СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Лектор курсу			**Легомінова Світлана Володимирівна,** доктор економічних наук, професор.		**Контактна інформація лектора (e-mail), сторінка курсу в GME**	**e-mail:** s.legominova@duikt.edu.ua **сторінка курсу в GME– https://classroom.google.com/c/NzA0ODk4NjcwMzMx?cjc=at3mcff**	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	Магістр	
Спеціальність			Кібербезпека та захист інформації		**Семестр**	1	
Освітня програма			Управління інформаційною та кібернетичною безпекою		**Тип дисципліни**	Вибіркова компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	-	36	-	96

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Мета курсу:	Оволодіння студентами основ аудиту інформаційної безпеки, формування знань і навичок щодо забезпечення проведення аудиту безпеки інформаційних систем і технологій.

Компетентності відповідно до освітньої програми

Soft- skills / Компетентності загальні (КЗ)	**Hard-skills / Компетентності фахові спеціальні (КФ)**
КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ-5. Здатність до пошуку, оброблення та аналізу інформації.	КФ-2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ-4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і

	технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Програмні результати навчання (РН)

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

ЗМІСТОВИЙ МОДУЛЬ 1. ОРГАНІЗАЦІЙНО-ПРАВОВІ ОСНОВИ ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1. Основи побудови систем інформаційної безпеки. ***Знати***: принципи побудови інформаційної безпеки, загрози та ризики інформаційної безпеки, основні методи захисту інформації, процеси аудиту та моніторингу безпеки, законодавчу базу в галузі інформаційної безпеки. ***Вміти:*** визначати вразливості в системах, реагувати на інциденти інформаційної безпеки. ***Формування компетенцій:*** КЗ-5 ***Програмні результати навчання:*** РН-5 ***Рекомендовані джерела:*** 1-3	Лекція 2 год		Лекція-візуалізація, пояснювально-ілюстративний метод.
Тема 1. Основи побудови систем інформаційної безпеки. ***Знати:*** основні загрози інформаційній безпеці, принципи шифрування та захисту даних, стандарти та регуляторні вимоги в галузі інформаційної безпеки, базові поняття щодо архітектури мереж та їх вразливостей. ***Вміти:*** визначати потреби в інформаційній безпеці для конкретного бізнесу, розробляти стратегії та політики інформаційної безпеки, встановлювати та налаштовувати захисне програмне забезпечення, реагувати на інциденти інформаційної безпеки та відновлювати системи після атак.	Практичне заняття 4 год	3	Метод-практика, метод «мозкового штурму».

Формування компетенцій: КЗ-5 ***Програмні результати навчання:*** РН-5 ***Рекомендовані джерела:*** 1-3			
Тема 1. Основи побудови систем інформаційної безпеки ***Знати:*** основні принципи інформаційної безпеки, загрози та ризики інформаційної безпеки, методи захисту інформаційних ресурсів, принципи шифрування даних, процедури реагування на інциденти інформаційної безпеки. ***Вміти:*** аналізувати вразливості інформаційних систем, встановлювати та конфігурувати захисні механізми, планувати та впроваджувати стратегії інформаційної безпеки. ***Формування компетенцій:*** КЗ-5 ***Програмні результати навчання:*** РН-5 ***Рекомендовані джерела:*** 1-3	Самостійна робота 13 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 2. Аудит безпеки та методи його проведення. ***Знати***: основні принципи аудиту безпеки, стандарти та нормативні вимоги до аудиту безпеки, методики оцінки ефективності заходів безпеки, сучасні інструменти для проведення аудиту безпеки, принципи конфіденційності та етики при проведенні аудиту безпеки. ***Вміти:*** визначати ризики безпеки в ІТ-системах, проводити технічний аналіз систем безпеки, аналізувати результати аудиту та розробляти рекомендації, документувати процес проведення аудиту та його результати. ***Формування компетенцій:*** КЗ-2, КЗ-4, КФ-9. ***Програмні результати навчання:*** РН-9, РН 14 ***Рекомендовані джерела:*** 1-3.	Лекція 2 год		Лекція-візуалізація, проблемно-пошуковий метод.
Тема 2. Аудит безпеки та методи його проведення. ***Знати:*** основні принципи інформаційної безпеки, методи інвентаризації активів та вразливостей, принципи захисту даних і конфіденційності, методи аналізу та виявлення інцидентів інформаційної безпеки, законодавчу базу з питань інформаційної безпеки.	Практичне заняття 4 год	3	Метод-практика, кейс-метод.

Вміти: розробляти стратегію інформаційної безпеки, впроваджувати технологічні рішення для захисту інформації, проводити аудит інформаційної безпеки на підприємстві. ***Формування компетенцій:*** КЗ-2, КЗ-4, КФ-9. ***Програмні результати навчання:*** РН-9, РН 14 ***Рекомендовані джерела:*** 1-3.			
Тема 2. Аудит безпеки та методи його проведення ***Знати***: основні принципи аудиту безпеки, стандарти та нормативні вимоги до аудиту безпеки, методики оцінки ефективності заходів безпеки. ***Вміти:*** проводити технічний аналіз систем безпеки, аналізувати результати аудиту та розробляти рекомендації, документувати процес проведення аудиту та його результати. ***Формування компетенцій:*** КЗ-2, КЗ-4, КФ-9. ***Програмні результати навчання:*** РН-9, РН 14 ***Рекомендовані джерела:*** 1-3.	Самостійна робота 13 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 3. Інформаційні ризики підприємства. ***Знати***: основні інформаційні ризики, методики оцінки інформаційних ризиків, методи захисту від інформаційних ризиків, принципи керування інформаційною безпекою підприємства. ***Вміти:*** визначати потенційні загрози безпеці інформації, обирати методи захисту від інформаційних ризиків, розробляти план дій для запобігання інформаційним ризикам. ***Формування компетенцій:*** КФ-5 ***Програмні результати навчання:*** РН-10 ***Рекомендовані джерела:*** 12-14	Лекція 2 год		Лекція-візуалізація, репродуктивний метод.
Тема 3. Методи управління інформаційними ризиками ***Знати:*** принципи інформаційних ризиків, методи оцінки ризиків, інструменти для аналізу і реагування на інциденти безпеки, принципи законодавства щодо захисту персональних даних. ***Вміти:*** визначати потенційні загрози безпеці інформації, класифікувати рівні інформаційних ризиків, розробляти	Практичне заняття 4 год	3	Метод-практика, метод «мозкового штурму».

стратегії зниження інформаційних ризиків, використовувати методи моніторингу і контролю ризиків. ***Формування компетенцій:*** КФ-5 ***Програмні результати навчання:*** РН-10 ***Рекомендовані джерела:*** 12-14			
Тема 3. Реагування на інцидент та його обробка (на прикладі AWS). ***Знати***: етапи реагування на інциденти безпеки: виявлення, оцінка, обмеження та відновлення; обрання інструментів та технологій, що використовуються для реагування на інциденти та обробка даних у реальному часі. ***Вміти***: планувати та реалізовувати стратегії реагування на інциденти безпеки, включаючи зупинку атак та відновлення систем; проводити аналіз інцидентів для виявлення їх причин та наслідків, а також для вдосконалення заходів безпеки в майбутньому. ***Формування компетенцій:*** КФ-5 ***Програмні результати навчання:*** РН-10 ***Рекомендовані джерела:*** 15-18	Самостійна робота 4 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 4. Стандарти інформаційної безпеки. ***Знати:*** стандарти інформаційної безпеки, процедури реагування на інциденти інформаційної безпеки, принципи безпечного користування комп'ютером та Інтернетом, законодавча база в галузі інформаційної безпеки. ***Вміти:*** використовувати вимоги стандартів, як нормативних документів для вирішення проблем з забезпеченням інформаційної та кібербезпеки. Використовувати методики впровадження процесного підходу до створення системи управління інформаційною безпекою, проводити аудит інформаційної безпеки організації. ***Формування компетенцій:*** КФ-2. ***Програмні результати навчання:*** РН-5. ***Рекомендовані джерела:*** 3-11	Лекція 2 год		Лекція-візуалізація, проблемно-пошуковий метод.

Тема 4. Міжнародні стандарти інформаційної безпеки ***Знати:*** основні принципи та концепції Міжнародних стандартів інформаційної безпеки, основні вимоги та рекомендації стандартів ISO/IEC 27001 та ISO/IEC 27002, основні процедури та практики забезпечення інформаційної безпеки в організаціях, методики аудиту інформаційної безпеки для перевірки відповідності стандартам. ***Вміти:*** аналізувати ризики інформаційної безпеки та використовувати методики їх оцінки, впроваджувати та підтримувати системи управління інформаційною безпекою відповідно до вимог стандартів. ***Формування компетенцій:*** КЗ-5, КФ-2. ***Програмні результати навчання:*** РН-5. ***Рекомендовані джерела:*** 3-11	Практичне заняття 4 год	3	Метод-практика, кейс-метод.
Тема 4. Стандарти інформаційної безпеки ***Знати:*** основні принципи і стандарти інформаційної безпеки, вимоги до захисту персональних даних. ***Вміти:*** розрізняти та аналізувати види загроз інформаційній безпеці, застосовувати положення стандартів під час оцінки ризиків інформаційної безпеки, аналізувати відповідність інформаційних систем вимогам стандартів. ***Формування компетенцій:*** КЗ-1, КФ-2. ***Програмні результати навчання:*** РН-5. ***Рекомендовані джерела:*** 3-11	Самостійна робота 13 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
ЗМІСТОВИЙ МОДУЛЬ 2. ПРИНЦИПИ, МЕТОДИ ТА ЕТАПИ ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ			
Тема 5. Внутрішній аудит системи менеджменту інформаційної безпеки підприємства ***Знати:*** загальну характеристику внутрішніх аудитів СМІБ; принципи проведення внутрішнього аудиту; управління програмою аудиту; процес проведення аудиту; ***Вміти:*** розробляти та впроваджувати програму проведення аудиту, виявляти та відновлювати після інцидентів інформаційні системи. ***Формування компетенцій:*** КЗ-4, КФ-4.	Лекція 2 год		Лекція-візуалізація, пояснювально-ілюстративний метод.

Програмні результати навчання: РН-9, РН-14. ***Рекомендовані джерела:*** 1-4.			
Тема 5. Внутрішній аудит системи менеджменту інформаційної безпеки підприємства ***Знати:*** зміст процесу аудиту, познайомитися з роботою компаній постачальниками послуг в сфері інформаційної безпеки. ***Вміти:*** визначати потенційні загрози безпеці інформації, налаштовувати та проводити моніторинг системи захисту інформації, аналізувати ринок аудиторських послуг. ***Формування компетенцій:*** КЗ-4, КФ-4. ***Програмні результати навчання:*** РН-9, РН-14. ***Рекомендовані джерела:*** 1-4	Практичне заняття 4 год	3	Метод-практика, кейс-метод
Тема 5. Захист даних підприємства у хмарних сховищах (AWS). ***Знати***: основні методи шифрування даних та їх застосування для різних типів інформації та даних; принципи та методи контролю доступу до даних у хмарних середовищах, включаючи різновиди політик доступу та методи ідентифікації; різноманітні методи та інструменти для моніторингу та виявлення потенційних загроз безпеці даних ***Вміти***: розробляти та реалізовувати стратегії шифрування даних для забезпечення конфіденційності в хмарних середовищах; використовувати методи та інструменти для контролю доступу до даних та ресурсів у хмарних обчисленнях; застосовувати техніки моніторингу та виявлення аномальної активності для захисту даних в реальному часі. ***Формування компетенцій:*** КЗ -1 ***Результати навчання:*** РН 14 ***Рекомендовані джерела:*** 15-18	Самостійна робота 13 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Тема 6. Вимоги до інформаційних ресурсів та систем підприємства ***Знати:*** основні принципи вибору інформаційних ресурсів для підприємства, критерії якості та надійності інформаційних систем, стандарти та нормативи, що регулюють використання інформаційних ресурсів, методи захисту інформаційних ресурсів від несанкціонованого доступу, принципи інтеграції інформаційних систем на підприємстві, стратегії розвитку інформаційних систем для оптимізації роботи підприємства. ***Вміти:*** аналізувати потреби підприємства в інформаційних ресурсах, оцінювати вартість та ефективність інформаційних ресурсів для підприємства, планувати та впроваджувати нові інформаційні ресурси на підприємстві. ***Формування компетенцій:*** КЗ-1 ***Програмні результати навчання:*** РН-9, РН-14. ***Рекомендовані джерела:*** 1-4, 12-14.	Лекція 2 год		Лекція-візуалізація, пояснювально-ілюстративний метод.
Тема 6. Вимоги до інформаційних ресурсів та систем підприємства ***Знати:*** основні принципи і стандарти інформаційної безпеки, процеси інвентаризації та класифікації інформації, процедури виявлення та реагування на інциденти безпеки, процеси впровадження рекомендацій після аудиту інформаційної безпеки. ***Вміти:*** оцінювати ризики інформаційної безпеки на підприємстві, озробляти та впроваджувати політики інформаційної безпеки, проводити внутрішній аудит інформаційної безпеки, співпрацювати з зовнішніми аудиторами під час проведення аудиту, підготувати звіт та аналіз результатів аудиту для внутрішніх та зовнішніх стейкхолдерів ***Формування компетенцій:*** КЗ-1, КФ-9. ***Програмні результати навчання:*** РН-14. ***Рекомендовані джерела:*** 1-4, 12-14.	Практичне заняття 6 год	3	Метод-практика, кейс-метод.

Тема 6. Вимоги до інформаційних ресурсів та систем підприємства ***Знати:*** основні принципи вибору інформаційних ресурсів для підприємства, стандарти та нормативи, що регулюють використання інформаційних ресурсів, стратегії розвитку інформаційних систем для оптимізації роботи підприємства. ***Вміти:*** аналізувати потреби підприємства в інформаційних ресурсах, планувати та впроваджувати нові інформаційні ресурси на підприємстві. ***Формування компетенцій:*** КЗ-1 ***Програмні результати навчання:*** РН-9. ***Рекомендовані джерела:***1-4, 12-14.	Самостійна робота 12 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 7. Вимоги до адміністрування комп'ютерних систем підприємства та доступу до них ***Знати:***. принципи безпечного адміністрування комп'ютерних систем, основні методи захисту даних підприємства, процедури резервного копіювання та відновлення даних, принципи сегментації мережі для забезпечення безпеки, стандарти та нормативні вимоги до захисту інформації. ***Вміти:*** налаштовувати права доступу користувачів до ресурсів системи, розпізнавати потенційні загрози та ризики для комп'ютерних систем, використовувати антивірусне програмне забезпечення, аналізувати журнали подій для виявлення аномалій в системі. ***Формування компетенцій:*** КФ-4. ***Програмні результати навчання:*** РН-9. ***Рекомендовані джерела:*** 1-4, 12-14.	Лекція 4 год		Лекція-візуалізація, репродуктивний метод.
Тема 7. Планування процедури аудиту інформаційної безпеки підприємства ***Знати:*** основні принципи аудиту інформаційної безпеки, методики проведення аудиту інформаційної безпеки, вимоги законодавства щодо інформаційної безпеки, процедури документування результатів аудиту. ***Вміти:*** визначити ключові ризики і загрози інформаційній безпеці підприємства, оцінювати ефективність заходів захисту	Практичне заняття 6 год	3	Метод-практика, метод «мозкового штурму».

інформації, складати план аудиту інформаційної безпеки, аналізувати та інтерпретувати отримані дані для покращення інформаційної безпеки. ***Формування компетенцій:*** КЗ-4, КФ-9. ***Програмні результати навчання:*** РН-14. ***Рекомендовані джерела:*** 1-4, 12-14.			
Тема 7. Вимоги до адміністрування комп'ютерних систем підприємства та доступу до них ***Знати:*** основні методи захисту даних підприємства, процедури резервного копіювання та відновлення даних, принципи сегментації мережі для забезпечення безпеки ***Вміти:*** використовувати антивірусне програмне забезпечення, розпізнавати потенційні загрози та ризики для комп'ютерних систем, налаштовувати права доступу користувачів до ресурсів. ***Формування компетенцій:*** КФ-4. ***Програмні результати навчання:*** РН-9. ***Рекомендовані джерела:*** 1-4, 12-14.	Самостійна робота 12 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 8. Вимоги до безперервної роботи підприємства ***Знати:*** принципи безперервної роботи підприємства, основні методики відновлення роботи підприємства після аварійних ситуацій, законодавчі вимоги щодо безперервності роботи підприємства. ***Вміти:*** аналізувати ризики та загрози для безперервності роботи, планувати та впроваджувати заходи забезпечення безперервної роботи, координувати роботу команди в екстрених ситуаціях. ***Формування компетенцій:*** КЗ-4 ***Програмні результати навчання:*** РН-10. ***Рекомендовані джерела:*** 1,2,3,4,16.	Лекція 2 год		Лекція-візуалізація, пояснювально-ілюстративний метод.
Тема 8. Організація та проведення робіт щодо аудиту інформаційної безпеки підприємства ***Знати:*** основні принципи і стандарти аудиту інформаційної безпеки, процеси організації аудиту інформаційної безпеки на підприємстві, методики та інструменти для виявлення слабких	Практичне заняття 4 год	3	Метод-практика, кейс-метод.

місць в інформаційній безпеці, процес валідації та верифікації результатів аудиту, основні етапи та підходи до підготовки звіту про аудит інформаційної безпеки. ***Вміти:*** проводити аналіз ризиків інформаційної безпеки, розробляти рекомендації для підвищення рівня інформаційної безпеки, проводити постійний моніторинг інформаційної безпеки після аудиту. ***Формування компетенцій:*** КФ-9. ***Програмні результати навчання:*** РН-14. ***Рекомендовані джерела:*** 1,2,3,4,16.			
Тема 8. Вимоги до безперебійної роботи підприємства ***Знати:*** основні методики відновлення роботи підприємства після аварійних ситуацій, законодавчі вимоги щодо безперервності роботи підприємства. ***Вміти:*** планувати та впроваджувати заходи забезпечення безперервної роботи, аналізувати ризики та загрози для безперервності роботи. ***Формування компетенцій:*** КЗ-4. ***Програмні результати навчання:*** РН-10. ***Рекомендовані джерела:*** 1,2,3,4,16.	Самостійна робота 16 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп'ютерне обладнання, мережа Інтернет ауд. 401. Програмне забезпечення: 1. Apache OpenOffice URL: https://www.openoffice.org/ 2. Microsoft Project URL: https://www.microsoft.com/uk-ua/microsoft-365/project/project-management-software

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Корченко О.Г., Гнатюк С.О., Казмірчук С.В. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. Київ: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. 190 с.
2. Тимофєєв Д.С. Методичні рекомендації до самостійної роботи студентів з дисципліни «Аудит інформаційної безпеки» Нац. гірн. ун-т, каф. безпеки інформації та телекомунікацій. Д. : НГУ, 2017. 60 с.
3. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звіт практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
4. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT)
5. ISO/IEC 27006:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems».
6. ДСТУ ISO/IEC 27006:2008 «Інформаційні технології. Методи і засоби забезпечення безпеки. Вимоги до органів, які забезпечують аудит і сертифікацію систем менеджменту ІБ».

7. NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 22, 2015). URL: https://doi.org/10.6028/NIST.SP.800- 53r4.
8. ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: URL: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
9. Control Objectives for Information and Related Technology (COBIT): URL:http://www.isaca.org/COBIT/Pages/default.aspx
10. CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): URL: https://www.cisecurity.org
11. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
12. Неторенко С.А. Управління інформаційними ризиками. Київ.:ДМК-Пресс, 2015. 384 с.
13. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. Житомир: ЖНАЕУ, 2016. 636 с.
14. Лісовська Ю. Кібербезпека. Ризики та заходи. Київ: Кондор, 2019. 272 с.

ІНФОРМАЦІЙНІ РЕСУРСИ
15. AWS Documentation. URL: https://docs.aws.amazon.com/
16. SoftServe Academy. URL: https://softserve.academy/login/index.php
17. Cyber Security Training. SANS Institute. Онлайн курси із захисту інформації. URL: http://www.sans.org
18. Інформаційний онлайн-журнал Infosecurity URL: https://www.infosecurity-magazine.com/

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.:*	
	• 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 (КОНТРОЛЬ)	Контроль № 1	максимальна оцінка 10 балів
	Контроль № 2	максимальна оцінка 10 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 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.	30 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 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	**Достатній** Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з	Добре / Зараховано (В)

	проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	прикладами, що розглянуті при вивчені дисципліни	
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 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*