СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Організаційне забезпечення захисту інформації »

Лектор курсу			**Щавінський Юрій Віталійович,** кандидат технічних наук, .		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:** yushchavinsky@ukr.net; **сторінка курсу в Moodle –** Курс: Організаційне забезпечення захисту інформації (dut.edu.ua)	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	перший (бакалаврський)	
Спеціальність			125 Кібербезпека та захист інформації		**Семестр**	7	
Освітня програма			УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ		**Тип дисципліни**	основна	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	4	120	18	-	36	-	66

АНОТАЦІЯ КУРСУ

Мета курсу:	вивчення організаційно-технічних заходів для забезпечення безпеки на об’єктах інформаційної діяльності та застосування знань при практичній організації заходів захисту інформації в організаціях

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.	**КФ 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки. **КФ 2**. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. **КФ 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **КФ 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. **КФ 7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) . **КФ 10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

Програмні результати навчання (ПРН)
ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та /або кібербезпеки. **ПРН 8.** Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. **ПРН 9.** Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. **ПРН 12.** Розробляти моделі загроз та порушника. **ПРН 14.** Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку якості прийнятих рішень. **ПРН 16.** Реалізовувати комплексні системи захисту інформації в автоматизованій системі організації (підприємства) відповідно до вимог нормативно-правових документів. **ПРН 17.** Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. **ПРН 21.** Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **ПРН 22.** Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і кібербезпеки. **ПРН 23.** Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **ПРН 27**. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

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. Роль організаційного забезпечення захисту інформації ***Знати***: сутність та основні поняття основних термінів і визначень в галузі інформаційної безпеки ***Вміти:*** Застосовувати основні поняття і визначення при здійсненні документообігу, плануванні і організації інформаційної безпеки	Лекція 1 2 год	15*	Лекція-візуалізація
	Практичне заняття 1,2 4 год		Практична робота, Аналітичний метод, , проблемно-пошуковий метод 1. Аналіз стану проблем забезпечення безпеки на ОІД 2. Вимоги і рекомендації по захисту інформації

Формування компетенцій: КЗ 1, КЗ 3, КФ 1, КФ 2, КФ 7 ***Результати навчання:*** ПРН7, ПРН8 ***Рекомендовані джерела:*** 1-5, 9-12, 17-19, 22, 26, 28-31	Самостійна робота 8 год		Аналітичний метод, Практична робота 1. Безпека інформації при здійсненні документообігу 2. Ідентифікація та управління доступом до інформації
Тема №2. Визначення інформаційних ресурсів, що підлягають захисту ***Знати***: сутність, види та основні поняття термінів і визначень інформаційних ресурсів, що підлягають захисту, класифікацію і вимоги до захисту інформаційних ресурсів ***Вміти***: застосовувати способи захисту інформаційних ресурсів ***Формування компетенцій:*** КЗ 3, КЗ 4, КЗ 5, КФ 2, КФ 3, КФ 10 ***Результати навчання:*** ПРН7, ПРН8, ПРН14, ПРН16, ПРН21, ПРН27 ***Рекомендовані джерела:*** 1-14, 16-19, 21	Лекція 2 2 год	15*	Лекція-візуалізація
	Практичне заняття 3,4 4 год		Дедуктивний метод, Практична робота 1. Ідентифікація та аутентифікація. Основні поняття і класифікація. 2. Визначення вимог до захисту ресурсів
	Самостійна робота 8 год		Аналітичний метод, Практична робота 1. Протоколювання, шифрування, контроль цілісності інформації
Тема №3 Виявлення загроз безпеки інформаційним ресурсам, які підлягають захисту ***Знати***: види загроз безпеки інформаційним ресурсам, які підлягають захисту, порядок проведення пошуку джерел витоку інформації, організацію і функції підрозділів технічного захисту інформації ***Вміти***: виявляти канали витоку інформації та планувати заходи по їх попередженню, застосовувати засоби захисту інформації від компютерних злочинців ***Формування компетенцій:*** КЗ 3, КЗ 4, КЗ 5, КФ 2, КФ 3, КФ 10 ***Результати навчання:*** ПРН7, ПРН8, ПРН14, ПРН16, ПРН21, ПРН27, ***Рекомендовані джерела:*** 1-15, 16-21	Лекція 3 2 год	15*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 5,6 7 год		Аналітичний метод, Практична робота 1. Порядок проведення пошукових заходів по витоку інформації. 2. Виявлення каналів витоку інформації
	Самостійна робота 8 год		Практична робота, аналітичний, частково-пошуковий метод 1. Характеристика загроз ІБ 2. Організація і функції підрозділів технічного захисту інформації 3. Комп'ютерні злочини і засоби захисту інформації
Тема №4 Організаційна структура системи забезпечення безпеки інформації ***Знати***: склад і структуру системи забезпечення безпеки інформації, організаційні заходи комплексної Служби ***Вміти***: визначати і планувати заходи інженерно-технічного захисту інформації ***Формування компетенцій:*** КЗ 1, КЗ 3, КФ 1-3, КФ 5 , КФ 7 ***Результати навчання:*** ПРН7, ПРН8, ПРН14, ПРН16, ПРН21, ПРН22 ***Рекомендовані джерела:*** 1-15, 17-19,	Лекція 4 2 год	15*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 7,8 4год		Аналітичний метод, Практична робота 1. Організаційні заходи комплексної Служби безпеки . 2. Структура захисту інформації в інтегрованій інформаційній системі управління підприємством
	Самостійна робота 8 год		Практична робота, аналітичний, частково-пошуковий метод 1. Інженерно-технічний захист інформації
ЗМІСТОВИЙ МОДУЛЬ **2 «ЗАХОДИ ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ»**			
Тема №5 Заходи з організації забезпечення захисту інформації в організаціях	Лекція 5 2год	15*	Лекція-візуалізація, експрес-опитування

Знати: зміст організаційних заходів забезпечення захисту інформації в організаціях ***Вміти***: планувати заходи забезпечення захисту інформації в організаціях ***Формування компетенцій:*** КЗ 1, КЗ 3, КФ 1-3, КФ 5 , КФ 7 ***Результати навчання:*** ПРН8, ПРН9, ПРН14, ПРН16, ПРН21, ПРН27 ***Рекомендовані джерела:*** 1-15, 17-25	Практичне заняття 9,10 6 год		Аналітичний метод, Практична робота 1. Організація захисту інформації в обчислювальному центрі крупного підприємства 2. Організаційні заходи захисту інформації на підприємстві
	Самостійна робота 8 год		Практична робота, аналітичний, частково-пошуковий метод 1. Охорона діяльність 2. Ліцензування діяльності в галузі ТЗІ 3. Плани захисту і плани забезпечення безперервної роботи і відновлення підсистем АС 4. Моделювання системи інженерно-технічного захисту інформації
Тема №6 Організація забезпечення режиму таємності ***Знати***: перелік інформації, що складає державну таємницю, заходи із забезпечення режиму таємності в організаціях ***Вміти***: планувати заходи із забезпечення режиму таємності, застосовувати заходи протидії технічним засобам розвідки, організовувати технічний захист інформації, що складає комерційну і державну таємницю ***Формування компетенцій:*** КЗ 1, КЗ 3, КФ 1, КФ 5 , ***Результати навчання:*** ПРН14, ПРН16, ПРН17, ПРН27 ***Рекомендовані джерела:*** 6, 9-15, 23-24, 26-27	Лекція 6 2 год	15*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 11,12 4год		Аналітичний метод, Практична робота 1. Засоби технічної охорони. 2. Захист від знімання інформації електронними засобами
	Самостійна робота 8 год		Практична робота, аналітичний, частково-пошуковий метод 1. Засоби прихованого спостереження 2. Технічні засоби підслуховування 3. Методи протидії підслуховуванню
Тема №7 Робота з персоналом ***Знати***: порядок роботи з персоналом, психологічну структуру особистості і колективу, підбір та підготовку співробітників відділу ІБ, порядок розробки моделі зловмисника. ***Вміти***: підбирати та готувати співробітників відділу ІБ, розробляти модель зловмисника ***Формування компетенцій:*** КЗ 1, КЗ 5, КФ 1, КФ 2 ***Результати навчання:*** ПРН7, ПРН8, ПРН9, ПРН12 ***Рекомендовані джерела:*** 9-15, 17-19, 23, 25	Лекція 7 2 год	15*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 13,14 4 год		Аналітичний метод, Практична робота 1. Підбір і підготовка співробітників відділу ІБ 2. Розробка моделі зловмисника
	Самостійна робота 6 год		Практична робота, аналітичний, частково-пошуковий метод 1. Підбір і підготовка співробітників відділу ІБ 2. Розробка моделі зловмисника
Тема №8 Політика інформаційної безпеки ***Знати***: склад і структуру політики інформаційної безпеки ***Вміти***: розробляти політику інформаційної безпеки організації, посадові інструкції щодо забезпечення інформаційної безпеки	Лекція 8 2 год	15*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 15 4год		Аналітичний метод, Практична робота 1. Розробка інструкцій по організації парольного та антивірусного захисту

Формування компетенцій: КЗ 1, КЗ 5, КЗ 4, КФ 1-3, КФ 5 , КФ 7, КФ 10 ***Результати навчання:*** ПРН12, ПРН16, ПРН17, ПРН21-23, ПРН27 ***Рекомендовані джерела:*** 1-15, 17-19, 21-23	Самостійна робота 6 год		Практична робота, аналітичний, частково-пошуковий метод 1. Структура і зміст Політики інформаційної безпеки. 2. Розробка інструкцій по організації парольного та антивірусного захисту
Тема №9 Забезпечення захисту інформації при здійсненні міжнародного науково-технічного та економічного співробітництва ***Знати***: зміст і структуру основних міжнародних нормативно-правових актів із забезпечення інформаційної безпеки, порядок їх застосування при організації науково-технічного та економічного співробітництва ***Вміти***: застосовувати міжнародні нормативно-правові акти забезпечення інформаційної безпеки при плануванні і організації захисту інформації ***Формування компетенцій:*** КЗ 1, КЗ 3, КЗ 4, КФ 1, КФ 2 , КФ 10 ***Результати навчання:*** ПРН7, ПРН9, ПРН23 ***Рекомендовані джерела:*** 1-15, 17-20, 25-27	Лекція 9 2 год	15*	Лекція-візуалізація, експрес-опитування
	Практичне заняття 16 4 год		Аналітичний метод, Практична робота 1. Протидія технічним засобам розвідки
	Самостійна робота 6 год		Практична робота, аналітичний, частково-пошуковий метод 1. Забезпечення захисту інформації при здійсненні міжнародного науково-технічного та економічного співробітництва 2. Міжнародна практика захисту інформації 3. Міжнародні нормативно-правові акти забезпечення захисту інформації

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.
17. Д. В. Голев, В. Й. Кільдишев, В. Г. Кононович. Інформаційна безпека інформаційно-комунікаційних систем: навчальний посібник. Лабораторний практикум. Частина 1. Комплекси засобів захисту інформації від НСД. [Електронний ресурс]. – Режим доступу : Організаційне забезпечення захисту інформації :: Кафедра Управління інформаційною та кібернетичною безпекою :: Державний університет телекомунікацій (dut.edu.ua)
18. Організаційне забезпечення захисту інформації : метод. рекомендації до виконання практичних робіт для студент. денної та заочної форми навч. за спец. 125 «Кібербезпека» / уклад. : С. А. Смірнов, В. А. Резніченко ; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т., каф. кібербезпеки та програм. забезпеч. - Кропивницький : ЦНТУ, 2022. - 88 с.
19. Д.В. Голев, О.Ю. Русляченко, Ю.В. Бєлова, Д.С. Гончарук. Інформаційна безпека інформаційно-комунікаційних систем: навчальний посібник. Лабораторний практикум. Частина 2. Комплекси технічного захисту інформації. [Електронний ресурс]. – Режим доступу : Організаційне забезпечення захисту інформації :: Кафедра Управління інформаційною та кібернетичною безпекою :: Державний університет телекомунікацій (dut.edu.ua)

Допоміжна

20. 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.
21. Габович А.Г., Гордієнко С.Б., Хорошко В.О., Чирков Д.В. – «Організаційно-технічне забезпечення інформаційної безпеки». Київ. ТОВ «Поліграф консалтинг», 2005. -180 с.
22. 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.
23. 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.
24. Автоматизовані системи обробки інформації з обмеженим доступом: Методичні вказівки до виконання лабораторних робіт / Уклад: С.М. Головань, В.В. Душеба, В.П. Щербина. – К: НАУ, 2004. – 28с.
25. Механізація і автоматизація обробки службових та технічних документів : Методичні вказівки до виконання лабораторних робіт / Уклад: С.М. Головань, В.В. Душеба, В.П. Щербина. – К: НАУ, 2005. – 40с.
26. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / НД Системи ТЗІ // Наказ ДСТСЗІ СБ України від 28.04.1999р. № 22.
27. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу / НД Системи ТЗІ // Наказ ДСТСЗІ СБ України від 28.04.1999р. № 22.

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 .
4. Постанова Кабінету Міністрів України від 29.03.2006 № 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 .

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 залікову книжку не 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 залікову книжку не проставляється*