МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
КАФЕДРА ПРИКЛАДНОЇ МАТЕМАТКИ ТА ІНФОРМАТИКИ

15.03.2025

# *Безпека та захист операційних систем*

Електронне видання

Методичні вказівки до організації самостійної роботи студентів (СРС) для студентів всіх форм навчання освітнього ступеня «Бакалавр» за спеціальністю 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології

Дрогобич
ДВНЗ «ДонНТУ»
2025

УДК 004.451.056

Б 39

Безпека та захист операційних систем. Методичні вказівки до організації самостійної роботи студентів (СРС) для студентів всіх форм навчання освітнього ступеня «Бакалавр» за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 Інформаційні технології. [Електронне видання] / Уклад.: Я.Ю. Дорогий. – Дрогобич : ДВНЗ «ДонНТУ», 2025. – 37 с.

Методичні вказівки призначені для студентів всіх форм навчання освітнього ступеня «Бакалавр» за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 Інформаційні технології. В посібнику наведена тематика СРС, теоретичні відомості, завдання для виконання робіт, список літератури.

Укладач Ярослав ДОРОГИЙ, д.т.н., проф., в.о. зав. каф. ПМІ

Відповідальний редактор Ярослав ДОРОГИЙ, д.т.н., проф., в.о. зав. каф. ПМІ

Рецензент Василь ЦУРКАН, доцент, к. т. н., доцент спеціальної кафедри №5 ІСЗЗІ КПІ ім. Ігоря Сікорсь-кого

Затверджено навчально-методичним відділом ДонНТУ,

протокол № 5 від 28.03.2025 р.

Розглянуто на засіданні кафедри прикладної математики та інформатики

протокол № 3 від 18.03.2025 р.

ЗМІСТ

# ВСТУП

Розподіл годин на дисципліну (із загальних 180 годин на дисципліну, 32 виділяється на лабораторні роботи та 100 — на самостійну роботу студентів) визначає основне навантаження із засвоєння цієї дисципліни саме на самостійну роботу студентів.

Практична суть освіти полягає в тому, що завдання викладача є не стільки передача певних знань студенту, скільки вміння навчити студента, маючи деякий мінімальний обсяг інформації, методам збільшення цього обсягу як на практичних заняттях під керівництвом викладача, так і вдома, в бібліотеці тощо.

Лише постійне самостійне навчання дає можливість наблизитись до глибин знань певної галузі, оволодіти достатньою сумою знань і вмінь, які б дали змогу почувати себе професіоналом.

# 1 МЕТА ТА ЗАВДАННЯ ДИСЦИПЛІНИ

Навчальна дисципліна «Безпека та захист операційних систем» спрямована на забезпечення студентів необхідними знаннями та практичними навичками у галузі захисту інформації, що оброблюється операційними системами. Ця інформація включає в себе технічні та організаційні механізми захисту, що становлять невід'ємну частину операційних систем. Переважно, навчальна дисципліна відповідає нормативним вимогам освітньо-професійної програми.

Метою цієї навчальної дисципліни є формування у студентів навичок аналізування проблем і загроз безпеці програмного забезпечення, які виникають під час обробки інформації в інформаційно-комунікаційних системах. Також метою є надання студентам здатностей до обґрунтованого вибору засобів захисту для операційних систем відповідно до вимог національних та міжнародних стандартів. Ця дисципліна також спрямована на розвиток умінь налаштовувати засоби захисту в операційних системах та оцінювати рівень захищеності інформації відповідно до встановлених критеріїв.

Основні завдання лабораторних занять включають у себе ознайомлення студентів із сучасними засобами захисту інформації в операційних системах, а також надання їм навичок щодо їх застосування для вирішення практичних завдань з реалізації політик безпеки операційних систем. Також проводиться перевірка і моніторинг рівня захищеності інформації з використанням вітчизняних і міжнародних критеріїв оцінювання.

Компетентності, які досягаються при вивченні дисципліни:

ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

ЗК01. Здатність застосовувати знання у практичних ситуаціях.

ЗК02. Знання та розуміння предметної області та розуміння професії.

ЗК05. Здатність до пошуку, оброблення та аналізу інформації.

ЗК08. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

ФК01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та Міжнародні вимоги, практики і стандарти у професійній діяльності.

ФК04. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

ФК05. Здатність відновлювати функціонування інформаційних, інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

ФК10. Здатність виконувати моніторинг інформаційних, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Програмні результати навчання за дисципліною наступні:

ПРН01. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків.

ПРН02. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

ПРН03. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійний діяльності.

ПРН04. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН05. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійний діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН06. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН07. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

ПРН09. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

ПРН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

ПРН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

ПРН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з

використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

ПРН15. Збирати, обробляти зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводили аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

ПРН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

ПРН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.

ПРН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дії з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Основними результатами опанування дисципліни «Безпека та захист операційних систем» є вміння:

– забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

– забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах

– вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

– вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та/або кібербезпеки;

– реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

– вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

– забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;

– здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;

– вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

– забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

– забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах

В результаті вивчення дисципліни студенти повинні

ЗНАТИ:

– основи розроблення захищених операційних систем;

– стандарти оцінювання захищеності операційних систем;

– законодавство України, яке регулює дану галузь;

– міжнародні стандарти, зокрема ISO/IEC 15408.

ВМІТИ:

– застосовувати отримані навики самостійного вивчення навчальної та наукової літератури, володіти понятійним апаратом;

– конфігурувати та використовувати для розв’язання задач засоби захисту ОС Windows;

– конфігурувати та використовувати для розв’язання задач засоби захисту ОС Linux;

– конфігурувати та використовувати для розв’язання задач засоби захисту ОС Android;

– конфігурувати та використовувати для розв’язання задач засоби захисту ОС IOS.

# 2 ВИДИ СРС

СРС може здійснюватись за допомогою:

– запам’ятовування певної інформації через опрацювання лекцій;

– активної роботи під час практичних та лабораторних занять;

– роботи над конспектами лекцій, планами практичних занять;

– опрацювання літературних джерел (самостійного конспектування вивченого матеріалу, рефератування окремих тем);

– роботи з каталогами звичайних і електронних бібліотек, інформаційно-пошуковими сервісами Internet;

– вивчення навчального матеріалу за підручниками, навчальними посібниками, практикумами тощо;

– опрацювання окремих тем матеріалу за першоджерелами, науковою і спеціальною літературою;

– підготовки доповідей, рефератів, презентацій за темами курсу;

– самотестування.

*СРС під час лекції*. Належне ведення конспекту під час лекції сприяє більш уважному засвоєнню нового матеріалу, збереженню необхідної інформації та дає студенту змогу в подальшому проаналізувати її. За умови класичного подання лекційного матеріалу засвоюється приблизно 20 % інформації. При викладанні дисципліни «Безпека та захист операційних систем» за допомогою візуального відтворення деяких аспектів налаштування операційних систем на лекціях показник засвоювання зростає до 40%.

*Робота над конспектами лекцій, планами практичних занять*. При опрацюванні матеріалу лекції слід зіставити законспектований матеріал з планом практичного заняття, що міститься у методичних матеріалах для практичних занять. Якщо у конспекті відсутній матеріал з окремих питань лекції або недостатньо розкриті деякі питання практичного заняття, або винесені на самостійне опрацювання, студент повинен звернутися до рекомендованих підручників, навчальних посібників і відповідних

методичних матеріалів. Підготовку практичного заняття з дисципліни слід здійснювати з використанням ПК з встановленим на ньому програмним забезпеченням Virtual Box. Також потрібно активно використовувати довідкові мережі операційних систем Linux та Windows, за допомогою якої можна отримати відповіді стосовно використання різних команд, їх синтаксису і т.п.

*Робота з літературою*. Працювати з підручниками, навчальними посібниками, методичними вказівками, практикумами, науковою і спеціальною літературою незалежно від типу їх носія (паперового чи електронного) необхідно таким чином, щоб отримати максимум теоретичних знань і навичок. Для самостійного поглибленого вивчення навчального матеріалу студенту слід створити свій список літератури для опрацювання, джерела якого можуть і не бути зазначеними в якості основної чи додаткової літератури.

*Робота з Internet*. Сервіси мережі Internet надають унікальні можливості знаходження літературних джерел у географічно віддалених фондах та архівах, а також шляхом участі у мережевих конференціях, де можна отримати відповіді та поради щодо питань з розшукуваної інформації. Для пошуку інформації слід скористатись пошуковими системами.

Пошукові системи є складними інформаційно-довідковими системами, що автоматично генеруються на основі даних, які збираються мережевими програмами-роботами по всьому Internet, і дають у відповідь на запит користувача посилання на різні Internet-ресурси. Запит здійснюється за певною процедурою (певною мовою), яка може відрізнятися в різних системах, проте в спрощеному вигляді вона зводиться до введення в спеціальному полі певного виразу пошуку, що складається з ключових слів та деяких операторів мови запитів.

До загальних положень мов запитів належать:

− ключові слова можна вводити у відповідне поле пошукової системи поодинці, послідовно звужуючи пошук, або ж вводити відразу декілька слів, розділяючи їх пробілами або комами. Регістр не має значення.

− режим пошуку “AND” (“І”) означає, що будуть знайдені тільки ті дані, де зустрічається кожне з ключових слів.

− при використанні режиму “OR” (“АБО”) результатом пошуку будуть всі дані, де зустрічається хоча б одне ключове слово.

− використання знаків «+» і «-» перед ключовим словом. Щоб виключити документи, де зустрічається певне слово, поставте перед ним «-». І навпаки, щоб певне слово обов’язково було присутнє в документі, поставте перед ним «+». Зверніть увагу на те, що між знаком і словом не повинно бути пропуску. Наприклад: “+таблиці -Excell”.

− за замовчуванням програма шукає всі дані, в яких зустрічається введене слово. Наприклад, при запиті “редактор” будуть знайдені слова “редактор”, “текстовий”, “графічний”, “газети”, “головний” і багато інших. Знак оклику перед або після ключового слова означає, що будуть знайдені тільки слова точно відповідні запиту (наприклад, “текстовий! редактор!”).

Також корисно пам’ятати і використовувати при пошуку такі прийоми:

− якщо потрібно шукати словосполучення, вкладіть його в лапки;

− якщо запит вводиться малими літерами, будуть знайдені всі варіанти його написання; якщо при введенні вказана хоча б одна прописна літера, то система шукатиме тільки такий варіант;

− якщо потрібно знайти не текст, а зображення, то можна скористатися словом image. Наприклад, image: алгоритм дасть список сторінок із зображенням алгоритмів;

− якщо ключове слово, що шукається, зустрічається в різних контекстах, можна виключити слова з непотрібним контекстом. Наприклад, вказати аргумент пошуку +ОС +Налаштування +Linux++ -Windows.

− використання синонімів може збільшити кількість знайдених сторінок.

Велику популярність мають різні тематичні форуми, на яких користувач може поставити конкретне питання і отримати відповідь від інших членів форуму.

Самостійна робота має такі складові і форми її оцінювання:

− підготовка та аудиторна робота під час практичних і лабораторних занять, результати якої оцінюються під час поточного контролю;

− виконання самостійних робіт у формі підготовки усних доповідей у вигляді презентацій, рефератів та домашніх контрольних робіт;

− опрацювання програмного матеріалу зі змістового модуля та оцінка результатів під час проміжного контролю;

− виконання МКР або ДКР (за наявності відповідного навантаження за дисципліною).

# 3 ТЕМАТИКА СРС

## 3.1 Загальні відомості

Програма вивчення дисципліни «Безпека та захист операційних систем» складається з таких розділів: «Мета, задачі, зміст курсу. Основні визначення», «Модель загроз для операційної системи», «Розроблення захищених операційних систем», «Стандарти оцінювання захищеності операційних систем», «Нормативно-правове регулювання в Україні», «Стандарт ISO/IEC 15408», «Засоби захисту ОС Windows», «Засоби захисту ОС Linux», «Архітектура безпеки і механізми захисту Android», «Архітектура безпеки і механізми захисту IOS».

В якості самостійної роботи студентами пропонується:

- підготувати реферат за обраною темою;
- створити презентацію за обраною темою та підготувати доповідь.

## 3.2 Тематика СРС

Тема 1. Мета, задачі, зміст курсу. Основні визначення.

1. Основні поняття інформаційної безпеки. Визначення конфіденційності, цілісності та доступності (CIA-тріада). Основні загрози та ризики для безпеки операційних систем.

2. Еволюція засобів захисту операційних систем. Особливості безпеки ранніх ОС (UNIX, Windows NT). Порівняння рівнів безпеки сучасних операційних систем (Windows, Linux, macOS).

3. Правові та нормативні аспекти безпеки операційних систем. Міжнародні стандарти у сфері кібербезпеки (ISO/IEC 27001, NIST, CIS). Законодавча база України щодо захисту інформації.

4. Архітектура захисту операційних систем. Основні компоненти моделі безпеки ОС. Ролі та рівні доступу користувачів у сучасних ОС.

5. Методи автентифікації та ідентифікації користувачів. Типи автентифікації (паролі, біометрія, багатофакторна автентифікація). Моделі управління доступом (DAC, MAC, RBAC).

6. Сучасні виклики та тенденції в безпеці операційних систем. Вразливості та експлойти у сучасних ОС. Використання штучного інтелекту для атак та захисту.

*Питання для самоперевірки з теми*

1. Яке мета дисципліни? Які її основні завдання?
2. Які основні складові інформаційної безпеки та їх значення в операційних системах?
3. Як змінювалися методи захисту операційних систем від ранніх версій до сучасних?
4. Які міжнародні та національні стандарти регулюють питання безпеки операційних систем?
5. Які існують моделі управління доступом в операційних системах, і в чому їхні відмінності?
6. Які сучасні загрози існують для операційних систем, і які методи використовуються для їх нейтралізації?

Тема 2. Модель загроз для операційної системи.

1. Поняття загроз в операційній системі. Визначення загрози безпеці операційної системи. Класифікація загроз за джерелом, способом реалізації та наслідками.

2. Моделі загроз та їх класифікація. Основні моделі загроз (STRIDE, DREAD, CVSS). Відмінності між моделями та їх застосування для оцінки ризиків безпеки операційних систем.

3. Класифікація атак на операційні системи. Локальні та віддалені атаки. Атаки на рівні ядра, файлової системи, мережевого стека. Методи захисту від різних типів атак.

4. Програмні та апаратні вразливості операційних систем. Поняття уразливостей та їх вплив на безпеку ОС. Експлуатація уразливостей: переповнення буфера, ескалація привілеїв, атаки на пам’ять.

5. Методи моделювання загроз для операційних систем. Використання методологій моделювання загроз (Microsoft Threat Modeling Framework, OCTAVE, ATT&CK). Аналіз ризиків та побудова захисних стратегій.

6. Захист операційної системи від загроз. Вбудовані механізми захисту (контроль доступу, брандмауери, антивірусні системи). Принципи побудови захищених операційних середовищ.

*Питання для самоперевірки з теми*

1. Що таке загроза для операційної системи і які її основні характеристики?

2. Які основні моделі загроз використовуються для аналізу безпеки операційних систем?

3. Чим відрізняються локальні та віддалені атаки на операційну систему?

4. Які основні вразливості операційних систем використовують зловмисники?

5. Які методи моделювання загроз існують і як вони застосовуються на практиці?

6. Які механізми безпеки вбудовані в сучасні операційні системи для протидії загрозам?

7. Як проводиться аналіз ризиків для операційної системи та які методи дозволяють його здійснити?

Тема 3. Розроблення захищених операційних систем.

1. Основи побудови захищених операційних систем. Принципи безпеки операційних систем. Вимоги до безпеки ОС згідно з міжнародними стандартами (Common Criteria, ISO/IEC 15408).

2. Архітектура захищених операційних систем. Основні компоненти захищених ОС. Механізми безпечного керування пам’яттю, ядро з мінімальними привілеями (Microkernel vs. Monolithic Kernel).

3. Моделі безпеки для операційних систем. Дискреційна (DAC), мандатна (MAC) та ролева (RBAC) моделі контролю доступу. Їх особливості, переваги та недоліки.

4. Методи шифрування даних в операційних системах. Використання криптографічних алгоритмів для захисту даних. Повнодискове шифрування (BitLocker, LUKS). Захист файлів та мережевих комунікацій.

5. Розмежування доступу в захищених операційних системах. Політики безпеки та механізми автентифікації. Використання багатофакторної автентифікації.

*Питання для самоперевірки з теми*

1. Які основні принципи побудови захищених операційних систем?
2. Які вимоги до безпеки операційних систем визначають міжнародні стандарти (Common Criteria, ISO/IEC 15408)?
3. Які основні відмінності між монолітним ядром і мікроядром у контексті безпеки операційних систем?
4. Які моделі контролю доступу (DAC, MAC, RBAC) застосовуються в операційних системах, і які їх особливості?
5. Які криптографічні методи використовуються для захисту даних в операційних системах?
6. Які основні механізми автентифікації використовуються в захищених операційних системах?

Тема 4. Стандарти оцінювання захищеності операційних систем.

1. Основи оцінювання захищеності операційних систем. Основні підходи до оцінювання рівня безпеки ОС. Значення стандартизації в оцінюванні безпеки.

2. Міжнародні стандарти безпеки операційних систем. Огляд основних стандартів: Common Criteria (ISO/IEC 15408), ISO/IEC 27001, NIST 800-53. Їх застосування для оцінювання безпеки ОС.

3. Методологія Common Criteria (CC). Основні концепції та структура стандарту. Рівні довіри до безпеки (Evaluation Assurance Levels, EAL).

4. Критерії безпеки Trusted Computer System Evaluation Criteria (TCSEC). Основні рівні безпеки за TCSEC. Порівняння TCSEC та Common Criteria.

5. Модель європейських критеріїв безпеки ITSEC. Принципи та структура ITSEC. Відмінності від TCSEC та CC.

6. Стандарти оцінювання безпеки від NIST. Підхід NIST до оцінки безпеки операційних систем. Стандарт NIST 800-53 та його застосування.

7. Методи оцінювання безпеки комерційних операційних систем. Як проводиться сертифікація ОС (Windows, Linux, macOS) за міжнародними стандартами.

8. Актуальні виклики та перспективи розвитку стандартів оцінювання безпеки ОС. Сучасні тенденції у стандартизації безпеки. Недоліки існуючих методів оцінки та перспективи їх вдосконалення.

*Питання для самоперевірки з теми*

1. Яке значення має стандартизація в оцінюванні захищеності операційних систем?

2. Які міжнародні стандарти оцінювання безпеки операційних систем є найпоширенішими?

3. Яка структура та основні принципи методології Common Criteria (CC)?

4. Що таке рівні довіри до безпеки (Evaluation Assurance Levels, EAL) у Common Criteria?

5. Які основні рівні безпеки визначає Trusted Computer System Evaluation Criteria (TCSEC)?

6. Чим відрізняються європейські критерії безпеки ITSEC від TCSEC та Common Criteria?

7. Які рекомендації щодо оцінювання безпеки операційних систем містяться у NIST 800-53?

8. Як проводиться сертифікація операційних систем відповідно до міжнародних стандартів?

9. Які основні відмінності між підходами CC, TCSEC, ITSEC та NIST у сфері оцінювання захищеності ОС?

10. Які сучасні виклики існують у стандартизації оцінювання безпеки операційних систем?

Тема 5. Нормативно-правове регулювання в Україні.

1. Законодавча база України у сфері інформаційної безпеки. Основні нормативно-правові акти, що регулюють захист інформації та кібербезпеку.

2. Закон України «Про захист інформації в інформаційно-комунікаційних системах». Основні положення, принципи захисту інформації, вимоги до безпеки інформаційних систем.

3. Закон України «Про основні засади забезпечення кібербезпеки України». Визначення основних суб'єктів кібербезпеки, їх функції та повноваження.

4. Державна політика у сфері кібербезпеки. Стратегії розвитку кібербезпеки, державні органи, що відповідають за регулювання інформаційної безпеки (Держспецзв’язку, НБУ, СБУ).

5. Стандарти та нормативні документи України з безпеки інформації. ДСТУ ISO/IEC 27001, ДСТУ 3396.1-96, вимоги до сертифікації засобів захисту інформації.

6. Захист персональних даних в Україні. Закон України «Про захист персональних даних», вимоги до обробки, зберігання та передачі персональних даних.

7. Ліцензування діяльності у сфері криптографічного та технічного захисту інформації. Вимоги до ліцензування, порядок отримання ліцензії на діяльність у сфері захисту інформації.

8. Відповідальність за порушення законодавства у сфері інформаційної безпеки. Адміністративна та кримінальна відповідальність за порушення вимог щодо захисту інформації, кіберзлочини в Україні.

*Питання для самоперевірки з теми*

1. Які основні нормативно-правові акти регулюють інформаційну безпеку в Україні?

2. Які ключові положення містить Закон України «Про захист інформації в інформаційно-комунікаційних системах»?

3. Які органи державної влади відповідають за регулювання кібербезпеки в Україні?

4. Які основні завдання та принципи викладені в Законі України «Про основні засади забезпечення кібербезпеки України»?

5. Які державні стандарти України (ДСТУ) визначають вимоги до інформаційної безпеки?

6. Які вимоги до обробки та захисту персональних даних встановлені в Законі України «Про захист персональних даних»?

7. Який порядок ліцензування діяльності у сфері криптографічного та технічного захисту інформації?

8. Яка відповідальність передбачена за порушення законодавства у сфері захисту інформації?

9. Які міжнародні стандарти інформаційної безпеки імплементовані в Україні?

10. Які вимоги до сертифікації засобів захисту інформації встановлені в Україні?

Тема 6. Стандарт ISO/IEC 15408.

1. Загальна характеристика стандарту ISO/IEC 15408. Основні цілі та призначення стандарту. Його роль у забезпеченні інформаційної безпеки.

2. Структура та складові частини стандарту ISO/IEC 15408. Основні частини стандарту: концепції та модель безпеки, функціональні вимоги, критерії гарантій.

3. Концепція «Common Criteria» у ISO/IEC 15408. Основні принципи «Загальних критеріїв» оцінювання безпеки інформаційних технологій.

4. Функціональні вимоги до безпеки в ISO/IEC 15408. Класифікація функціональних вимог безпеки: контроль доступу, шифрування, аудит.

5. Рівні гарантії безпеки (Evaluation Assurance Levels, EAL). Визначення та характеристика рівнів довіри до безпеки (від EAL1 до EAL7).

6. Процес сертифікації безпеки згідно з ISO/IEC 15408. Вимоги до сертифікації продуктів та систем безпеки відповідно до міжнародних стандартів.

7. Застосування ISO/IEC 15408 у практиці оцінювання безпеки. Впровадження стандарту в державному та комерційному секторах.

8. Порівняння ISO/IEC 15408 з іншими стандартами безпеки. Відмінності від TCSEC, ITSEC, ISO/IEC 27001, їх взаємозв’язок.

*Питання для самоперевірки з теми*

1. Яке основне призначення стандарту ISO/IEC 15408 у сфері інформаційної безпеки?

2. Які основні частини входять до структури стандарту ISO/IEC 15408?

3. Що таке «Common Criteria» і яку роль вони відіграють у ISO/IEC 15408?

4. Які основні категорії функціональних вимог безпеки передбачені у стандарті ISO/IEC 15408?

5. Що таке рівні гарантії безпеки (Evaluation Assurance Levels, EAL) і як вони класифікуються?

6. Які ключові вимоги висуваються до сертифікації інформаційних систем згідно з ISO/IEC 15408?

7. Як застосовується стандарт ISO/IEC 15408 у державному та комерційному секторах?

8. Які основні відмінності між ISO/IEC 15408 та іншими стандартами безпеки, такими як TCSEC та ITSEC?

9. Які організації займаються сертифікацією безпеки згідно з ISO/IEC 15408?

10. Які переваги отримують компанії та державні установи від впровадження стандарту ISO/IEC 15408?

Тема 7. Засоби захисту ОС Windows.

1. Архітектура безпеки Windows. Основні компоненти системи безпеки Windows. Моделі безпеки, реалізовані в ОС Windows.

2. Механізми аутентифікації та контролю доступу. Локальні та доменні облікові записи. Політики паролів. Використання Windows Hello та багатофакторної аутентифікації (MFA).

3. Керування правами користувачів та контроль доступу. Механізми DAC, MAC, RBAC. Контроль доступу через групові політики (GPO).

4. Шифрування та захист даних. BitLocker та EFS (Encrypting File System). Захист даних на рівні файлової системи.

5. Брандмауер Windows та безпека мережевих з'єднань. Налаштування Windows Firewall. Використання IPsec для захисту трафіку.

6. Антивірусний захист у Windows. Функціональність Windows Defender. Виявлення та запобігання загрозам за допомогою Microsoft Defender Antivirus.

7. Моніторинг безпеки та реагування на загрози. Використання Windows Event Viewer для аналізу подій безпеки. Роль Windows Security Center.

8. Механізми ізоляції та захисту від експлойтів. Windows Sandbox, Controlled Folder Access, функція Application Guard.

9. Групові політики та безпека корпоративного середовища. Використання Active Directory (AD) та Group Policy Object (GPO) для забезпечення безпеки.

10. Оновлення та підтримка безпеки ОС Windows. Роль Windows Update у виправленні вразливостей. Політики оновлення та їхній вплив на безпеку.

*Питання для самоперевірки з теми*

1. Які основні компоненти системи безпеки реалізовані в ОС Windows?
2. Які механізми аутентифікації використовуються в Windows для захисту облікових записів?
3. Які моделі контролю доступу підтримуються в ОС Windows і як вони працюють?
4. Як працює BitLocker та Encrypting File System (EFS) для шифрування даних у Windows?
5. Які функції виконує Windows Firewall і як його можна налаштувати?
6. Яку роль відіграє Microsoft Defender Antivirus у забезпеченні безпеки Windows?
7. Як можна використовувати Windows Event Viewer для моніторингу подій безпеки?
8. Які механізми захисту від експлойтів передбачені в Windows, зокрема Windows Sandbox та Application Guard?
9. Як групові політики (GPO) та Active Directory допомагають у забезпеченні безпеки корпоративного середовища?
10. Яке значення має Windows Update у підтримці безпеки операційної системи?

Тема 8. Засоби захисту ОС Linux.

1. Архітектура безпеки ОС Linux. Основні принципи безпеки Linux. Рівні доступу та моделі безпеки.

2. Аутентифікація та управління обліковими записами. Системи аутентифікації PAM (Pluggable Authentication Modules). Керування обліковими записами та групами користувачів.

3. Моделі контролю доступу в Linux. Дискреційний контроль доступу (DAC). Мандатний контроль доступу (MAC). Рольовий контроль доступу (RBAC).

4. Файлова система та контроль доступу. Права доступу в файловій системі Linux (rwx-права, UID, GID). ACL (Access Control Lists) та атрибути файлів.

5. Шифрування даних та захист файлової системи. Використання LUKS (Linux Unified Key Setup) для шифрування дисків. Файлові системи з підтримкою шифрування (eCryptfs, Btrfs, ZFS).

6. Мережева безпека Linux. Конфігурація брандмауера iptables/nftables. Захист мережевих сервісів за допомогою TCP Wrappers та Fail2Ban.

7. Антивірусний та антишпигунський захист. Використання ClamAV, Rootkit Hunter (rkhunter), Chkrootkit для виявлення шкідливих програм.

8. Механізми підвищення безпеки ядра Linux. Використання SELinux (Security-Enhanced Linux) та AppArmor. Захист пам'яті (ASLR, NX-bit).

9. Логування та моніторинг безпеки. Використання системи логування journald та syslog. Інструменти моніторингу (Auditd, Tripwire, OSSEC).

10. Оновлення та підтримка безпеки Linux. Політики оновлення системи. Інструменти управління оновленнями (APT, YUM, DNF, Zypper).

*Питання для самоперевірки з теми*

1. Які основні принципи забезпечення безпеки в операційній системі Linux?

2. Яку роль відіграють PAM (Pluggable Authentication Modules) у системі аутентифікації Linux?

3. Які моделі контролю доступу підтримуються в Linux і чим вони відрізняються?

4. Як налаштовуються права доступу до файлів у Linux за допомогою rwx-прав та ACL?

5. Які методи шифрування даних використовуються в Linux (LUKS, eCryptfs, Btrfs, ZFS)?

6. Як можна налаштувати брандмауер в Linux за допомогою iptables або nftables?

7. Які антивірусні інструменти використовуються в Linux для виявлення шкідливого ПЗ?

8. Як працюють механізми підвищеної безпеки ядра Linux, такі як SELinux та AppArmor?

9. Які інструменти моніторингу та логування використовуються в Linux для аналізу безпеки?

10. Як здійснюється оновлення безпеки Linux та які пакети для цього використовуються (APT, YUM, DNF, Zypper)?

Тема 9. Архітектура безпеки і механізми захисту Android.

1. Загальні принципи безпеки Android. Особливості архітектури безпеки Android. Рівні захисту в системі.

2. Модель безпеки операційної системи Android. Ключові компоненти безпеки. Політика розмежування доступу між додатками.

3. Архітектура Android і її вплив на безпеку. Роль ядра Linux у безпеці Android. Захист ядра та процесів.

4. Механізми аутентифікації та управління обліковими записами. Використання паролів, PIN-кодів, біометричних методів. Google Smart Lock.

5. Механізми контролю доступу в Android. Модель дозволів (Permissions Model). SEAndroid (Security-Enhanced Android) та механізми SELinux.

6. Захист додатків та файлової системи. Пісочниця додатків (Application Sandbox). Безпечне зберігання даних (Scoped Storage, Encrypted File System).

7. Криптографічний захист в Android. Шифрування даних (Full Disk Encryption, File-Based Encryption). Захист API для роботи з криптографією.

8. Мережевий захист і безпека з’єднань. Використання VPN, DNS over HTTPS (DoH), захист Wi-Fi та мобільних мереж.

9. Механізми оновлення безпеки Android. Ролі Google Play Protect, Verified Boot, Android Security Patches у підтримці безпеки.

10. Основні загрози безпеці Android і методи їхньої нейтралізації. Шкідливе програмне забезпечення, фішинг, рутинг пристроїв та їхні ризики.

*Питання для самоперевірки з теми*

1. Які основні принципи безпеки реалізовані в операційній системі Android?

2. Як модель безпеки Android забезпечує ізоляцію додатків?

3. Яку роль відіграє ядро Linux у безпеці Android?

4. Які методи аутентифікації підтримуються в Android для захисту пристрою?

5. Як працює система дозволів (Permissions Model) у сучасних версіях Android?

6. Що таке SEAndroid і яку функцію виконує SELinux у контексті безпеки Android?

7. Які механізми шифрування даних використовуються в Android?

8. Як працює система пісочниці додатків (Application Sandbox) у Android?

9. Які механізми захисту використовуються для забезпечення безпеки мережевих з'єднань в Android?

10. Яку функцію виконує Google Play Protect у системі безпеки Android?

11. Як працює Verified Boot і яку роль відіграють оновлення безпеки в Android?

12. Які основні загрози безпеці Android існують і як можна з ними боротися?

Тема 10. Архітектура безпеки і механізми захисту iOS.

1. Загальні принципи безпеки iOS. Основи архітектури безпеки iOS. Відмінності iOS від інших мобільних ОС у контексті безпеки.

2. Модель безпеки операційної системи iOS. Політика розмежування доступу між додатками (App Sandbox). Контроль роботи процесів.

3. Ядро XNU та його роль у безпеці iOS. Захист пам'яті, цілісність ядра, механізми ізоляції.

4. Аутентифікація та управління доступом. Використання Touch ID, Face ID, паролів, двофакторної аутентифікації (2FA).

5. Система контролю доступу та дозволів. Механізм App Permissions. Контроль доступу до мікрофона, камери, геолокації.

6. Шифрування та збереження даних. File Data Protection, Keychain, апаратне шифрування Secure Enclave.

7. Мережева безпека iOS. Використання VPN, HTTPS, DNS-over-HTTPS, Wi-Fi Security.

8. App Store і безпека програмного забезпечення. Процес перевірки додатків (App Review). Захист від несанкціонованого встановлення додатків (Jailbreak Detection).

9. Оновлення безпеки та контроль цілісності системи. Механізм Secure Boot, оновлення iOS та патчі безпеки.

10. Основні загрози безпеці iOS та методи їхньої нейтралізації. Шкідливі програми, фішингові атаки, соціальна інженерія, експлойти.

*Питання для самоперевірки з теми*

1. Які основні принципи безпеки реалізовані в операційній системі iOS?
2. Як працює модель безпеки iOS та яку роль відіграє App Sandbox?
3. Яку функцію виконує ядро XNU у безпеці iOS?
4. Які методи аутентифікації підтримуються в iOS для захисту пристрою?
5. Як реалізована система дозволів для додатків у iOS?

6. Які механізми шифрування використовуються для захисту даних в iOS?

7. Що таке Secure Enclave і як він забезпечує безпеку в iOS?

8. Які механізми використовуються для забезпечення мережевої безпеки iOS?

9. Як App Store забезпечує безпеку програмного забезпечення для iOS?

10. Що таке Secure Boot і яку роль відіграє контроль цілісності системи в iOS?

11. Які основні загрози існують для iOS і як можна з ними боротися?

12. Чим iOS відрізняється від інших мобільних операційних систем у контексті безпеки?

### 3.3 Теми рефератів (доповідей)

1. Основні поняття інформаційної безпеки в операційних системах.
2. Роль конфіденційності, цілісності та доступності в захисті ОС.
3. Основні загрози безпеці операційних систем.
4. Еволюція методів захисту операційних систем.
5. Класифікація загроз операційним системам.
6. Моделі загроз у кібербезпеці: STRIDE, DREAD, CVSS.
7. Методи моделювання загроз для операційних систем.
8. Аналіз ризиків в ОС: сучасні підходи.
9. Архітектура захищених операційних систем.
10. Дискреційний, мандатний та ролевий контроль доступу в ОС.
11. Захищені операційні системи: Qubes OS, SELinux, Tails.
12. Використання криптографічного захисту в операційних системах.
13. Стандарт Common Criteria (ISO/IEC 15408) та його роль у безпеці ОС.
14. Порівняльний аналіз стандартів TCSEC, ITSEC та ISO/IEC 15408.

15. Впровадження стандартів безпеки в комерційні операційні системи.

16. Рівні гарантії безпеки (EAL) у стандартах оцінювання ОС.

17. Законодавча база України у сфері інформаційної безпеки.

18. Закон «Про основні засади забезпечення кібербезпеки України».

19. Стандарти безпеки інформаційних технологій в Україні.

20. Відповідальність за порушення вимог інформаційної безпеки.

21. Основні положення стандарту ISO/IEC 15408.

22. Функціональні вимоги безпеки в ISO/IEC 15408.

23. Процедура сертифікації за стандартом Common Criteria.

24. Порівняння ISO/IEC 15408 з іншими міжнародними стандартами безпеки.

25. Архітектура безпеки ОС Windows.

26. Антивірусні технології в Windows: Windows Defender та Microsoft Security Essentials.

27. Використання BitLocker для шифрування даних у Windows.

28. Налаштування Windows Firewall та мережевої безпеки.

29. Моделі контролю доступу в Linux: DAC, MAC, RBAC.

30. Використання SELinux та AppArmor для підвищення безпеки.

31. Інструменти моніторингу та аналізу загроз у Linux.

32. Захист файлової системи в Linux: LUKS, eCryptfs, Btrfs.

33. Основи архітектури безпеки Android.

34. Політика безпеки Google Play Protect.

35. Захист мобільних додатків у Android: модель дозволів та пісочниця додатків.

36. Використання шифрування в Android (Full Disk Encryption, File-Based Encryption).

37. Особливості безпеки iOS у порівнянні з Android.

38. Використання Secure Enclave у системі безпеки iOS.

39. Процес перевірки додатків в App Store як захист від шкідливого ПЗ.

40. Оновлення безпеки та механізм Secure Boot в iOS.

41. Порівняльний аналіз безпеки Windows, Linux та macOS.

42. Методи атаки на операційні системи та засоби їх виявлення.

43. Використання віртуалізації для підвищення безпеки операційних систем.

44. Роль штучного інтелекту у виявленні загроз для ОС.

45. Фішинг та соціальна інженерія як загрози для операційних систем.

46. Захист від експлойтів у сучасних операційних системах.

47. Використання Zero Trust Architecture (ZTA) у безпеці операційних систем.

48. Критичні вразливості операційних систем та методи їх усунення.

49. Роль відкритого коду у безпеці ОС: переваги та ризики.

# 4 ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ ТА ВИМОГИ ДО РОБОТИ

## 4.1 Вимоги до виконання самостійної роботи

При виконанні самостійної роботи необхідно дотримуватись таких вимог:

– теоретичні питання та умови задач вибираються студентом згідно відповідного варіанту та наводяться перед відповіддю та відповідним рішенням;

– розв’язок задач має супроводжуватись поясненням, при необхідності, формулами тощо.

– самостійна робота повинна бути оформлена в електронному вигляді та надіслана у відповідні встановлені строки;

– сторінки роботи повинні бути пронумеровані, а також мати поля для зауважень;

– в кінці самостійної роботи наводиться список використаної студентом літератури згідно встановлених вимог.

При неповному та неправильному (виконано правильно менше 60% завдань) виконанні самостійної роботи, недотриманні умов вибору варіанту і порушенні інших вимог самостійна робота не зараховується.

## 4.2 Вимоги до змісту самостійної роботи

Пояснювальна записка реферату (доповіді) повинна містити наступні розділи:

– титульний лист (див. Додаток 1);

– зміст;

– список використаної літератури.

## 4.3 Вимоги до оформлення самостійної роботи

Самостійна робота має бути набрана 14 кеглем, з полуторним інтервалом, на аркуші паперу формату А4, з полями таких розмірів:

– верхнє поле – 25 мм;

– нижнє поле: до тексту – 35 мм, до колонцифри – 25 мм;

– внутрішнє поле – 25 мм;

– зовнішнє поле – 25 мм.

Номери сторінок проставляють на нижньому полі аркуша посередині, починаючи з третьої, дотримуючись наскрізної нумерації без пропусків і буквених доповнень. Титульний аркуш включають до загальної нумерації сторінок. Номер сторінки на титульному аркуші не проставляють.

У текстовій частині:

– заголовки розміщуються посередині рядка та друкуються великими літерами без крапки в кінці, без підкреслення;

– заголовки підрозділів, пунктів і підпунктів тексту друкуються з великої літери (без підкреслення) без крапки в кінці;

– усі заголовки мають бути супідрядними і відповідати змісту роботи, абревіатури в заголовках не вживають, їх треба розшифровувати в тексті;

– заголовки з двох чи більше речень слід відокремлювати крапками;

– відстань між заголовком і текстом становить 28 пт, відстань між заголовками розділу та підрозділу – 14 пт;

– заголовок не розміщують внизу сторінки, якщо після нього уміщується лише один рядок тексту;

– таблиці та ілюстрації мають бути пронумерованими і міститися після посилань на них у тексті, примітки друкують під таблицею;

– у додатках розміщують офіційні, допоміжні і розрахункові матеріали, висновки, тощо, всі додатки нумеруються. Нумерація формул, таблиць і рисунків у кожному з додатків має бути самостійною.

# СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Бондаренко М.Ф. Операційні системи : навч. посіб. / М.Ф. Бондаренко, О.Г. Качко. – Харків : Компанія СМІТ, 2018. – 432 с.

2. Яковина В.С. Операційні системи. Конспект лекцій / В. С. Яковина. – Львів : Львівська політехніка, 2016. – 128 с.

3. Авраменко В. С. Основи операційних систем : навч. посіб. / В. С. Яковина, А. С. Авраменко. – Черкаси: ЧНУ ім. Богдана Хмельницького, 2018. – 524 с.

4. Глоба Л. С. Розробка інформаційних ресурсів та систем. Том 1: Розподілені системи [Електронний ресурс] / Л. С. Глоба. – Режим доступу: https://surl.gd/tdusfk. – Назва з екрана.

5. Глоба Л. С. Розробка інформаційних ресурсів та систем. Том 2: Розподілені системи [Електронний ресурс] / Л. С. Глоба. – Режим доступу: https://surl.gd/sjkbnp. – Назва з екрана.

6. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-002-99 [Електронний ресурс]. – Режим доступу: https://surl.li/icyapz. – Назва з екрана.

7. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-003-99 [Електронний ресурс]. – Режим доступу : https://surl.li/rwzikm. – Назва з екрана.

8. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99 [Електронний ресурс]. – Режим доступу : https://surl.li/vcoazs. – Назва з екрана.

9. Схемоконспект лекцій з навчальної дисципліни «Безпека та захист операційних систем» : ел. навч.-наоч. посіб. для студентів всіх форм навчання галузі знань 12 Інформаційні технології / уклад. Я.Ю. Дорогий. – Луцьк : ДонНТУ, 2024. – 896 с. – Назва з екрану. – Режим доступу: https://surl.li/srrrgm.

10. Методичні вказівки до виконання лабораторних занять з дисципліни «Безпека та захист операційних систем. Ч.І.» для студентів всіх

форм навчання спеціальностей 122 Комп’ютерні науки та 125 Кібербезпека [Електронне видання] / уклад. Я.Ю. Дорогий. – Луцьк : ДВНЗ «ДонНТУ», 2023. – 187 с. – Режим доступу : https://surl.li/fwbnvg. – Назва з екрана.

# ДОДАТОК 1 ПРИКЛАД ТИТУЛЬНОГО ЛИСТА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кафедра прикладної математики та інформатики

РЕФЕРАТ (ДОПОВІДЬ)

з дисципліни «БЕЗПЕКА ТА ЗАХИСТ ОПЕРАЦІЙНИХ СИСТЕМ»

Варіант №5

Виконав студент гр. ІПЗ-21

Водомір П.Ф.

Перевірив проф. каф. ПМІ

Дорогий Я.Ю.

Дрогобич, 2025

ДонНТУ

# ПРИМІТКИ