Державний університет інтелектуальних технологій і зв'язку
Факультет інформаційних технологій та кібербезпеки
Кафедра кібербезпеки та технічного захисту інформації

“**ЗАТВЕРДЖУЮ**”

Ректор ДУІТЗ
_____ Олександр НАЗАРЕНКО
"____" _____ 2023 року

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Управління доступом до інформаційних ресурсів
(шифр і назва навчальної дисципліни)

Рівень вищої освіти	другий (магістерський)
Галузь знань	12 «Інформаційні технології»
Спеціальність	125 «Кібербезпека та захист інформації»
Спеціалізація (за наявності)	_____
Освітня програма	магістра
Статус дисципліни	обов’язкова
Мова викладання	українська

Одеса 2023

Програма навчальної дисципліни «Управління доступом до інформаційних ресурсів» для студентів освітнього рівня магістр за спеціальністю 125 «Кібербезпека та захист інформації».

Розробник(и): викладач(і) д.т.н., проф. кафедри кібербезпеки та технічного захисту інформації Корчинський В.В.

Навчальна програма затверджена на засіданні кафедри кібербезпеки та технічного захисту інформації
Протокол від "21" березня 2023 року № 8

Завідувач кафедри _____ В.В. Корчинський
(підпис) (ініціали та прізвище)
"21" березня 2023 року

Програму погоджено з гарантом освітньо-професійних програм к.т.н., доцент кафедри Кібербезпеки та технічного захисту інформації В.В. Корчинський

Гарант освітньо-професійної програми _____ В.В. Корчинський
(підпис) (ініціали та прізвище)

Програму погоджено з в.о. декана факультету інформаційних технологій та кібербезпеки

_____ Є.В.Васіліу
(підпис) (ініціали та прізвище)

Програму схвалено навчально-методичною радою ДУІТЗ

Голова навчально-методичної ради ДУІТЗ,

Проректор з навчальної роботи _____ А.Г. Ложковський
(підпис) (ініціали та прізвище

Протокол № ____ від _____ «____» _____ 2023 р.

ВСТУП

Програма вивчення навчальної дисципліни "*Управління доступом до інформаційних ресурсів*" складена відповідно до освітньо-професійної програми підготовки *магістрів* спеціальності *125* «*Кібербезпека та захист інформації».*

Предметом вивчення навчальної дисципліни є механізмів управління доступом до інформаційних ресурсів інтелектуальних мереж та заходів забезпечення захисту інформації в процесі її зберігання та передавання по каналам зв'язку.

Міждисциплінарні зв'язки:

- дисципліну забезпечують навчальні курси: Основи телекомунікацій і комп'ютерні мережі, Теорія інформації та кодування, Забезпечення безпеки телекомунікацій, Законодавство в області інформаційної безпеки, методи та засоби захисту інформації, Криптографічний захист інформації, Безпека і експлуатація мережних і хмарних технологій;
- дисципліна забезпечує навчальні курси: Сучасна теорія та техніка інформаційної безпеки, Інтернет речей: безпека та приватність.

1. Мета та завдання навчальної дисципліни

1.1. Метою викладання навчальної дисципліни «*Управління доступом до інформаційних ресурсів*» є формування у студентів сучасного погляду на структуру і тенденції розвитку інтелектуальних мереж, механізми управління доступом до інформаційних ресурсів та заходи забезпечення захисту інформації в процесі її зберігання та передавання.

1.2. Основними завданнями вивчення дисципліни «*Управління доступом до інформаційних ресурсів*» є набуття знань щодо принципів побудови та функціонування інтелектуальних мереж, поділу функцій керування послугами, механізмів управління доступом до інформаційних ресурсів та заходів забезпечення захисту інформації в процесі її зберігання та передавання по каналам зв'язку.

1.3. Згідно з вимогами освітньо-професійної програми студенти повинні:

знати:

Базові визначення інформаційних ресурсів та інтелектуальної мережі . Національні інформаційні ресурси. Принципи побудови та архітектура інтелектуальної мережі. Послуги, що надаються інтелектуальною мережею. Створення системи управління інтелектуальною надбудовою. Захист інформації в сучасних інтелектуальних мережах. Доступ до інформаційних ресурсів на основі бездротової мережі стандарту IEEE 802.15. Мережі широкосмугового бездротового доступу сімейства стандартів IEEE 802.16 (WiMAX). Стратегію радіоелектронної боротьби та конфлікту. Поняття прихованості: інформаційна, структурна, енергетична, часова, просторова і та інше. Методи побудови завадозахищених систем радіозв'язку. Методи формування шумоподібних сигналів в на основі прямого розширення спектру, псевдовипадкового перестроювання робочої частоти та ЛЧМ модуляції;

вміти:

аналізувати інформаційні ресурси на основі моделі інтелектуальної мережі і взаємодії основних її компонентів. Аналізувати умови передавання конфіденційної інформації в умовах радіоелектронної боротьби та конфлікту. Розробляти методи захисту інформації від НСД та засобів радіотехнічної розвідки. Здійснювати вибір метода захисту інформації у залежності від вимог до якості для конкретних умов передавання сигналів. Здійснювати вибір ортогональних послідовностей для систем з кодовим розділенням каналів. Вміти виконувати необхідні розрахунки, пов'язані із забезпеченням необхідного рівня захищеності та якості передавання інформації в умовах навмисних завад.

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів **компетентностей**:

***Загальних*:**

КЗ 1. Здатність застосовувати знання у практичних ситуаціях;

КЗ 2. Знання та розуміння предметної області та розуміння професії;

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

Фахових:

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Результати навчання:

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

У результаті вивчення навчальної дисципліни студент повинен отримати наступні професійні компетенції (**А**, **Б**, **Д**, **Е**), знання (**З**) та навички/уміння (**У**) з професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022.

А3. Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах.

А6. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності.

А3.З2. Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи ешелонованого захисту (прикладна система ешелонованого захисту).

А6.З5. Поняття показників захищеності інформації засобів обробки інформації та показників захищеності мовної інформації на об'єкті інформаційної діяльності.

А6.З15. Статистична радіотехніка (прийом звісних сигналів на фоні шумів, оцінка параметрів сигналів, що приймаються на фоні шумів).

А3.У1. Обґрунтовувати та розробляти політику безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

А6.У3. Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об’єкті інформаційної діяльності.

Змістовний модуль: Управління доступом до інформаційних ресурсів: (кредитів ECTS – 4, 120 год).

2. Інформаційний обсяг навчальної дисципліни

Змістовий модуль. Управління доступом до інформаційних ресурсів

Тема 1. Введення в дисципліну. Поняття інформаційних ресурсів та інтелектуальної мережі. Національні інформаційні ресурси. Правовий режим інформаційних ресурсів. Правове регулювання відносин щодо окремих видів інформаційних ресурсів.

Тема 2. Концептуальна модель інтелектуальної мережі. Стандартизація в галузі інтелектуальних мереж. Концепція інтелектуальної мережі. Функція комутації послуг SSF.

Тема 3. Послуги, що надаються інтелектуальною мережею. Послуги інтелектуальної мережі. Класифікація послуг та їх призначення.

Тема 4. Створення системи управління інтелектуальною надбудовою. Загальні положення. Завдання та організаційна структура системи керування інтелектуальною надбудовою. Адміністративне керування потребує надання інформації про роботу усіх рівнів системи.

Тема 5. Захист інформації в сучасних інтелектуальних мережах. Характеристика захищених телекомунікаційних систем. Способи захисту інформації від перехоплення. Вимоги до радіоприймачів захищених систем. Забезпечення енергетичної прихованості. Вимоги до шумових характеристик компонентів захищених систем.

Тема 6. Доступ до інформаційних ресурсів на основі бездротових мереж. Захисту інформації від несанкціонованого доступу в сучасних телекомунікаційних системах. Захист передавальної інформації за рахунок передавання сигнальних конструкцій. Принципи методів розширення спектру для забезпечення енергетичної прихованості. Метод псевдовипадкової перебудови робочої частоти.

Тема 7. Мережі широкосмугового бездротового доступу сімейства стандартів IEEE 802.16 (WiMAX). Захист інформації в широкосмугових системах зв'язку з розширенням спектру методом прямої послідовності (DSSS). Принцип роботи системи з кодовим розділенням каналів.

3. Рекомендована література

Базова

1. Конспект лекцій з дисципліни Управління доступом до інформаційних ресурсів. Корчинський В.В. ДУІТЗ, 2022 р.

2. Практикум до лабораторних робіт з дисципліни Управління доступом до інформаційних ресурсів. Корчинський В.В. ДУІТЗ, 2022 р.

3. Практикум до практичних робіт з дисципліни Управління доступом до інформаційних ресурсів. Корчинський В.В. ДУІТЗ, 2022 р.

4. Захарченко М.В., Кононович В.Г., Кільдішев В.Й., Голев Д.В. Інформаційна безпека інформаційно-комунікаційних систем. Частина 1: лаб. практ. – Одеса: ОНАЗ ім. О.С. Попова, 2011.

5. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.

Допоміжна

1. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. No 3475-IV-BP//ВВР. – 2006. – № 30 (в редакції Закону № 1194-VII від 09.04.2014). – С. 258.
3. Юдін О. К. Правові аспекти формування системи державних інформаційних ресурсів [Електронний ресурс] / О. К. Юдін, С. С. Бучик // Безпека інформації. – 2014. – Т. 20 (1). – С. 76–82.
2. Юдін О. К. Аналіз загроз державним інформаційним ресурсам [Електронний ресурс] / О. К. Юдін, С. С. Бучик // Проблеми інформатизації та управління. – 2013. – № 4 (44). – С. 93–99.
3. Концепції формування системи національних електронних інформаційних ресурсів: розпорядження Кабінету Міністрів України від 5 травня 2003 р. № 259-р.
4. Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління : затверджено Постановою Кабінету Міністрів України від 3 серпня 2005 р. № 688.
5. Юдін О. К. Загрози державним інформаційним ресурсам: терміни та визначення / О. К. Юдін, С. С. Бучик // Захист інформації. – 2014. – Т. 16 (2). – С. 121–125.

13. Інформаційні ресурси

1 What is Information Resources . [Електроний ресурс]. – Режим доступу: https://www.igi-global.com/dictionary/information-resources/35622/.
2 Управління політикою доступу до мережних ресурсів. [Електроний ресурс]. – Режим доступу: http://referat-ok.com.ua/work/upravlinnja-politikoju-dostupu-do-mere/.

4. Форма підсумкового контролю успішності навчання іспит

5. Оцінювання знань

(Шкала оцінювання: національна та ЄКТС)

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою	
	для екзамену, курсового проекту (роботи), практики	для заліку
90-100	відмінно	зараховано
82-89	добре	
74-81		
64-73	задовільно	
60-63		
35-59	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

Засоби діагностики успішності навчання:
виконання лабораторних робіт, відповіді на практичних заняттях, виконання та захист комплексного завдання та курсового проекту.