(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Факультет комп'ютерних наук та технологій
Кафедра технічного захисту інформації

ЗАТВЕРДЖУЮ
Декан ФКНТ
_____ Андрій ФЕСЕНКО
«___»_____ 2025 р.

КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ

РОБОЧА ПРОГРАМА
навчальної дисципліни
«Автоматизація обробки інформації з обмеженим доступом»

Освітньо професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»
Галузь знань: F «Інформаційні технології»
Спеціальність: F5 «Кібербезпека та захист інформації»

Форма здобуття освіти	Сем.	Усього (год. / кредитів ECTS)	ЛКЦ	ПР.З	Л.З	СРС	ДЗ / РГР / К.р	КР / КП	Форма сем. контролю
Денна	2	150/5	36	-	18	96	-	КР-2с	екзамен 2 с

Індекс: № НМ-4-F5-2/25-2.1.6,

КАІ РП 14.08–01–2025

Робочу програму навчальної дисципліни «Автоматизація обробки інформації з обмеженим доступом» розроблено на основі освітньо-професійних програм «Системи технічного захисту інформації, автоматизація її обробки», навчального плану № НМ-4-F5-2/25 та робочого навчального плану №РМ-4-F5-2/25, підготовки здобувачів вищої освіти освітнього ступеня «Магістр» за спеціальністю F5 «Кібербезпека та захист інформації» та відповідних нормативних документів.

Робочу програму розробив
Професор кафедри технічного захисту інформації,
к.т.н., доцент:_____ Валеріан ШВЕЦЬ

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки», спеціальності F5 «Кібербезпека та захист інформації» – кафедри технічного захисту інформації, протокол №11 від « 25 » серпня 2025 р.

Гарант освітньо-професійної програми
«Системи технічного захисту інформації,
автоматизація її обробки»_____ Сергій ЛАЗАРЕНКО

Завідувач кафедри _____ Валерій КОЗЛОВСЬКИЙ

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету комп'ютерних наук та технологій, протокол №10 від «01» вересня 2025 р.

Голова НМРР _____ Оксана ПОЛІЩУК

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контольний примірник

ЗМІСТ

ВСТУП

Робоча програма (РП) навчальної дисципліни «Автоматизація обробки інформації з обмеженим доступом» розроблена на основі «Методичних рекомендацій до розроблення і оформлення робочої програми навчальної дисципліни денної та заочної форм навчання», затверджених наказом ректора від 29.04.2021 № 249/од, та відповідних нормативних документів.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

1.1. Місце, мета, завдання навчальної дисципліни.

Дана навчальна дисципліна є теоретичною та практичною основою сукупності знань і вмінь, що формують профіль фахівця в галузі управління інформаційною безпекою.

Метою вивчення навчальної дисципліни є підготовка висококваліфіко- ваних фахівців, є освоєння методів автоматизації оброблення інформації з обмеженим доступом, становлення фахівців з питань ТЗІ.

Завданнями вивчення навчальної дисципліни є підготовка фахівців з таких питань:

— освоєння підходів до створення вбудованих засобів захисту сучасних операційних систем і програмних застосунків, виявлення причин їх уразливості на основі наявної статистики загроз з метою обґрунтування загальних вимог до механізмів захисту;

— оволодіння навичками побудови та проектування систем захисту інформації з обмеженим доступом та архітектурними принципами побудови систем захисту інформації.

У результаті вивчення цієї навчальної дисципліни студент повинен:

Знати

— принципи побудови моделей керування доступом і механізми реалізації мандатної і дискреційної моделей доступу, моделей доступу механізмами вбудованої і додаткової захисту;

— принципи побудови системи автоматизованої обробки інформації з обмеженим доступом і її архітектури; функціональну модель системи захисту;

— принципи оцінки захищеності автоматизованої системи обробки інформації з обмеженим доступом;

— принципи розмежування доступу в системах електронного документообігу інформації з обмеженим доступом;

— формалізовані вимоги до захисту конфіденційної і таємної ітрормації та їх класифікації;

— вбудовані механізми захисту операційних систем і їх недоліки; механізми контролю цілісності;

— методи резервування вбудованих в операційні системи механізмів захисту;

— поняття додаткового захисту інформації та способи комплексування механізмів захисту;

— задачі та методи додаткових механізмів у межах посилення парольного захисту;

Завданнями вивчення навчальної дисципліни є підготовка фахівців з таких питань:

— освоєння підходів до створення вбудованих засобів захисту сучас- них операційних систем і програмних застосунків, виявлення причин їх ураз- ливості на основі наявної статистики загроз з метою обґрунтування загальних вимог до механізмів захисту;

— оволодіння навичками побудови та проектування систем захисту ін- формації з обмеженим доступом та архітектурними принципами побудови систем захисту інформації.

1.2. Результати навчання, які дає можливість досягти навчальна дисципліна.

За результатами вивчення навчальної дисципліни «Автоматизація обробки інформації з обмеженим доступом» студенти набувають таких знань та вмінь:

ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а та- кож виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

ПРН11. Аналізувати, контролювати та забезпечувати ефективне функці- онування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес операційних процесів у сфері інформаційної та або кібербезпеки в цілому.

ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої до- ступної інформації.

Трудові функції:

А. Здатність аналізувати статистику загроз для операційних систем сімейств Windows і Unix.

Б. Здатність здійснювати оцінку надійності систем захисту інформації (поняття відмови, часу відновлення тощо).

В. Здатність проектувати системи захисту інформації з обмеженим доступом, а також у складі локальних обчислювальних мереж.

Г. Здатність застосовувати засоби апаратного захисту.

Е. Здатність контролювати коректність функціонування механізмів захисту з використанням методів контролю цілісності.

1.3. Компетентності, які дає можливість здобути навчальна дисципліна.

У результаті вивчення даної навчальної дисципліни студенти повинні набути такі **компетентності**:

Інтегральну

1К1. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

Фахові

ФК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

ФК4. Здатність аналізувати, розробляти і супроводжувати систему уп- равління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

1.4. Міждисциплінарні зв'язки.

Дана дисципліна базується на знаннях таких дисциплін, як: : «Методи побудови та аналізу криптосистем», «Методологія прикладних досліджень у сфері кбербезпеки», «Моделювання та оптимізація безпекових процесів авіаційної галузі», та є базою для вивчення таких дисциплін, як: «Науково-дослідна практика у сфері систем технічного захисту інформації, автоматизації її обробки», «Переддипломна практика», «Кваліфікаційна робота» та інших.

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Зміст навчальної дисципліни

Навчальний матеріал дисципліни структурований за модульним принципом і складається з двох навчальних модулів, а саме:

— **навчального** модуля №1 «Сучасні підходи, вимоги, особливості систем автоматизації обробки інформації з обмеженим доступом і принципи побудови архітекту ри систем захисту інформації»;

— навчального **модуля №2 «Методи ідентифікації та автентифікації користувача та керування доступом до ресурсів»,** з яких є логічно завершеною, відносно самостійною, цілісною частиною навчальної дисципліни, засвоєння якої передбачає проведення модульної контрольної роботи та аналіз результатів її виконання.

Окремим **№3 модулем** (освітнім компонентом) є курсова робота **(КР),** який виконується у 2 семестрі. **КР** є важливою складовою закріплення та поглиблення теоретичних та практичних знань та вмінь, набутих студентом у процесі засвоєння навчального матеріалу дисципліни

2.2. Модульне структурування та інтегровані вимоги до кожного модуля

Модуль №1 «Сучасні підходи, вимоги, особливості систем автоматизації обробки інформації з обмеженим досту пом і принципи побудови архітектури систем захисту інформації».

Інтегровані вимоги модуля №1:

Знати:

— принципи формування архітектури системи захисту інформації організації (підприємства);

— основи основних механізми захисту ОС підприємства (підрозділу підприємства) з урахуванням питань захисту інформації з обмеженим доступом:

— основні організаційні засоби забезпечення проектування системи захисту

Вміти:

— вирішувати питання щодо здійснення процесу оцінки надійності систем захисту інформації з урахуванням проблем інформаційної безпеки;

— формулювати цілі, забезпечувати та контролювати впровадження розроблених заходів управління;

— зробити класифікація об'єктів загроз для досягнення цілей організації (підприємства);

провести аналіз ефективності централізовано-розподіленої системи захисту;

Тема 1. Класифікація інформації з обмеженим доступом

Розглядаються основні категорії інформації з обмеженим доступом: державна, службова, комерційна та конфіденційна. Вивчаються принципи класифікації інформації, правові норми та нормативно-правові акти, що регламентують її захист. Окреслюється роль політик безпеки в підтриманні конфіденційності даних.

Тема 2. Вимоги до захисту інформації різних типів

Описуються вимоги до забезпечення безпеки для різних видів інформації: державної таємниці, службової, конфіденційної. Розглядаються критерії оцінки рівнів захисту, а також практичні підходи до реалізації політик безпеки відповідно до класифікації інформації.

Тема 3. Механізми захисту операційних систем

Тема присвячена розгляду основних механізмів безпеки операційних систем: аутентифікації, авторизації, аудиту, шифрування даних і контролю доступу. Аналізується роль політики безпеки користувачів та моделі розмежування доступу.

Тема 4. Відповідність формалізованим вимогам безпеки

Розглядаються міжнародні стандарти інформаційної безпеки, такі як ISO/IEC 27001, Common Criteria, Orange Book. Порівнюються підходи до сертифікації ОС, аналізуються відмінності між Windows, Linux і macOS щодо виконання формалізованих вимог.

Тема 5. Статистика загроз для сучасних ОС

Висвітлюються сучасні тенденції у сфері кіберзагроз для операційних систем. Розглядаються основні типи атак — вірусні, мережеві, експлойти та атаки соціальної інженерії. Наводяться статистичні дані та узагальнення щодо найпоширеніших вразливостей.

Тема 6. Надійність і відмовостійкість систем захисту

Визначаються ключові показники надійності та відмовостійкості систем захисту інформації. Розглядаються поняття часу відновлення, коефіцієнта готовності, а також методи резервування системних механізмів безпеки для підвищення стабільності роботи ОС.

Тема 7. Комплексування механізмів захисту

Вивчаються підходи до поєднання вбудованих і додаткових засобів безпеки з метою підвищення ефективності захисту. Аналізується вплив комплексування на продуктивність і стійкість системи до атак. Розглядаються методи оцінки ефективності захисту.

Тема 8. Архітектурні принципи системи захисту інформації

Описується системний підхід до проектування архітектури захисту в межах локальних обчислювальних мереж. Розглядаються функціональні блоки системи, класифікація об'єктів загроз, принципи побудови функціональної моделі та взаємодії її компонентів.

Тема 9. Централізовано-розподілені системи захисту

Висвітлюються принципи побудови мережевих систем захисту інформації з централізовано-розподіленою архітектурою. Пояснюється структура підсистем, модулів і методів оцінки ефективності таких систем. Наводяться критерії оптимізації безпеки в складних мережах.

Модуль №2 «Методи ідентифікації та автентифікації користувача га керування доступом до ресурсів».

Інтегровані вимоги модуля №3:

Знати:

— основи авторизації, управління доступу к ресурсам персоналом підприємства (підрозділу підприємства) з урахуванням питань захисту інформації з обмеженим доступом;

— основи створення загальні правила призначення міток безпеки ієрархічним об'єктам доступу в організації (на підприємстві) та їх підрозділах.

Вміти:

— вирішувати питання щодо класифікації механізмів авторизації, реалізованих у сучасних системах захисту з урахуванням проблем інформаційної безпеки;

— визначенити задачі, що вирішуються механізмами управління доступом до ресурсів для досягнення цілей організації (підприємства);

— провести управління доступом до пристроїв;

— забезпечувати контроль коректності функціонування системи захисту з інтересами організації (підприємства);

— створювати реалізацію програмно-апаратного контролю (моніторингу) активності системи захисту .

Тема 1. Авторизація. Методи ідентифікації.

Поняття ідентифікації і автентифікації. Вимоги до ідентифікації і автентифікації. Авторизація в контексті кількості і виду зареєстрованих користувачів. Класифікація завдань, що вирішуються механізмами ідентифікації і автентифікації. Можливі класифікації механізмів авторизації, реалізованих у сучасних системах захисту. Механізми та способи посилення парольного захисту. Загрози подолання парольного захисту. Основні механізми введення пароля. Перевага біометричних систем контролю доступу. Основні способи посилення парольного захисту, які використовують у сучасних ОС і застосуйках.

Тема 2. Управління доступом до ресурсів.

Дискреційна модель управління доступом. Мандатна модель управління доступом. Додаткові вимоги до захисту секретної інформації в контексті використання дискреційної та мандатної моделей управління доступом. Визначення і класифікація задач, іцо вирішуються механізмами управління доступом до ресурсів. Коректність і повнота реалізації розмежувальної політики доступу Класифікація суб'єктів і об'єктів доступу. Протидія загрозам сучасними ОС. Практичний аналіз сучасних ОС в контексті прийнятої класифікації загроз подолання розмежувальної політики доступу.

Тема 3, Моделі управління доступом.

Канонічна модель управління доступом. Умова коректності механізму управління доступом. Поняття і класифікація каналів взаємодії суб'єктів доступу. Модель управління доступом при взаємодії суб'єктів доступу за допомогою виділених (віртуальних) каналів.

Тема 4. Реалізація моделей доступу механізмами додаткового та вбудованого захисту. Механізми реалізації дискреційної та мандатної моделей управління доступом. Категоризація прав доступу. Загальні правила призначення міток безпеки ієрархічним об'єктам доступу. Правила

розмежування доступу для різних моделей управління доступом до ієрархічних об'єктів. Обґрунтування коректності механізму мандатного управління доступом до ієрархічних об'єктів. Налаштування мандатного механізму доступу до ієрархічних об'єктів. Аналіз можливості коректної реалізації моделей управління доступом вбудованими в ОС механізмами захисту. Управління доступом до пристроїв і відчужуваних накопичувачів.

Тема 5. Контроль коректності функціонування механізмів захисту. Методи контролю цілісності.

Метод пошарового (рівнів) контролю списків санкціонованих подій. Основи методу рівнів контролю списків санкціонованих подій. Контроль за діями користувачів. Контроль коректності функціонування системи захисту.

Тема 6. Рівневе управління контролем санкціонованих подій та аудит у реальному часі

Загальні принципи побудови та функціонування механізму рівнів контролю списків санкціонованих подій. Контроль рівнів списків як механізм реального часу. Оцінка можливості застосування в сучасних системах механізму рівнів контролю в реальному режимі часу. Дворівнева модель аудиту на базі механізму контролю рівнів списків санкціонованих подій. Розроблення та оптимізація механізмів контролю рівнів як механізму реального часу.

Тема 7 Механізми контролю цілісності файлових об'єктів.

Задачі га проблеми реалізації механізмів контролю цілісності. Асинхронний запуск процедури контролю цілісності і його реалізація. Проблема контролю цілісності контролюючої програми

Тема 8. Застосування засобів апаратного захисту.

Технологія програмно-апаратного захисту. Реалізація програмно-апаратного контролю (моніторингу) активності системи захисту. Метод контролю цілісності і активності програмних компонент системи захисту програмно-апаратними засобами. Механізм мережевого моніторингу активності системи захисту як альтернатива застосуванню апаратної компоненті захисту.

Тема 9. Додатковий захист від несанкціонованого доступу.

Антивірусний захист. Загальноприйнятий підхід до анти вірус ного захисту і його недоліки. Використання розширених можливостей механізмів управління доступом до ресурсів у вирішенні завдань антивірусної протидії. Межмережеве екранування. Міжмережевий екран і його призначення. Атаки на міжмережеві екрани. Використання розширених можливостей механізмів управління доступом до ресурсів у вирішенні завдань міжмережевого екранування.

Модуль №3 «Курсова робота»

Курсова робота виконується у другому семестрі, відповідно до затверджених в установленому порядку методичних рекомендацій.

Конкретною метою курсової роботи є системний підхід до проектування системи захисту комп'ютерної інформації від несанкціонованого **доступу.**

Завдання різні за варіантами.

Курсова робота дається для закріплення та розширення теоретичних знань та вмінь та є важливим етапом засвоєння навчальних матеріалів, що дається у 2-му семестрі

2.3. Тематичний план.

№ з/п	Назва теми	Обсяг навчальних занять (год.)			
		Денна форма здобуття освіти			
		Усього	Лекції	Лабор. заняття	СРС
Модуль №1 «Сучасні підходи, вимоги, особливості систем автоматизації обробки інформації з обмеженим доступом і принципи побудови архітектури систем захисту інформації»					
		2 семестр			
1.1	Тема 1. Класифікація інформації з обмеженим доступом	7	2	2	3
1.2	Тема 2. Вимоги до захисту інформації різних типів	5	2	-	3
1.3	Тема 3. Механізми захисту операційних систем	7	2	2	3
1.4	Тема 4. Відповідність формалізованим вимогам безпеки	5	2	-	3
1.5	Тема 5. Статистика загроз для сучасних ОС	8	2	2	4
1.6	Тема 6. Надійність і відмовостійкість систем захисту	5	2	-	3
1.7	Тема 7. Комплексування механізмів захисту	6	2	-	4
1.8	Тема 8. Архітектурні принципи системи захисту інформації	7	2	2	3
1.9	Тема 9. Централізовано-розподілені системи захисту	6	2	-	4
1.10	Модульна контрольна робота №1	4	-	1	3
	Усього за модулем №1	**60**	**18**	**9**	**33**
Модуль №2 «Методи ідентифікації та автентифікації користувача та керування доступом до ресурсів».					
2.1	Тема 1. Авторизація. Методи ідентифікації	5	2	-	3
2.2	Тема 2. Управління доступом до ресурсів	5	2	-	3
2.3	Тема 3. Моделі управління доступом	7	2	2	3
2.4	Тема 4. Реалізація моделей доступу механізмами додаткового та вбудованого захисту	5	2	-	3
2.5	Тема 5. Контроль коректності функціонування механізмів захисту. Методи контролю цілісності.	8	2	2	4
2.6	Тема 6. Рівневе управління контролем санкціонованих подій та аудит у реальному часі	5	2	-	3
2.7	Тема 7 Механізми контролю цілісності файлових об'єктів	8	2	2	4
2.8	Тема 8. Застосування засобів апаратного захисту	5	2	-	3
2.9	Тема 9. Додатковий захист від несанкціонованого доступу	8	2	2	4
2.9	Контрольна робота (домашня) (ЗФН)	-	-	-	-
2.11	Модульна контрольна робота №2	4	-	1	3
	Усього за модулем №2	**60**	**18**	**9**	**33**
Модуль 3 “Курсова робота”					

3.1	Проектування системи захисту комп'ютерної інформації від несанкціонованого доступу	30	-	-	30
	Усього за модулем №3	30	-	-	30
	Усього за навчальною дисципліною	**150**	**36**	**18**	**96**

2.4. Перелік питань для підготовки до екзамену.

Перелік питань та зміст завдань для підготовки до екзамену розробляються провідним викладачем кафедри відповідно до робочої програми, затверджується на засіданні кафедри та доноситься до відома студентів.

3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

3.1. Методи навчання

При вивченні навчальної дисципліни «Автоматизація обробки інформації з обмеженим доступом» використовуються навчальні технології, що застосовуються для активізації навчально-пізнавальної діяльності студентів, а саме: робота в малих групах, семінар-дискусія, мозкова атака, кейс, презентація, рольова гра, дидактична гра тощо.

Використання технології *дистанційного навчання* реалізуються за допомогою комп'ютерної техніки, шляхом проведення занять з використанням чат-технологій, дистанційних занять, конференцій, семінарів, ділових ігор, лабораторних робіт, практикумів й Інших форм навчальних занять, які проводяться за допомогою засобів телекомунікацій з використанням веб- технологій.

Також, використовується *проблемно-орієнтоване навчання* (яке передбачає формулювання та вирішення проблеми під час лекцій, розв'язання ситуативних задач на семінарах, практичних заняттях, дослідження проблеми під час самостійної роботи студентів) та *практико-орієнтоване навчання*

3.2. Рекомендована література

Базова література

3.2.1. 3.2.1. Закон України «Про інформацію».

3.2.2. Закон України «Про державну таємницю».

3.2.3. Закон України «Про захист інформації в інформаційно- комунікаційних системах».

3.2.4. Закон України «Про захист персональних даних».

3.2.5. Закон України «Про основні засади забезпечення кібербезгіеки України».

3.2.6. Положення «Про технічний захист інформації» (із змінами), затверджене Указом Президента України від 27.09.1999 № 1229/99.

3.2.7. ДСТУ 3396.0-96. «Захист інформації. Технічний захист інформації. Основні положення».

3.2.8. ДСТУ 3396.1-96. «Захист інформації. Технічний захист інформації. Порядок проведення робіт».

3.2.9. НД ТЗІ 3.7-003-05. «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

3.2.10. НД ТЗІ 1.1-005-07. Захист Інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

3.2.11. НД ТЗІ НД ТЗІ 2.5-008-2002 .Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

3.2.12. Хорошко В. О. Основи інформаційної безпеки : навчальний посібник/ Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є./ - Вінниця : ВНТУ, 2018.-316с.

3.2.13. Браіловський **М.М.** Технології захисту інформації: підручник / Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.С./

- К.: ЦК "Компринт", 2021. - 296 с.

3.2.14. Богуш В.М. Технічний захист інформації: навчальний посібник/ Богуш В.М., Бровко В.Д., Коус О.В., Козюра В.Д./ - Дніпро.: "Ліра-К", 2022.

- 508с.

Допоміжна література

3.2.15. НД ТЗІ 2.6-001-11. «Порядок проведення робіт з державної пертизи засобів ТЗІ від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-комунікаційних системах».

3.2.16. Наказ Адміністрації Держспецзв'язку від 02.12.2014 No 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів В інформаційних, телекомунікаційних та інформаційно- телекомунікаційних системах», зареєстрований в Міністерстві юстиції Укра- їни 28.01.2015 за No 90/26535.

3.3. Інформаційні ресурси в інтернеті

3.3.1.http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article;jsessionid-BA075F688F4E729D7C88A20E1C636EA4?art id=40393&cat_id=38835.

3.3.2.http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40396&cat_id=38835.

3.3.3. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&catid=38835.

3.3.4. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40381&catid=38835.

3.3.5. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id= 40374&catid=38835.

3.3.6. http://tzi.com.ua/rubzh-rso-versya-20.html.

3.3.7. http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art id=46074.

4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ

Оцінювання окремих видів виконаної студентом навчальної роботи здійснюється в балах відповідно до табл.4.1.

Таблиця 4.1

Вид навчальної роботи	**Максимальна кількість балів**
	Денна форма здобуття освіти
2 семестр	
Модуль № 1 «Сучасні підходи, вимоги, особливості систем автоматизації обробки інформації з обмеженим доступом і принципи побудови архітектури сист ем захисту інформації»	
Виконання та захист лабораторних робіт	20
Для допуску до виконання модульної контрольної роботи №1 студент має набрати не менше	12
Виконання модульної контрольної роботи № 1	15
Усього за модулем № 1	35

Модуль № 2 «Методи ідентифікації та автентифікації користувача та доступом до ресурсів»	
Виконання та захист лабораторних робіт	35
Контрольна (домашня)робота	-
Для допуску до виконання модульної контрольної роботи №2 студент має набрати не менше	21
Виконання модульної контрольної роботи № 2	10
Виконання підсумкової модульної контрольної роботи	-
Усього за модулем № 2	**45**
Екзамен	**20**
Усього за за модулями №1, №2	**100**
Усього за дисципліною	**100**
Модуль № 3 «Курсова робота»	
Виконання курсової роботи	**60**
Захист курсової роботи	**40**
Виконання та захист курсової роботи	**100**
Усього за дисципліною	**100**

4.2. Виконані види навчальної роботи зараховуються студенту, якщо він отримав за них позитивну рейтингову оцінку (табл. 4.2).

4.3. Сума рейтингових оцінок, отриманих студентом за окремі види виконаної навчальної роботи, становить поточну модульну рейтингову оцінку, яка заноситься до відомості модульного контролю.

4.4. Сума підсумкової семестрової модульної та **екзаменаційної** рейтингових оцінок, у балах становить підсумкову семестрову рейтингову оцінку, яка перераховується в оцінки за національною шкалою та шкалою ECTS (табл. 4.3)

4.5. Підсумкова семестрова рейтингова оцінка в балах, за національною шкалою та шкалою ECTS заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента, наприклад, так: ***92/Відм./A, 87/Добре/B, 79/Добре/C, 68/Задов./D, 65/Задов./E*** тощо.

4.6. Підсумкова рейтингова оцінка з дисципліни дорівнює підсумковій семестровій рейтинговій оцінці. Зазначена підсумкова рейтингова оцінка з дисципліни заноситься до Додатку до диплома.

Таблиця 4.2

Відповідність рейтингових оцінок за окремі види навчальної роботи в балах оцінкам за національною шкалою

Рейтингова оцінка в балах					**Оцінка за національною шкалою**
Виконання та захист лабораторних робіт		**Екзамен**	**Виконання модульної роботи**		
32-35	18-20	18-20	14-15	18-20	Відмінно
27-31	15-17	15-17	12-13	15-17	Добре
21-26	12-14	12-14	9-11	12-14	Задовільно
менше 21	Менше 12	Менше 12	менше 9	Менше 12	Незадовільно

Таблиця 4.3

Відповідність підсумкової семестрової рейтингової оцінки в балах оцінці за національною шкалою та шкалою ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
90-100	**Відмінно**	**A**	**Відмінно** (відмінне виконання лише з незначною кількістю помилок)
82 – 89	**Добре**	**B**	**Дуже добре** (вище середнього рівня з кількома помилками)
75 – 81		**C**	**Добре** (в загальному вірне виконання з певною кількістю суттєвих помилок)
67 – 74	**Задовільно**	**D**	**Задовільно** (непогано, але зі значною кількістю недоліків)
60 – 66		**E**	**Достатньо** (виконання задовольняє мінімальним критеріям)
35 – 59	**Незадовільно**	**FX**	**Незадовільно** (з можливістю повторного складання)
1 – 34		**F**	**Незадовільно** (з обов'язковим повторним курсом)

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1	03.02	02.09.25	Федоренко К.П.		

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				