МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

МЕТОДИЧНІ ВКАЗІВКИ

до підготовки реферату з дисципліни

«ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ»

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

Одеса 2025

Розробник: Кобозєва Алла Анатоліївна, доктор технічних наук, професор, завідувач 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

Інформаційна безпека держави в сучасних умовах є однією з найбільш пріоритетних галузей, оскільки вона охоплює захист не лише технічних систем, а й національних інтересів у цифровому просторі. Для студента першого курсу спеціальності F5 Кібербезпека та захист інформації підготовка реферату є першим кроком до формування професійного світогляду.

Ця робота не повинна бути простим копіюванням чужих думок, адже справжній фахівець має вміти самостійно збирати, перевіряти та узагальнювати дані. Вивчення цієї дисципліни дозволяє зрозуміти, як функціонують механізми захисту інформаційного суверенітету та яку роль відіграє кожен елемент державної системи у протидії сучасним загрозам. Під час роботи над темою студент вчиться розрізняти об'єктивну інформацію та маніпулятивні вкиди, що є критично важливою навичкою для майбутнього фахівця з кібербезпеки.

1. Роль самостійної роботи та пошук джерел

Самостійне опанування тем з інформаційної безпеки вимагає особливої відповідальності у виборі джерел інформації. У сучасному світі, де дезінформація та фейки стали інструментами гібридної війни, студент має орієнтуватися насамперед на офіційні державні ресурси, закони України, звіти профільних міністерств та наукові публікації авторитетних фахівців. Неприпустимим є використання анонімних повідомлень із соціальних мереж або сумнівних сайтів, які не несуть відповідальності за достовірність контенту.

Кожне твердження в рефераті повинно бути підкріплене посиланням на першоджерело, що демонструє повагу до авторського права та дотримання принципів академічної доброчесності. Важливо пам'ятати, що наукова робота - це насамперед чесність перед собою та аудиторією, тому будь-яке запозичення чужих ідей без належного оформлення вважається плагіатом і нівелює цінність дослідження.

2. Пояснення щодо вибору теми, змісту та аналізу теми

Вибір теми реферату є визначальним етапом, від якого залежить не лише якість майбутньої роботи, а й рівень залученості студента у навчальний процес. Першокурснику варто орієнтуватися на ті аспекти інформаційної безпеки, які викликають у нього щирий професійний інтерес, адже робота над захоплюючою темою перетворюється з формального виконання завдання на глибоке творче дослідження. Коли обрана проблема резонує з власними інтересами студента, це стимулює до пошуку нестандартних джерел, аналізу складних кейсів та формулювання самостійних, нестандартних висновків. Саме такий підхід дозволяє закласти міцний фундамент для подальшої наукової діяльності, оскільки вдало обрана тема на першому курсі може

перерости у серйозне дослідження в межах курсової чи навіть дипломної роботи.

Окрім особистого інтересу, критично важливим критерієм вибору є актуальність обраної проблеми в контексті сучасних викликів, з якими стикається Україна та світ. Студентам рекомендується звертати увагу на питання, що перебувають на вістрі технологічного прогресу або мають безпосередній вплив на національну безпеку в умовах реальних кіберзагроз. Робота над актуальною темою дозволяє першокурснику відчути причетність до розв'язання реальних державних завдань та зрозуміти практичну цінність отриманих теоретичних знань. Аналіз свіжих прикладів інформаційних атак чи новітніх методів захисту даних робить реферат сучасним і затребуваним, демонструючи здатність майбутнього фахівця тримати руку на пульсі динамічних змін у галузі інформаційних технологій.

Збалансоване поєднання особистої зацікавленості та суспільної значущості обраного питання дозволяє підготувати роботу, яка буде цікавою не лише автору, а й аудиторії під час захисту. Глибоке розуміння того, чому саме ця тема є важливою «тут і зараз», надає студенту впевненості у своїх аргументах і дозволяє вийти за межі простого переказу підручника. Слід пам’ятати, що сфера кібербезпеки не терпить застарілих підходів, тому вміння ідентифікувати найбільш гострі та актуальні проблеми є професійною рисою, яку варто розвивати з перших днів навчання в університеті. Такий відповідальний підхід до вибору напряму дослідження свідчить про високий рівень мотивації студента та його готовність до професійного зростання у складній і відповідальній системі забезпечення інформаційної безпеки держави.

Підготовка основної частини реферату передбачає глибоке занурення у зміст обраної проблеми, де студент має продемонструвати не лише знання термінології, а й здатність логічно викладати свої думки. Аналітичний підхід полягає в тому, щоб не просто перерахувати факти, а спробувати знайти причини виникнення певної загрози та запропонувати можливі шляхи її нейтралізації. Наприклад, розглядаючи питання інформаційно-психологічного впливу, варто звернути увагу на те, як саме маніпулятивні технології впливають на свідомість людини та які методи самозахисту є найбільш ефективними для пересічного громадянина.

Особливу увагу слід приділити висновкам, які повинні бути логічним завершенням всієї роботи. У висновках студент має підсумувати все вищевикладене та сформулювати власну позицію щодо перспектив розвитку системи інформаційної безпеки в Україні, спираючись на опрацьований матеріал.

3. Поради щодо оформлення та візуалізації матеріалу

Якість подання матеріалу безпосередньо впливає на його сприйняття, тому оформлення реферату та презентації повинно відповідати встановленим стандартам. Окрім текстового наповнення, велике значення має візуальна складова, як-от схеми, таблиці чи графіки, що допомагають краще розкрити

складні поняття. Кожна ілюстрація має бути доречною та супроводжуватися поясненням у тексті. Під час створення презентації варто уникати надмірного нагромадження тексту на слайдах, оскільки вони слугують лише фоном для вашого виступу. Головне завдання студента під час захисту - впевнено володіти матеріалом, вміти аргументовано відповідати на запитання та демонструвати щирий інтерес до обраної теми. Це перший досвід публічного виступу з професійної тематики, який закладає фундамент для майбутніх конференцій та захисту дипломних робіт.

4. Вимоги до оформлення

- Обсяг роботи: 10–15 сторінок друкованого тексту (без урахування титульного аркуша, змісту та списку літератури).
- Шрифт: Times New Roman, кегль 14.
- Міжрядковий інтервал: 1.
- Поля: ліве – 30 мм, праве – 15 мм, верхнє та нижнє – 20 мм.
- Абзац: відступ 1,25 см.
- Нумерація сторінок: обов’язкова, внизу сторінки по центру (починаючи зі змісту).

Титульний аркуш: містить назву університету, кафедри, назву дисципліни, тему реферату, дані про студента (ПІБ, група) та викладача, рік виконання (Додаток 1).

5. Вимоги до структури роботи

Реферат повинен мати чітку структуру:

5.1. Титульний аркуш.

5.2. Зміст. (із зазначенням сторінок)

5.3. Вступ:
- актуальність теми;
- мета і завдання роботи;
- короткий опис проблеми.

5.4. Основна частина:
- 2–3 розділи, кожен із підрозділами;
- теоретичний огляд теми (визначення, підходи, приклади);
- практичні аспекти (сучасний стан, ситуація в Україні, приклади з життя).

5.5.Висновки:
- узагальнення матеріалу;
- власні висновки студента;
- можливі шляхи вирішення проблеми.

5.6. Список використаної літератури:
- не менше 5 джерел;
- обов’язково включати навчальні матеріали, наукові статті, законодавчі документи, офіційні сайти.

5.7. Додатки (за наявності: схеми, таблиці, графіки).

6. Вимоги до змісту

Реферат має показувати самостійність студента у роботі з джерелами. Текст повинен бути написаний науковим стилем (без зайвої емоційності). Використовувати терміни та поняття дисципліни «Інформаційна безпека держави» («інформаційна безпека», «дезінформація», «кібербезпека» тощо).
У тексті обов'язково робити посилання на джерела, що вказані в списку використаної літератури.
Важливі положення рекомендується ілюструвати прикладами з практики (особливо в сучасному контексті України).
У висновках потрібно відобразити **власну позицію студента** щодо досліджуваної проблеми.

7. Критерії оцінювання

- Відповідність змісту заявленій темі.
- Повнота розкриття питання.
- Логічність та структурованість викладу.
- Використання наукових джерел і правильне оформлення посилань.
- Самостійність аналізу та власні висновки студента.
- Дотримання вимог до оформлення.

8. Вимоги до презентації для захисту реферату

При захисті роботи викладення матеріалу повинно супроводжуватися презентацією.

8.1. Загальні вимоги

- Презентація створюється у PowerPoint.
- Кількість слайдів: 7–12 (не більше 15).
- Використовувати єдиний стиль оформлення (шрифт, кольори, фон).
- Текст повинен бути коротким і чітким.

8.2. Структура презентації

- Титульний слайд: тема реферату; ПІБ студента, група; викладач, рік.
- Вступ: актуальність теми, мета і завдання роботи.
- Основні слайди:
  - виклад ключових положень реферату (загрози, приклади, аналіз);
  - використання схем, таблиць тощо.
- Висновки: підсумки дослідження, власні думки студента.
- Список джерел (можна одним слайдом із найважливішими).

8.3. Вимоги до оформлення

- Шрифт: не менше 18 pt для основного тексту.
- Кольори: контрастні, текст має бути легко читабельним.
- Використовувати ілюстрації, діаграми, графіки, зображення для підсилення матеріалу.
- Анімація допускається, але має бути стриманою (без зайвих ефектів).
- Кожен слайд повинен відображати одну основну думку.

9. Вимоги до захисту

- Час основного виступу: 7–10 хвилин.
- Студент не повинен читати текст із слайдів, а лише пояснювати основні тези.
- Виклад має бути логічним, аргументованим, супроводжуватися прикладами.
- Важливо показати власне розуміння теми та зробити акцент на висновках.
- Відповіді на питання аудиторії.

10. Можливі теми рефератів

1. ***Роль ЗМІ у розпаді СРСР***
   - Система радянських ЗМІ та їхня підконтрольність державі.
   - Лібералізація у період перебудови (гласність).
   - Вплив незалежних і західних медіа на суспільну думку.
   - Роль інформації у формуванні настроїв, що призвели до розпаду.

2. ***Дослідження ролі "ворожих голосів" (західне радіомовлення на територію СРСР)***
   - Поняття «ворожі голоси» та їх цілі.
   - Основні канали (Radio Liberty, Voice of America тощо).
   - Методи глушіння сигналу та реакція СРСР.
   - Вплив на населення та підрив довіри до радянської влади.

3. ***Вплив діяльності релігійних неокультів на національну безпеку держави.***
   - Поняття неокультів та їхні особливості.
   - Методи впливу на особистість і суспільство.
   - Приклади небезпечних неокультів в Україні та світі.
   - Загрози для національної безпеки.

4. ***Порівняльна характеристика пропаганди Німеччини та СРСР на окупованих територіях у роки Другої світової війни***
   - Основні цілі німецької та радянської пропаганди.
   - Методи впливу на населення.
   - Подібності та відмінності в підходах.

- Наслідки пропагандистської діяльності.

5. ***Кремлівська пропаганда на окупованих територіях України. Протистояння кремлівській пропаганді***.
   - Основні наративи кремлівської пропаганди.
   - Методи поширення інформації.
   - Вплив на місцеве населення.
   - Українські та міжнародні заходи протидії.

6. ***Інформаційна гігієна як засіб протидії інформаційним впливам у контексті російсько-української війни***
   - Поняття інформаційної гігієни.
   - Основні правила безпечного споживання інформації.
   - Приклади інформаційних атак Росії.
   - Як інформаційна гігієна допомагає протидіяти впливам.

7. ***Місце та роль засобів масової комунікації в національній системі протидії корупції в Україні***
   - Роль ЗМІ у викритті корупційних схем.
   - Журналістські розслідування як антикорупційний інструмент.
   - Приклади впливових публікацій у ЗМІ.
   - Співпраця держави та медіа у боротьбі з корупцією.

8. ***Організаційно-правові аспекти взаємодії держав у глобальному інформаційному просторі***
   - Поняття глобального інформаційного простору.
   - Міжнародні норми та угоди у сфері інформаційної безпеки.
   - Приклади співпраці держав у кіберсфері.
   - Виклики та проблеми правового регулювання.

9. ***Дезінформація в Інтернет ЗМІ***
   - Особливості інтернет-медіа.
   - Методи поширення дезінформації онлайн.
   - Приклади фейкових кампаній.
   - Способи виявлення та протидії.

10. ***Технологія Deep Fake. Створення Deep Fake***
    - Що таке deepfake та як він працює.
    - Сфери використання (позитивні та негативні).
    - Загрози для безпеки та довіри.
    - Приклади відомих deepfake-відео.

11. ***«Фабрики тролей» як сучасний вид інформаційної зброї. Дослідження діяльності мережевих тролів та їх впливу на громадську думку***
    - Хто такі «фабрики тролів» та як вони працюють.
    - Методи впливу на аудиторію.
    - Приклади діяльності у світі та в Україні.
    - Наслідки для суспільства та демократії.

12. ***Роль сучасних інформаційних технологій для створення неправдивої інформації (зокрема зображення, відео) в інформаційному просторі***.
    - Інструменти створення фейкового контенту.
    - Приклади використання в політиці та війні.
    - Небезпеки для суспільства.
    - Методи протидії.

13. ***Інформаційні можливості нейтралізації стресу серед українського населення в період війни***
    - Роль інформації у формуванні психологічного стану.
    - Методи підтримки через медіа та соціальні мережі.
    - Приклади інформаційних кампаній для зниження стресу.
    - Висновки для державної політики.

14. ***Приховані (стеганографічні) канали зв'язку як загроза інформаційному простору***
    - Поняття стеганографії.
    - Методи приховування інформації.
    - Використання прихованих каналів у злочинній чи шпигунській діяльності.
    - Загроза для держави та шляхи протидії.

15. ***Інформація як найдорожчий товар у цифрову епоху***
    - Чому інформацію називають «новою нафтою».
    - Приклади цінної інформації (дані, бази, технології).
    - Інформаційні ресурси як стратегічний актив держави.

16. ***Соціальні мережі як виклик інформаційній безпеці***
    - Роль соцмереж у житті суспільства.
    - Позитивний вплив (інформування, комунікація).
    - Негативні наслідки (фейки, маніпуляції, кібербулінг).

17. ***Захист персональних даних у повсякденному житті***
    - Що таке персональні дані.

- Приклади витоків та їх наслідки.
- Як громадяни можуть захищати свої дані.

18. ***Основи кібергігієни студента***
    - Правила створення безпечних паролів.
    - Захист у соціальних мережах.
    - Використання антивірусів і резервних копій.

19. ***Відповідальність за поширення недостовірної інформації***
    - Різниця між свободою слова і фейком.
    - Цивільна, адміністративна та кримінальна відповідальність.
    - Приклади в українському законодавстві.

20. ***Роль журналістики у сфері інформаційної безпеки***
    - Журналістика як четверта влада.
    - Відповідальність журналістів за достовірність.
    - Приклади позитивної та негативної ролі ЗМІ.

21. ***Месенджери як інструмент інформування та маніпуляції***
    - Популярність месенджерів у суспільстві.
    - Позитивні приклади (новини, координація).
    - Небезпеки (анонімні фейки, паніка).

22. ***Використання мемів у інформаційних атаках***
    - Мем як спосіб комунікації.
    - Як меми формують суспільну думку.
    - Приклади мемів у пропаганді та контрпропаганді.

23. ***Хакерські угруповання як виклик для держави***
    - Хто такі хакери та які бувають їхні типи.
    - Мотиви та методи діяльності.
    - Відомі приклади атак хакерських груп.

24. ***Інформаційна культура сучасного студента***
    - Поняття інформаційної культури.
    - Вміння працювати з даними.
    - Відповідальність у соцмережах.

25. ***Кібербулінг як загроза особистій безпеці***
    - Визначення та форми кібербулінгу.
    - Наслідки для особистості.
    - Як захистити себе від кібербулінгу.

26. ***Досвід України у боротьбі з дезінформацією***
- Приклади інформаційних атак проти України.
- Інструменти протидії.
- Роль громадянського суспільства.

27. ***Баланс між інформаційною безпекою та особистою свободою***
- Свобода слова і право на інформацію.
- Обмеження заради безпеки.
- Приклади пошуку балансу.

28. ***Майбутні виклики інформаційної безпеки України***
- Тенденції розвитку інформаційних технологій.
- Нові загрози (штучний інтелект, кіберзброя).
- Шляхи розвитку системи захисту України.

Додаток 1.
Титульний аркуш реферату з дисципліни «Інформаційна безпека держави»

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

КАФЕДРА КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Інформаційна безпека держави

Тему реферату: «_____»

Робота виконана студентом групи _____
ПІБ
Викладач: проф. Кобозєва А.А.

Одеса, 2025