(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки та програмної інженерії
Кафедра засобів захисту інформації

УЗГОДЖЕНО
Декан
_____ Олександр Пономарено
«04» 04 2024 р.

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
_____ Анатолій Полухін
«04» 04 2024 р.

Система менеджменту якості

РОБОЧА ПРОГРАМА

навчальної дисципліни
«Автоматизація обробки інформації з обмеженим доступом»

Освітньо-професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека»

Форма навчання	Сем.	Усього (годин/кредитів ECTS)	ЛКЦ	ПР.З	Л.З	СРС	ДЗ/ РГР/ К.р	КР/ КП	Форма сем. контролю
Денна	2	210/7,0	36	–	36	138	–	КР – 2 с.	Диф.залік – 2 с.
Заочна	1,2	210/7,0	12	–	12	186	К.р.– 2 с.	КР – 2 с.	Диф.залік – 2 с.

Індекс: РМ-4-125-2/22 - 2.1.6
Індекс: НМ-4-125-2з/21 - 2.1.6

СМЯ НАУ РП 18.03-01-2024

Робочу програму навчальної дисципліни «Автомитазації обробки інформації з обмеженним доступом» розроблено на основі освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки», професійних стандартів, навчальних та робочих навчальних планів № НМ(РМ)-4-125-2/22 , № НМ(РМ)-4-125-2з/21 , підготовки здобувачів вищої освіти освітнього ступеня «Магістр» за спеціальністю 125 «Кібербезпека» та відповідних нормативних документів.

Робочу програму розробив:

Доцент кафедри засобів захисту інформації_____ Тетяна Щербак

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки», спеціальності 125 «Кібербезпека» – кафедри засобів захисту інформації (випускова), протокол № 4 від «12» 01 2024 р.

Гарант освітньо-професійної програми _____ Сергій Лазаренко

Завідувач кафедри _____ Валерій Козловський

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради Факультету кібербезпеки та програмної інженерії, протокол № 3 від «19» березня 2024 р.

Голова НМРР _____ Олекснадр Пономаренко

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний 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 висококваліфікованих 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 інформації 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 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.

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:

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 також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування 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 доступної інформації.

ПРН24. Визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки.

ПРН25. Організовувати внутрішньо-об'єктовий та пропускний режими на підприємстві.

ПРН26. Здійснювати оцінювання захищеності інформації, що циркулює на об'єкті інформаційної діяльності.

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

ІК1. 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 управління 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.

ФК11. Здатність проводити ліцензування, атестацію та сертифікацію об'єктів інформаційної діяльності.

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 архітектури 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 доступом 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. Вимоги до захисту комп'ютерної інформації.

Вимоги до захисту інформації з обмеженим доступом і їх класифікація, у томі числі вимоги до захисту конфіденційної, службової інформації, державної таємниці. Аналіз стану захищеності операційних систем. Системний підхід до проектування системи захисту комп'ютерної інформації від несанкціонованого доступу. Архітектура системи захисту інформації.

Тема 2. Аналіз стану захищеності операційних систем.

Основні механізми захисту ОС. Аналіз виконання сучасними ОС формалізованих вимог до захисту інформації від несанкціонованого доступу. Принципові відмінності в підходах щодо забезпечення захисту. Відмінності концепцій. Основні вбудовані механізми захисту ОС і їх недоліки. Аналіз статистики загроз для сучасних ОС. Додаткові вимоги до захисту комп'ютерної інформації. Сімейства ОС і загальна статистика загроз. Огляд і статистика методів, що є в основі атак на сучасні ОС.

Тема 3. Підходи до проектування системи захисту. Підходи до проектування системи захисту. Оцінка надійності систем захисту інформації. Відмовостійкість системи захисту. Поняття відмови. Час відновлення системи захисту. Коефіцієнт готовності. Вимоги до системи захисту інформації з урахуванням відмовостійкості. Завдання і методи резервування вбудованих в ОС механізмів захисту для підвищення відмовостійкості системи захисту. Поняття додаткового захисту інформації, способи комплексування механізмів захисту. Поняття вбудованого та додаткового захисту. Загальний підхід до оцінки ефективності системи додаткового захисту. Способи задання вихідних параметрів для оцінки захищеності. Особливості проектування системи захисту на основі оцінки захищеності системи. Методи проектування системи захисту з надлишковими механізмами захисту.

Тема 4. Принципи побудови архітектури системи захисту інформації. Особливості системного підходу до проектування системи захисту комп'ютерної інформації в складі локальних обчислювальних мереж. Архітекту-

ра системи захисту. Класифікація об'єктів загроз. Функціональна модель системи захисту. Склад і призначення функціональних блоків. Основні групи механізмів захисту. Загальні рекомендації за окремими рівнями функціональної моделі. Особливості архітектури мережевої системи захисту. Архітектура мережевої системи захисту. Централізовано-розподілена архітектура системи захисту. Аналіз ефективності централізовано-розподіленої системи захисту. Кількісна оцінка показників ефективності централізовано-розподілених систем захисту і пошук оптимального рішення. Функціональні підсистеми та модулі центрально-розподіленої системи захисту.

Модуль №2 «Методи ідентифікації та автентифікації користувача та 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 застосунках.

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, що 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. 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 6 Механізми контролю цілісності файлових об'єктів. Задачі та проблеми реалізації механізмів контролю цілісності. Асинхронний запуск процедури контролю цілісності і його реалізація. Проблема контролю цілісності контролюючої програми

Тема 7. 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 8. Додатковий захист від несанкціонованого доступу. Антивірусний захист. Загальноприйнятий підхід до антивірусного 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 навчання				Заочна форма навчання			
		Усього	Лекції	Лабор. заняття	СРС	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				**2 семестр**			

1.1	Вимоги до захисту комп'ютерної інформації	20	2	2	16	14	2		12
1.2	Аналіз стану захищеності операційних систем	14	2	2	10	14		2	12
1.3	Підходи до проектування системи захисту	18	2	2	14	14	2		12
1.4	Принципи побудови архітектури системи захисту інформації	16	2 2	2	10	14		2	12
1.5	Модульна контрольна робота №1	6	–	2	4	–	–	–	–
	Усього за модулем №1	**74**	**10**	**10**	**54**	**56**	**4**	**4**	**48**
Модуль №2 «Методи ідентифікації та автентифікації користувача та керування доступом до ресурсів».									
2.1	Авторизація. методи ідентифікації	9	2	2	5	10			10
2.2	Управління доступом до ресурсів	9	2	2	5	12	2		10
2.3	Моделі управління доступом	7		2	5	12		2	10
2.4	Реалізація моделей доступу механізмами додаткового та вбудованого захисту.	20	2 2	2 2	12	16	2		14
2.5	Контроль коректності функціонування механізмів захисту. Методи контролю цілісності.	13	2 2	2 2	5	14		2	12
2.6	Механізми контролю цілісності файлових об'єктів	16	2 2	2 2	8	14	2		12
2.7	Застосування засобів апаратного захисту	13	2 2	2 2	5	3			3
2.8	Додатковий захист від несанкціонованого доступу	13	2 2 2	2	5	18	2	2	14
2.9	Контрольна робота (домашня) (ЗФН)	–		–		8	–	–	8
2.10	Підсумкова контрольна робота (ЗФН)					4			4
2.11	Модульна контрольна робота №2	6		2	4	3		2	1
	Усього за модулем № 2	106	26	26	54	120	8	8	104
	Модуль 3 «Курсова робота»								
3.1	Проектування системи захисту комп'ютерної інформації від несанкціонованого доступу	30			30	30			30
	Усього за модулем №3	**30**			**30**	**30**			**30**
	Усього за навчальною дисципліною	**210**	**36**	**36**	**138**	**210**	**12**	**12**	**186**

2.4. Завдання на контрольну (домашню) роботу (ЗФН).

Контрольна (домашня) робота виконується у другому семестрі з метою закріплення та поглиблення теоретичних знань та вмінь студентів в області організації захисту інформації нвід загроз і є складовою модуль №2 «Методи ідентифікації та автентифікації користувача та керування доступом до ресурсів»

Конкретна мета контрольної (домашньої) роботи полягає у розробці пропозицій та рекомендацій щодо дій керівника підрозділу захисту інформації механізм мережевого моніторингу активності системи захисту як альтернатива застосуванню апаратної компоненті захисту.

Виконання, оформлення та захист контрольної (домашньої) роботи здійснюється студентом в індивідуальному порядку.

Час, потрібний для виконання контрольної (домашньої) роботи, – до 8 годин самостійної роботи.

2.5. Перелік питань для підготовки до підсумкової контрольної роботи

Перелік питань та зміст завдань для підготовки до підсумкової контрольної роботи 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*

(здійснюється через різні види практик на підприємствах, установах та організаціях різних форм власності).

3.2. Рекомендована література (базова і допоміжна)

Базова література

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 кібербезпеки 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. – 316 с.

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 екс-

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 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», зареєстрований в Міністерстві юстиції України 28.01.2015 за № 90/26535.

3.3. Інформаційні ресурси в Інтернет

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&cat_id=38835.

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

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

3.3.8. http://www.nau.edu.ua.

3.3.9. http://www.kzzi.nau.edu.ua.

Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment).

Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua.

Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua.

4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ

4.1. 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 навчання	**Заочна форма навчання**
2 семестр		
Модуль № 1 «Сучасні підходи, вимоги, особливості систем автоматизації обробки інформації з обмеженим доступом і принципи побудови архітектури систем захисту інформації»		
Виконання та захист лабораторних робіт	30	30
Для допуску до виконання модульної контрольної роботи №1 студент має набрати не менше	15	15
Виконання модульної контрольної роботи № 1	15	–
Усього за модулем № 1	**45**	**30**
Модуль № 2 «Методи ідентифікації та автентифікації користувача та керування доступом до ресурсів»		
Виконання та захист лабораторних робіт	45	25
Контрольна (домашня)робота		10
Для допуску до виконання модульної контрольної роботи №2 студент має набрати не менше	19	5
Виконання модульної контрольної роботи № 2	10	–
Виконання підсумкової модульної контрольної роботи	–	30
Усього за модулем № 2	**55**	**70**
Усього за за модулями №1, №2	**100**	**100**
Усього за дисципліною	**100**	
Модуль № 3 «Курсова робота»		
Виконання курсової роботи	**60**	**50**
Захист курсової роботи	**40**	**50**
Виконання та захист курсової роботи	**100**	**100**
Усього за дисципліною	**100**	

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

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 лабораторної роботи		Виконання та захист контрольної роботи (домашньої)	Виконання підсумкової модульної контрольної роботи	Виконання модульних контрольних робіт №№ 1, 2	
15-16	9	18-20	27-30	17-18	Відмінно
12-14	7-8	15-17	23-26	14-16	Добре
10-11	6	12-14	18-22	11-13	Задовільно
менше 10	менше 6	менше 12	менше 18	менше 11	Незадовільно

4.3. Сума рейтингових оцінок, отриманих студентом за окремі види виконаної навчальної роботи, становить підсумкову модульну рейтингову оцінку.

4.4. Сума підсумкових модульних рейтингових оцінок становить підсумкову семестрову рейтингову оцінку.

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.

4.7. Підсумкова модельна рейтиногва оцінка отриана студентом за результатом виконання та захисту курсої роботи в балах, за національною шкалою та заноситься до відомості, навчальної картки та індивідуального плану студента (залікової книжки) та Додатку диплома, наприклад, так: ***92/Відм./A, 87/Добре/B, 79/Добре/C, 68/Задов./D, 65/Задов./E*** тощо

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	04.04.24	Федорчук К.В		

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ з/п	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайомлення	Примітки
1	Щербак Т.М.			

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ з/п	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	Номер листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульованого			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				