

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут інформаційних технологій та інноваційного
підприємництва

Кафедра кібербезпеки та захисту інформації

МЕТОДИЧНІ ВКАЗІВКИ

до виконання практичних робіт з дисципліни

«МЕТОДОЛОГІЯ НАУКОВИХ ДОСЛІДЖЕНЬ В ІТ-ГАЛУЗІ»

для здобувачів
другого (магістерського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Розробник: Кобозєва Алла Анатоліївна, доктор технічних наук, професор,
завідувачка кафедри «Кібербезпека та захист інформації»

Методичні вказівки схвалено на засіданні кафедри «Кібербезпека та захист
інформації»

(Протокол від «06» жовтня 2025 р. № 2)

Методичні вказівки схвалено на засіданні НМК ННІ ІТІП

(Протокол від «14» жовтня 2025 р. № 2)

ЗМІСТ

ВСТУП	4
Практична робота №1. Формулювання проблеми, об'єкта, предмета, мети та завдань наукового дослідження в ІТ-галузі	5
Практична робота №2. Написання рецензії на наукову статтю	14
Рекомендована література	20

ВСТУП

У сучасних умовах розвитку інформаційних технологій та кібербезпеки якісна підготовка фахівців освітнього ступеня магістра неможлива без глибокого оволодіння методологією наукових досліджень. Магістерська робота є першим самостійним науково-дослідним проєктом майбутнього фахівця, який вимагає не лише технічних знань, а й уміння чітко формулювати науковий апарат, критично оцінювати наявні літературні джерела та аргументовано представляти результати.

Практичні завдання з дисципліни «Методологія наукових досліджень в ІТ-галузі» спрямовані на те, щоб допомогти майбутнім магістрам подолати розрив між теоретичними концепціями та реальною науковою практикою. Набуття навичок структурного аналізу проблем, об'єктів і предметів досліджень, а також опанування навичок рецензування наукових статей дозволяють майбутнім дослідникам:

- свідомо обирати актуальні теми для власних пошуків;
- критично підходити до вибору методів аналізу та моделювання;
- уникати поширених методичних помилок під час оформлення наукових публікацій.

Таким чином, виконання даних практичних робіт формує аналітичне мислення, необхідне для успішного проведення майбутнього кваліфікаційного дослідження та презентації його результатів при захисті та у фахових виданнях.

ПРАКТИЧНА РОБОТА №1

Тема: ФОРМУЛЮВАННЯ ПРОБЛЕМИ, ОБ'ЄКТА, ПРЕДМЕТА, МЕТИ ТА ЗАВДАНЬ НАУКОВОГО ДОСЛІДЖЕННЯ В ІТ-ГАЛУЗІ

У сучасних умовах стрімкого розвитку цифрових технологій та ескалації кіберзагроз якісна підготовка магістрів у галузі ІТ, зокрема кібербезпеки, вимагає не лише технічних компетенцій, а й високої методологічної культури. Одним із найскладніших та водночас найважливіших етапів будь-якого наукового чи практичного дослідження є вміння правильно сформулювати його апарат: визначити проблему, об'єкт, предмет, мету та завдання.

Для сфери кібербезпеки та захисту інформації це має особливе, критичне значення з огляду на специфіку галузі:

- у кібербезпеці невірно ідентифікована вразливість або хибно окреслений вектор атаки призводять до хибних архітектурних рішень, реальних фінансових чи репутаційних втрат для підприємств і держави тощо;
- процеси захисту даних, криптографічного перетворення, моніторингу мережевого трафіку чи протидії несанкціонованим модифікаціям (зокрема у стеганографії та цифровій криміналістиці) охоплюють безліч пов'язаних систем. Без чіткого розмежування об'єкта (ширшої системи) та предмета (конкретного алгоритму чи механізму) дослідження неминуче втрачає науковий фокус;
- вміння побачити суперечність між новими типами загроз (наприклад, інтелектуальними фішинговими атаками чи складними кіберфізичними інцидентами) та обмеженнями існуючих засобів захисту дозволяє створювати дійсно ефективні, адаптивні та перевірювані рішення.

Практична робота №1 з дисципліни «Методологія наукових досліджень в ІТ-галузі» спрямована саме на те, щоб сформулювати у майбутніх магістрів навичку системного мислення, критичного аналізу та коректного планування власних наукових пошуків, що є запорукою успішного виконання та захисту майбутньої кваліфікаційної роботи.

Мета роботи - формування навичок правильного визначення основних елементів наукового дослідження на прикладі актуальних тем з ІТ та кібербезпеки.

Практична робота №1 спрямована на досягнення здобувачами наступних програмних результатів навчання:

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

Загальні рекомендації

1. Вибір теми дослідження

Тема має бути не лише цікавою для дослідника, а й відповідати предметній області спеціальності F5 згідно з ОПП «Кібербезпека та захист інформації» або сучасним тенденціям розвитку ІТ-галузі, тобто об'єктами дослідження можуть виступати сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; системи управління інформаційною безпекою та/або кібербезпекою; технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки.

Порада: варто обирати порівняно вузькоспрямовані теми (наприклад, захист конкретних компонентів архітектури, оптимізація певних алгоритмів або аналіз специфічних векторів атак), оскільки занадто широкі теми розмивають фокус дослідження та ускладнюють формулювання висновків. Завжди доцільно узгоджувати тему з майбутньою магістерською роботою, щоб напрацювання можна було інтегрувати у випускне дослідження.

Тема може бути обрана з запропонованих нижче або власна після узгодження з викладачем.

Теми та приклади проблем:

1. Біометрія у смартфонах (FaceID, відбиток пальця): наскільки це безпечніше за паролі?

Проблема: біометрія зручна, але чи справді вона надійніша за класичний пароль?

2. Двофакторна автентифікація (MFA): чи завжди вона гарантує захист акаунта?

Проблема: навіть з MFA трапляються випадки викрадення акантів.

3. Паролі студентів: чому навіть складні правила створення паролів часто не працюють?

Проблема: існують політики «8 символів, великі/малі букви, символи», але користувачі обходять їх простими трюками.

4. VPN-сервіси: чи завжди вони захищають дані користувачів?

Проблема: VPN рекламується як «повна безпека», але дослідження показують витоки даних і зловживання політиками «no log».

5. Соціальні мережі та приватність: чи реально допомагають налаштування конфіденційності?

Проблема: навіть при «закритому» профілі соцмережа збирає дані

користувача й може їх продавати.

6. Наскрізне шифрування в месенджерах (Signal, WhatsApp): чи захищає воно від усіх видів прослуховування?

Проблема: наскрізне шифрування не запобігає витоку даних через зараження пристрою або збереження резервних копій.

7. Фішинг через QR-коди: наскільки небезпечні ці атаки?

Проблема: користувачі довіряють QR-кодам, але вони можуть вести на фішингові сайти або запускати шкідливі дії.

8. Штучний інтелект у кібербезпеці: допомога чи нові ризики?

Проблема: AI може виявляти атаки, але водночас кіберзлочинці використовують AI для створення більш переконливих атак.

9. Хмарні сервіси (Google Drive, Dropbox): чи безпечні вони для конфіденційних документів?

Проблема: хмарні сервіси зручні, але хто має доступ до даних — лише користувач чи ще й провайдер/держава?

10. Смарт-годинники та фітнес-трекери: чи несуть вони ризики для приватності?

Проблема: дані про здоров'я та геолокацію збираються виробником і можуть бути використані третіми сторонами.

2. Формулювання проблеми дослідження

У наукових та прикладних дослідженнях у галузі IT та кібербезпеки правильне визначення проблеми є фундаментом усього подальшого проекту. Проблема - це не просто брак певної програми чи загальне побажання «зробити систему безпечнішою». Це чітко зафіксована об'єктивна суперечність між (новими) викликами практики (появою складніших кіберзагроз, зростанням обсягів даних, новими вимогами до швидкодії) та обмеженістю існуючих на сьогодні технологій, методів чи алгоритмів.

Точне формулювання проблеми є надзвичайно важливим для кібербезпеки. Дійсно, у сфері захисту інформації невірно ідентифікована прогалина призводить до впровадження неефективних захисних механізмів, які не закривають реальні вектори атак; чітко окреслена проблема доводить, що дослідження спрямоване на вирішення ще не вирішеного науково-технічного завдання, а не на банальне копіювання вже існуючих програмних продуктів.

Для того, щоб уникнути розмитості, неточності, у магістерських та наукових роботах з IT-галузі рекомендовано використовувати конструкцію-шаблон на кшталт:

«Є потреба [вказати практичну або виробничу необхідність], але існує обмеження / невизначеність [вказати технічний бар'єр або прогалину в існуючих методах]»,

що дозволяє чітко зафіксувати дослідницький бар'єр, який належить подолати

Тут частина «є потреба...» описує запит від сучасного бізнесу, державних систем чи цифрового середовища (наприклад, потреба в реалізації швидкого моніторингу трафіку в реальному часі або потреба в захисті передачі даних у динамічних мережах); частина «...але існує обмеження / невизначеність» розкриває причину, чому існуючі інструменти не справляються з цим

завданням повністю (наприклад, високий рівень хибнопозитивних спрацьовувань традиційних сигнатурних систем, значні часові затримки під час криптографічних перетворень або вразливість поточних алгоритмів до нових типів атак).

Приклад формулювання проблеми: «Є потреба у забезпеченні високого рівня захисту корпоративних розподілених мереж від новітніх цілеспрямованих атак, але існує обмеження у тому, що наявні статичні системи виявлення вторгнень не здатні адаптуватися до раніше невідомих аномалій без значного зростання обчислювальних витрат і часу на перевірку трафіку».

Типовими помилками при формулюванні проблеми є:

- підміна проблеми темою: формулювання на кшталт «Проблема полягає в дослідженні алгоритмів шифрування» є помилковим, оскільки це тема чи предмет, а не суперечність.
- занадто широкий масштаб: Формулювання на рівні «Кібербезпека в інтернеті є ненадійною» є занадто глобальним і не дозволяє запропонувати конкретне технічне рішення в межах магістерської роботи.
- відсутність технічної конкретики: Використання загальних фраз без прив'язки до конкретних параметрів (швидкість, точність, стійкість, обчислювальна складність).

3. Формулювання мети дослідження

Мета - це стратегічний орієнтир і кінцевий результат, який дослідник прагне отримати після завершення роботи.

Існує принципове методичне правило: мета дослідження не може полягати в розробці методу, моделі чи алгоритму як такого, а в досягненні конкретного якісного чи кількісного покращення (наприклад, підвищенні точності, зменшенні часу обробки даних, підвищенні рівня захищеності, зниженні обчислювальної складності тощо). При цьому розробка методу чи алгоритму є інструментом (шляхом) для досягнення цієї мети.

Формулювання мети зазвичай починається з дієслова у значенні отримання результату («*підвищити*», «*удосконалити*», «*зменшити*», «*оптимізувати*»), після чого вказується що саме покращується і за рахунок чого (або в межах чого):

«[Дієслово покращення, наприклад: Підвищення / Удосконалення] [назва показника ефективності чи характеристика процесу] у [сфера або система] шляхом [розробки/застосування методу, алгоритму чи моделі]».

Приклад формулювання мети: «Підвищення точності виявлення аномалій у мережевому трафіку корпоративних систем шляхом удосконалення алгоритмів машинного навчання з урахуванням динаміки параметрів трафіку». (Тут мета - підвищити точність виявлення, а вдосконалення алгоритмів - це шлях).

Типові помилки при формулюванні мети:

- підміна мети процесом: використання формулювань на кшталт «Дослідити питання захисту даних» або «Вивчити роботу алгоритмів

- шифрування». Дослідження - це шлях, а не мета. Мета завжди має фіксувати приріст знань чи покращення характеристик;
- перетворення інструменту на саму мету: формулювання на кшталт «Розробити алгоритм виявлення вторгнень» є неповним або хибним. Розробка алгоритму - це завдання або засіб. Завжди слід відповідати на запитання: «Заради чого розробляється цей алгоритм? Що це покращить?». Якщо алгоритм створено, але він працює повільніше чи гірше за існуючі, то навіщо було його розробляти.
 - відсутність вимірюваності (розмитість): мета на кшталт «Зробити систему безпечнішою» є занадто загальною. Показник має передбачати хоча б якісне (а в ідеалі - кількісне) покращення (наприклад, зменшення часу реакції на інциденти, зниження рівня хибнопозитивних спрацьовувань тощо);
 - невідповідність проблемі: мета повинна дзеркально відповідати зафіксованій у проблемному полі суперечності. Якщо в проблемі йшлося про обмеження швидкодії, то мета має бути спрямована саме на підвищення швидкодії, а не на захищеність від іншого типу загроз.

4. Визначення об'єкта та предмета дослідження

У науковому дослідженні правильне співвідношення об'єкта та предмета визначає системність роботи, її чіткі межі та фокус. Неправильно розведені поняття призводять до розмиття теми або підміни суті дослідження.

- *Об'єкт дослідження* - це процес, система або явище об'єктивної реальності, що породжує проблемну ситуацію і існує незалежно від свідомості дослідника. Об'єкт завжди ширший за тему дослідження і є «простором», у межах якого ведеться пошук. Об'єкт дослідження **відповідає на запитання: що досліджується загалом?**

Приклади об'єктів дослідження в ІТ та кібербезпеці: «процеси забезпечення інформаційної безпеки в хмарних середовищах», «системи моніторингу та аналізу мережевого трафіку», «процеси обробки та захисту цифрового контенту».

- *Предмет дослідження* - це конкретна властивість, сторона, елемент, відношення або закономірність усередині об'єкта, яка підлягає безпосередньому вивченню. Предмет становить ядро наукового інтересу і безпосередньо фігурує в назві роботи. Предмет дослідження **відповідає на запитання: що саме всередині об'єкта вивчається, які його параметри чи механізми вдосконалюються?**

Приклади предмета дослідження в ІТ та кібербезпеці: «механізми виявлення аномалій на основі машинного навчання», «алгоритми швидкої фільтрації пакетів у реальному часі», «методи стеганографічного приховування даних у цифрових відеопотоках».

Об'єкт і предмет співвідносяться як ціле і частина (або загальне і одиничне). Предмет завжди вкладений в об'єкт і не може виходити за його межі. Якщо об'єкт - це корпоративна мережа підприємства, то предметом не може бути мобільний додаток, який не пов'язаний із цією мережею.

Типові помилки при визначенні об'єкта і предмета:

- ототожнення об'єкта і предмета: найчастіша помилка, коли студент копіює формулювання об'єкта у предмет або робить предмет ширшим за об'єкт;
- перетворення предмета на технічний засіб (інструмент): предмет - це метод, алгоритм, а не сам пристрій чи програма. Наприклад, помилкою є вказувати предметом «програму Wireshark» чи «флеш-накопичувач». Предметом у такому разі будуть «методи аналізу захищеності»;
- занадто абстрактний предмет: формулювання на кшталт «безпека в інтернеті» для предмета є неприпустимим, оскільки воно занадто розмите і не окреслює конкретну наукову задачу;
- Відсутність логічного зв'язку з проблемою: предмет має безпосередньо вирішувати ту суперечність (обмеження), яка була зафіксована у формулюванні проблеми дослідження.

5. Побудова завдань дослідження

Завдання (задачі) дослідження - це поетапні наукові та практичні кроки (зазвичай 3–5), які у своїй сукупності забезпечують досягнення поставленої мети. Кожне завдання починається з дієслова (*проаналізувати, розробити, удосконалити, експериментально перевірити*) і відокремлює окрему логічну мікрозадачу.

Для повноцінного наукового дослідження в галузі ІТ та кібербезпеки структура завдань може виглядати так:

1. *Аналітичний етап (огляд і стан питання)*: проаналізувати наявні підходи, стандарти, протоколи та літературні джерела у сфері дослідження. Виявити критичні обмеження, недоліки чи незахищені вектори в існуючих методах та засобах.
2. *Теоретико-методологічний етап*: розробити (або формалізувати) теоретичні засади, концептуальну модель чи архітектуру запропонованого підходу (описати як саме вирішується проблема на концептуальному рівні).
3. *Практичний етап*: реалізувати запропонований алгоритм, метод чи програмний прототип.
4. *Експериментальний етап*: провести експериментальне дослідження досягнення мети роботи. Сформулювати практичні рекомендації.

Примітка: залежно від специфіки роботи, теоретичний та практичний етапи можуть частково об'єднуватися, але наявність етапу теоретичного обґрунтування є критично важливою для магістерського рівня.

Типові помилки при формулюванні завдань:

- дублювання мети: формулювання завдання у вигляді «Метою є...» або повторення тексту мети в завданні. Завдання - це кроки, а мета – результат;
- порушення логічної послідовності: наприклад, винесення практичного експерименту на перше місце до аналізу проблем чи побудови моделі.

Завдання мають вибудовуватися за принципом «від загального аналізу - до теорії, від теорії - до практики й оцінки результату»;

- занадто велика кількість завдань: формулювання 7–10 завдань часто свідчить про їх подрібнення або відсутність фокусу. Оптимальна кількість - 4–5 чітких кроків;
- перетворення завдань на опис технічних дій: завдання на кшталт «купити сервер», «встановити операційну систему» чи «написати код програми» є занадто низькорівневими і не відображають науково-методичного змісту дослідження. Завдання описують дослідницькі кроки.

6. Пошук та опрацювання інформації

Для забезпечення високої академічної якості та достовірності результатів слід базувати роботу виключно на авторитетних джерелах:

- Міжнародних наукометричних базах та бібліотеках (*Google Scholar, IEEE Xplore, SpringerLink, Scopus, Web of Science*);
- Офіційних технічних звітах і рекомендаціях профільних організацій (*NIST, ENISA, CERT-UA*);
- Аналітичних і практичних матеріалах провідних компаній у сфері кібербезпеки (*ESET, Check Point, Cisco Systems* тощо).

Треба уникати використання низькоякісних блогів, неперевічених форумів та популярних статей без зазначення технічної аргументації.

7. Вимоги до оформлення результатів (звіту)

7.1. Загальні технічні параметри звіту

Обсяг: 1–3 сторінки друкованого тексту (оптимальний обсяг, що дозволяє викласти весь науковий апарат без зайвої "води", але з достатньою глибиною пояснень).

Форматування:

- Шрифт: *Times New Roman*, кегль - 14 пт.
- Міжрядковий інтервал: 1.0.
- Вирівнювання тексту: за шириною.
- Абзацний відступ: 1.25 см.
- Поля сторінки: верхнє/нижнє - 20 мм, ліве - 30 мм, праве - 10 мм).

7.2. Обов'язкова структура звіту

Звіт має складатися з чітко виділених структурних елементів (бажано використовувати підзаголовки або нумерацію):

Титульна сторінка:

- Назва університету, кафедри та дисципліни («Методологія наукових досліджень в ІТ-галузі»).
- ПІБ студента, група, спеціальність (F5 Кібербезпека та захист інформації).
- Тема практичної роботи та обрана тема дослідження.

Вступна частина (актуальність):

Коротке обґрунтування (на 1–2 абзаци), чому обрана тема є важливою, актуальною та сучасною для галузі ІТ чи кібербезпеки.

Науковий апарат дослідження (ядро звіту):

- *Проблема дослідження* (оформлена за формулою «є потреба..., але існує обмеження...»).
- *Мета дослідження* (кінцевий результат через покращення показників).
- *Об'єкт дослідження* (ширша система чи процес).
- *Предмет дослідження* (конкретний аспект, що вдосконалюється).
- *Завдання дослідження* (поетапні кроки від аналізу до оцінки результату).

Аналітичний огляд джерел (Інформаційна база):

Коротка довідка (0.5 сторінки) про те, які джерела були опрацьовані (наприклад, стандарти NIST, статті з IEEE Xplore, звіти CERT-UA), з якими ключовими труднощами чи підходами зіткнувся автор під час аналізу літератури.

Список використаних джерел:

Перелік із 3–5 авторитетних джерел, оформлених відповідно до чинних академічних вимог.

7.3. Вимоги до академічного стилю та якості тексту

- Науковий стиль викладу: текст має бути написаний безособовою формою («проведено аналіз», «розроблено підхід», «визначено обмеження»), без використання емоційно забарвлених слів чи розмовної лексики;
- Логічна цілісність: усі елементи наукового апарату (проблема, об'єкт/предмет, мета, завдання) мають бути тісно пов'язані між собою. Наприклад, завдання мають розкривати шлях досягнення мети, а мета вирішувати сформульовану проблему.
- Уникнення плагіату та копіювання: навіть на етапі формулювання загальних тем та проблем забороняється просто копіювати чужі анотації без переосмислення. Магістр повинен продемонструвати розуміння суті сформульованих завдань.

Контрольні запитання для підготовки до захисту практичної роботи №1

1. У чому полягає принципова відмінність між об'єктом і предметом дослідження у сфері ІТ та кібербезпеки?
2. Яку структуру (формулу) рекомендовано використовувати при формулюванні проблеми дослідження і чому недостатньо просто описати актуальність теми?
3. Чому головна мета дослідження не може формулюватися як «розробка методу чи алгоритму»? У чому полягає справжня мета наукового пошуку?
4. Яку логічну послідовність повинні відображати завдання дослідження (від першого до останнього кроку)?

5. Чому для досліджень у галузі кібербезпеки критично важливо опиратися на авторитетні джерела (такі як стандарти NIST, звіти CERT-UA чи бази IEEE Xplore), уникаючи поверхневих блогів?

ПРАКТИЧНА РОБОТА №2

Тема: НАПИСАННЯ РЕЦЕНЗІЇ НА НАУКОВУ СТАТТЮ

Для майбутнього магістра та дослідника написання наукової рецензії - це не просто формальна вимога навчального плану, а ключовий інструмент професійного становлення. Аналізуючи чужу наукову працю, здобувач опановує кілька фундаментальних компетенцій, які є критично важливими для написання власної магістерської роботи:

- **розвиток критичного мислення:** вміння бачити не лише загальну ідею публікації, а й слабкі місця в аргументації, недостатність експериментальної бази чи невизначеність наукових висновків;
- **оволодіння академічним стандартом:** ознайомлення з тим, як вчені структурують свої результати, формують науковий апарат та доводять новизну;
- **навички конструктивної наукової дискусії:** здатність аргументовано, об'єктивно та коректно вказувати на недоліки без переходу на особистості, опираючись виключно на факти та стандарти галузі.

Метою Практичної роботи №2 є набуття навичок експертного оцінювання науково-технічних публікацій та рішень, що дозволяє магістранту самостійно виявляти критичні обмеження й приховані вразливості чужих технологій для обґрунтованого вибору власних інженерних рішень у кібербезпеці.

Практична робота №2 спрямована на досягнення здобувачами наступних програмних результатів навчання:

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

1. Завдання

Для обраної наукової статті (бажано за темою майбутньої магістерської роботи з наукометричних баз *Scopus*, *Web of Science*, *IEEE Xplore*, *ACM Digital Library* або провідних фахових видань України категорії «Б») необхідно провести глибокий експертний аналіз, критично опрацювати статтю за такими ключовими напрямками:

- **Аналіз актуальності та постановки проблеми:**
 - Чи дійсно визначена проблема є актуальною для сучасної кібербезпеки/ІТ, чи це вирішення застарілої або надуманої проблеми?
 - Чи простежується чітке протиріччя (наприклад, між необхідністю підвищення пропускну здатності прихованого каналу та вимогою стійкості до стеганоаналізу)?
- **Перевірка наукового апарату (цілісність дослідження):**

- Чи логічно пов'язані між собою проблема, об'єкт, предмет, мета та завдання статті?
- Чи не підмінюється мета дослідження (наприклад, чим є розробка алгоритму кінцевою метою чи лише інструментом досягнення кращих показників захисту)?
- **Оцінка методичної та експериментальної бази:**
 - Чи є використані методи (математичні моделі, архітектурні підходи, криптографічні чи стеганографічні схеми) адекватними поставленій задачі?
 - Чи достатньою є експериментальна перевірка? (Зверніть увагу: чи тестувався алгоритм на реальних/стандартних датасетах та умовах, чи в «теплих» симуляціях).
- **Аналіз результатів та їхньої наукової новизни:**
 - Чи підтверджені заявлені результати кількісними показниками (графіками, таблицями, порівняльним аналізом з існуючими аналогами), чи обмежуються загальними фразами на кшталт «покращено ефективність»?
 - У чому полягає реальна науково-технічна новизна, а що є лише комбінацією відомих рішень?
- **Верифікація висновків і джерел:**
 - Чи витікають фінальні висновки з отриманих результатів, чи є вони надмірно оптимістичними?
 - Чи спирається автор на авторитетні джерела (стандарти NIST, RFC, провідні конференції), чи посилається на застарілу літературу чи сумнівні веб-ресурси?

2. Структура та зміст звіту (експертного висновку)

Фінальний документ оформлюється у вигляді структурованого звіту-рецензії, що складається з таких обов'язкових розділів:

- **Шапка та вступні дані:**
 - Назва роботи, ПІБ студента, група.
 - Бібліографічний опис проаналізованої статті (автори, назва, журнал/конференція, рік, DOI або посилання).
 - Коротка анотація статті (2–3 речення про те, чому присвячена робота та яке рішення пропонують автори).
- **Результати експертного аналізу (змістова частина):**
 - Оцінка адекватності методичної бази та якості експериментальної перевірки (чи є докази переконливими).
 - Виявлені сильні сторони рішення (що саме варто взяти на озброєння чи використати у власній магістерській роботі).
- **Виявлені недоліки та "сліпі зони" (критичний блок):**
 - Логічні розриви в доведенні, слабкі місця в архітектурі або алгоритмі.

- Методологічні чи технічні обмеження, про які автори умовчали (наприклад, уразливість до певних типів атак, надмірні обчислювальні витрати, втрата ефективності при масштабуванні).

• **Конструктивні пропозиції щодо покращення:**

Що варто було б додати, змінити чи перевірити авторам, щоб робота стала бездоганною? (Наприклад: «доцільно провести тестування за умов наявності активного перешкоджання в каналі зв'язку»).

• **Загальний експертний висновок:**

Чи рекомендується ця стаття до практичного застосування/цитування у магістерській роботі та чому.

3. Стиль викладу та професійна етика

Уся критика будується виключно на технічних фактах, логіці та стандартах галузі, а не на емоційних оцінках.

Використовуйте коректні конструкції наукового та експертного стилю:

- *«У розділі 3 автор обґрунтовано доводить переваги запропонованого методу...»*
- *«Слабким місцем роботи є відсутність аналізу часової складності алгоритму в умовах високого навантаження...»*
- *«Доцільно було б розширити експериментальну базу шляхом включення...»*
- *«Задекларована висока стійкість методу потребує додаткової перевірки через...»*

4. Шаблон рецензії наукової статті

Назва статті: _____

Автор(и): _____

Журнал / джерело: _____

1. Короткий зміст статті

(2–3 речення: яку проблему розглядає стаття, які методи застосовані, які отримані результати).

2. Оцінка актуальності

Чи є тема сучасною і важливою для наукової спільноти?

Чи чітко обґрунтована проблема, яка вирішується?

3. Оцінка методів

Чи описані методи достатньо докладно?

Чи відповідають вони заявленій меті й задачам?

Чи є методологія коректною і науково обґрунтованою?

4. Оцінка результатів

Чи результати нові та значущі?

Чи підтверджені вони достатньою кількістю експериментів / доказів?

Чи зрозуміло, як їх можна застосувати на практиці?

5. Оцінка висновків

Чи узгоджуються висновки з результатами дослідження?

Чи відповідають вони заявленим меті й задачам?

Чи не є висновки занадто загальними або голослівними?

6. Сильні сторони статті

(навести 2–3 приклади: чітка структура, цікава постановка задачі, оригінальність, корисні експериментальні дані).

7. Недоліки статті

(навести 2–3 приклади: недостатня кількість експериментів, слабкий огляд літератури, нечіткі висновки, мовні помилки).

8. Пропозиції для покращення

(конкретні рекомендації: додати експеримент, порівняти з іншими підходами, уточнити мету, розширити аналіз джерел).

9. Загальна оцінка

Рівень роботи: високий / середній / низький.

Чи відповідає стаття вимогам наукової публікації?

Чи можна рекомендувати її до публікації (якщо це симуляція рецензії для журналу).

5. Приклад рецензії

Назва статті: «Метод виявлення фішингових атак із застосуванням машинного навчання»

Автори: Іваненко О., Петров С.

Журнал / джерело: Умовний журнал «Кібербезпека і технології», 2023

1. Короткий зміст статті

У статті запропоновано метод виявлення фішингових атак у корпоративних системах на основі алгоритмів машинного навчання. Автори використали набір даних із 20 000 електронних листів, провели попередню обробку й навчання моделей SVM та Random Forest. Результати показали підвищення точності виявлення на 12% у порівнянні з базовими рішеннями.

2. Актуальність

Тема є надзвичайно актуальною, оскільки фішинг залишається одним із найпоширеніших векторів атак у світі та в Україні. Проблема чітко сформульована, і дослідження спрямоване на практичну загрозу для бізнесу та державних установ.

3. Методи

Методологія дослідження відповідає поставленій меті. Автори використали відомі алгоритми машинного навчання, коректно описали процес підготовки даних. Проте відсутній аналіз інших сучасних моделей (наприклад,

нейронних мереж), що зменшує наукову новизну.

4. Результати

Отримані результати переконливі: показники точності (accuracy = 93%), повноти (recall = 91%) та F1-міри підтверджують ефективність методу. Водночас результати обмежені конкретним датасетом, і невідомо, як метод працюватиме на реальних корпоративних даних.

5. Висновки

Висновки відповідають результатам дослідження і узгоджуються з метою. Проте вони занадто узагальнені: авторам варто було б вказати обмеження методу та перспективи його подальшого вдосконалення.

6. Сильні сторони

Актуальність теми.

Використання сучасних методів машинного навчання.

Чітка структура статті.

7. Недоліки

Вузький набір досліджених моделей.

Обмеженість експериментів одним датасетом.

Відсутність порівняння з реальними комерційними рішеннями.

8. Пропозиції

Додати експерименти з іншими алгоритмами (нейронні мережі, ансамблеві методи).

Перевірити метод на реальних корпоративних листах.

Розширити огляд літератури, включивши сучасні міжнародні дослідження.

9. Загальна оцінка

Стаття є цікавою, актуальною і корисною для розвитку галузі кібербезпеки. Незважаючи на певні обмеження, вона відповідає вимогам наукової публікації та може бути рекомендована до друку після доопрацювання.

Контрольні запитання для підготовки до захисту Практичної роботи №2

1. Як відрізнити реальну науково-технічну новизну статті від простого маркетингового опису чи комбінації відомих рішень?
2. Чому відсутність реальної або достатньої експериментальної перевірки (тестування лише в «теплих» симуляціях) є критичним недоліком статті?
3. Який зв'язок має виявлення «сліпих зон» та обмежень у чужій статті з написанням власної магістерської роботи?
4. У чому полягає різниця між коректною технічною критикою в рецензії та емоційною оцінкою?
5. Чому перед впровадженням будь-якого нового алгоритму або методу захисту (наприклад, нового протоколу прихованого каналу чи методу виявлення аномалій) фахівець зобов'язаний проаналізувати побічні ефекти - такі як обчислювальні витрати чи втрата продуктивності?

Рекомендована література

1. Мокін, Б. І. Методологія та організація наукових досліджень: підручник – вид.3-є, змін. та доп. [Електронний ресурс] / Б.І.Мокін, О.Б.Мокін, В.Б. Мокін. – Вінниця: ВНТУ, 2023. 230 с. <https://press.vntu.edu.ua/index.php/vntu/catalog/view/805/1408/2677-1>
2. Методологія наукових досліджень та приклади її використання [Електронний ресурс] : навчальний посібник / Самсонов В. В., Сільвестров А. М., Тачиніна О. М. – Київ : Національний університет харчових технологій, 2022. – 385 с. <https://ela.kpi.ua/items/f5445ef1-700d-4ab6-a00d-391c5c6439b7>
3. Зацерковний В. І. Методологія наукових досліджень : навч. посіб. / В. І. Зацерковний, І. В. Тішасв, В. К. Демидов. – Ніжин: НДУ ім. М.Гоголя, 2017. – 236 с. <https://dspace.ksaeu.kherson.ua/bitstream/handle/123456789/4642/%D0%9C%D0%95%D0%A2%D0%9E%D0%94%D0%9E%D0%9B%D0%9E%D0%93%D0%86%D0%AF%20%D0%9D%D0%90%D0%A3%D0%9A%D0%9E%D0%92%D0%98%D0%A5.pdf?sequence=1>
4. Трифонова О.М. Інформаційні технології в наукових дослідженнях / О.М.Трифопова, М.І.Садовий // Збірник наукових праць "Педагогічні науки". 2022. № 98. С.27-33. <https://ps.journal.kspu.edu/index.php/ps/article/view/4502>