

За час роботи над дисертацією Дика Анастасія Іванівна проявила себе як відповідальний, наполегливий і висококваліфікований дослідник. Вона демонструє здатність до самостійного наукового пошуку, системного аналізу складних технічних проблем, критичного осмислення результатів та формування обґрунтованих висновків. Здобувачка активно брала участь у наукових конференціях, підготовці публікацій, а також у навчально-методичній роботі кафедри. Відзначається високий рівень її академічної доброчесності, організованість і вміння працювати в науковому колективі.

За темою дисертації опубліковано 28 наукових праць, з яких 11 статей – у наукових фахових виданнях України, що відповідає встановленим вимогам до апробації результатів дослідження.

Дисертаційна робота Дикої Анастасії Іванівни є завершеним самостійним науковим дослідженням, що містить нові науково обґрунтовані результати, які мають теоретичне та практичне значення для розвитку методів тестування безпеки веборієнтованого програмного забезпечення.

У процесі підготовки дисертації Дика Анастасія Іванівна плідно співпрацювала з науковим керівником протягом усього терміну навчання в аспірантурі, результатом чого є написання дисертаційного дослідження. Здобувачка виконала індивідуальний план наукової роботи та індивідуальний навчальний план у повному обсязі. Всі заплановані види робіт були виконані своєчасно.

Щодо загальної оцінки роботи Дикої Анастасії Іванівни у процесі підготовки дисертації та виконання індивідуального плану наукової роботи та індивідуального навчального плану вона оцінюється на відмінно.

Окремо слід відзначити високий педагогічний потенціал Дикої Анастасії Іванівни. Вона є талановитим викладачем, який поєднує ґрунтовну наукову підготовку з сучасними освітніми підходами. Здобувачка вміло інтегрує результати власних наукових досліджень у навчальний процес, впроваджує елементи практикоорієнтованого та проєктного навчання, використовує інструменти штучного інтелекту й сучасні технології тестування безпеки під час викладання фахових дисциплін. Вона є співавтором навчально-методичних

посібників та розробником методичних матеріалів з тестування і забезпечення якості програмних систем, що свідчить про її системний підхід до підготовки висококваліфікованих фахівців у сфері інформаційних технологій та кібербезпеки.

Викладене дозволяє зробити висновок про те, що дисертація Дикої Анастасії Іванівни на тему: «Методи машинного навчання в тестуванні безпеки веборієнтованого програмного забезпечення» є самостійним науковим дослідженням, яке відповідає всім встановленим вимогам, може бути рекомендована до захисту на здобуття наукового ступеня доктора філософії за спеціальністю за спеціальністю 122 «Комп'ютерні науки», галузі знань 12 «Інформаційні технології» у разовій спеціалізованій вченій раді, а її автор заслуговує, на основі захисту, присвоєння наукового ступеня доктора філософії.

У обговоренні дисертаційного дослідження брали участь:

Доктор технічних наук, професор Соколов А.В. відзначив, що дисертаційна робота Дикої Анастасії Іванівни справляє цілісне та концептуально завершене враження. Авторкою не лише сформульовано актуальну науково-прикладну проблему, але й запропоновано її системне вирішення на основі поєднання математичних методів спектрального аналізу та сучасних алгоритмів машинного навчання. Особливо має бути відзначена глибина опрацювання перетворення Уолша-Адамара та його адаптація до задач виявлення стеганографічних каналів у веборієнтованому програмному забезпеченні.

Робота містить елементи фундаментальності, що проявляється у встановленні статистичних закономірностей поведінки трансформант, а також у формалізації критеріїв детектування. При цьому дослідження не є відірваним від практики, запропоновані алгоритми мають чітко окреслену сферу застосування в процесах тестування безпеки. Вважаю, що дисертація виконана на високому науковому рівні та відповідає вимогам до робіт на здобуття ступеня доктора філософії.

Доктор економічних наук, професор Горбаченко С.А. відзначив коректність математичного апарату, використаного в роботі. Авторка продемонструвала вміння працювати з багатовимірними даними, грамотно застосовувати методи класифікації та оцінювати їх ефективність за сучасними метриками. Окремо відзначається експериментальна база дослідження: результати не декларативні, а підтверджені статистично.

Також позитивним є те, що здобувачка не обмежилася використанням стандартних моделей, а провела порівняльний аналіз різних підходів, що дозволило обґрунтувати вибір оптимальної архітектури. Робота демонструє зрілість наукового мислення та здатність до самостійного формування нових підходів у межах спеціальності 122 «Комп'ютерні науки».

Доктор технічних наук, професор Казакова Н.Ф. відзначила, що з практичної точки зору дисертація є надзвичайно актуальною. Сьогодні

вебзастосунки залишаються однією з найуразливіших ланок інформаційних систем, а питання виявлення фішингових атак та прихованих каналів передачі даних є стратегічно важливими.

Запропоновані у роботі алгоритми можуть бути інтегровані в інструменти автоматизованого тестування безпеки. Важливо, що авторка враховує вимоги до обчислювальної ефективності, що дозволяє застосовувати розроблені методи у середовищах реального часу.

Кандидат фізико-математичних наук, доцент Чепурна О.Є. відзначила, що з позицій індустрії можна сказати, що робота має прикладну цінність. Виявлення складних форм фішингу та прихованих механізмів витоку інформації є реальним викликом для компаній. Результати дисертації можуть бути використані при розробці систем моніторингу безпеки та автоматизованого аудиту коду.

Особливо позитивним є поєднання теоретичних досліджень із програмною реалізацією та апробацією в умовах, наближених до реальних.

Кандидат технічних наук, доцент Чикунів П.О. відзначив здатність здобувачки інтегрувати результати власних досліджень у навчальний процес. Розроблені нею підходи використовуються під час викладання дисциплін з тестування програмного забезпечення та кібербезпеки. Це свідчить про високий рівень професійної зрілості та відповідальності.

Поєднання наукової та педагогічної діяльності є безумовною перевагою Анастасії Іванівни як молодого науковця.

Кандидат технічних наук, доцент Ахмаметьєва Г.В. відзначила, що дисертаційна робота Дикої Анастасії Іванівни є комплексним і логічно завершеним дослідженням у галузі комп'ютерних наук. Особливої уваги заслуговує теоретичне обґрунтування використання перетворення Уолша-Адамара у задачах стеганоаналізу веборієнтованих систем. Отримані результати мають ознаки наукової новизни та можуть слугувати підґрунтям для подальших досліджень у сфері інтелектуалізації тестування безпеки.

Кандидат педагогічних наук, доцент Логінова Н.І. що дисертація Дикої А.І. характеризується чіткою структурою, логічністю викладу та відповідністю поставленої мети отриманим результатам. Авторка продемонструвала здатність до самостійного наукового пошуку та формування обґрунтованих висновків. Всі положення, що виносяться на захист, достатньо аргументовані.

На основі результатів обговорення присутніх на засіданні вирішили запропонувати наступний

ВИСНОВОК

**про наукову новизну, теоретичне та практичне значення дисертації
Дикої Анастасії Іванівни «Методи машинного навчання в тестуванні
безпеки веборієнтованого програмного забезпечення», поданої на здобуття
ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за
спеціальністю 122 «Комп'ютерні науки»**

Обґрунтування вибору теми дослідження. Вибір теми дослідження зумовлений науковими інтересами здобувачки у сфері тестування безпеки вебзастосунків, штучного інтелекту та стеганоаналізу, а також практичним досвідом у галузі забезпечення якості програмного забезпечення. У процесі наукової та професійної діяльності було виявлено наявність недостатньо досліджених аспектів щодо виявлення прихованих каналів і фішингових атак у середовищі вебзастосунків, що й визначило доцільність поглибленого дослідження саме цієї проблематики та формування комплексного підходу до її розв'язання.

Актуальність теми дисертаційного дослідження зумовлена стрімкою цифровізацією суспільства та зростанням ролі вебзастосунків як складової критичної інформаційної інфраструктури держави. В умовах постійного збільшення кількості та складності кібератак, зокрема фішингових кампаній і використання прихованих каналів передавання інформації, традиційні засоби тестування безпеки (SAST, DAST, IAST, SCA) не забезпечують належного рівня виявлення сучасних загроз. Особливої гостроти проблема набуває у контексті впровадження CI/CD та концепції DevSecOps, де безпека повинна інтегруватися у всі етапи життєвого циклу програмного забезпечення.

Дисертаційна робота спрямована на розв'язання актуального науково-прикладного завдання – підвищення ефективності тестування безпеки вебзастосунків шляхом розроблення теоретично обґрунтованих та практично придатних методів виявлення фішингових атак і стеганографічних загроз на основі перетворення Уолша-Адамара та методів машинного навчання. Запропоновані підходи відповідають сучасним викликам кібербезпеки, мають значення для розвитку наукових засад стеганоаналізу та інтелектуального тестування безпеки й можуть бути інтегровані у процеси DevSecOps та Runtime Security веборієнтованого програмного забезпечення.

Аналіз наукових джерел свідчить, що питання інтеграції безпеки у життєвий цикл розробки програмного забезпечення та впровадження практик DevSecOps ґрунтовно досліджені в працях Kuhrmann M., Prates L., Pereira R., Sinan M., Shahin M., Gondal I. Значну увагу приділено також автоматизованому тестуванню вебзастосунків, зокрема методам SAST, DAST та SCA (Li K., Croft R., Albahar M., Imtiaz N., Zhao L.). Водночас проблематика стеганоаналізу активно розвивалася у межах просторових і частотних підходів (DCT, DWT, SVD) у роботах Holub V., Fridrich J., Setiadi D.R.I.M., Shehab D.A., Alhaddad M.J., а також вітчизняних дослідників. Методи машинного навчання для задач

класифікації загроз, включаючи фішинг і стеганоаналіз, широко представлені у працях Jain A.K., Gupta B.B., Catal C. та інших авторів.

Разом із тим, в науковій літературі відсутній комплексний підхід до виявлення прихованих стеганографічних каналів саме у вебзастосунках із використанням спектральних характеристик перетворення Уолша-Адамара та їх подальшої інтеграції у процеси тестування безпеки в межах DevSecOps і Runtime Security. Більшість наявних досліджень розглядають стеганоаналіз ізольовано від специфіки функціонування вебсередовища або без урахування вимог реального часу та масштабованості.

Аналогічно, попри значну кількість робіт, присвячених виявленню фішингових атак, переважна їх частина орієнтована на клієнтські механізми захисту або аналіз текстового контенту, тоді як питання інтеграції інтелектуальних методів виявлення фішингового контенту безпосередньо у серверну логіку вебзастосунків та процедури автоматизованого тестування безпеки залишаються недостатньо дослідженими. Таким чином, формування теоретично обґрунтованого базису виявлення прихованих каналів у поєднанні з розробленням адаптивних методів протидії фішингу на основі машинного навчання становить невирішене науково-прикладне завдання, що й зумовлює наукову новизну та доцільність виконаного дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами, грантами. По-перше, дослідження узгоджується зі Стратегією національної безпеки України (Указ Президента України від 14 вересня 2020 р. № 392/2020, з урахуванням змін, внесених Указом Президента від 6 січня 2025 р. № 16/2025), де у п. 52 Розділу III визначено ключове завдання розвитку системи кібербезпеки – «гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації». По-друге, дисертація відповідає «Концепції розвитку штучного інтелекту в Україні» (схвалена Розпорядженням Кабінету Міністрів України від 2.12.2020 № 1556-р), Розпорядженню Кабінету Міністрів України «Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки» від 12.05.2021 р. № 438-р, Постанові Верховної Ради України «Про затвердження завдань Національної програми інформатизації на 2022-2024 роки» від 8.07.2022 № 2360-IX, Постанові Кабінету Міністрів України «Про затвердження Національної економічної стратегії на період до 2030 року» від 3.03.2021 р. № 179. По-третє, результати дисертаційної роботи пов'язані з положеннями Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 р. № 447/2021 (на підставі рішення РНБО від 14 травня 2021 р.). У документі визначено оновлені стратегічні цілі та завдання держави у сфері кібербезпеки, серед яких – розвиток національної спроможності з виявлення та протидії кібератакам, захист критичної інформаційної інфраструктури, інтеграція інноваційних підходів і технологій, у тому числі на основі штучного інтелекту. Дисертаційне дослідження виконано в межах плану науково-дослідної роботи кафедри інформаційних технологій

Національного університету «Одеська юридична академія» «Інформаційні технології в сучасному суспільстві» на 2021-2025 роки як складової плану науково-дослідної роботи Національного університету «Одеська юридична академія» «Правове і соціальне життя сучасної України у людиноцентристському вимірі в цифрову еру» (державний реєстраційний номер 0122U000266), а також плану науково-дослідної роботи кафедри програмної інженерії «Інтелектуалізація процесів розроблення та експлуатації інформаційних систем на основі інтеграції методів штучного інтелекту та сучасних архітектурних підходів» у межах виконання теми науково-дослідної роботи Національного університету «Одеська юридична академія» «Соціально-політична стабільність в період воєнних та післявоєнних трансформацій: правові, економічні, гуманітарні, інноваційно-технічні можливості в цифрову еру» на 2026-2030 роки.

Мета і завдання дослідження. Метою роботи є підвищення ефективності виявлення фішингових атак та прихованих стеганографічних каналів у вебзастосунках шляхом розроблення теоретичних моделей, алгоритмів і методів тестування безпеки на основі перетворення Уолша-Адамара та методів машинного навчання, придатних для інтеграції у CI/CD-середовище.

Для досягнення поставленої мети необхідно розв'язати такі задачі:

1. Аналіз сучасного стану проблеми щодо вразливостей вебзастосунків, зокрема загроз фішингових атак та створення прихованих каналів передачі інформації засобами стеганографії в контексті життєвого циклу розробки ПЗ (CI/CD) та процесів тестування безпеки.
2. Розробка теоретичного базису для виявлення прихованих каналів, побудованих на основі концепції кодового управління, шляхом аналізу статистичних властивостей трансформант перетворення Уолша-Адамара.
3. Узагальнення розробленого теоретичного базису виявлення прихованих каналів у просторі перетворення Уолша-Адамара на випадок каналів, створених за допомогою SVD UV-методів, через аналіз характерних зсувів у їх спектрі.
4. Розробка методів стеганоаналізу на основі машинного навчання для виявлення стеганографічних повідомлень, сформованих сучасними методами (зокрема з кодовим управлінням та SVD UV), орієнтованих на роботу у реальному часі та інтеграцію у Runtime Security вебзастосунків для тестування мультимедійної інформації, що надходить від користувачів.
5. Формування ансамблевих підходів до стеганоаналізу сучасних стеганоалгоритмів шляхом інтеграції розроблених теоретичних засад та сучасних алгоритмів машинного навчання, з подальшим дослідженням їхньої точності, стійкості та швидкодії при виявленні прихованих каналів у вебзастосунках.
6. Інтеграція алгоритмів штучного інтелекту та машинного навчання у процедури автоматизованого тестування безпеки вебзастосунків з метою

створення адаптивних методів виявлення фішингу з високою точністю детектування.

7. Проведення порівняльного аналізу ефективності запропонованих методів із відомими аналогами за базовими критеріями у контексті тестування безпеки вебзастосунків.

8. Розробка підходів до інтеграції запропонованих стеганоаналітичних методів і методу захисту від фішингу у життєвий цикл вебзастосунків у межах концепції DevSecOps.

Методи дослідження. Для розробки теоретичної бази захисту від прихованих каналів у вебзастосунках використовувався ЗПАІС, методи матричного аналізу, спектрального та сингулярного розкладу, теорії інформації та кодування, теорії досконалих алгебраїчних конструкцій. Для створення стеганоаналітичних методів виявлення прихованих каналів, зокрема на основі трансформант дискретного косинусного перетворення, сингулярного розкладу та перетворення Уолша-Адамара, застосовувалися методи теорії сигналів, статистичного аналізу та машинного навчання. Для побудови моделей виявлення фішингових атак і адаптивних методів безпеки вебзастосунків використовувалися методи машинного навчання та штучного інтелекту. Для оцінки якісних і кількісних характеристик запропонованих методів застосовувалися методи математичного моделювання, теорія алгоритмів і методи статистичної оцінки стохастичної якості.

Наукова новизна одержаних результатів:

1. *Вперше* на основі ЗПАІС встановлено та строго доведено твердження щодо модальностей і зсувів статистичних характеристик коефіцієнтів перетворення Уолша-Адамара у контейнерах мультимедійних даних, що на відміну від існуючих підходів, що ґрунтуються переважно на евристичному аналізі просторових або DCT/SVD-представлень, дало можливість обґрунтувати ефективність використання цього перетворення як математичного апарату для побудови теоретичного базису виявлення прихованих каналів у вебзастосунках.

2. *Вперше* на основі доведених тверджень щодо статистичних характеристик трансформант перетворення Уолша-Адамара запропоновано теоретичний базис для виявлення прихованих каналів, побудованих на основі концепції кодового управління та SVD UV-методів, що на відміну від наявних рішень, що розглядають зазначені методи ізольовано або без формалізованого спектрального узагальнення, дозволило закласти основу створення ефективних методів стеганоаналізу для виявлення прихованих каналів у вебзастосунках.

3. *Подальшого розвитку* за рахунок застосування розробленого теоретичного базису набула технологія виявлення прихованих каналів у вебзастосунках, у межах якої запропоновано нові методи стеганоаналізу стеганоповідомлень на основі кодового управління та SVD UV-методів, які забезпечують підвищену ефективність і швидкодію, порівняно з наявними аналогами.

4. *Подальшого розвитку* отримала технологія автоматизованого виявлення фішингових сторінок у вебзастосунках за рахунок використання методів обробки контенту та машинного навчання, що дозволило, на відміну від наявних аналогів, враховувати структурні й семантичні ознаки у реальному часі.

5. *Удосконалено* підхід до інтеграції методів тестування та забезпечення безпеки вебзастосунків у життєвий цикл розробки ПЗ, що дозволило поєднати традиційні засоби SAST/DAST/IAST із розробленими у дисертації інтелектуальними методами стеганоаналізу й виявлення фішингових атак, на відміну від наявних сучасних аналогів, які не забезпечують комплексної інтеграції у процеси CI/CD та DevSecOps.

Практичне значення Практична цінність роботи полягає у тому, що здобуті наукові результати були реалізовані у вигляді конкретних методів та алгоритмів, придатних до використання в прикладних системах захисту інформації. Запропоновані методи відзначаються високою обчислювальною ефективністю та відносною простотою алгоритмічної реалізації, що забезпечує їхню придатність для інтеграції у серверні або клієнтські частини вебзастосунків. Зокрема:

1. Розроблено методи виявлення стеганографічних повідомлень з кодовим управлінням на основі запропонованого математичного апарату аналізу характеристик модальностей розподілу трансформант перетворення Уолша-Адамара, реалізовані у вигляді мережі Multilayer Perceptron та ансамблю згорткових нейронних мереж. Обидва підходи забезпечують високий рівень точності класифікації (Precision = 0.95...0.98, Recall = 0.96...0.98, F1-score $\approx$ 0.96...0.97), що перевищує відомі аналоги на 5.6–6.6%. При цьому метод на основі MLP характеризується високою швидкістю (виділення ознак із зображення великого розміру займає близько 0.45 с, класифікація одного зображення – 0.0044 с), що дозволяє обробляти понад 200 зображень за секунду, а метод на основі ансамблю CNN забезпечує підвищену надійність і стійкість до випадкових похибок, демонструючи загальну достовірність виявлення понад 94.3%.

2. На основі запропонованого математичного апарату дослідження змін, які вносить стеганографічний SVD UV-метод в області перетворень Уолша-Адамара, запропоновано метод виявлення прихованих каналів передавання інформації у вебзастосунках. Запропонований підхід ґрунтується на аналізі зсувів у гістограмах трансформант перетворення Уолша-Адамара та класифікації на основі ансамблю методів опорних векторів (SVM). Це дозволило досягти високих показників точності (Precision = 0.96, Recall = 0.94, F1-score $\approx$ 0.95) та забезпечити загальну правильність класифікації понад 90.57%.

3. Метод виявлення фішингового контенту, який поєднує побайтову візуалізацію HTML-коду та машинне навчання. Запропонований підхід забезпечує коректне відображення структури вебсторінок у вигляді числових векторів ознак і дозволяє ефективно відокремлювати легітимні ресурси від

шкідливих. Точність класифікації, досягнута на тестових вибірках (92.45% при збалансованих значеннях precision, recall та F1-score), свідчить про надійність методу і його здатність з мінімальною кількістю помилок виявляти потенційно небезпечні вебресурси. Висока швидкодія та невисокі вимоги до ресурсів дозволяють реалізувати метод як модуль безпеки браузера або як компонент серверної частини вебзастосунків для оперативного аналізу посилань у режимі, наближеному до реального часу.

4. Результати дисертаційної роботи використовуються в ІТ-компанії ЕРАМ та впроваджені у навчальний процес на факультеті кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», що підтверджено відповідними актами.

Апробація результатів дисертації. Результати досліджень, викладені у дисертації, доповідались на міжнародних та всеукраїнських конференціях, серед яких: Міжнародна науково-практична конференція «Європейські орієнтири розвитку України: нові виміри у воєнний час», м. Одеса, Україна, 16 травня 2025 р.; X Всеукраїнська науково-практична конференція «Інформаційне суспільство: проблеми та перспективи», м. Одеса, Україна, 23 травня 2025 р.; V Всеукраїнська науково-практична інтернет-конференція «Інформаційні технології: моделі, алгоритми, системи», м. Миколаїв, 30-31 жовтня 2024 р.; Міжнародна науково-практична конференція «Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів», м. Одеса, Україна, 26 квітня 2024 р.; VII Міжнародна науково-практична конференція «Актуальні тенденції розвитку освіти, науки та технологій», м. Харків – Бахмут, Україна, 15 травня 2024 р.; IX Всеукраїнська науково-практична конференція «Інформаційне суспільство: проблеми та перспективи», м. Одеса, 24 травня 2024 р.; Міжнародна науково-практична конференція «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика», м. Одеса, 24 листопада 2023 р.; Міжнародна науково-практична конференція «Електронні інформаційні ресурси: створення, використання, доступ», м. Вінниця, 20-21 листопада 2023 р.; Всеукраїнська науково-практична конференція «Інформаційне суспільство: проблеми та перспективи», м. Одеса, 2 червня 2023 р.; Міжнародна науково-практична конференція «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень», м. Одеса, 19 травня 2023 р.; Міжнародна наукова конференція «Інформаційні технології та менеджмент у вищій освіті та науці», м. Фергана, Республіка Узбекистан, 28 листопада 2022 р.; IV Всеукраїнська науково-практична конференція «Кібербезпека в сучасному світі: актуальні виклики», м. Одеса, 25 листопада 2022 р.; Міжнародна науково-практична конференція «Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття», м. Одеса, 17 червня 2022 р.

Публікації. Матеріали дисертації повною мірою викладені у 28 публікаціях, з яких 24 наукові публікації розкривають основний зміст

дисертації, зокрема, опубліковано 11 статей у наукових виданнях, включених до Переліку наукових фахових видань України з технічних наук. Опубліковано: 13 тез доповідей у матеріалах всеукраїнських та міжнародних наукових конференцій, які засвідчують апробацію матеріалів дисертації; 4 наукові праці, які додатково відображають наукові результати дисертації, зокрема авторське свідоцтво України на комп'ютерну програму.

Список публікацій здобувача за темою дисертації та відомості про апробацію матеріалів дисертації:

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Dyka A. I. Detection of SVD-based hidden data in web applications using Walsh-Hadamard transformant analysis. *Scientific notes of V. I. Vernadsky Taurida National University*. 2025. Vol. 36 (75), No. 4. P. 110-118. <https://doi.org/10.32782/2663-5941/2025.4.2/15>
2. Dyka A. I. Detection of covert channels in web applications based on unimodality violation in the Walsh-Hadamard spectrum. *Informatics and Mathematical Methods in Simulation*. 2025. Vol.15, No 1. P. 5-14. DOI: <https://doi.org/10.15276/imms.v15.no1.5>
3. Dyka A. I. Intelligent methods for steganalysis of code-controlled covert messages in web applications. *Scientific notes of V. I. Vernadsky Taurida National University*. 2025. Vol. 36(75), No 2. P. 324-333. DOI: <https://doi.org/10.32782/2663-5941/2025.2.2/44>
4. Дика А. І., Трофименко О. Г., Ковальжі А. С. Інтелектуальне виявлення фішингових сторінок у середовищі вебзастосунків із застосуванням візуального подання. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: Технічні науки. 2025. Т. 36(75), № 1. С. 298-308. DOI: <https://doi.org/10.32782/2663-5941/2025.1.2/43>
5. Трофименко О.Г., Дика А.І., Задерейко О.В., Шевченко О.В. Сфери застосування штучного інтелекту в розробці та тестуванні ігор. *Кібербезпека: освіта, наука, техніка*. 2025. № 1(29). С. 41-59. DOI: <https://doi.org/10.28925/2663-4023.2025.29.832>
6. Трофименко О. Г., Дика А. І., Лобода Ю. В., Толокнов А. А., Бондаренко М. Є. Штучний інтелект у розробці ігор. *Кібербезпека: освіта, наука, техніка*. 2025. № 3(27). С. 109-119. DOI: <https://doi.org/10.28925/2663-4023.2025.27.701>
7. Трофименко О., Дика А. І., Логінова Н., Задерейко О., Струк Н. Штучний інтелект у військових навчальних симуляторах. *Інформаційні технології та суспільство*. 2024. № 2(13). 2024. С. 89-95. DOI: <https://doi.org/10.32689/maup.it.2024.2.13>
8. Трофименко О. Г., Лобода Ю. Г., Гура В. І., Дика А. І., Стрілець М. І. Інструменти штучного інтелекту для системного аналізу. *Вісник Херсонського національного технічного університету*. 2024. № 4. С. 349-357. DOI: <https://doi.org/10.35546/kntu2078-4481.2024.4.46>

9. Трофименко О. Г., Дика А. І., Лобода Ю. Г. Аналіз уразливостей та проблем безпеки вебзастосунків. *Системні технології*. 2023. № 3(146). С. 25-37. DOI: <https://doi.org/10.34185/1562-9945-3-146-2023-03>

10. Трофименко О. Г., Дика А. І., Лобода Ю. Г. Аналіз інструментів тестування вебзастосунків. *Кібербезпека: освіта, наука, техніка*. 2023. № 4(20). С. 62-71. DOI: <https://doi.org/10.28925/2663-4023.2023.20.6271>

11. Трофименко О. Г., Савельєва О. С., Прокоп Ю. В., Логінова Н. І., Дика А. І. Soft skills для розробників програмного забезпечення. *Кібербезпека: освіта, наука, техніка*. 2023. № 3(19). С. 6-19. DOI: <https://doi.org/10.28925/2663-4023.2023.19.619>

Наукові праці, які засвідчують апробацію матеріалів дисертації:

12. Дика А. І. Застосування контекстуальних ембедінгів для виявлення ознак шкідливих введень. *Інформаційне суспільство: проблеми та перспективи*: матер. X Всеукр. наук.-практ. конф. (Одеса, 23 травня 2025 р.). Одеса. 2025. С. 158-160. DOI: <https://doi.org/10.32837/11300.29842>

13. Дика А. І. Застосування NLP-методів для виявлення XSS-атак. *Європейські орієнтири розвитку України: нові виміри у воєнний час*: матер. міжнар.наук.-практ. конф. у 2 т. (Одеса, 16 травня 2025 р.). Одеса: Фенікс, 2025. Т. 2. С. 520-522. URL: <https://hdl.handle.net/11300/30820>

14. Дика А. І. Сучасні інтерактивні інструменти тестування безпеки застосунків. *Інформаційні технології: моделі, алгоритми, системи (ITMAS-2024)*: матер. V Всеукр. наук.-практ. інтернет-конф. (Миколаїв, 30-31 жовтня 2024 р.) Миколаїв: НУК імені адмірала Макарова, 2024. С. 188-190. URL: <https://itconf.nuos.edu.ua/2024/publications/analysis-of-project-management-software/>

15. Дика А. І. Роль штучного інтелекту у тестуванні безпеки вебзастосунків. *Інформаційне суспільство: проблеми та перспективи* : матер. IX всеукр. наук.-практ. конф. (Одеса, 24 травня 2024). Одеса: НУ «ОЮА», 2024. С. 153-156. DOI: <https://doi.org/10.32837/11300.27842>

16. Дика А. І. Тестування безпеки вебзастосунків за допомогою ChatGPT. *Актуальні тенденції розвитку освіти, науки та технологій*: матер. VII міжнар. наук.-практ. конф. (Харків-Бахмут, 15 травня 2024 р.) Т. 2. С. 28-30. URL: <https://www.nnppi.in.ua/index.php/abit/2-uncategorised/270-naukovi-konferentsiyi>

17. Дика А. І., Трофименко О. Г. Аналіз потенційних загроз засобами ChatGPT для тестування безпеки вебзастосунків. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів*: матер. міжнар. наук.-практ. конф. (Одеса, 26 квітня 2024 р.) Одеса: НУ «ОЮА», 2024. С. 876-878. URL: <https://hdl.handle.net/11300/28085>

18. Дика А. І., Максименко А. Ж. Штучний інтелект у веброзробці: революція персоналізації користувача. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика*: матер. міжнар. наук.-практ. конф. (Одеса, 24 листопада 2023 р.) Одеса: НУ «ОЮА», 2023. С. 174-176. DOI: <https://doi.org/10.32837/11300.27179>

19. Дика А. І. Тестування штучного інтелекту: ключові виклики, стратегії вдосконалення. *Електронні інформаційні ресурси: створення, використання, доступ*: матер. міжнар. наук.-практ. інтернет-конф. (Вінниця, 20-21 листопада 2023 р.). Вінниця: КЗВО "Вінницька академія безперервної освіти". С.93-95. URL: <https://hdl.handle.net/11300/27979>

20. Манаков С. Ю., Дика А. І. Вибір сучасних засобів розробки мобільних застосунків. *Інформаційне суспільство: проблеми та перспективи* : матер. VIII всеукр. наук.-практич. конф. (Одеса, 2 червня 2023 р.). Одеса: НУ «ОЮА», 2023. С.86-89. DOI: <https://doi.org/10.32837/11300.25263>

21. Дика А. І., Лобода Ю. Г. Розвиток застосування WebAssembly у веброзробці. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень*: у 2 т.: матер. міжнар. наук.-практ. конф. (Одеса, 19 травня 2023 р.) Одеса: Видавництво «Юридика», 2023. Т. 1. С. 594-596. URL: <https://dspace.onua.edu.ua/items/c77ed43d-fe00-43d4-958d-0f60923956cd>

22. Трофименко О. Г., Дика А. І. Проблеми тестування вебсайтів е-комерції. *Інформаційні технології та менеджмент у вищій освіті та науці*: матер. міжнар. наук. конф. (Фергана, 28 листопада 2022 р.). Izdevniecība "Baltija Publishing". 2022. С. 195-199.

23. Дика А.І. Регресійне тестування в Agile. *Кібербезпека в сучасному світі: актуальні виклики*: матер. IV всеукр. наук.-практ. конф. (Одеса, 25 листопада 2022 р.). Одеса: НУ «ОЮА», 2022. С. 44-48.

24. Логінова Н.І., Дика А.І., Янковський О.Г. Аналіз вразливостей систем керування базами даних. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права): матер. міжнар. наук.-практ. конф. (Одеса, 17 червня 2022 р.). Одеса: Видавничий дім «Гельветика», 2022. Т. 1. С. 682-685.

Наукові праці, які додатково відображають наукові результати дисертації:

25. Задерейко О.В., Троянський О.В., Чанишев Р.І., Дика А.І. Концептуальні основи захисту інформаційного суверенітету України: монографія. Одеса: Фенікс, 2022. 220 с. ISBN 978-966-928-812-7.

26. Тестування та забезпечення якості програмних систем: навч.-метод. посібник [Електронне видання] / О.Г. Трофименко, А.І. Дика; Нац. ун-т «Одес. юрид. академія». Одеса: Фенікс, 2024. 140 с. URL: <https://hdl.handle.net/11300/27246>. ISBN 978-617-8395-32-2

27. Тестування та забезпечення якості програмних систем: навч. посібник [Електронне видання] / О.Г. Трофименко, А.І. Дика; Нац. ун-т «Одес. юрид. академія». Одеса: Фенікс, 2024. 195 с. URL: <https://hdl.handle.net/11300/27717>. ISBN 978-617-8395-88-9.

28. Комп'ютерна програма «Black Sea Hunter»: авторське свідоцтво № 129198 від 21.08.2024 / Струк Н.О., Дика А.І., Задерейко О.В., Логінова Н.І., Трофименко О. Г. <https://sis.nipo.gov.ua/uk/search/detail/1821799/>

Характеристика особистості здобувача. Дика Анастасія Іванівна має вищу юридичну освіту. У 2011 році закінчила Національний університет «Одеська юридична академія». Наразі працює асистентом кафедри програмної інженерії Національного університету «Одеська юридична академія».

Особистий внесок здобувача. Усі наукові результати, представлені в дисертаційній роботі, отримані здобувачем самостійно. Роботи [6, 8, 12, 14, 16, 19, 20, 22, 23, 26] – одноосібні. У співавторстві опубліковано праці [1-5, 7, 9-11, 13, 15, 17, 18, 21, 24, 25, 27], де здобувачка відповідала за розробку методології досліджень та практичне втілення результатів. Зокрема, внесок здобувача у зазначені роботи такий: [11] – здобувачем запропоновано інтелектуальні методи виявлення фішингових сторінок у вебзастосунках із використанням візуального подання; проведено порівняльний аналіз алгоритмів машинного навчання; побудовано прототип системи. У [3, 7, 18] – виконано системний аналіз уразливостей вебзастосунків та оцінку ефективності сучасних інструментів тестування безпеки; розроблено рекомендації щодо вдосконалення процедур тестування. У [15, 17, 21, 25] – розроблено концепції застосування методів штучного інтелекту в експериментальних програмних прототипах. У [2, 9, 10] – проведено аналіз проблем тестування вебсайтів електронної комерції; розроблено методологічні підходи для оцінки ефективності тестування та забезпечення безпеки користувацьких даних. У [4, 5] – досліджено сучасні засоби розробки мобільних застосунків; виконано аналіз вразливостей систем керування базами даних; здійснено порівняльний аналіз платформ та інструментів; запропоновано рекомендації щодо оптимізації розробки. У [1] – розглянуто сучасні умови та технології інформаційного впливу на громадян держави, які цілеспрямовано впроваджуються у суспільство з метою зламу інформаційного суверенітету держави. У [13] – досліджено застосування WebAssembly у веброботці; розроблено методику інтеграції WebAssembly у сучасні вебсервіси; сформовано рекомендації щодо підвищення продуктивності та безпеки. У [24] – проведено аналіз потенційних загроз вебзастосунків; запропоновано практичні підходи до оцінки безпеки вебсервісів із використанням штучного інтелекту. У [27] – сформовано методологію оцінки soft skills розробників програмного забезпечення та інтегровано її в навчальні та практичні модулі для ІТ-фахівців.

Оцінка мови та стилю та математичного апарату дисертації. Дисертація написана сучасною науковою мовою, стиль викладання відповідає прийнятому у науковій літературі та забезпечує логічність, послідовність і доступність сприйняття наукових положень, висновків і рекомендацій дослідження. Слід відзначити коректність і високий рівень використаного математичного апарату: авторкою ґрунтовно застосовано методи спектрального аналізу, статистичної обробки даних, елементи лінійної алгебри та теорії

машинного навчання. Формалізація задач, обґрунтування критеріїв прийняття рішень і математична інтерпретація отриманих результатів виконані на належному науковому рівні, що забезпечує достовірність і відтворюваність дослідження.

Дисертація 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 від 12.01.2022 р. № 44 (зі змінами від 03.05.2024, № 507).

Загальний висновок. Враховуючи викладене вважаємо, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Дикої Анастасії Іванівни на тему «Методи машинного навчання в тестуванні безпеки веборієнтованого програмного забезпечення», відповідає 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 (зі змінами від 08.04.2025, № 426), Вимогам до оформлення дисертації, затвердженими наказом Міністерства освіти і науки України від 12 січня 2017 р. № 40 (зі змінами від 31.05.2019, № 759) та 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 12.01.2022 р. № 44 (зі змінами від 03.05.2024, № 507) та **рекомендується до захисту на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.**

У результаті відкритого голосування учасники засідання розширеного засідання кафедри в кількості 25 осіб подали голоси «за». Ніхто із учасників фахового семінару не проголосував «проти» рекомендації дисертаційної роботи Дикої Анастасії Іванівни до захисту в разовій спеціалізованій вченій раді. Науковий керівник Трофименко О.Г., здобувачка Дика А.І. та декан Факультету кібербезпеки та інформаційних технологій Дикий О.В. участі в голосуванні не приймали.

УХВАЛИЛИ:

1. Затвердити висновок про дисертаційне дослідження Дикої Анастасії Іванівни на тему «Методи машинного навчання в тестуванні безпеки веборієнтованого програмного забезпечення», представленій на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки».

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

Анастасії Іванівни відповідає спеціальності 122 «Комп'ютерні науки» та 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 (зі змінами від 08.04.2025, № 426), Вимогам до оформлення дисертації, затвердженими наказом Міністерства освіти і науки України від 12 січня 2017 р. № 40 (зі змінами від 31.05.2019, № 759) та 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 12.01.2022 р. № 44 (зі змінами від 03.05.2024, № 507).

3. Рекомендувати дисертацію Дикої Анастасії Іванівни на тему «Методи машинного навчання в тестуванні безпеки веборієнтованого програмного забезпечення» до захисту на здобуття ступеня доктора філософії у разовій спеціалізованій вченій раді за спеціальністю 122 «Комп'ютерні науки».

4. Запропонувати Вченій раді наступний склад разової спеціалізованої вченої ради для проведення публічного захисту:

Голова: в.о. завідувача кафедри кібербезпеки Національного університету «Одеська юридична академія», д.т.н., професор Соколов Артем Вікторович;

Опонент: професор кафедри програмних засобів Національного університету «Запорізька політехніка», д.т.н., професор Олійник Андрій Олександрович;

Опонент: доцент кафедри програмного забезпечення комп'ютерних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», к.т.н., доцент Олещенко Любов Михайлівна;

Рецензент: доцент кафедри програмної інженерії Національного університету «Одеська юридична академія», к.т.н., доцент Чикунов Павло Олександрович;

Рецензент: доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», к.т.н., доцент Ахмаметьєва Ганна Валеріївна.

Результати голосування присутніх на засіданні докторів та кандидатів наук за профілем поданої на розгляд дисертації: за – 12; проти – немає; утримались – немає; науковий керівник участі у голосуванні не приймав.

**Головуюча на засіданні,
в.о. завідувача кафедри
програмної інженерії
Національного університету
«Одеська юридична академія»
к.пед.н., доцент**

Наталія ЛОГІНОВА