СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Методи і моделі управління доступом»

Лектор курсу				**Контактна інформація лектора (e-mail), сторінка курсу в GWE**		**e-mail:** **сторінка курсу в GWE –** Курс: Методи і моделі управління доступом (dut.edu.ua)	
Галузь знань			12 Інформаційні технології	**Рівень вищої освіти**		магістр	
Спеціальність			125 Кібербезпека та захист інформації	**Семестр**		2	
Освітня програма			УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ	**Тип дисципліни**		вибіркова	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	-	36	-	96

АНОТАЦІЯ КУРСУ

Мета курсу:	формування у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи у органах та структурах з кібербезпеки, навчити їх застосуванню методів та засобів захисту інформації в умовах широкого використання сучасних кібертехнологій.

Компетентності відповідно до освітньої програми

Загальні компетентності (КЗ)	**Фахові компетентності (КФ)**
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. **КЗ 3**. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **КЗ 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **КЗ 5.** Здатність до пошуку, оброблення та аналізу інформації.	ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі захисту інформації. ФК7. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-комунікаційних систем згідно встановленої політики безпеки. ФК8. Здатність ефективно аналізувати, виявляти та оцінювати можливі загрози та уразливості інформації. ФК9. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення. ФК10. Здатність використовувати управлінсько-організаційні, математичні, технічні та правові методи захисту інформації. ФК11. Здатність до застосування математичного та комп'ютерного моделювання для вирішення широкого спектру задач захисту інформації. ФК12. Здатність організовувати роботу колективів виконавців, приймати

	управлінські рішення в умовах спектра думок, визначати порядок виконання робіт, вибирати оптимальні рішення при створенні систем захисту інформації.

Програмні результати навчання (РН)

РН4. Здатність демонструвати знання та розуміння архітектури систем захисту інформації та описати в загальних поняттях архітектуру, характеристики та принципи їх дії.
РН5. Здатність демонструвати знання та розуміння сучасних методів і моделей захисту інформації.
РН7. Здатність демонструвати знання та розуміння захисту інформації у комп'ютерних системах та обґрунтовано обирати і застосовувати на практиці методи протидії спробам несанкціонованого доступу до інформаційних ресурсів, а також організаційні та адміністративні заходи підвищення рівня інформаційної безпеки комп'ютерних систем.
РН9. Володіння та орієнтування в базових аспектах законодавства України, а також відповідних міжнародних стандартів у галузі кібербезпеки.
РН10. Здатність демонструвати уміння фахово вести дискусію й викладати основи кібербезпеки
РН13. Системно мислити та застосовувати творчі здібності до формування принципово нових ідей.
РН14. Здатність продемонструвати знання та навики щодо проведення експериментів, збору даних та моделювання у сфері захисту інформації.
РН15. Оцінювати отримані результати та аргументовано захищати прийняті рішення.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
ЗМІСТОВИЙ МОДУЛЬ **1 «ЗМІСТ ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ»**			
Тема №1. **Тема 1. Загальні теоретичні підходи до управління доступом.**	Лекція 1 2 год	15*	Лекція-візуалізація
Знати: Загальні теоретичні підходи до управління доступом. Інформаційні ресурси, як об'єкт захисту інформації. ***Вміти:*** формувати бази даних, як компонент автоматизованої системи обробки інформації та об'єкт захисту.	Практичне заняття 1,2 6 год		Практична робота, Аналітичний метод, проблемно-пошуковий метод 1. Аналіз теоретичних підходів до управління доступом. 2. Вимоги і рекомендації по захисту інформації

Формування компетенцій: КЗ 1, КЗ 3, КФ 1, КФ 7 ***Результати навчання:*** ПРН7, ПРН9 ***Рекомендовані джерела:*** 1-3, 9-12	Самостійна робота 16 год		Аналітичний метод, Практична робота 1. Безпека інформації при здійсненні документообігу 2. Ідентифікація та управління доступом до інформації
Тема №2. **Забезпечення конфіденційності інформації в інформаційних системах** ***Знати***: Управління доступом для регулювання та регламентування здійснення операцій обробки даних. Гарантований доступ до ресурсів системи автоматизованої обробки даних авторизованим користувачам. ***Вміти***: оцінювати ефективність механізмів управління доступом. Функції, процедури та засоби захисту інформаційних ресурсів. ***Формування компетенцій:*** КЗ 3, КЗ 5, ФК 1, ФК 11 ***Результати навчання:*** ПРН7, ПРН9, ПРН13 ***Рекомендовані джерела:*** 1-10	Лекція 2 4 год	15*	Лекція-візуалізація
	Практичне заняття 3,4 6 год		Практична робота 1. Вимоги до конфіденційності інформації. Ідентифікація та аутентифікація. Основні поняття і класифікація. 2. Визначення вимог до захисту ресурсів
	Самостійна робота 18 год		Аналітичний метод, Практична робота 1. Контроль конфіденційності інформації
Тема №3 **Проблема логічного аналізу інформаційних ресурсів** ***Знати***: Методи прямої, непрямої та відстежуючої атак. Лінійна вразливість системи. Методи боротьби з атаками, побудованими на статистичному аналізі. ***Вміти***: застосовувати методи захисту, що звикористовуються до елементів захищеної інформації (придушення та приховування). ***Формування компетенцій:*** КЗ 3, ФК 11, ФК 12 ***Результати навчання:*** ПРН7, ПРН9 ***Рекомендовані джерела:*** 1-15, 16-21	Лекція 3 4 год	15*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 5,6 6 год		Аналітичний метод, Практична робота 1. Порядок проведення логічного аналізу інформаційних ресурсів
	Самостійна робота 20 год		Практична робота, аналітичний, частково-пошуковий метод 1. Характеристика інформаційних ресурсів
Тема №4 **Цілісність інформаційних ресурсів.** ***Знати***: систему гарантованого збереження інформації в інформаційних ресурсах при відмовах апаратури або збоях програмного забезпечення (захист від втрати даних). Систему управління інформаційних ресурсів для підтримки цілісності кожного елемента інформаційного ресурсу. шляхи посилення рівня небезпеки кібертероризму. ***Вміти***: оцінювати цілісність інформаційних ресурсів, елементів, точність елементів інформації як три рівні цілісності. Визначати технологію оновлення інформації. Відновлення інформації. .	Лекція 4 4 год	15*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 7,8 12 год		Аналітичний метод, Практична робота 1. Поняття критерію цілісність інформаційного ресурсу.
	Самостійна робота 20 год		Практична робота, аналітичний, частково-пошуковий метод 1. Інженерно-технічний захист інформації

Формування компетенцій: КЗ 1, КЗ 3, ФК 8, ФК 12 ***Результати навчання:*** ПРН 13, ПРН15 ***Рекомендовані джерела:*** 1-15.			
Тема №5 Методи і моделі управління доступом	Лекція 5 4 год	15*	Лекція-візуалізація, експрес-опитування
Знати: Аналітичну модель ефективності забезпечення захисту даних від загроз порушення цілісності. Модель забезпечення цілісності на основі диверсного підходу. Модель Хартсона (п'ятивимірна статична модель). П'ятивимірна модель розмежуваня доступу Хартсона. Модель на основі мереж Петрі-Маркова. Модель Бела-Лападули. Модель Бела-Лападули та модель Біба. Абстрактна модель MMS Лендвера і Мак-Ліна. Модель розповсюдження прав доступу Take-Grant. Модель Кларка-Вільсона. Модель Біба. Модель порушення фізичної цілісності. безпечення кібербезпеки у приватному секторі. ***Вміти***: застосовувати метод забезпечення цілісності інформації на основі організації паралельних з'єднань захисту на мережевому рівні (теорія множин та метод Монте-Карло). Модель Мельникова В. В (грунтується на математичному базисі теорії ймовірностей). Застосовувати модель з повним перекриттям. Моделювати процес НСД до інформації за моделлю Мухіна-Волокіти. ***Формування компетенцій:*** КЗ 1, КЗ 3, ФК 8, ФК 12 ***Результати навчання:*** ПРН 5, ПРН 15 ***Рекомендовані джерела:*** 1-15	Практичне заняття 9,10 6 год		Аналітичний метод, Практична робота 1. Поняття про методи та моделі управління доступом.
	Самостійна робота 22 год		Практична робота, аналітичний, частково-пошуковий метод 1. Моделювання процесів управління доступом.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- мультимедійна система Acer X113 DLP
- комп'ютери Asus
- комп'ютерний клас для проведення занять: Спеціалізована лабораторія: «Управління інформаційною та кібербезпекою».
- програмне забезпечення перевірки СУІБ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Базова

1. ДСТУ 3396.0-96.Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. No 423.
2. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. No 511.
3. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. No 200.
4. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" – К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 2000. [Електронний ресурс]. – Режим доступу : [http://www.dut.edu.ua/uploads/l_1023_75718671.pdf]
5. НД ТЗІ 2.7-011-2012 "Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв". – 2012 [Електронний ресурс]. – Режим доступу : http://www.dut.edu.ua/uploads/l_5623_75714589.pdf .
6. Про затвердження Змін до Зводу відомостей, що становлять державну таємницю / 27 березня 2019 р. за N 306/33277 [Електронний ресурс]. – Режим доступу : http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920 .
7. Постанова Кабінету Міністрів України від 29.03.2006 No 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [Електронний ресурс]. –Режим доступу : http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920 .
8. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир: Вид-во ЖДУ ім. І.Франка, 2015. – 226 с.
9. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.
10. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – К.: ДУТ- КНУ, 2016. – 178 с.
11. Логінова Н. І. Правовий захист інформації: навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.
12. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД "Гельветика", 2017. – 168 с.
13. Носов В.В., Манжай О.В. Організація та забезпечення інформаційної безпеки: Навч. посібник. – Харків: Вид-во Харк. нац. ун-ту внутр. справ, 2007.
14. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
15. Яремчук Ю. Є. Комплексні системи захисту інформації : навчальний посібник /Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця: ВНТУ, 2017. – 120 с.
16. Богуш В. М., Кудін А. М., Моніторинг і аудит систем інформаційної безпеки. - К.: ДУІКТ, 2006, - 340с.

Допоміжна

17. Браіловський М.М., Головань С.М., Домарєв В.В., Коженевський С.Р., Чирков Д.В. Технічний захист інформації на об'єктах інформаційної діяльності. К.: ДУІКТ, 2007 –178 с.
18. Габович А.Г., Гордієнко С.Б., Хорошко В.О., Чирков Д.В. – «Організаційно-технічне забезпечення інформаційної безпеки». Київ. ТОВ «Поліграф консалтинг», 2005. -180 с.
19. Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Методологічні засади викладання інформаційної безпеки у вищих навчальних закладах : [підруч. для студ. вищ. навч. закл.] – Луганськ: Східноукраїнський національний університет ім. В. Даля, 2010. – 200 с.
20. Головань С.М. Документаційне забезпечення робіт із захисту інформації з обмеженим доступом: Підручник // С.М. Головань, В.Б. Дудикевич, В.С. Зачепило, Л.Т. Пархуць, В.О. Хорошко, Л.М. Щербак. – Львів: Видавництво Національного університету «Львівська політехніка», 2005. – 288с.

Інформаційні ресурси

1. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" – К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 2000. [Електронний ресурс]. – Режим доступу : http://www.dut.edu.ua/uploads/l_1023_75718671.pdf .
2. НД ТЗІ 2.7-011-2012 "Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв". – 2012 [Електронний ресурс]. – Режим доступу : http://www.dut.edu.ua/uploads/l_5623_75714589.pdf .
3. Про затвердження Змін до Зводу відомостей, що становлять державну таємницю / 27 березня 2019 р. за N 306/33277 [Електронний ресурс]. – Режим доступу : http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920 .

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.

- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації, студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

***КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 бала
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату	за кожну презентацію (реферат) максимум 3 бали
	• усне опитування, тестування, рішення практичних задач	за кожну правильну відповідь 0,5 бала
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали
	• участь у діловій грі	за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 «ОСНОВИ ПРОФЕСІЙНОЇ ТА КОРПОРАТИВНОЇ ЕТИКИ»»	максимальна оцінка – 15балів
	Модульний контроль № 2 «ЕТИКА ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ»	максимальна оцінка –15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових робіт за спеціальністю, створення кейсів тощо.	Звільняється від іспиту
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному	Відмінно / Зараховано (А)

	об ‘єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов’язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об’єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	
82-89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (B)
75-81	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)

64-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В заліковукнижкуне проставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі іспиту.	**Незадовільний** Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В заліковукнижкуне проставляється*