МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

до виконання кваліфікаційної роботи другого (магістерського) рівня вищої освіти для здобувачів спеціальності F5 «Кібербезпека та захист інформації» освітньо-професійної програми «Технічні системи інформаційного та кібернетичного захисту»

КИЇВ 2026

УДК 004.056(076.5)

Рекомендовано до друку вченою радою
Навчально-науковий інститут кібербезпеки та захисту інформації
Державний університет інформаційно-комунікаційних технологій
(протокол № 1 від «03» вересня 2026 р.)

Туровський О. Л., Рижаков М. М., Пепа Ю. В.
Методичні рекомендації до виконання кваліфікаційної роботи другого (магістерського) рівня вищої освіти для здобувачів спеціальності F5 «Кібербезпека та захист інформації» освітньо-професійної програми «Технічні системи інформаційного та кібернетичного захисту». Київ: ДУІКТ, 2026.
Обсяг визначається після остаточного макетування.

Методичні рекомендації встановлюють вимоги до вибору теми, планування, структури, змісту, оформлення та захисту магістерської кваліфікаційної роботи інженерного профілю. Особливу увагу приділено технічному завданню, моделюванню, програмно-апаратній реалізації, вимірюванням, експериментальній перевірці, відтворюваності результатів і безпечному поводженню з даними.

Видання призначене для здобувачів ОПП «Технічні системи інформаційного та кібернетичного захисту», наукових керівників, консультантів, рецензентів та членів екзаменаційних комісій.

ЗМІСТ

ПЕРЕДМОВА

Кваліфікаційна робота другого (магістерського) рівня вищої освіти є самостійним завершеним дослідженням або інженерною розробкою, у якій здобувач розв’язує актуальне завдання у сфері технічного захисту інформації та кіберзахисту. Робота має підтвердити здатність визначати проблему, формувати вимоги, обирати методи, створювати або вдосконалювати технічне рішення та перевіряти його результативність.

Тематика робіт за ОПП «Технічні системи інформаційного та кібернетичного захисту» охоплює виявлення і блокування технічних каналів витоку, захист об’єктів інформаційної діяльності, моніторинг побічних випромінювань, безпеку мереж і радіоканалів, криптографічні та програмно-апаратні засоби, кіберфізичні системи, захищені комплекси Інтернету речей, аналіз сигналів, оцінювання захищеності та випробування засобів кіберзахисту.

Обов’язковою ознакою магістерської роботи є власний перевірюваний результат. Ним може бути метод, модель, алгоритм, архітектура, програмно-апаратний прототип, методика вимірювання, експериментально встановлена залежність або обґрунтована сукупність технічних заходів. Опис відомих технологій без постановки задачі, критеріїв і перевірки результату не є достатнім.

Методичні рекомендації визначають єдиний підхід кафедри до організації, змісту, оформлення та оцінювання роботи. Вони не обмежують обґрунтований вибір методів для конкретної теми, але вимагають прозоро показати походження даних, умови експерименту, похибки, обмеження, ризики та особистий внесок здобувача.

1. ОРГАНІЗАЦІЯ ПІДГОТОВКИ ТА ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

1.1. Призначення та статус кваліфікаційної роботи

Кваліфікаційна робота виконується на завершальному етапі навчання і є підставою для встановлення відповідності результатів підготовки вимогам освітньої програми. Робота виконується індивідуально; здобувач відповідає за зміст, достовірність наведених даних, коректність розрахунків, дотримання правил безпеки та академічної доброчесності.

Результат повинен бути достатнім для фахового оцінювання. З тексту та додатків має бути зрозуміло, що саме створено або вдосконалено, за яких умов виконано перевірку, які метрики використано, з чим порівняно результат і в яких межах він може бути відтворений.

1.2. Вибір і затвердження теми

Тема обирається з переліку кафедри або пропонується здобувачем разом із керівником. Вона повинна відповідати профілю ОПП, містити конкретний об’єкт і технічну проблему, не дублювати раніше виконану роботу та передбачати результат, який можна перевірити за визначеними критеріями.

Назва теми формулюється стисло, без невизначених слів на кшталт «дослідження деяких питань». Доцільно використовувати конструкції «метод підвищення…», «модель оцінювання…», «програмно-апаратний засіб…», «методика виявлення…», якщо вони точно відповідають очікуваному внеску.

Під час погодження теми перевіряють:

– актуальність проблеми та відповідність напряму підготовки;

– наявність доступних вихідних даних, обладнання, програмних засобів і джерел;

– реалістичність обсягу робіт у межах календарного плану;

– можливість безпечного проведення експерименту без впливу на робочі системи;

– наявність кількісних або якісних критеріїв оцінювання результату.

1.3. Наукове керівництво та відповідальність здобувача

Керівник допомагає уточнити тему, завдання, структуру, методи і календарний план; консультує щодо джерел, експерименту та оформлення; контролює виконання ключових етапів; оцінює готовність роботи до подання. Керівник не виконує за здобувача розрахунки, програмування, оброблення даних або написання тексту.

Здобувач самостійно планує роботу, веде журнал експериментів і змін, зберігає вихідні дані, конфігурації, версії програмного забезпечення, проміжні результати та матеріали, що підтверджують авторство. За потреби до роботи залучають консультантів з метрології, охорони праці, економіки або окремих технічних питань.

1.4. Етапи виконання і календарне планування

Планування має відображати реальну послідовність інженерного дослідження. Кожний етап завершується матеріальним результатом: погодженою постановкою задачі, таблицею вимог, моделлю, схемою, кодом, протоколом вимірювань, набором даних, графіком або текстом відповідного розділу.

Етап	Зміст роботи	Контрольний результат
1	Уточнення проблеми, об’єкта, предмета, мети та критеріїв	Затверджене завдання
2	Аналіз стандартів, наукових джерел і відомих рішень	Аналітичний огляд і таблиця порівняння
3	Формування вимог, моделі загроз і технічного завдання	Перелік вимог та обмежень
4	Розроблення методу, моделі, алгоритму або архітектури	Схеми, моделі, специфікації
5	Підготовка стенда, програмної реалізації та даних	Працездатний прототип і план випробувань
6	Експеримент, вимірювання або моделювання	Протоколи та первинні дані
7	Статистичне оброблення, порівняння, аналіз похибок	Таблиці, графіки, оцінка достовірності
8	Оформлення, перевірка доброчесності, апробація	Завершений рукопис і супровідні матеріали
9	Попередній захист і підготовка доповіді	Презентація та демонстраційний сценарій

Строки в календарному плані визначаються індивідуально. Перенесення контрольної дати погоджується з керівником до її настання. Систематичне невиконання плану враховується під час допуску і в оцінці організації самостійної роботи.

1.5. Академічна доброчесність і використання цифрових засобів

Усі запозичені положення, формули, рисунки, таблиці, програмні фрагменти, набори даних та результати інших авторів супроводжуються посиланням. Фабрикація даних, підміна результатів, приховування негативних вимірювань, повторне подання чужої або власної раніше оціненої роботи як нової та несанкціоноване співавторство є неприпустимими.

Системи штучного інтелекту можуть використовуватися як допоміжний інструмент для пошуку напрямів, мовного редагування, пояснення коду або генерування чернеток, якщо це не суперечить правилам Університету. Здобувач перевіряє факти, джерела, формули та код, не передає сервісам дані з обмеженим доступом і не подає згенерований матеріал як власний неперевірений результат.

Якщо використання цифрового інструмента істотно вплинуло на методику, код, ілюстрації або текст, у роботі зазначають назву інструмента, мету використання, спосіб перевірки результату та межі відповідальності автора. За вимогою кафедри додають журнал запитів або інший підтверджувальний матеріал.

1.6. Попередній захист, рецензування і допуск

До попереднього захисту подають завершений текст, презентацію, відгук керівника та матеріали, що підтверджують працездатність рішення. Комісія перевіряє відповідність темі й завданню, наявність власного результату, повноту експериментальних доказів, коректність висновків та готовність здобувача пояснити прийняті рішення.

Завершена робота передається рецензентові у строк, визначений кафедрою. Рецензія оцінює актуальність, технічний рівень, новизну,

коректність методів, достовірність перевірки, практичну цінність, оформлення та особистий внесок. Зауваження рецензента не вилучаються; здобувач готує аргументовані відповіді на них.

1.7. Захист кваліфікаційної роботи

Захист проводиться на відкритому засіданні екзаменаційної комісії. Рекомендована тривалість доповіді становить 10–12 хвилин. Здобувач послідовно показує проблему, мету, критерії, відомі рішення, власний підхід, умови перевірки, результати, похибки, безпековий ефект, обмеження та рекомендації.

Демонстрацію виконують на безпечному стенді або за допомогою попередньо підготовленого відеозапису. Заборонено виводити на екран реальні паролі, криптографічні ключі, персональні дані, адреси критичних систем або іншу інформацію, розголошення якої створює ризик.

2. ВИМОГИ ДО ЗМІСТУ ТА СТРУКТУРИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

2.1. Обов’язкові структурні елементи

Кваліфікаційна робота містить такі елементи в наведеній послідовності:

– титульний аркуш;

– завдання на кваліфікаційну роботу і календарний план;

– реферат українською та англійською мовами;

– зміст; за потреби — перелік умовних позначень і скорочень;

– вступ;

– основну частину, як правило, з трьох розділів;

– висновки;

– перелік посилань;

– додатки та матеріали, необхідні для відтворення результатів.

Орієнтовний обсяг основного тексту становить 60–80 сторінок без додатків. Конкретний обсяг визначається змістом теми. Штучне збільшення обсягу загальновідомими відомостями, лістингами коду, знімками інтерфейсів або повторенням однакових положень не допускається.

2.2. Титульний аркуш

Титульний аркуш оформлюють за зразком у додатку А. Назва теми повинна дослівно відповідати наказу. Найменування Університету, інституту, кафедри, спеціальності та освітньої програми наводять повністю. Відомості про здобувача, керівника, консультантів і рецензента зазначають без довільних скорочень.

2.3. Завдання і календарний план

У завданні фіксують тему, строк подання, вихідні дані, перелік питань, які необхідно розробити, очікувані ілюстративні матеріали та календарні етапи. Вихідні дані мають бути конкретними: характеристики об’єкта, діапазони параметрів, нормативні вимоги, типи сигналів, обладнання, програмні середовища, обмеження безпеки.

Зміна затвердженого завдання допускається лише за погодженням із керівником і кафедрою. Після завершення роботи фактичний зміст розділів і висновків повинен відповідати поставленим завданням.

2.4. Реферат

Реферат обсягом до 400 слів складають українською та англійською мовами. Він містить відомості про обсяг роботи, мету, об’єкт, предмет, методи, одержаний технічний результат, наукову новизну, практичне значення, галузь застосування та 8–10 ключових слів.

Короткий зміст формулюють через виконані дії та отримані результати: розроблено, удосконалено, реалізовано, виміряно, перевірено, порівняно, встановлено. Твердження про підвищення ефективності супроводжують кількісним показником або чітко визначеним критерієм.

2.5. Зміст, перелік позначень і скорочень

Зміст відображає фактичну ієрархію заголовків і номери сторінок, на яких вони починаються. Назви у змісті та в тексті повинні бути ідентичними. Титульний аркуш, завдання, реферат і сам зміст до переліку не включають.

Перелік умовних позначень і скорочень подають, якщо робота містить спеціальні символи або більше п’яти маловідомих скорочень. Ліворуч за абеткою наводять позначення, праворуч — повне розшифрування. Загальновідомі одиниці SI до переліку не включають.

2.6. Вступ

Вступ обсягом до трьох сторінок починають з обґрунтування актуальності. Показують суперечність між потрібним і досягнутим рівнем захисту, нові загрози, обмеження наявних засобів або потребу конкретного класу об’єктів. Посилання на актуальність галузі загалом без аналізу проблеми недостатнє.

Мету формулюють як очікуваний перевірюваний результат: підвищення імовірності виявлення, зменшення похибки або часу оброблення, забезпечення заданого рівня захищеності, створення методу чи прототипу з визначеними

властивостями. Завдання утворюють логічний маршрут від аналізу відомих рішень до розроблення, перевірки та рекомендацій.

У вступі також визначають об’єкт, предмет, методи дослідження, наукову новизну, практичне значення, особистий внесок, апробацію та публікації. Новизна не може зводитися до використання сучасного програмного продукту; вона описує відмінність запропонованого результату від відомих рішень.

2.7. Основна частина

Основна частина, як правило, складається з трьох розділів. Кожний розділ починають з нової сторінки і завершують короткими висновками, у яких фіксують отримані результати. Назва розділу повинна відображати його функцію у розв’язанні поставленої задачі.

2.7.1. Перший розділ: аналіз предметної області

У першому розділі аналізують об’єкт захисту, моделі загроз і порушника, нормативні вимоги, технічні канали, відомі методи та засоби. Огляд має бути критичним: для кожного підходу визначають принцип дії, потрібні ресурси, переваги, обмеження, припущення та умови застосування.

Порівняння виконують за попередньо визначеними критеріями, наприклад: імовірність виявлення, частота хибних спрацьовувань, діапазон частот, затримка, продуктивність, стійкість до шуму, обчислювальна складність, вартість і можливість інтеграції. Результатом розділу є постановка задачі, перелік вимог та обґрунтований вибір напряму дослідження.

2.7.2. Другий розділ: розроблення рішення

Другий розділ містить власне рішення: математичну модель, метод, алгоритм, структурну і функціональну схеми, архітектуру програмно-апаратного комплексу, специфікацію модулів, інтерфейсів та параметрів. Кожне прийняте рішення пов’язують із вимогами, сформованими у першому розділі.

Опис має бути достатнім для відтворення. Для програмної реалізації зазначають мови, бібліотеки, версії, формати даних, ключові параметри та репозиторій; для апаратної — елементну базу, схему з’єднань, характеристики, калібрування, режими роботи та обмеження. Окремо описують межі довіри, можливі відмови та заходи безпечного проведення експерименту.

2.7.3. Третій розділ: експериментальна перевірка

Третій розділ містить програму й методику випробувань, опис стенда, вихідних даних і сценаріїв, результати вимірювань або моделювання, статистичне оброблення та порівняння з базовими рішеннями. Для кожного досліду вказують змінні, контрольовані параметри, кількість повторів, одиниці вимірювання та спосіб оцінювання похибки.

Результати подають у таблицях і графіках з підписаними осями. Поряд із середніми значеннями наводять розкид, довірчі інтервали або іншу оцінку невизначеності. Негативні результати не приховують; їх аналізують разом з обмеженнями валідності та сценаріями, у яких запропоноване рішення не забезпечує очікуваного ефекту.

2.8. Технічне, безпекове та економічне обґрунтування

За потреби порівнюють точність, швидкодію, надійність, масштабованість, ресурсоємність, енергоспоживання, складність упровадження і вартість запропонованого рішення з аналогами. Усі варіанти оцінюють за однаковими метриками й умовами. Джерело цін і дату оцінювання зазначають.

Безпекове обґрунтування показує, які загрози зменшуються, які залишкові ризики зберігаються, як рішення впливає на доступність і продуктивність та чи не створює нових каналів атаки або витоку. Якщо фінансова оцінка не відповідає меті роботи, її не підміняють формальним розрахунком.

2.9. Висновки

Висновки подають відповідно до поставлених завдань. Для кожного результату зазначають кількісний або якісний ефект, умови отримання, порівняння з базовим рівнем і практичне значення. Висновки не містять нових даних, яких немає в основній частині, і не повторюють дослівно текст розділів.

2.10. Перелік посилань

До переліку включають лише фактично використані джерела: нормативні акти, стандарти, наукові статті, монографії, технічну документацію, специфікації протоколів, набори даних і репозиторії коду. Перевагу надають первинним та актуальним джерелам. Рекомендована кількість — не менше 40 позицій, якщо інше не зумовлено специфікою теми.

2.11. Додатки і матеріали апробації

У додатках розміщують матеріали, потрібні для перевірки й відтворення, але громіздкі для основного тексту: схеми, специфікації, протоколи, фрагменти коду, конфігурації, додаткові графіки, акти випробувань, сертифікати, інструкції з розгортання та матеріали апробації.

Повні лістинги та великі набори даних доцільно розміщувати у репозиторії з постійним посиланням, описом версії та умов доступу. Конфіденційні відомості, реальні ключі, персональні дані та параметри робочих захищених систем до відкритої версії роботи не включають.

3. ВИМОГИ ДО ОФОРМЛЕННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

3.1. Загальні параметри сторінки і тексту

Роботу оформлюють на аркушах формату А4. Поля: ліве — 30 мм, праве — 15 мм, верхнє і нижнє — по 20 мм. Основний текст набирають шрифтом Times New Roman, кегль 14, міжрядковий інтервал 1,5. Абзацний відступ — 1,25 см; вирівнювання — по ширині; додаткові інтервали між абзацами не ставлять.

Текст викладають державною мовою; за погодженням кафедри допускається англійська. Терміни, позначення та одиниці SI вживають послідовно. Уникають розмовних конструкцій, невизначених тверджень, надмірних скорочень, повторів і необґрунтованого виділення жирним або курсивом.

3.2. Нумерація сторінок і структурних елементів

Сторінки нумерують арабськими цифрами наскрізно. Титульний аркуш входить до загальної нумерації, але номер на ньому не ставлять. Номер розміщують у правому верхньому куті без крапки. Сторінки, повністю зайняті рисунком або таблицею, також включають до нумерації.

Розділи нумерують у межах роботи, підрозділи — у межах розділу, наприклад 2.3. Пункти можуть мати номер 2.3.1. Реферат, зміст, перелік скорочень, вступ, висновки та перелік посилань не нумерують як розділи.

3.3. Заголовки та рубрикація

Заголовки структурних частин і розділів друкують напівжирними великими літерами по центру. Заголовки підрозділів друкують напівжирними малими літерами з першої великої, без абзацного відступу. Крапку наприкінці заголовка не ставлять. Переноси слів у заголовках не допускаються.

Кожний розділ починають з нової сторінки. Заголовок не залишають внизу сторінки без щонайменше двох наступних рядків тексту. Відстань і стиль заголовків задають засобами стилів Word, а не порожніми абзацами.

3.4. Ілюстрації

До ілюстрацій належать схеми, графіки, діаграми, знімки екрана та фотографії. Кожна ілюстрація повинна бути необхідною, читабельною і мати посилання в тексті. Позначення на схемі не повинні бути меншими за 10 пт після вставлення в документ. Осі графіків підписують із зазначенням одиниць вимірювання.

Ілюстрації нумерують у межах розділу: «Рис. 2.4». Підпис розміщують під зображенням по центру без крапки в кінці. Запозичена або адаптована ілюстрація супроводжується посиланням на джерело. Рисунок і підпис не розділяють між сторінками.

3.5. Таблиці

Таблицю розміщують після першого згадування або на наступній сторінці. Номер подають праворуч над таблицею, назву — наступним рядком по центру. Таблиці нумерують у межах розділу. Усі графи мають заголовки, а числові значення — одиниці вимірювання та однакову точність.

Заголовок таблиці повторюють на кожній сторінці. Рядок не розривають між сторінками. Для продовження пишуть «Продовження табл. 3.1». Якщо клітинка не заповнюється, ставлять тире; нульове значення не замінюють тире.

3.6. Формули та програмний код

Формули створюють засобами редактора формул Word і нумерують у межах розділу. Номер розміщують праворуч у круглих дужках. Після формули пояснюють усі символи й одиниці у порядку їх появи. Розрахунки подають із обґрунтованою кількістю значущих цифр та оцінкою невизначеності.

Короткий фрагмент програмного коду наводять моноширинним шрифтом 10–11 пт із номером і назвою. Великі лістинги виносять у додаток або репозиторій. Для програмної реалізації зазначають версію, залежності, параметри запуску та ліцензії використаних компонентів.

3.7. Цитування і бібліографічні посилання

Посилання у тексті подають у квадратних дужках за номером джерела, наприклад [12], або за правилами, установленими Університетом. Пряму цитату беруть у лапки та супроводжують сторінкою. Переказ чужої думки своїми словами також потребує посилання.

Бібліографічний опис складають мовою оригіналу відповідно до ДСТУ 8302:2015. Для вебресурсів указують автора або організацію, назву, URL і дату звернення; для стандарту — номер, назву, рік і видавця; для коду або набору даних — версію, репозиторій, DOI або URL та ліцензію.

3.8. Дані, програмні засоби та матеріали з обмеженим доступом

Для авторських наборів даних описують спосіб збирання, очищення, анонімізації, поділу на вибірки, формат, версію та дату отримання. Результати мають бути пов’язані з конкретною версією даних і коду. Випадкові процеси супроводжують фіксованим seed або описом повторюваності.

Робота з уразливостями, шкідливим кодом і засобами подвійного використання проводиться лише у контрольованому середовищі. Відкритий текст не повинен містити інструкцій, секретів або конфігурацій, які створюють невиправданий ризик. Обмеження доступу до додатків погоджують з кафедрою завчасно.

4. ОЦІНЮВАННЯ І ПІДГОТОВКА ДО ЗАХИСТУ

4.1. Умови допуску до захисту

До захисту допускається завершена робота, що відповідає затвердженій темі та завданню, має позитивний відгук керівника, рецензію, результат перевірки академічної доброчесності та належно оформлені супровідні матеріали. Програмний засіб, стенд або модель повинні бути доступні для демонстрації чи підтверджені протоколом випробувань.

4.2. Доповідь, презентація і демонстрація

Презентація підтримує доповідь, а не дублює текст роботи. Один слайд містить одну основну тезу; суцільний дрібний текст не використовують. Рекомендовано 10–15 слайдів: проблема і мета; об’єкт, предмет і критерії; аналіз аналогів; власний метод або архітектура; стенд і дані; результати; порівняння; новизна; практична цінність; висновки.

На графіках виділяють власний результат, підписують осі та одиниці. Під час демонстрації здобувач пояснює сценарій, вхідні дані, очікуваний ефект і межі безпеки. На запитання відповідає по суті, посилаючись на результати роботи, а не на загальні твердження.

4.3. Критерії оцінювання

Підсумкова оцінка формується за результатами рукопису, технічної реалізації, експериментальної перевірки, доповіді, демонстрації та відповідей. Максимальна кількість балів — 100.

Критерій	Максимум	Ознаки повного виконання
Актуальність, постановка задачі та відповідність ОПП	10	Проблему, мету, критерії й обмеження визначено однозначно
Аналітичний огляд і обґрунтування підходу	15	Порівняно актуальні рішення; вибір методу підтверджено критеріями
Технічна коректність і власний результат	25	Модель, метод, алгоритм або архітектура коректні та становлять особистий внесок
Експериментальна перевірка і достовірність	20	Описано стенд, дані, повтори, похибки; виконано порівняння
Безпековий ефект, практична цінність і відтворюваність	10	Результат має визначену користь; матеріали дають змогу перевірити його

Критерій	Максимум	Ознаки повного виконання
Оформлення, джерела та академічна доброчесність	5	Дотримано вимог; джерела і цифрові інструменти розкрито
Доповідь, демонстрація та відповіді	15	Власний внесок представлено переконливо; відповіді точні й аргументовані
Разом	100	

Наявність працездатного прототипу сама по собі не гарантує високої оцінки, якщо відсутні постановка задачі, методика перевірки та аналіз результатів. Так само якісний текст без власного технічного результату не відповідає вимогам до магістерської роботи інженерного профілю.

4.4. Шкала оцінювання

Бали	ECTS	Національна оцінка
90–100	A	відмінно
82–89	B	добре
75–81	C	добре
64–74	D	задовільно
60–63	E	задовільно
35–59	FX	незадовільно з можливістю повторного захисту
1–34	F	незадовільно з повторним виконанням роботи

4.5. Типові недоліки кваліфікаційної роботи

Оцінку знижують, зокрема, такі недоліки:

– тема, мета, завдання і висновки не утворюють єдиної логіки;

– огляд джерел є описовим і не містить критеріїв порівняння;

– власний внесок не відокремлено від відомих рішень;

– методика експерименту не дає змоги повторити перевірку;

– результати наведено без одиниць, похибок, базового порівняння або аналізу негативних випадків;

– висновки містять твердження, не підтверджені текстом і даними;

– рисунки та таблиці нечитабельні або не мають посилань у тексті;

– джерела, код, дані чи використання цифрових інструментів не розкрито;

– під час захисту здобувач не може пояснити походження даних, параметри і межі застосування результату.

ДОДАТОК А. ЗРАЗОК ТИТУЛЬНОГО АРКУША

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ»

на здобуття освітнього ступеня магістра
зі спеціальності F5 «Кібербезпека та захист інформації»
освітньо-професійної програми «Технічні системи інформаційного та кібернетичного захисту»

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів має посилання на відповідне джерело.

_____ Ім'я ПРІЗВИЩЕ здобувача

Керівник: науковий ступінь, вчене звання
_____ Ім'я ПРІЗВИЩЕ
Рецензент: науковий ступінь, вчене звання
_____ Ім'я ПРІЗВИЩЕ

Київ 2026

ДОДАТОК Б. ЗРАЗОК ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра технічних систем кіберзахисту

ЗАТВЕРДЖУЮ

Завідувач кафедри _____

«___» _____ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачу ПРІЗВИЩЕ Ім’я По батькові

1. Тема роботи: «Метод підвищення ефективності виявлення технічних каналів витоку інформації на об’єкті інформаційної діяльності».

Керівник роботи: ПРІЗВИЩЕ Ім’я По батькові, науковий ступінь, вчене звання.

Затверджено наказом Університету від «___» _____ 2026 р. № ____.

2. Строк подання роботи: «___» _____ 2026 р.

3. Вихідні дані: модель об’єкта інформаційної діяльності; перелік потенційних технічних каналів витоку; вимоги нормативних документів; характеристики засобів вимірювання; результати попереднього обстеження.

4. Питання, які необхідно розробити:

– проаналізувати моделі технічних каналів витоку та відомі засоби їх виявлення;
– сформувати критерії ефективності й вимоги до методу контролю;
– розробити метод оброблення вимірювальних даних і структурну схему стенда;
– реалізувати алгоритм та провести серію контрольованих експериментів;
– оцінити імовірність виявлення, хибні спрацьовування, похибки й обмеження;
– сформувати рекомендації щодо практичного застосування.

5. Ілюстративний матеріал: структурна схема, алгоритм, схема стенда, графіки та таблиці результатів.

6. Дата видачі завдання: «___» _____ 2026 р.

Здобувач _____ Ім’я ПРІЗВИЩЕ

Керівник _____ Ім’я ПРІЗВИЩЕ

ДОДАТОК В. КАЛЕНДАРНИЙ ПЛАН

№	Назва етапу	Строк	Відмітка
1	Уточнення технічної проблеми, мети, критеріїв та обмежень	___	
2	Аналіз наукових джерел, стандартів і відомих рішень	___	
3	Формування моделі загроз і технічного завдання	___	
4	Розроблення методу, моделі, алгоритму або структурної схеми	___	
5	Підготовка програмно-апаратного стенда, даних і методики	___	
6	Проведення вимірювань, експериментів або моделювання	___	
7	Оброблення даних, оцінювання похибок і порівняння	___	
8	Формування висновків, рекомендацій та матеріалів апробації	___	
9	Оформлення роботи та перевірка академічної доброчесності	___	
10	Попередній захист, підготовка презентації та захист	___	

Здобувач _____ Ім’я ПРІЗВИЩЕ

Керівник _____ Ім’я ПРІЗВИЩЕ

ДОДАТОК Г. ПОДАННЯ ЩОДО ДОПУСКУ ДО ЗАХИСТУ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач ПРІЗВИЩЕ І. П. до захисту кваліфікаційної роботи за спеціальністю F5 «Кібербезпека та захист інформації», ОПП «Технічні системи інформаційного та кібернетичного захисту», на тему «Метод підвищення ефективності виявлення технічних каналів витоку інформації на об’єкті інформаційної діяльності». Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Ім’я ПРІЗВИЩЕ

Висновок керівника кваліфікаційної роботи

Здобувач самостійно проаналізував відомі методи виявлення технічних каналів витоку, сформував критерії, розробив метод оброблення даних і експериментальний стенд. Проведені вимірювання підтверджують працездатність запропонованого рішення; похибки й обмеження проаналізовано. Результати мають практичну цінність для обстеження об’єктів інформаційної діяльності. Здобувач дотримався календарного плану та вимог академічної доброчесності. Робота може бути допущена до захисту.

Керівник _____ Ім’я ПРІЗВИЩЕ

Висновок кафедри

Кваліфікаційну роботу розглянуто. Здобувач ПРІЗВИЩЕ І. П. допускається до захисту в екзаменаційній комісії.

Завідувач кафедри _____ Ім’я ПРІЗВИЩЕ

ДОДАТОК Д. ВІДГУК РЕЦЕНЗЕНТА

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу освітнього ступеня магістр

здобувача ПРІЗВИЩЕ Ім’я По батькові на тему «Метод підвищення ефективності виявлення технічних каналів витоку інформації на об’єкті інформаційної діяльності».

Актуальність. Виявлення технічних каналів витоку потребує поєднання теорії сигналів, метрологічно коректних вимірювань і сучасних методів оброблення даних. Тема відповідає профілю освітньої програми та практичним потребам захисту об’єктів інформаційної діяльності.

Позитивні сторони

1. Проведено критичний аналіз відомих методів та сформовано модель технічного каналу витоку.
2. Запропоновано структурну схему засобу виявлення та обґрунтовано параметри.
3. Метод перевірено на експериментальному стенді; наведено дані, графіки, порівняння й оцінку похибки.
4. Сформульовано практичні рекомендації та межі застосування результату.

Недоліки. Доцільно розширити перевірку для додаткових типів обладнання та дослідити стійкість результату до зміни фонового шуму. Зауваження не знижує загальної позитивної оцінки роботи.

Висновок. Робота відповідає вимогам до магістерських кваліфікаційних робіт, а її автор заслуговує присвоєння кваліфікації за ОПП «Технічні системи інформаційного та кібернетичного захисту».

Рецензент _____ Ім’я ПРІЗВИЩЕ

науковий ступінь, вчене звання; місце роботи, посада

ДОДАТОК Е. ПРИКЛАД РЕФЕРАТУ

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 72 сторінки, 18 рисунків, 9 таблиць, 48 джерел.
Мета роботи — підвищення ефективності виявлення технічних каналів витоку інформації на об’єкті інформаційної діяльності.
Об’єкт дослідження — процес виявлення технічних каналів витоку інформації.
Предмет дослідження — методи та засоби вимірювання і класифікації інформативних сигналів у потенційних технічних каналах витоку.
Методи дослідження: системний аналіз, теорія сигналів, спектральний аналіз, статистичне оброблення, математичне моделювання, натурний експеримент і порівняльне оцінювання.
Розроблено метод оброблення вимірювальних даних з адаптивним порогом і структурну схему експериментального стенда. Виконано серію вимірювань, оцінено імовірність виявлення, частоту хибних спрацьовувань і похибку. Визначено умови застосування та обмеження методу.
Ключові слова: ТЕХНІЧНИЙ КАНАЛ ВИТОКУ, ІНФОРМАТИВНИЙ СИГНАЛ, СПЕКТРАЛЬНИЙ АНАЛІЗ, ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, ЕКСПЕРИМЕНТАЛЬНИЙ СТЕНД, ІМОВІРНІСТЬ ВИЯВЛЕННЯ, ПОХИБКА.

ABSTRACT

The qualification work comprises 72 pages, 18 figures, 9 tables, and 48 references.
The purpose is to improve the effectiveness of detecting technical information leakage channels at an information activity facility.
The research develops an adaptive measurement-data processing method and a test-bench architecture, performs controlled experiments, and evaluates detection probability, false alarms, measurement error, and limitations.
Keywords: TECHNICAL LEAKAGE CHANNEL, INFORMATIVE SIGNAL, SPECTRAL ANALYSIS, TECHNICAL INFORMATION PROTECTION, TEST BENCH, DETECTION PROBABILITY, MEASUREMENT ERROR.

ДОДАТОК Ж. ПРИКЛАД ЗМІСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

ЗМІСТ

ДОДАТОК И. ПРИКЛАД ВСТУПУ

ВСТУП

Актуальність теми. На об’єктах інформаційної діяльності інформація може поширюватися за межі контрольованої зони через акустичні, вібраційні, електромагнітні, оптичні та інші фізичні поля й кола. Зміна компонентної бази, цифрових інтерфейсів і бездротових технологій ускладнює своєчасне виявлення таких каналів.

Відомі засоби контролю часто використовують фіксовані порогові значення та потребують значного обсягу ручного аналізу. За змінного фонового шуму це збільшує кількість пропусків і хибних спрацьовувань. Тому актуальним є метод, який поєднує попереднє оброблення вимірювань, виділення інформативних ознак та адаптивне прийняття рішення.

Мета роботи — підвищення ефективності виявлення технічних каналів витоку інформації за рахунок адаптивного аналізу вимірювальних даних.

Для досягнення мети необхідно розв’язати такі завдання:

1. проаналізувати моделі технічних каналів витоку, методи вимірювання та алгоритми виявлення інформативних сигналів;
2. сформувати критерії ефективності й розробити метод оброблення даних з адаптивним порогом;
3. розробити структурну схему стенда та програмну реалізацію алгоритму;
4. провести експериментальну перевірку, оцінити точність, імовірність виявлення, хибні спрацьовування та обмеження.

Об’єкт дослідження — процес виявлення технічних каналів витоку інформації на об’єкті інформаційної діяльності.

Предмет дослідження — методи та засоби оброблення вимірювальних даних для виявлення інформативних сигналів.

Методи дослідження: системний аналіз, теорія сигналів, спектральний аналіз, статистичне оцінювання, математичне моделювання та натурний експеримент.

Наукова новизна полягає в удосконаленні методу виявлення інформативного сигналу шляхом адаптації порогового значення до оціненого рівня фонового шуму та сукупності спектральних ознак.

Практичне значення полягає у можливості використання алгоритму в програмно-апаратних засобах обстеження об’єктів інформаційної діяльності та під час вибору заходів технічного захисту.

Апробація результатів: назва заходу, місце проведення, дата, бібліографічні відомості про публікацію або інший документ, що підтверджує апробацію.

ДОДАТОК К. ПРИКЛАДИ БІБЛІОГРАФІЧНОГО ОПИСУ

Нормативно-правові акти

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 31.08.2026).

2. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 31.08.2026).

3. Про академічну доброчесність : Закон України від 18.12.2025 № 4742-IX. URL: https://zakon.rada.gov.ua/laws/show/4742-20 (дата звернення: 31.08.2026).

4. Про внесення змін до переліку галузей знань і спеціальностей : постанова Кабінету Міністрів України від 30.08.2024 № 1021. URL: https://zakon.rada.gov.ua/laws/show/1021-2024-п (дата звернення: 31.08.2026).

Стандарти вищої освіти та оформлення

5. Стандарт вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня : наказ МОН України від 18.03.2021 № 332.

6. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. Київ : ДП «УкрНДНЦ», 2016.

7. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. Київ : ДП «УкрНДНЦ», 2016.

Стандарти інформаційної та кібербезпеки

8. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : ISO, 2022.

9. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva : ISO, 2022.

10. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva : ISO, 2022.

11. ISO/IEC 15408-1:2022. Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1. Geneva : ISO, 2022.

Технічні настанови

12. NIST. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD : National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

13. NIST. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5. Gaithersburg, MD, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-53r5.

14. NIST. Technical Guide to Information Security Testing and Assessment. NIST SP 800-115. Gaithersburg, MD, 2008.

15. MITRE. ATT&CK Knowledge Base. URL: https://attack.mitre.org/ (date of access: 31.08.2026).

Наукова стаття

16. Прізвище І. І., Прізвище І. І. Назва статті про методи технічного захисту інформації. Назва журналу. 2026. Т. 10, № 2. С. 15–27. DOI: https://doi.org/xx.xxxx/xxxxx.

Матеріали конференції

17. Прізвище І. І. Назва доповіді. Кібербезпека та захист інформації : матеріали науково-практичної конференції, м. Київ, 15 травня 2026 р. Київ, 2026. С. 45–48.

Монографія

18. Прізвище І. І. Технічні системи захисту інформації : монографія. Київ : Видавництво, 2025. 320 с.

Технічна документація

19. Назва виробника. Назва приладу або програмного комплексу. User Guide. Version 3.2. 2026. URL: https://example.org/documentation (date of access: 31.08.2026).

Специфікація або RFC

20. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Internet Engineering Task Force, 2018. DOI: https://doi.org/10.17487/RFC8446.

Набір даних

21. Автор або організація. Назва набору даних. Version 2.0. Repository, 2026. DOI або URL (date of access: 31.08.2026). License: CC BY 4.0.

Репозиторій програмного коду

22. Автор або організація. Назва програмного засобу : source code. Version 1.4. GitHub, 2026. URL: https://github.com/owner/project (date of access: 31.08.2026). License: MIT.

Патент

23. Спосіб виявлення інформативного сигналу в технічному каналі витоку інформації : пат. України № _____ ; заявл. __.__.2026 ; опубл. __.__.2026, Бюл. № __.

Примітка. У фінальному переліку залишають лише фактично використані джерела. Дані умовних прикладів замінюють реальними бібліографічними відомостями.

ДОДАТОК Л. ПРИКЛАД ОФОРМЛЕННЯ РИСУНКА

У тексті перед рисунком наводять посилання та пояснюють, що саме демонструє схема. Позначення мають бути читабельними після вставлення в документ.

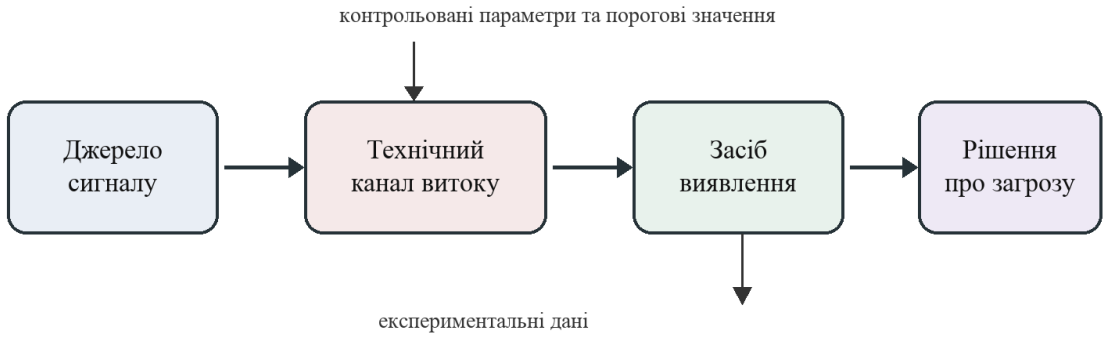

Рис. 2.4. Структурна схема виявлення технічного каналу витоку інформації

Після рисунка аналізують зв’язки між блоками, контрольовані параметри, вхідні дані та критерій прийняття рішення. Рисунок не замінює текстового пояснення алгоритму.

ДОДАТОК М. ПРИКЛАД ОФОРМЛЕННЯ ТАБЛИЦІ

Таблиця 2.1

Результати вимірювання інформативного сигналу в контрольних точках

Контрольна точка	**Смуга частот, МГц**	**Фоновий рівень, дБ**	**Рівень сигналу, дБ**	**Запас виявлення, дБ**
КТ-1	30–100	−72,4	−54,2	18,2
КТ-2	100–300	−68,1	−51,7	16,4
КТ-3	300–600	−66,9	−49,6	17,3
КТ-4	600–1000	−65,3	−46,8	18,5

Примітка. Для серії вимірювань у тексті додатково зазначають кількість повторів, статистичну характеристику та оцінку невизначеності.

ДОДАТОК Н. ПРИКЛАД ОФОРМЛЕННЯ ФОРМУЛ

Імовірність виявлення інформативного сигналу за результатами N незалежних випробувань оцінюють за формулою

$$P\_d = N\_d / N, \qquad (Н.1)$$

де P_d — оцінка імовірності виявлення; N_d — кількість правильних виявлень; N — загальна кількість випробувань.

Для подання результату разом з оцінкою невизначеності можна використати довірчий інтервал для біноміальної частки. Обраний метод побудови інтервалу та рівень довіри зазначають у тексті.

$$P\_fa = N\_fa / N\_0, \qquad (Н.2)$$

де P_fa — частота хибних спрацьовувань; N_fa — кількість рішень про наявність сигналу за його фактичної відсутності; N_0 — кількість контрольних випробувань без сигналу.

ДОДАТОК П. КОНТРОЛЬНИЙ ПЕРЕЛІК ПЕРЕД ПОДАННЯМ РОБОТИ

Перевірка	Так	Потрібне виправлення
Назва теми дослівно відповідає наказу і завданню	□	□
Мета, завдання, результати і висновки логічно узгоджені	□	□
Особистий внесок відокремлено від відомих рішень	□	□
Стенд, дані, параметри, версії та кількість повторів описано	□	□
Наведено базове порівняння, похибки й обмеження	□	□
Усі рисунки, таблиці та формули мають номери, назви і посилання	□	□
Усі запозичення, код і набори даних мають джерела	□	□
Використання систем ШІ та інших цифрових інструментів розкрито	□	□
У відкритій версії немає секретів, персональних чи конфіденційних даних	□	□
Зміст і номери сторінок перевірено після остаточного форматування	□	□
Презентацію, демонстрацію і відповіді на зауваження підготовлено	□	□

Здобувач _____ Дата _____

Керівник _____ Дата _____

Навчальне видання

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

до виконання кваліфікаційної роботи другого
(магістерського) рівня вищої освіти
здобувачів спеціальності F5 «Кібербезпека та захист інформації»

Туровський Олександр Леонідович
Рижаков Микола Миколайович
Пепа Юрій Володимирович

Підписано до друку __.__.2026. Формат 148×210.
Гарнітура Times New Roman. Тираж 100 прим.

Адреса редакції та видавця:
Україна, 03110, Київ, вул. Солом’янська, 7
Державний університет інформаційно-комунікаційних технологій