Затверджено
Завідувач кафедри УКБЗІ _____ С. Легомінова
“ 31 “ серпня 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Лектор курсу	**Запорожченко Михайло Михайлович,** доцент кафедри управління кібербезпекою та захистом інформації	**Контактна інформація лектора (e-mail), сторінка курсу в Google Classroom**	**e-mail:** m.zaporozhchenko@duikt.edu.ua ; **сторінка курсу в Google Classroom –** https://classroom.google.com/c/ODQzNjg1NDM1ODIy?hl=ru&cjc=tx3riwj5	
Галузь знань	F «Інформаційні технології»	**Рівень вищої освіти**	перший (бакалаврський)	
Спеціальність	F5 «Кібербезпека та захист інформації»	**Семестр**	6	
Освітня програма	«Управління інформаційною та кібернетичною безпекою» «Інформаційна та кібернетична безпека» «Технічні системи інформаційного та кібернетичного захисту»	**Тип дисципліни**	Обов’язкова	

Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Мета курсу:
- формування у студентів комплексного бачення сфери діяльності, пов’язаної з управлінням процесом забезпечення інформаційної безпеки;
- забезпечення усвідомлення студентами порядку та особливостей вирішення різних завдань управління інформаційною безпекою підприємства (установи, організації), їхнього кадрового та ресурсного забезпечення.

Програмні компетенції

Загальні компетентності (ЗК)	**Спеціальні (фахові, предментні) компетентності (СК)**
ІК. Здатність розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.	**СК 3.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. **СК 7.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

Програмні результати навчання (РН)
РН 2. Спілкуватися іноземною мовою з метою забезпечення професійної комунікації. **РН 11.** Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. **РН 17.** Забезпечувати функціонування системи управління кібербезпекою і захистом інформації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Розділ 1 "ОСНОВНІ ПОНЯТТЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ"			
Тема 1. Вступ до системи менеджменту інформаційної безпеки ***Знати***: ключові терміни та визначення у сфері інформаційної безпеки та систем менеджменту; місце та роль СМІБ у загальній системі управління підприємством / організацією; структуру, сутність та призначення міжнародних стандартів у сфері ІБ та кібербезпеки (ISO/IEC 27000-серія, NIST, COBIT тощо); основні положення та вимоги ISO/IEC 27001:2022; етапи та особливості процесу впровадження СМІБ в організації. ***Вміти***: визначати внутрішній та зовнішній контекст організації в аспекті безпеки інформації; ідентифікувати та класифікувати зацікавлені сторони і їхні очікування; формулювати область застосування СМІБ; визначати склад та структуру необхідної документації для створення, впровадження й підтримки СМІБ; розподіляти обов'язки, повноваження та ресурси, необхідні для ефективного функціонування СМІБ. ***Формування компетенцій:*** ІК, СК 3, СК 7 ***Результати навчання:*** РН 2, РН 11, РН 17 ***Рекомендовані джерела:*** 1-28	Лекція 1 2 год	5	Лекція-візуалізація
	Практичне заняття 1 2 год		Практична робота: Аналіз документації для впровадження СМІБ (ідентифікація ключових документів: політика ІБ, оцінка ризиків, процедури інцидент-менеджменту тощо).
	Самостійна робота		Огляд міжнародних стандартів у сфері ІБ та їх взаємозв'язків Характеристики захищеності інформаційних ресурсів Модель CIA. Задачі забезпечення цілісності, доступності та конфіденційності Бізнес-процеси організації та їх залежність від інформаційної безпеки Вимоги до забезпечення інформаційної безпеки організації відповідно до ISO/IEC 27001:2022.
Тема 2. Методика оцінки загроз інформаційній безпеці ***Знати***: порядок та особливості ідентифікації й оцінювання загроз інформаційній безпеці; систему вимог до інформаційної безпеки організації; види інформації, що підлягає захисту, об'єкти та суб'єкти захисту; методи визначення внутрішніх і зовнішніх чинників впливу на інформаційну безпеку; типові загрози ІБ (технічні, організаційні, людські тощо); сучасні технології та підходи до протидії загрозам. ***Вміти***: оцінювати актуальні загрози інформаційної безпеки організації; визначати джерела та мотиви загроз; класифікувати загрози; здійснювати ранжування загроз за критеріями значущості та ймовірності; визначати потенційних порушників і їхні можливості;	Лекція 2 2 год	5	Лекція-візуалізація
	Практичне заняття 2 2 год		Практична робота: Визначення вимог до забезпечення інформаційної безпеки організації. Ідентифікація чинників впливу та класифікація загроз для конкретного підприємства.
	Самостійна робота		Визначення та оцінювання загроз інформаційній безпеці організації.

встановлювати вимоги до захисту інформації залежно від її типу та цінності; аналізувати взаємозв'язки між чинниками впливу й оцінювати можливі наслідки для організації. ***Формування компетенцій:*** ІК, СК 3, СК 7 ***Результати навчання:*** РН 2, РН 11, РН 17 ***Рекомендовані джерела:*** 1-28			Оцінювання ризиків ІБ із використанням базових методів (якісний та кількісний підходи). Аналіз організаційної структури забезпечення інформаційної безпеки. Вивчення прикладів політик інформаційної безпеки підприємств.
Тема 3. Ризик-менеджмент як невід'ємна частина СМІБ ***Знати***: основні поняття та принципи ризик-менеджменту; місце ризик-менеджменту в СМІБ та його взаємозв'язок з іншими процесами; вимоги міжнародних стандартів (ISO/IEC 27005, ISO 31000, NIST SP 800-30) щодо оцінки ризиків; порядок проведення аналізу й оцінювання ризиків інформаційної безпеки; класифікацію ризиків (технічні, організаційні, правові, людські, природні тощо). ***Вміти***: ідентифікувати ризики, що впливають на інформаційну безпеку організації; оцінювати й аналізувати ризики із застосуванням якісних і кількісних методів; визначати рівень ризику з урахуванням ймовірності та наслідків; формувати стратегії реагування: уникнення, зменшення, передавання чи прийняття ризику; застосовувати інструменти управління ризиками (GRC-системи, матриці ризиків, методи сценарного аналізу); здійснювати моніторинг і вдосконалення системи ризик-менеджменту в контексті ІБ. ***Формування компетенцій:*** ІК, СК 3, СК 7 ***Результати навчання:*** РН 2, РН 11, РН 17 ***Рекомендовані джерела:*** 1-28	Лекція 3 2 год	5	Лекція-візуалізація
	Практичне заняття 3 2 год		Практична робота: Огляд і застосування інструментів управління ризиками інформаційної безпеки на прикладі GRC-системи SimpleRisk.
	Самостійна робота		Побудова матриці ризиків для вибраної організації. Класифікація ризиків інформаційної безпеки за джерелами та характером. Якісні та кількісні методи оцінки ризиків (порівняння). Сучасні стратегії управління ризиками інформаційної безпеки (ISO 31000, NIST RMF).
Тема 4. Внутрішні загрози інформаційній безпеці, пов'язані з діяльністю персоналу ***Знати***: основні загрози інформаційній безпеці, що виникають через персонал (навмисні та ненавмисні дії, людський фактор); типові методи атак, які використовують слабкі місця поведінки персоналу (фішинг, соціальна інженерія, інсайдерські дії); ризики неналежної обробки інформації та їх наслідки; засоби ІБ, спрямовані на зниження ризику внутрішніх загроз (контроль доступу, моніторинг, розмежування повноважень). ***Вміти***: розпізнавати ознаки потенційних внутрішніх загроз; застосовувати методи аутентифікації та авторизації для захисту даних; впроваджувати політики безпеки для мінімізації ризиків, пов'язаних із персоналом; виявляти та документувати порушення безпеки; ефективно комунікувати з персоналом щодо важливості дотримання правил безпеки. ***Формування компетенцій:*** ІК, СК 3, СК 7	Лекція 4 2 год	5	Лекція-візуалізація
	Практичне заняття 4 2 год		Практична робота: Практичне застосування методики Hogan для оцінки персоналу (психологічні профілі ризику).
	Самостійна робота		Аналіз кейсів інцидентів ІБ, спричинених діями персоналу.

Результати навчання: РН 2, РН 11, РН 17 ***Рекомендовані джерела:*** 1-28			
Розділ 2 "ЗАХОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ"			
Тема 5. Організаційні заходи та політики інформаційної безпеки ***Знати***: структуру та зміст стандарту ISO/IEC 27002; принципи і положення, що регламентують організаційні заходи ІБ; роль керівництва та вимоги до його залучення в систему забезпечення ІБ; вимоги до формування та змісту політики інформаційної безпеки; ключові організаційні заходи: управління доступом, управління інцидентами, навчання персоналу, управління постачальниками тощо. ***Вміти***: визначати та адаптувати організаційні заходи відповідно до ідентифікованих ризиків; розробляти й впроваджувати політики та процедури у відповідності до рекомендацій ISO/IEC 27002; обґрунтовувати необхідність залучення керівництва до управління ІБ; інтегрувати організаційні заходи у бізнес-процеси організації. ***Формування компетенцій:*** ІК, СК 3, СК 7 ***Результати навчання:*** РН 2, РН 11, РН 17 ***Рекомендовані джерела:*** 1-28	Лекція 5 2 год	5	Лекція-візуалізація
	Практичне заняття 5 2 год		Практична робота: Адаптація організаційних заходів ІБ до виявлених ризиків та специфіки підприємства. Тестування знань студентів щодо організаційних заходів та вимог стандарту ISO/IEC 27002:2022.
	Самостійна робота		Аналіз прикладів політик інформаційної безпеки реальних компаній. Вивчення кейсів інцидентів, пов'язаних із відсутністю або неефективністю організаційних заходів. Розробка структури Політики інформаційної безпеки для конкретної організації.
Тема 6. Заходи забезпечення інформаційної безпеки, пов'язані з персоналом ***Знати***: вимоги ISO/IEC 27002:2022 щодо заходів ІБ для роботи з персоналом; роль і відповідальність працівників у забезпеченні інформаційної безпеки; принципи формування обізнаності персоналу; методи навчання та тренування персоналу у сфері ІБ. ***Вміти***: розробляти та впроваджувати програми навчання з ІБ; залучати персонал до виконання політик і процедур безпеки; створювати та підтримувати культуру безпеки; організовувати внутрішній контроль і моніторинг дотримання заходів; ефективно спілкуватися з працівниками для підвищення їх відповідальності у сфері ІБ. ***Формування компетенцій:*** ІК, СК 3, СК 7 ***Результати навчання:*** РН 2, РН 11, РН 17 ***Рекомендовані джерела:*** 1-28	Лекція 6 2 год	5	Лекція-візуалізація
	Практичне заняття 6 2 год		Практична робота: Виявлення внутрішніх загроз з боку персоналу організації, розробка навчальних програм для персоналу.
	Самостійна робота		Аналіз політик безпеки різних організацій, розробка власної концепції навчання персоналу.
Тема 7. Фізичні заходи та інфраструктурна безпека ***Знати***: основні принципи фізичної безпеки в контексті інформаційної безпеки; вимоги стандартів ISO/IEC 27002:2022 та ISO/IEC 22301 до	Лекція 7 2 год	5	Лекція-візуалізація

фізичної інфраструктури; технічні засоби контролю доступу (електронні замки, карткові системи, біометрія, багаторівнева ідентифікація); системи моніторингу та охорони (відеоспостереження, сигналізація, датчики проникнення); засоби резервного копіювання та відновлення для фізичної інфраструктури; заходи протидії техногенним, природним та антропогенним загрозам (пожежа, повінь, аварії). ***Вміти***: проектувати та реалізовувати заходи фізичної безпеки відповідно до стандартів; оцінювати ризики для фізичної безпеки та формувати стратегії їх мінімізації; впроваджувати та підтримувати процеси резервного копіювання й відновлення як частину плану безперервності бізнесу; визначати й застосовувати системи контролю доступу та моніторингу для захисту приміщень і ресурсів; інтегрувати фізичні заходи в загальну систему менеджменту інформаційної безпеки. ***Формування компетенцій:*** ІК, СК 3, СК 7 ***Результати навчання:*** РН 2, РН 11, РН 17 ***Рекомендовані джерела:*** 1-28	Практичне заняття 7 2 год		Практична робота: Аналіз кейсів порушення фізичної безпеки та їх наслідків для інформаційної безпеки.
	Самостійна робота		Аналіз вимог ISO/IEC 27002:2022 та ISO/IEC 22301 до фізичної безпеки (огляд контрольних заходів і рекомендацій). Побудова моделі загроз фізичній інфраструктурі організації (ідентифікація ризиків: пожежа, затоплення, несанкціонований доступ, відмова електропостачання). Розробка плану резервного копіювання та відновлення IT-інфраструктури (backup & recovery plan) для умовної організації. Порівняльний аналіз систем контролю доступу (механічні, карткові, біометричні, багаторівневі системи) з визначенням переваг і недоліків. Вивчення кейсів інцидентів порушення фізичної безпеки (на прикладі відомих атак на дата-центри або офіси IT-компаній) з оцінкою їхніх наслідків для інформаційної безпеки.
Тема 8. ***Технології та інструменти кіберзахисту*** ***Знати***: основні види технологій та інструментів ІБ, їхнє призначення, принципи роботи та роль у системі безпеки (IDS/IPS, файрволи, антивірусні рішення, SIEM, DLP, EDR/XDR, SOAR); засоби шифрування та їх застосування для захисту конфіденційної інформації; принципи захисту мобільних пристроїв та бездротових мереж; сучасні концепції (Zero Trust, багаторівневий захист). ***Вміти***: обирати й впроваджувати відповідні технології для захисту інформаційних ресурсів; налаштовувати та оптимізувати засоби захисту; використовувати інструменти моніторингу та аналізу журналів подій; впроваджувати заходи безпеки для мобільних пристроїв і бездротових мереж; управляти системами шифрування для забезпечення конфіденційності при зберіганні та передачі даних; інтегрувати різні інструменти у єдину систему кіберзахисту організації. ***Формування компетенцій:*** ІК, СК 3, СК 7 ***Результати навчання:*** РН 2, РН 11, РН 17 ***Рекомендовані джерела:*** 1-28	Лекція 8 2 год	5	Лекція-візуалізація
	Практичне заняття 8 2 год		Практична робота: Аналіз технічних засобів забезпечення інформаційної безпеки.
	Самостійна робота		Порівняльний аналіз IDS та IPS (переваги, недоліки, приклади систем). Аналіз сучасних інструментів EDR/XDR і їхнього місця в СМІБ. Вивчення прикладів застосування DLP-систем у корпоративному середовищі. Підготовка огляду методів захисту мобільних пристроїв і бездротових мереж.
Тема 9. Управління інцидентами інформаційної безпеки ***Знати***: основні принципи та етапи управління інцидентами (виявлення, повідомлення, класифікація, реагування, відновлення, аналіз); вимоги міжнародних стандартів (ISO/IEC 27035, NIST SP 800-	Лекція 9 2 год	5	Лекція-візуалізація

61) до управління інцидентами; різновиди інцидентів ІБ (фішинг, шкідливе ПЗ, витік даних, DoS-атаки, інсайдерські дії тощо) та їх характеристики; роль і відповідальність CSIRT / CERT-команди, взаємодія з іншими відділами організації; техніки виявлення, класифікації та аналізу інцидентів. ***Вміти***: розробляти та впроваджувати план управління інцидентами (Incident Response Plan) відповідно до вимог стандартів і специфіки організації; визначати та класифікувати інциденти за рівнем критичності; використовувати базові методи аналізу інцидентів (Root Cause Analysis, постінцидентний аналіз); застосовувати практичні сценарії реагування для різних типів інцидентів; формувати пропозиції щодо вдосконалення системи безпеки на основі отриманого досвіду. ***Формування компетенцій:*** ІК, СК 3, СК 7 ***Результати навчання:*** РН 2, РН 11, РН 17 ***Рекомендовані джерела:*** 1-28	Практичне заняття 9 2 год		Практична робота: Розбір кейсу інциденту.
	Самостійна робота		Огляд вимог ISO/IEC 27035 до управління інцидентами. Порівняльний аналіз NIST Incident Response Lifecycle та ISO-підходу. Розробка прикладу «Журналу інцидентів» для організації (які дані повинні міститися). Аналіз відомого кейсу кіберінциденту з точки зору процесу реагування. Розробка пропозицій щодо вдосконалення процесів управління інцидентами в умовній організації.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор; комп'ютерний клас для проведення практичних занять; перелік питань для самостійної підготовки, перелік навчальної літератури та доступ до тексту лекцій та слайдів до лекцій через систему Google Classroom для підготовки до практичних занять.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Рекомендовані джерела та інші навчальні ресурси:

1. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
3. Закон України «Про авторське право і суміжні права». URL: https://zakon.rada.gov.ua/laws/show/3792-12#Text;
4. Закон України «Про захист від недобросовісної конкуренції». URL: https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80#Text;
5. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 року N 1229/99. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text;
6. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 року N 505/98. URL: https://zakon.rada.gov.ua/laws/show/505/98#Text;
7. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29 березня 2006 р. N 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text;
8. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text;
9. Накази Адміністрації ДССЗЗІ України, державні стандарти України та нормативні документи України у сфері технічного та криптографічного захисту інформації. URL: https://cip.gov.ua/ua/docs;
10. Міжнародні стандарти серії ISO/IEC 27000
11. Стандарт безпеки даних індустрії платіжних карток Payment Card Industry Data Security Standard (PCI DSS);
12. Стандарти інформаційної безпеки США NIST Special Publications 800 Series;

13. Відкритий IT-стандарт Асоціації з аудиту та контролю інформаційних система (ISACA) спільно із Інститутом управлінням IT (ITGI) CoBiT (Control Objectives for Information and Related Technology – «Контрольні цілі для інформаційних та суміжних технологій»);
14. Загальний регламент про захист даних ЄС GDPR (General Data Protection Regulation, GDPR; Regulation (EU) 2016/679
15. Манжай О. В., Манжай І.А. Правові засади захисту інформації: підручник. – Харків : Панов, 2020. – 162 с. URL: http://univd.edu.ua/science-issue/issue/4315;
16. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О .Г. Корченко, М. Є. Шелест, С. В. Казмірчук, Ю. М. Ткач, Є. В. Іванченко. – Ніжин : ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл. URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19244/%d0%9c%d0%b5%d0%bd%d0%b5%d0%b4%d0%b6%d0%bc%d0%b5%d0%bd%d1%82%20%d1%96%d0%bd%d1%84%d0%be%d1%80%d0%bc.%20%d0%b1%d0%b5%d0%b7%d0%bf.%20New%20booklet%201.pdf?sequence=1&isAllowed=y;

Постанови Кабінету Міністрів України:
17. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури (від 19.06.2019 № 518)
18. Про затвердження Положення про організаційно-технічну модель кіберзахисту (від 29.12.2021 № 1426)
19. Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури(від24.03.2023 № 257)
20. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі (від 04.04.2023 № 299)
21. Деякі питання функціонування Національного центру резервування державних інформаційних ресурсів (від 07.04.2023 № 311)
22. Деякі питання створення та функціонування державних електронних платформ для ведення публічних електронних реєстрів (від 18.04.2023 № 356)
23. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (від 16.05.2023 № 497)

Накази Адміністрації Держспецзв'язку:
24. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (від 06.10.2021 № 601, в редакції наказу від 10.07.2022 № 343)
25. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами (від 29.05.2023 № 463)
26. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі (від 03.07.2023 № 570)
27. Запорожченко М.М., Легомінова С.В., Капелюшна Т.В., Рабчун Д.І. Формалізація системи показників оцінювання результативності програм навчання персоналу з інформаційної безпеки. Кібербезпека: освіта, наука, техніка. 2026. Том 1, № 33. С. 55-64. URL: https://doi.org/10.28925/2663-4023.2026.33.1179
28. Svitlana Lehominova, Mykhailo Zaporozhchenko, Tetiana Kapeliushna, Yuriy Shchavinsky, Tetiana Muzhanova. Method for assessing the risk of user compromise based on individual security profile. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2026. Vol. 16, № 1. P. 130-137. URL: https://doi.org/10.35784/iapgos.7754

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 40 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 балу
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 балу
	• 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 балу
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 3 бали
РУБІЖНЕ ОЦІНЮВАННЯ	Розділ № 1 «ОСНОВНІ ПОНЯТТЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»	максимальна оцінка – 30 балів
	Розділ № 2 «ЗАХОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»	максимальна оцінка – 30 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від Заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить у письмовій формі.	40 балів
ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ		**100 балів**

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в заліковій 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 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.	**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 поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)

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)
67-74	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)
60-66	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 заліку.	**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*

ДОТРИМАННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Виконання навчальних завдань на практичних заняттях та під час самостійної підготовки, проведення поточного контролю результатів навчання, з використанням самостійних (індивідуальних) форм роботи, зокрема за допомогою системи **GWE** перевіряється **на плагіат у відповідності з Кодексом академічної доброчесності Державного університету інформаційно-комунікаційних технологій**

https://duikt.edu.ua/uploads/p_447_96297052.pdf?2